RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

Informe 2016

La protección de datos de los menores de edad

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

Informe 2016

Tema monográfico: la protección de datos de los menores de edad

Director
Guillermo Escobar

trama
EDITORIAL.ES

Producción: Trama editorial, 2017
Blanca de Navarra, 6
28010 Madrid
Tel: 91 702 41 54
www.tramaeditorial.es

ISBN: 978-84-945692-4-1
Depósito legal: M-29808-2017

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

INFORME 2016

Director
Guillermo Escobar (*Universidad de Alcalá*)

Colaboradores
Mónica Arenas – *Universidad de Alcalá*
Adriana Báez – *INAI* (México)
Alejandra Celi – *PRADPI/ Universidad de Alcalá*
Joan Crespo – *Agencia Andorrana de Protección de Datos*
Diana Cristina Gil – SIC – *Delegatura para la Protección de Datos Personales* (Colombia)
María Alejandra González – *Autoridad Nacional de Protección de Datos* (Perú)
Joana Marí Cardona – *Autoridad Catalana de Protección de Datos*
Laura Nahabetian y Gonzalo Sosa – AGESIC – *Unidad Reguladora y de Control de Datos Personales* (Uruguay)
Miguel Ángel Pérez Grande – *Agencia Española de Protección de Datos*
Loreto Pozo – *Consejo para la Transparencia* (Chile)
Julián Prieto – *Agencia Española de Protección de Datos*
Pablo Segura – *Dirección Nacional de Protección de Datos Personales* (Argentina)
Lidia Suárez – *PRADPI/ Universidad de Alcalá*

ÍNDICE

PRESENTACIÓN

La Red Iberoamericana de Protección de Datos (RIPD) surgió en el Encuentro Iberoamericano de Protección de Datos, celebrado en La Antigua, Guatemala, en junio de 2003, con la asistencia de representantes de 14 países iberoamericanos. Ya desde sus inicios, contó con apoyo político del más alto nivel, 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, en noviembre del mismo 2003.

La Red pretende ser 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, así como promover los desarrollos normativos necesarios para garantizar una regulación avanzada de este derecho, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común.

La actividad de la Red durante estos catorce años ha sido intensa y fructífera, promoviendo el desarrollo de quince Encuentros, uno por año (el último, en Santiago de Chile, en junio de 2017), y de otros tantos Seminarios sobre los más variados temas de interés: protección de datos de los menores: datos de salud; sector financiero (fraude); sector comercial y marketing, en especial la lucha contra el Spam; las nuevas tecnologías y su impacto sobre la privacidad; transferencias internacionales, etc.

Esta trayectoria ha llevado a que la Red se haya consolidado como principal promotor del diálogo e impulsor de iniciativas y políticas en la región, que ha significado que más de 150 millones de ciudadanos latinoamericanos dispongan en la actualidad, junto al tradicional amparo de habeas data, de normas que permitan garantizar eficazmente el uso de su información personal y de autoridades especializadas con competencias para tutelar dichas garantías. Las instituciones que forman la Red quieren seguir impulsando el desarrollo del derecho fundamental a la protección de datos de carácter personal, instando a los gobiernos nacionales a que elaboren y mejoren la regulación en esta materia, a efectos de lograr la obtención de la Declaración de Adecuación por parte de la Comisión Europea.

La Agencia Española de Protección de Datos, como Secretaría Permanente de la Red, asume las tareas de coordinación técnica y seguimiento de las actividades de la Red. Entre sus funciones se cuentan el establecimiento de contactos con organismos nacionales e internacionales, instituciones afines y cooperantes a fin de gestionar posibles apoyos técnicos y logísticos para el desempeño de las actividades de la Red y el desarrollo de las decisiones y proyectos aprobados en los Encuentros. En este sentido, en el Programa de Acción de la Red para el período 2015-2017 se recuerda la necesidad de promover la cooperación, el diálogo y el uso compartido de la información para el desarrollo de iniciativas y políticas de protección de datos, así como de promover acuerdos con instituciones públicas o privadas que permitan el desarrollo y ejecución de proyectos de interés mutuo. Más en concreto, en el XIV Encuentro de la Red, celebrado en Santa Marta (Colombia) en junio de 2016, se

acordó la elaboración del Primer Informe anual de la Red, dirigido fundamentalmente a promover el intercambio de experiencias y conocimientos entre sus miembros y a potenciar la difusión internacional de sus actividades.

En uso de sus atribuciones y considerando conveniente el apoyo técnico externo para la ejecución de esta nueva actividad de la Red, la Secretaría Permanente solicitó la coordinación de este primer Informe al Prof. Dr. Guillermo Escobar, de la Universidad de Alcalá, dada su previa experiencia investigadora en materia de derechos humanos y fundamentales y en la dirección, durante quince años, de un Informe similar para la Federación Iberoamericana de Ombudsman.

El Informe que ahora se presenta tiene dos partes bien diferenciadas: una descripción, articulada conforme a un esquema común, de la actividad de las Autoridades de Protección de Datos en 2016 y el estudio de un tema monográfico, en esta primera ocasión la protección de datos de los menores de edad. Las dos partes del Informe se cierran con una síntesis, centrada en la comparación de normas y experiencias de los países que conforman la Red. Es de lamentar que no haya sido posible incorporar las contribuciones de Costa Rica ni Portugal, pero esperamos que puedan aparecer en el Informe 2018.

La primera parte (Informe de actividades 2016) se articula en torno a los ejes siguientes: 1) Introducción (visión general de la Autoridad, ley de creación, puesta en funcionamiento, funciones, evolución hasta hoy); 2) Planificación (si existe algún tipo de planificación estratégica, expresa o no, y cómo se implementó en 2016; decisiones estratégicas principales durante 2016); 3) Acción normativa (normas aprobadas –si la Autoridad tiene potestad reglamentaria–, informes sobre proyectos de normas aprobadas por otros órganos, propuestas de reforma normativa); 4) Procedimientos de garantía del derecho de las personas a la protección de datos; 5) Procedimientos de inspección y sanción (tipos de procedimiento y tipos de sanciones); 6) Cooperación con otras instituciones públicas (centrales o descentralizadas, nacionales e internacionales); 7) Cooperación con la sociedad (en un sentido positivo, como p. ej., fomento de la autorregulación, facilitación del cumplimiento de la ley, relaciones con los responsables, con los profesionales de la privacidad y con otros colectivos; 8) Otras actividades (autorizaciones, información y capacitación a los ciudadanos, acciones de promoción y sensibilización, consultas de profesionales y ciudadanos, etc.); 9) Datos estadísticos sobre las actividades descritas en los apartados anteriores.

Como se advierte, en esta primera parte, las autoridades hemos realizado un esfuerzo de síntesis, meramente descriptiva, destacando las actuaciones más relevantes realizadas el año anterior, poniendo el énfasis en la doctrina de la Autoridad, especialmente en la más novedosa. Las conclusiones de esta primera parte hablan por sí solas. Sin duda, las Autoridades que conforman la Red cuentan con amplias competencias para la protección de los derechos ARCO en sus respectivos territorios, que han ido ampliándose desde su creación. Nuestras Instituciones han desarrollado una labor trascendente para la garantía del derecho a la protección de datos personales en 2016, tanto desde actividades de sensibilización y promoción como con el ejercicio de sus funciones de inspección y sanción. No obstante, las Autoridades de la Red aún se enfrentan a varios retos para la protección de los datos personales en la Región, que en algunos casos incluye su propio fortalecimiento institucional, al no estar dotadas de suficientes medios y facultades de inspección, sanción y acción normativa.

La segunda parte del Informe desarrolla como tema monográfico la protección de datos de los menores de edad, uno de los temas que más preocupa a nuestras Instituciones. Esta segunda parte no se limita a resumir las actuaciones de la Autoridad, sino que incluye un estudio sistemático de la normativa (y de sus carencias y defectos) sobre el tema vigente en el país y de su aplicación (incluyendo jurisprudencia relevante), haciendo especial incidencia en las actuaciones de la Autoridad, pero no como apartado independiente ni limitado al último año.

El esquema común a esta segunda parte es el siguiente: 1) Normativa (qué dice la legislación nacional sobre el tema específico de la protección de datos de los menores, o qué se deduce de sus silencios, reglamentos aprobados en su caso por la Autoridad; propuestas normativas; en especial, la opinión de la Autoridad sobre la normativa vigente y sobre sus carencias); 2) El consentimiento del menor para el tratamiento de sus datos personales (normativa general sobre la capacidad de obrar de los menores, capacidad del menor para consentir el tratamiento de sus datos, prueba de la edad, consentimiento por representación); 3) Ámbitos problemáticos (entre ellos, promociones y concursos dirigidos a menores, publicidad dirigida a menores, contratos realizados con menores, imagen de menores, datos de menores tutelados y en riesgo de exclusión social); 4) Especial consideración del tratamiento de datos en Internet; 5) Ejercicio por los menores de su derecho a la protección de datos (menores sin y con capacidad de consentir, legitimación en vía administrativa y judicial); 6) Herramientas y recursos de la Autoridad en materia de menores.

Especialmente en esta segunda parte se pone de manifiesto la vocación de la Red de servicio al progreso de la región, desde el entendimiento de que poco puede avanzarse sin la previa reflexión compartida sobre la situación, jurídica y fáctica, del derecho a la protección de datos, y en especial de las debilidades en su protección y de las vías más adecuadas para superarlas. Sólo desde el conocimiento de la realidad esta podrá cambiarse y sigue siendo válida la clásica propuesta ilustrada que confiaba encontrar las mejores soluciones tras el diálogo, público, plural y abierto, sobre las distintas alternativas posibles. Con este Primer Informe, la Red da nuevos pasos en su consolidación como organismo a tener en cuenta en la pequeña pero cada vez más importante comunidad internacional de los Derechos Humanos. Frente a la lógica de lo económico, en este ámbito no debe existir competencia sino cooperación y coordinación.

Este Primer Informe de la Red es, entre otras cosas, un trabajo de investigación, y para ello se apoya en la Universidad, como institución dedicada especialmente al estudio y la investigación, considerándose que debía realizarse una aproximación sistemática al tema escogido, conforme a un objeto y método común y, a la vez, aprovechar la oportunidad del trabajo colectivo para cubrir una laguna evidente: la falta de estudios de ámbito netamente iberoamericano sobre protección de datos. También se creyó necesario dar todavía un paso más y construir una auténtica comparación que sintetizara los elementos comunes a los ordenamientos nacionales y la actuación de las Defensorías. Sin duda, todas estas tareas (recopilación de datos, exposición sistemática de los mismos, análisis y síntesis) son científicas y de ahí la colaboración de la Universidad, personalizada en el Director del Informe, quien diseñó su estructura (con una detallada relación de materias) y el plan de trabajo (incluyendo amplias indicaciones de estilo y método) y coordinó todas las contribuciones.

En la elaboración de esta segunda parte se comienza con la descripción sistematizada de las normas jurídicas vigentes, partiendo de la creencia de que el Derecho es el marco obligado, para bien o para mal, y el instrumento principal de actuación de las Agencias, lo que evidentemente no implica que deba esperarse sólo de él, ni mucho menos, la satisfacción de todas las demandas de protección del derecho a la protección de datos en general y de los menores en particular, habida cuenta de que hay normas que no se aplican o que se aplican mal, muchas veces por desconocimiento, de ahí la importancia de la tarea, bien destacada en el Informe, de que las Agencias continúen desarrollando actividades de sensibilización y capacitación.

Las Autoridades que conforman la Red tienen naturaleza pública, indudable legitimación democrática, son creadas y regidas por el Derecho público y se dirigen directamente a garantizar el derecho a la protección de datos. En un Estado de Derecho, ello implica que las críticas y propuestas de actuación que las Autoridades formulen van a tomar como marco de referencia las normas jurídicas, incluyendo, naturalmente, sus omisiones y su

aplicación. Hay que precaverse frente a la moda de situar el estudio de las políticas públicas en el centro del análisis de los Derechos Humanos (perspectiva sin duda útil para otros objetivos), pues puede acabar diluyendo el componente obligacional de los mismos. Los Derechos Humanos son, ante todo, normas exigibles y cualquier otro planteamiento nos desviaría de la cuestión fundamental. Evidentemente, la exposición no es sólo la exposición de las normas sino también de su contexto histórico y social, sin perder de vista el dato de su aplicación efectiva, llamándose la atención, en caso necesario, sobre los supuestos más evidentes de distorsión entre norma y realidad. El obligado seguimiento de un esquema común, además de facilitar la posterior síntesis comparativa, pone de manifiesto las carencias del Derecho en determinados países. Téngase en cuenta que, en esta materia, como en todas las que exigen una actuación positiva de los poderes públicos, tan importante es lo regulado como lo no regulado.

Los apartados correspondientes a cada país han sido redactados por funcionarios de las Autoridades respectivas, designados en cada caso por el titular de la Institución. Los colaboradores siguieron de forma continuada las indicaciones de método y contenido remitidas por el Director del Informe. Gracias a Internet, la comunicación entre colaboradores y Director fue permanente, lo que permitió el intercambio recíproco de sugerencias, que sin duda contribuyó a mejorar el resultado final del trabajo colectivo.

Al igual que en la primera parte, el tono empleado en la segunda es predominantemente descriptivo o expositivo. La Red considera que la valoración y crítica de la realidad y la propuesta de alternativas sólo pueden llegar, en su caso, tras el conocimiento exhaustivo y libre de prejuicios de dicha realidad. Esta opción metodológica no implica, ni mucho menos, la aceptación de lo existente ni la dejación del deber de las Autoridades de alertar sobre las vulneraciones, más o menos graves, más o menos frecuentes, al derecho a la protección de datos. No hay crítica más contundente que la exposición de los datos de la realidad. Así, el señalamiento de las carencias de la legislación o de su ineficacia implica ya una denuncia evidente. También la segunda parte concluye con una síntesis comparada de los respectivos panoramas nacionales. Creemos que la comparación, fruto del intercambio de experiencias y del diálogo sobre las soluciones adoptadas ante los mismos desafíos, es la base para el progreso común, en la línea de los objetivos fundacionales de la Red.

No nos queda sino agradecer a los colaboradores del Informe, designados por cada una de las autoridades participantes, su excelente trabajo, así como la coordinación y asistencia técnica de la Universidad de Alcalá, y hacer votos para que esta iniciativa pueda consolidarse en años sucesivos.

PARTE PRIMERA:
ACTIVIDAD DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS EN 2016

I. ANDORRA

1. INTRODUCCIÓN

La construcción de un marco jurídico de garantías efectiva en la protección de datos personales en el Principado de Andorra es difícil de entender sin conocer antes las peculiaridades de Andorra, caracterizadas por la influencia del *ús i costum* (uso y tradición), en un mundo sin fronteras donde la información personal y la protección de la intimidad de las personas se encuentran expuestos a riesgos que no se le escapan a nadie, riesgos que vienen determinados en una sola palabra: globalización.

Características del Principado de Andorra

Andorra es un pequeño país situado en los Pirineos, entre Francia y España, es el sexto país más pequeño del mundo en superficie y tiene unos 70.000 habitantes aproximadamente, aunque de estos, solo la mitad de la población ostenta la nacionalidad andorrana. Su actividad económica se basa en el sector terciario (en el que se inscriben el 80% de las empresas que operan en el país) y especialmente en el turismo. En los últimos tiempos Andorra evoluciona con una apertura hacia Europa y al mundo, formando parte de organizaciones europeas e internacionales sin dejar de ser un país tercero, presentando características peculiares ya que no es miembro ni de la Unión Europea ni del Espacio Económico Europeo. Estas peculiaridades son particularmente significativas en lo que se refiere a la protección de datos personales y concretamente, en las transferencias internacionales de datos.

Evolución de Andorra en materia de protección de datos

La evolución del Principado de Andorra en el ámbito de la protección de datos ha sido muy positiva en los últimos veinte años. Desde la aprobación del Código de la Administración, el 10 de abril de 1989. Sobre todo, con la promulgación el 14 de marzo de 1993 de la Constitución del país, en la que el artículo 14 proclama entre los derechos fundamentales de la persona y las libertades públicas, la garantía del derecho a la intimidad, al honor y a la propia imagen declarando que todo ciudadano tiene derecho a ser protegido por las leyes contra intromisiones ilegítimas en la vida privada o familiar. Es por la promulgación de este objetivo donde debemos situar la Ley 15/2003, Cualificada de Protección de Datos Personales, que fue desarrollada además por el Decreto de 1 de julio de 2004, del Registro Público de Inscripción de Ficheros y el Decreto del 9 de junio de 2010, en el que se aprueba el Reglamento de Desarrollo de la Agencia Andorrana de Protección de Datos.

En el ámbito internacional, Andorra ha firmado y ratificado el Convenio 108 del Consejo de Europa para la protección de las per-

sonas con respecto al tratamiento automatizado de datos de carácter personal y el Protocolo adicional, debiendo indicarse que, según el sistema jurídico andorrano (art. 3 de la Constitución de Andorra) los tratados y acuerdos internacionales entran en vigor a partir de su publicación en el Boletín Oficial del Principado de Andorra y no pueden ser derogados por la legislación nacional. Es decir, que dichos tratados y acuerdos forman parte, desde el momento de su ratificación, del Derecho andorrano y son directamente aplicables en el país. Conviene añadir que, por la resolución de la Comisión Europea publicada en el Diario Oficial de las Comunidades Europeas del mes de octubre de 2010, Andorra goza de la consideración de tener un nivel adecuado de protección según dicha Comisión.

Modelo andorrano de protección de datos

El modelo andorrano de protección de datos se basa pues en el reconocimiento de dicho derecho como fundamental, lo que supone que, como tal, debe ser supervisado por los poderes públicos, por la autoridad de protección de datos y por los tribunales, de forma que las personas a las que se lesiona el derecho tienen, por un lado, una tutela administrativa ejercida por una autoridad independiente; y por otro, un control y tutela judicial efectiva.

La Agencia Andorrana de Protección de Datos

Para una efectiva aplicación de la legislación de protección se requiere que en cada Estado exista una Autoridad independiente que garantice el respeto de las normas sobre protección de datos de carácter personal, exigencia que vienen reiterando las normativas de nuestro entorno. El Tribunal de Justicia de la Unión Europea ha considerado la creación de estas autoridades de control en cada uno de los Estados miembros como un "elemento crucial de la protección de las personas en lo que respecta al tratamiento de datos personales" (STJUE de 9 de marzo de 2010). En Andorra, la autoridad independiente que garantiza la normativa referida a la protección de datos es la *Agència Andorrana de Protecció de Dades* (en castellano Agencia Andorrana de Protección de Datos, y en adelante la Agencia), ente público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia orgánica y funcional de las Administraciones públicas en el ejercicio de sus funciones. Regida por la Ley 15/2003, cualificada de protección de datos personales, y desarrollada por el Reglamento de Desarrollo de 9 de junio de 2010, su principal función es garantizar los derechos a la protección de datos personales y el acceso a la información vinculados a la misma. Como hemos dicho, la Agencia ejerce sus funciones con total independencia y objetividad, no estando sujeta por tanto a ninguna instrucción en el desempeño de las mismas, ni sometida a la tutela de ningún órgano del Estado. Esta independencia es válida tanto para el sector público como el sector privado. Las funciones de la Agencia se desarrollan en el artículo 25 del Reglamento que establece:

Funciones de la Agencia

Son funciones de la Agencia:

– Dictar instrucciones y recomendaciones necesarias para adecuar los tratamientos de datos personales a los principios recogidos por la legislación vigente en materia de protección de datos.
– Emitir informes, cuando así se le requiera, con carácter consultivo acerca de proyectos de ley, proyectos de disposiciones

normativas elaboradas por el Gobierno o de los proyectos de reglamentos o disposiciones que afecten la protección de datos.
– Emitir sus opiniones acerca de otras leyes y normas que afecten a la privacidad de personas físicas y los tratamientos y seguridad de datos personales.
– Proponer mejoras respecto a la normativa vigente de protección de datos
– Responder a las consultas de las Administraciones Públicas, entes públicos o privados o de la ciudadanía sobre la aplicación de la legislación de protección de datos
– Proporcionar información sobre los derechos de las personas mediante la realización de campañas de difusión que consideren oportunas.
– Redactar, aprobar y publicar la lista de países que dispongan de una protección equivalente en materia de protección de datos y atender a las consultas relativas a la comunicación internacional de datos a países que no tengan un nivel de protección suficiente y adecuado.
– Resolver de forma motivada sobre la procedencia de las solicitudes de inscripción, modificación o supresión de ficheros que hayan de practicarse en el Registro Público de Inscripción de Ficheros de Datos Personales
– Requerir a los responsables de tratamiento y a los encargados de ficheros la adopción de medidas adecuadas para el tratamiento de datos objetos de investigación según la ley vigente e instar judicialmente el cese de tratamiento y cancelación de ficheros cuando así corresponda.
– Incoar, instruir y resolver los expedientes sancionadores relativos a los responsables del tratamiento de ficheros de titularidad privada.
– Instar la incoación de expedientes disciplinarios en los casos de infracciones cometidas por responsables de ficheros de la administración pública.
– Elaborar una memoria anual en la que se incluya información sobre la aplicación de la Ley 15/2003 y de otras disposiciones legales y reglamentarias relativas a la protección de datos.

Gestión del Registro de Ficheros de Protección de Datos

La gestión del Registro de Ficheros de Protección de Datos es una de las funciones principales de la Agencia. El Registro es un órgano integrado en la propia Agencia en el que deben ser inscritos, conforme al procedimiento establecido en el Decreto de 1 de julio de 2004, del Registro Público de Inscripción de Ficheros: los ficheros de titularidad privada y las autorizaciones a las que se refiere la Ley 15/2003. Además del procedimiento de inscripción, el Reglamento regula también el contenido de la inscripción, su modificación, cancelación y las reclamaciones y recursos contra las resoluciones correspondientes.

Características y organización interna de la Agencia

En funcionamiento desde 2005, la Agencia está integrada por el Director de la Agencia, dos inspectores (designados por el poder legislativo) y el Registro Público de Inscripción de Ficheros. Es una institución independiente que vela por que los datos de la ciudadanía se traten, por parte de organizaciones privadas y Administraciones públicas,

garantizando siempre el derecho fundamental a la protección de datos personales. Desde su creación, la Agencia se ha esforzado para acercarse día a día a la ciudadanía y a los responsables del tratamiento de entidades públicas y privadas, con el fin de difundir de forma pro-activa el respeto hacia el derecho de todo ciudadano de ver protegidos sus datos personales. Todo esto desde el absoluto convencimiento de que para ejercer correctamente un derecho debemos conocerlo y solo un ejercicio responsable y consciente, es garantía de libertad. A lo largo de los años la actividad de la Agencia ha ido en aumento tanto en la emisión de informes, consultas telemáticas o presenciales, inscripción de ficheros, etc. Ante los nuevos retos las Autoridades de protección de datos hemos de adaptarnos continuamente, sin perder nuestros valores fundamentales e inherentes que motivaron nuestra creación.

2. PLANIFICACIÓN

Retos de la Agencia

La Agencia se encuentra ante grandes retos: una capacidad constante de adaptación ante las nuevas cuestiones que puedan surgir en la sociedad y el cumplimiento de sus funciones o potestades previstas legalmente. El artículo 40 de la Ley 15/2003, dispone que son sus potestades:

- Velar por el correcto cumplimiento de la Ley
- Gestionar el Registro Público de inscripción de Ficheros de Datos Personales.
- Publicar anualmente la lista de países con protección equivalente (de acuerdo con lo dispuesto en el artículo 36 de la misma ley).
- Ejercer la potestad inspectora y de sanción para infracciones tipificadas en la Ley 15/2003.
- Proponer las mejoras que considere convenientes en la normativa de protección de datos.

Estrategia de actuación para 2016

Para el año 2016 la Agencia diseñó su estrategia de actuación orientada en varios ámbitos. Por un lado el tratamiento de datos de los menores, por otro una incidencia en el tratamiento de datos en el sector inmobiliarios y las comunidades de propietarios, debido al aumento de las consultas efectuadas ante la Agencia en este sector y la mejora de los procedimientos internos para dar respuesta a las consultas efectuadas por los ciudadanos y las Administraciones públicas, así como al mismo tiempo, la adaptación de los procedimientos de inspección al nuevo Decreto Legislativo del Código de la Administración. Cabe señalar que la Agencia, sin ser una excepción al resto de Autoridades de control, se encuentra en muchas ocasiones desbordada por el día a día y el incremento de las tareas hace que tengan que definirse objetivos realistas y realizables.

3. ACCIÓN NORMATIVA

Instrucciones, recomendaciones e informes sobre proyectos legislativos

La Agencia tiene potestad para aprobar y publicar instrucciones, recomendaciones e informes sobre proyectos legislativos en lo que a la

adecuación de la normativa protección de datos se refiere. Durante 2016 la Agencia emitió los Informes que se enuncian a continuación (a petición del Gobierno):

- Proyecto de Ley de derechos y deberes del paciente y de la Historia Clínica.
- Proyecto de Reglamento del Consejo Regulador del Juego.
- Proyecto de Decreto de publicación de los ficheros de datos personales del Consejo Regulador del Juego
- Solicitado por el Tribunal de Cuentas respecto al tratamiento de los datos personales en el control de la financiación de los partidos políticos y la financiación de las campañas electorales.
- Proyecto de decreto de ficheros de datos personales el responsable del cual es el Tribunal de cuentas.
- Proyecto de Ley del Plan de estadística cuatrienal.
- Proyecto de creación de un fichero de Registro de Morosos.
- Solicitado por la Secretaria General del Consell General sobre la utilización de datos de participación en campañas electorales.
- Sobre la licitud de la cesión de datos de los propietarios de edificios al Ministerio de Medio ambiente para el control de la seguridad de las instalaciones de almacenaje y distribución de carburante.
- Solicitado por un ayuntamiento sobre el proyecto de actualización del Decreto regulador de los ficheros de datos personales de menores.
- Solicitado por la representación del Consell General ante la OCDE sobre la propuesta de adopción de una resolución.
- Sobre la cesión de datos de la Caixa Andorrana de Seguretat Social al Departamento de Estadística.
- Sobre la destrucción de documentación de un centro de acogida de minusvalorados.
- Sobre el tratamiento de datos por la Asociación de administradores de fincas y gestores inmobiliarios.
- Sobre el tratamiento de datos en las Comunidades de propietarios.
- Sobre el proyecto de Decreto del fichero de datos personales del Ministerio de Cultura para actividades culturales.
- Sobre los derechos de las personas afectadas en el tratamiento de sus datos personales en la página web del Ministerio de Cultura. Derecho de información, cláusula legal, y ejercicio de derechos.
- Sobre la adecuación a la Ley de protección de datos en la instalación de cámaras de videovigilancia por parte de entidades de naturaleza pública, comunidades de propietarios, entidades financieras y entidades privadas.
- Sobre la cesión de datos de un fichero de naturaleza pública a una asociación deportiva.
- Sobre la adecuación a la Ley de protección de datos de la cesión de datos del Ministerio de asuntos sociales al Departamento de Tributos y Fronteras.
- Proyecto de Reglamento, de los ficheros de datos personales y de la transferencia internacional de datos de los datos de los deportistas tratados por la Agencia andorrana anti-dopaje.

4. PROCEDIMIENTOS DE GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS

Acceso, rectificación, oposición y supresión como derechos personalísimos

Los derechos de las personas interesadas de acceso, rectificación, oposición y supresión, están regulados en los artículos 20 y siguientes de la Ley y desarrollados por los artículos 10 y siguientes del Reglamento. De conformidad a las disposiciones del artículo 25 de la Ley y 16 del Reglamento son derechos personalísimos y solo pueden ejercerse por el interesado o mediante representante. Estos son independientes entre sí, no necesitando del ejercicio previo de ninguno de ellos para su ejercicio. La persona afectada se ha de dirigir al responsable del tratamiento para solicitar el ejercicio de sus derechos. El ejercicio de los derechos es gratuito para la persona afectada, por lo que el responsable del fichero no puede obstaculizar el ejercicio solicitando el reintegro de los gastos que pueda ocasionar su tramitación.

Derecho de acceso

El derecho de acceso garantiza que todo el mundo tiene derecho a ser informado detalladamente de la existencia de ficheros que contengan datos sobre sí mismo y de la finalidad del mismo, entre otros. El responsable del fichero tendrá 5 días hábiles desde la recepción de la solicitud escrita del interesado para contestar de forma inteligible y clara. El derecho de acceso puede ser denegado en los supuestos previstos en la misma Ley, pero en todo caso, el rechazo a la solicitud deberá ser motivado y deberá comunicarse también por escrito y en el mismo plazo, siendo siempre recurrible ante la Agencia.

Derecho de rectificación

El derecho de rectificación consiste en la capacidad de las personas de dirigirse a los responsables de ficheros en caso de que los datos del fichero no se correspondan con la realidad. En este caso, el responsable tendrá 1 mes desde la recepción de los documentos que justifiquen la modificación, para rectificar los datos o para rechazar, de forma motivada, dicha rectificación en base al artículo 32 de la Ley. En caso de que los datos se hubieran comunicado a un tercero, este mismo deberá ser informado de la rectificación y deberá modificar también su fichero.

Derecho de supresión

El derecho de supresión, además de las causas del artículo 32, también podrá denegarse en supuestos de: una norma obligue al responsable a la conservación de los datos; cuando la conservación sea necesaria para la finalidad legítima del responsable y del fichero; y cuando la información sea necesaria en virtud de la relación contractual del interesado y el responsable. Ante la solicitud de supresión, el responsable dispondrá de 1 mes para proceder o bien a la denegación motivada del derecho de supresión; o bien al bloqueo de los datos que deberán conservarse únicamente para la disposición de administraciones públicas y de los tribunales con el objeto de poder atender a posibles responsabilidades relativas al tratamiento durante el plazo de prescripción de los datos. Después de dicho plazo, los datos se suprimirán.

Derecho de oposición

Finalmente, el derecho de oposición se ejercerá cuando un interesado no quiera que se comunique a un tercero sus datos. Una vez un destinatario reciba los datos, este deberá identificarse ante el interesado reiterando la finalidad del fichero en un plazo no superior

a 15 días. Desde dicha comunicación, los interesados tendrán 1 mes para oponerse a la comunicación y de no hacerlo, se entenderá su aceptación tácita al mismo.

Todas las denegaciones motivadas al ejercicio de los derechos aquí descritos serán en todo caso recurribles ante la Autoridad de control que evaluará la posible infracción y tramitará el expediente administrativo de conformidad a los procedimientos de inspección y sanción.

Resoluciones destacadas en 2016

En 2016 entre las resoluciones de procedimientos sancionadores por vulneración a los derechos de acceso, podemos destacar:

- Exp 261/16 Resolución que se formula ante reclamación del 26 de enero, contra un centro deportivo privado por no atender las reiteradas demandas del derecho de acceso del denunciante. Resolución imponiendo una sanción de 2.000 €.
- Exp. 263/16 Resolución de archivo que se dicta ante la falta de acreditación del denunciante respecto a la reclamación presentada por correo electrónico solicitando el derecho de acceso a una página web a la que el mismo había facilitado sus datos personales.
- Exp. 271 i 272/016 Resolución que se formula ante reclamación del 19 de octubre presentada por no atender debidamente las demandas del denunciante por parte de la Seguridad Social andorrana. Se resuelve el expediente admitiendo por motivos formales la reclamación por haber sido atendida fuera del plazo.

Durante el 2016 no se han presentado reclamaciones de tutelas de derechos de cancelación, oposición y modificación.

5. PROCEDIMIENTOS DE INSPECCIÓN Y SANCIÓN

Habilitación legal de inspección y sanción

De acuerdo con las normas de protección de datos y las reguladoras de la propia Agencia, la Agencia realizará procedimientos de inspección y, si procede, de sanción. La potestad de inspección se desarrolla en los artículos 41 de la Ley 15/2003 y 35 del Reglamento. La Agencia está legalmente habilitada para inspeccionar los ficheros y recabar cuantas informaciones precisen para el cumplimiento de sus cometidos de vigilancia.

Procedimiento de inspección

El procedimiento de inspección puede iniciarse de oficio o por solicitud de cualquier persona interesada que considere vulnerados sus derechos por un responsable de fichero. Se abre entonces una fase de investigación previa en la que se analiza si el hecho denunciado vulnera o no la normativa vigente de protección de datos; ya sea de un fichero público como de uno privado. Ante esta solicitud de parte o ante un inicio de oficio, el Director de la Agencia autoriza a los inspectores para que inicien la fase de investigación, especificando en dicha autorización la finalidad de la inspección y la conveniencia de las actuaciones a realizar sobre el hecho denunciado. En esta fase de investigación, la Agencia puede dirigirse directamente a los responsables o encargados de ficheros y solicitar toda la información que sea necesaria, personarse en las dependencias si así lo estima conveniente o acceder a los recursos informáticos o de otra índole

destinados al tratamiento de datos (en aquellos casos que los locales a investigar sean a su vez domicilios privados deberá ajustarse la actuación a las reglas de la inviolabilidad). Practicada la inspección, los instructores presentarán su propuesta de resolución al Director de la Agencia quien decidirá sobre el inicio de un expediente administrativo sancionador o no. Además resolverá si se archiva o no la causa y se pronunciará sobre la existencia o no de una violación de la normativa de protección de datos. En el supuesto que se considere que efectivamente existe una vulneración de la normativa, se incoará el expediente administrativo sancionador a través del procedimiento previsto en el Texto Refundido del Código de la Administración, del 29 de marzo de 1989, conforme a lo dispuesto por el artículo 42 de la Ley 15/2003, sobre la potestad sancionadora de la Agencia.

En el supuesto de protección de datos, al ya haberse realizado una investigación por parte del inspector y habiéndose evaluado los hechos como vulneradores de la legislación sobre la materia, el procedimiento administrativo se verá reducido meramente a la calificación de la infracción acarreando en su caso las sanciones correspondientes. En una resolución motivada, el Director de la Agencia razonará los hechos que considere probados, la norma legal en que se tipifica como infracción dicha actividad y la norma legal que establece la sanción.

Regulación de las sanciones

La sanción administrativa se prevé en la Ley 15/2003 (arts. 33 y 34) donde se dispone que el incumplimiento de la legislación de protección de datos acarreará sanción, tanto en personas físicas como jurídicas de naturaleza privada o pública.

En el caso de ficheros privados, el primer incumplimiento se sancionará con un importe máximo de 50.000 euros y de haber subsiguientes infracciones, la multa podrá aumentar hasta los 100.000 euros. Dada la amplitud de la cuantía de la sanción y para evitar la fijación discrecional por parte del órgano sancionador, la cantidad es graduada por la Autoridad de control teniendo en cuenta: las circunstancias de la infracción, la gravedad del incumplimiento, el número de afectados, el daño efectivamente causado y supuestos de reincidencia. Esto se aplica a la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.

En el caso de ficheros de naturaleza pública, la Agencia tiene la capacidad de sancionar de acuerdo con el régimen disciplinario regulado en las normas de dichas entidades públicas y deberá dictar una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Por tanto, se trata propiamente de una sanción, pues en estos casos la Agencia emite un requerimiento imperativo de medidas a adoptar.

Inmovilización de ficheros

Las infracciones y consecuentes sanciones pueden suponer a su vez la inmovilización de ficheros, es decir, el órgano sancionador puede, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos personales, tanto de titularidad pública como privada la cesación en la utilización o cesión ilícita de datos en los supuestos constitutivos de infracciones graves o muy graves, en que la persistencia en el tratamiento de los datos de carácter personal o su

comunicación o transferencia internacional posterior pueda suponer un grave menoscabo de los derechos fundamentales de los afectados y, en particular, de su derecho a la protección de datos de carácter personal. Si el requerimiento es desatendido, el órgano sancionador puede, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

Prescripción de infracciones y sanciones

En ambos casos, el procedimiento sancionador pone fin a la vía administrativa. Las infracciones tendrán un plazo de prescripción de 3 años desde su comisión y los procedimientos de inspección y sanción que la Agencia haya iniciado caducaran a los 6 meses de la última actuación realizada si no se producen nuevas actuaciones o no se emite una resolución.

Procedimientos de sanción destacados en 2016

De los procedimientos de sanción instruidos en 2016 destacamos los siguientes: 1) Exp. 264/16 Resolución de archivo de las diligencias previas de investigación en la denuncia presentada por un particular al denunciar falta de medidas de seguridad en la página web de una entidad financiera. 2) Varios expedientes denunciando la utilización de sistemas de videovigilancia por entidades públicas en lugares públicos, así como por denunciantes particulares (comunidades de propietarios) resolviendo el archivo de los mismos por no vulnerar la legislación vigente de protección de datos.

6. COOPERACIÓN CON OTRAS INSTITUCIONES PÚBLICAS

Convenios de cooperación con instituciones públicas

Desde la Agencia y para garantizar una correcta difusión de la normativa de protección de datos, se han firmado distintos convenios de cooperación con instituciones públicas nacionales e internacionales. Los convenios de colaboración con instituciones públicas nacionales responden al principio de lealtad institucional en la actuación y la relación de Administraciones públicas que debe transformarse en actuaciones de cooperación, colaboración y asistencia mutua para el ejercicio eficaz de las competencias mutuas de cada institución. Por ejemplo, encontramos aquí convenios ratificados por la Agencia y la Cámara de Comercio de Andorra o entre la Agencia y el *Raonador del Ciutadà* (Defensor del pueblo).

Colaboración con el *Raonador del Ciutadà*

En este último, la finalidad es el fomentar la defensa, vigilancia, cumplimiento y aplicación de los derechos y libertades recogidas en la Constitución de Andorra y, entre las mismas, la protección del derecho fundamental a la protección de datos personales. Para conseguir dicha finalidad, el Convenio prevé una serie de actuaciones como son, entre otras, la asistencia verbal escrita o presencial entre ambas instituciones, la función de la Agencia de asesorar al Raonador mediante la formación de sus funcionarios o personal en el ámbito de la protección de datos, la contribución mutua en el desarrollo de estudios, proyectos o investigaciones en la materia, etc.

Carta de intenciones con la Agencia Española de Protección de Datos

A nivel internacional, la Agencia tiene firmada una Carta de intenciones con la Agencia Española de Protección de Datos (AEPD) para tejer una red de soporte logístico entre ambas instituciones. Me-

diante el Convenio bilateral firmado, ambas instituciones reconocen el inicio de una etapa de colaboración y cooperación institucionales para fomentar una mayor difusión del derecho fundamental a la protección de datos de carácter personal. En este sentido, ambas Agencias se comprometen, entre otras actividades, a un intercambio de información automático cuando la Agencia que tenga atribuida la competencia para conocer del caso sea distinta a la Agencia que dispone de la información relativa al mismo, la contribución mutua al desarrollo de estudios, investigaciones o informes, la actuación conjunta cuando sea necesario para la eficaz protección del derecho fundamental que aquí nos ocupa o el apoyo mutuo en la tramitación de expedientes, etc.

Participación en organizaciones internacionales

Además, la Agencia es miembro de pleno derecho de la Red Iberoamericana de Protección de Datos, de la Asociación Francófona de Protección de Datos, de las conferencias de Primavera de Protección de Datos e Internacional de Protección de Datos y, además, representa al Principado de Andorra en el Grupo de Trabajo del Convenio 108 del Consejo de Europa, de 28 de Enero de 1981, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal.

7. COOPERACIÓN CON LA SOCIEDAD

Actividades de capacitación y sensibilización

La principal prioridad de la Agencia es la ciudadanía, por eso la protección efectiva de los ciudadanos en el uso de sus datos personales exige, no solo un mayor conocimiento de la normativa que les protege y un ejercicio efectivo de los derechos que se les reconoce, sino también que su nivel de concienciación se adapte a los nuevos riesgos que acechan a nuestra sociedad. Por este motivo, la Agencia seguirá respondiendo a las necesidades de los ciudadanos y a las cuestiones planteadas por sectores empresariales o colegiales (abogados, médicos, consultores, gestores, etc.) mediante charlas y formaciones. Al mismo tiempo, se buscará seguir atrayendo a los jóvenes, principales usuarios de Internet y redes sociales y colectivo que más peligro de desprotección en su privacidad tiene debido al desconocimiento de los riesgos que un mal uso de estas plataformas puede conllevar. Por todo esto los objetivos prioritarios de la Agencia son:

- Conseguir una auténtica cultura de protección de datos personales
- Disponer de los medios adecuados que garanticen una prestación de servicios óptima
- Facilitar el cumplimiento de las exigencias legales a quienes les sean de aplicación
- Cooperar con las instituciones con la finalidad de profundizar en la armonización y la coherencia del marco jurídico y su aplicación.

Las Autoridades de protección de datos son un garante institucional del derecho a la protección de datos personales y, por esto, la

cooperación activa en la sociedad mediante campañas informativas, asistencia a eventos y formaciones es un rasgo y una tarea esencial para el buen desarrollo de las funciones de la Agencia.

8. OTRAS ACTIVIDADES

Actividades de difusión y sensibilización

Conforme se señaló anteriormente, una de las principales misiones de la Agencia es difundir y sensibilizar sobre los derechos y las obligaciones relacionadas con los datos de carácter personal. Con esta finalidad, se organizan conferencias, se editan folletines y se realizan reuniones formativas con los responsables de ficheros de datos. Entre otras actividades se desarrollaron:

- Día Internacional de la Protección de Datos. El Consejo de Europa, la Comisión Europea y las autoridades de protección de datos de los Estados miembros promueven desde 2007 el Día Europeo de la Protección de Datos, que se celebra el 28 de enero. Esta jornada sirve para publicitar el derecho fundamental a la protección de datos y velar para que se respeten. Ejemplos de actuaciones que la Agencia ha realizado durante esta jornada han sido emisión de recomendaciones relativas a vídeo-vigilancia, al uso de redes sociales y seguridad en Internet o recomendaciones para la protección de datos en el ámbito laboral. Estas recomendaciones se publican en la página web y en formato papel o trípticos para su difusión.
- La Agencia en los medios de comunicación. Los medios de comunicación del país representan un buen aliado en el momento de difundir los principios de protección de datos. Por este motivo, la Agencia mantiene una buena relación con los representantes de estos, que se han hecho eco de distintas actividades realizadas, como las publicaciones de las recomendaciones anteriormente citadas del Día Europeo de la Protección de Datos, jornadas formativas celebradas para el colegio de abogados o para los operarios de un centro comercial.
- Acciones Formativas. Cada año, la Agencia organiza y participa de formaciones y reuniones tanto con organizaciones públicas y privadas con la intención de ofrecer un asesoramiento global en cuestiones relacionadas con la protección de datos personales. Además de las que ya hemos ido comentando anteriormente, también hemos realizado formaciones con fundaciones cuyo objetivo es fundar "*smart cities*", encuentros con agrupaciones de jóvenes y charlas en centros educativos, formaciones a trabajadores de notarías, sociedades de autores y representantes del gobierno y de la seguridad social.

9. DATOS ESTADÍSTICOS

De las funciones realizadas por la Agencia durante 2016, podemos destacar las siguientes cifras:

Incremento del 25% en informes emitidos

– Informes: Se han incrementado en un 25% el número de informes emitidos (55). De estos los más relevantes que aún no hemos mencionado son: 1) Adecuación del Proyecto de captación de propietarios de perros incumpliendo la Ley 15/2003; 2) Adecuación de la Ley andorrana del proyecto de resolución de la OSCE; 3) Informe sobre la cesión de datos al departamento de tributos y asuntos sociales; 4) Informe sobre la cesión de datos al departamento de Medio Ambiente por parte de los suministradores de carburantes; 5) Capacidad de crear un fichero de datos personales por el Tribunal de Cuentas; 6) Informe sobre el procedimiento de recogida de datos en la celebración de concursos privados (de grandes almacenes) o públicos (departamento de turismo).

Consultas recibidas

– Consultas: Vía correo electrónico: aumento del 12% (1.185); Vía telefónica: aumento del 5% (1.379); Vía presencial o en reuniones de trabajo: aumento del 17% (79).

2.878 ficheros inscritos por entidades privadas

– Registro de ficheros: 55% (497 tramitaciones) con un total de 2.878 ficheros inscritos por entidades privadas. Los de naturaleza pública se publican en el Boletín Oficial del Estado.

II. ARGENTINA

1. INTRODUCCIÓN

Un mundo más conectado y el incesante avance de las nuevas tecnologías en la actual era digital requieren un mayor esfuerzo por parte del Estado en preservar la protección de la intimidad y privacidad de los titulares de datos personales, como así también en garantizar la seguridad en el tratamiento de los mismos. El gran desafío es cumplir con aquellos objetivos sin constituirse como una barrera para la innovación tecnológica y el desarrollo económico.

Capacitación, control, fiscalización y asesoramiento

Durante el 2016 la Dirección Nacional de Protección de Datos Personales (DNPDP), dependiente de la Subsecretaría de Asuntos Registrales del Ministerio de Justicia y Derechos Humanos de la Nación, se abocó a continuar reforzando sus programas de capacitación, planes de control, fiscalización y asesoramiento en materia de protección de datos personales, según lo dispone la Ley 25.326, la cual la establece como Autoridad de Aplicación. En la DNPDP su principales función es la de trabajar en la concientización de la importancia de la protección de los datos personales y de un adecuado uso de los dispositivos electrónicos a través de los cuales se utilizan servicios y productos en Internet.

Evolución de la legislación de protección de datos

Teniendo en cuenta que la Ley sobre protección de datos personales fue sancionada en octubre de 2000, que los avances y desarrollos tecnológicos son cada vez mayores y que Europa ha actualizado su normativa, la DNPDP ha iniciado en 2016 un proceso de reflexión sobre la necesidad de una reforma a la Ley citada. Este proceso fue convocado en el marco del programa "Justicia 2020" del Ministerio de Justicia y Derechos Humanos de la Nación. Contó con el aporte, las sugerencias de expertos y especialistas del sector privado, del ámbito académico como así también de la sociedad civil. El concepto sobre el cual se trabajó tiene su basamento en considerar que los avances de la tecnología deben ir de la mano de la protección de los derechos. De este modo, la DNPDP tiene previsto dentro de su planificación futura iniciar el proceso de redacción de un Anteproyecto de ley que, en caso de considerarlo oportuno el Poder Ejecutivo Nacional, impulse formalmente la reforma de la norma vigente.

Creación del Registro Nacional "No Llame"

El 30 de julio de 2014 se promulgó la Ley 26.951 que crea el Registro Nacional "No Llame" (RNNLL) en el ámbito de la Dirección Nacional De Protección De Datos Personales. Su finalidad es concentrar los números telefónicos de titulares o usuarios –autorizados por este–, que manifiesten su decisión de no ser contactados por las empresas que publiciten, oferten, vendan o regalen bienes o servicios

mediante servicios de telefonía (cualquiera sea su modalidad), tales como: telefonía básica, móvil, servicios de radiocomunicación móvil celular, comunicaciones móviles, SMS por IP, voz por IP, y cualquier otro servicio similar que la tecnología permita en el futuro.

Trámite de inscripción ante el Registro Nacional "No Llame"

El trámite de inscripción ante el Registro Nacional "No Llame" es gratuito, sencillo y de alcance nacional. Puede efectuarse las 24 horas del día por la línea telefónica 146, o mediante la página web "www.nollame.gob.ar". Quienes publiciten, oferten, vendan o regalen bienes o servicios utilizando como medio de contacto los servicios de telefonía, no podrán dirigirse a ninguno de los inscriptos en el Registro Nacional No Llame. Para ello, deberán consultar al menos cada 30 días la base de datos de inscriptos proporcionada por la DNPDP, previa inscripción en el Registro Nacional de Bases de Datos. El titular de la línea telefónica o usuario autorizado, podrá denunciar ante este organismo el incumplimiento de lo establecido en esta ley.

El 16 de enero de 2015 se reglamentó mediante la Disposición 3/2015 entrando en plena vigencia. Se reciben las denuncias de particulares por los presuntos incumplimientos a la Ley 26.951. Se trata de personas que encontrándose inscriptas en el Registro Nacional "No Llame" son contactados con la finalidad de publicidad, oferta, venta y regalo de bienes o servicios no solicitados.

En agosto 2016 se volvió a reunir el Consejo Consultivo de la DNPDP, que llevaba más de 9 años sin convocarse. En la cita, los miembros del Consejo pudieron tratar junto con el Director Nacional, Eduardo Bertoni, aspectos relevantes de la función de protección de datos personales y del organismo en particular, como por ejemplo mejoras en la implementación del "Registro Nacional No Llame" y la importancia de una reforma de la Ley 25.326.

Creación del Registro Nacional de Bases de Datos

La Ley 25.326, en su artículo 21, también crea el Registro Nacional de Bases de Datos, el cual se implementa por Disposición 02/05. Es la herramienta que permite al titular de los datos personales acceder a la información necesaria para el ejercicio de los derechos que le otorga la Ley. El ciudadano podrá confirmar a través de la página web si un titular o usuario de bases de datos se encuentra registrado y, en ese caso, obtener los datos de contacto para ejercer sus derechos de manera que, ante la falta de respuesta, genere la posibilidad de solicitar el inicio de las actuaciones administrativas para la sanción que corresponda. Los responsables de archivos o bancos de datos, deben declarar sus bases de datos destinadas a dar informes, mediante la inscripción en el Registro Nacional de Bases de Datos, a través de formularios disponibles en la página web: https://www.sitioseguro.jus.gov.ar/dnpdp/login.epl

Esta inscripción, emparentada con el Registro Nacional "No Llame" es requisito ineludible para las empresas que realicen publicidad, oferta, venta o regalos de bienes y servicios no solicitados mediante los servicios de telefonía y deberán tener su inscripción vigente ante el Registro Nacional de Bases de Datos. Solo de esa forma estarán habilitados para descargar el archivo con la lista de los inscriptos en el Registro "No Llame".

2. PLANIFICACIÓN

Planificación Operativa para 2016

En su Propuesta de Planificación Operativa de la unidad organizativa para el año 2016, la DNPDP planteo como ejes los siguientes programas/proyectos:

Difusión del Programa "Con vos en la web"

– P.1. Difusión del Programa de concientización Con vos en la web. El Programa Con vos en la web surge para concientizar acerca de la importancia de la protección de datos personales en el entorno de las nuevas tecnologías. Problemática a abordar: Desarrollar nuevos talleres y capacitaciones para niños y docentes. Creación de nuevos contenidos. Objetivo del programa: concientizar y lograr un uso responsable de las nuevas tecnologías, mediante la generación de capacidades críticas y reflexivas.

Inspecciones al sector privado

– P.2. Continuar con las Inspecciones al sector privado y aumentar la cantidad de inspecciones. La Ley 25.326 establece la facultad de controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley. Problemática a abordar: Aumentar la cantidad y calidad de las inspecciones anuales iniciadas. Objetivo del programa: Aumentar la capacidad operativa y de fiscalización aportando mayor eficiencia a la competencia legalmente encomendada.

Sistema informático del Registro Nacional de Bases de Datos

– P.3. Modernizar el sistema informático del Registro Nacional de Bases de Datos. La Ley 25.326 establece la inscripción obligatoria al Registro Nacional de Bases de Datos (RNBD). Esa inscripción se lleva a cabo mediante un sistema informático que ha quedado desactualizado, no permite una buena administración de la base de datos y está programado en un lenguaje obsoleto y con escasa capacidad de recibir soporte técnico y nula capacidad de mejoras. Problemática a abordar: Modernizar el Sistema informático del Registro. Objetivo del programa: Modernizar el sistema informático del RNBD, que permitirá una mejor administración de la base de datos, y un entorno más amigable y sencillo para los obligados a la inscripción.

Centro de Capacitación, Investigación y Difusión

– P.4. Centro de Capacitación, Investigación y Difusión de la Protección de los Datos Personales. Representa el área de la PDP que canaliza la capacitación, investigación y difusión de la protección de los datos personales sobre distintas temáticas involucradas con las tareas de incumbencia de la PDP: seguridad de la información, niños/adolescentes, sus interacciones en la redes sociales, sus relaciones con las nuevas tecnologías, el resguardo del derecho de privacidad e intimidad ante los avances tecnológicos, las amenazas y los riesgos en el uso de las TICs, la reputación online, los delitos informáticos, la Deep Web, las plataformas móviles y el resguardo de la información personal, el desarrollo de software y videojuegos online, comercio electrónico y las políticas de privacidad. Problemática a abordar: Promover la cul-

tura de la protección de los datos personales y brindar las herramientas educativas para el resguardo de la privacidad y la intimidad, educar sobre la importancia de proteger nuestros datos personales y la privacidad, eliminando las barreras de la distancia para llegar con la información hacia la comunidad y los titulares de datos personales. Objetivo del programa / proyecto: Desarrollar e implementar nuevos cursos presenciales y virtuales en plataforma propia Campus Virtual PDP sobre temáticas relacionadas a los derechos de los titulares de los datos personales, procedimientos para garantizarlos, funciones de la autoridad de control Registro No Llame, Situaciones prácticas, demostraciones en vivo, estudio de casos de amenazas en la web y riesgos en el uso de las TICs, Previsiones para el diseño y desarrollo de software y apps Disp. 18/2015 Guía de Buenas Prácticas lineamientos para garantizar la protección de los datos personales y el resguardo de la privacidad de los titulares.

Centro de Asistencia a las Víctimas de Robo de Identidad y del Registro Nacional de Documentos de Identidad Cuestionados

– P.5. Difusión y desarrollo del Centro de Asistencia a las Víctimas de Robo de Identidad y del Registro Nacional de Documentos de Identidad Cuestionados. Descripción general: El "Centro de Asistencia a las Víctimas de Robo de Identidad" tiene como objetivo facilitar orientación y asistencia a quienes como consecuencia del robo de información que contiene datos personales, puedan ver perjudicados sus derechos en caso de su utilización ilegal. El "Registro Nacional de Documentos de Identidad Cuestionados" es parte componente del "Centro de Asistencia a las Víctimas de Robo de Identidad" y tiene como objetivo principal organizar y mantener actualizado un registro informatizado donde consten el número, tipo y ejemplar de documentos de identidad que fueran denunciados a este registro por las autoridades públicas competentes y/o los propios titulares de los mismos con motivo de pérdida, hurto, robo o cualquier otra alteración. Con fecha 28 de agosto de 2015 se suscribió el Convenio Marco de Asistencia y Cooperación Recíproca entre el Ministerio de Justicia y Derechos Humanos y el Ministerio Público Fiscal de la Nación con el objeto de promover la actuación de la justicia en forma coordinada y generar un procedimiento ágil a fin de dar respuesta a las denuncias que recibe la Dirección Nacional de Protección de Datos Personales sobre suplantación o robo de identidad, cuyo accionar pueda derivar en la comisión de diversos delitos. Problemática a abordar: Orientar y Asistir a víctimas del accionar conocido como Robo de Identidad. Objetivo del programa: Aumentar la difusión del Centro de Asistencia a las Víctimas de Robo de Identidad y Desarrollo y del Registro Nacional de Documentos de Identidad Cuestionados. Lograr la colaboración de comisarías y fiscalías de todo el país.

Implementación del Registro Nacional "No Llame"

– P.6. Continuación en la Implementación del Registro Nacional No Llame. Lograr mayor eficiencia en el funcionamiento del Registro Nacional No Llame y aumentar la cantidad de inscriptos. Problemática a abordar: Lograr el efectivo cumplimiento

de las empresas obligadas y un mayor conocimiento de la existencia del Registro. Objetivo del programa: Sistema gratuito, de alcance nacional, mediante el cual los titulares y usuarios de servicios de telefonía –cualquiera sea su modalidad– pueden inscribir sus líneas telefónicas en el "Registro Nacional No Llame" a fin de evitar ser contactados por las empresas que realizan publicidad, oferta, venta, y regalo de bienes o servicios.

3. ACCIÓN NORMATIVA

Disposiciones sobre Registros

En 2016 la DNPDP publicó la Disposición 17/2016 donde establece que, a los fines de mantener actualizada la nómina de obligados por el Registro Nacional "No Llame", también resulta indispensable establecer un límite temporal a la validez de la misma dándole un tope anual a esta obligación.

Por otra parte, en 2016 se publicó la Disposición 56/2016 readecuando los formularios de inscripción del Registro Nacional de Bases de Datos, unificándolos a fin de facilitar los trámites a los responsables de tratamientos de datos personales obligados como así también rediseñados para incluirlos a la plataforma mediante el TAD (trámites a distancia).

4. PROCEDIMIENTOS DE GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS

Consulta o denuncia ante el área de Denuncias

Los titulares de datos personales que consideren vulnerado alguno de los derechos consagrados en la Ley 25.326, como: derecho de acceso, rectificación, actualización, supresión, o confidencialidad, pueden presentar su consulta o denuncia ante el área de Denuncias de la Dirección Nacional de Protección de Datos Personales. Se encuentra habilitada una dirección de correo electrónico denuncias_pdp@jus.gob.ar y una línea telefónica específica (+54 11) 5300-4089, a fin de canalizar las consultas y denuncias de los ciudadanos. Durante 2016 se publicaron un centenar de disposiciones, algunas de ellas sancionatorias y otras sobre aspectos sustantivos que hacen a la protección de datos.

Dictámenes de la Autoridad

En ejercicio de sus funciones, la DNPDP dictamina respecto de los alcances de la Ley 25.326. Las consultas provienen tanto de organismos públicos como de particulares, ya sean personas físicas o jurídicas, de todas las jurisdicciones. La mayoría de los dictámenes se encuentran accesibles en el sitio web de la DNPDP[1]. En el trascurso de este año, se duplicaron los dictámenes elaborados por esta Dirección Nacional. En ellos se ha expedido respecto del alcance e interpretación de la Ley 25.326 y sus normas reglamentarias y complementarias, en temas relativos a cesión de datos personales, aplicabilidad de la norma legal citada, creación de bases de datos, contratos de transferencia internacional y consultas sobre el ejercicio del derecho de

[1] http://www.jus.gob.ar/datos-personales/normativa/dictamenes-pdp.aspx

acceso a la información pública contenido en el Decreto 1.172/03, así como sobre consultas formuladas por organismos públicos en cuanto adoptan medidas que implican tratamiento de datos personales. Algunos temas abordados en dictámenes por la DNPDP en 2016 fueron:

– Contrato de Transferencia Internacional
– Acceso a la Información Pública (Decreto 1.172/03), solicitud de información a la Secretaría General de la Presidencia de la Nación.
– Video vigilancia. Ejercicio del Derecho de Acceso.

Consentimiento libre, expreso e informado del titular de la información

Cabe destacar que en el artículo 5, referido al consentimiento, la Ley 25.326, establece que el tratamiento de datos personales, para ser lícito, debe contar con el consentimiento libre, expreso e informado del titular de la información, posibilidad que otorga el derecho a la autodeterminación informativa, esto es, a elegir el nivel de protección que cada persona quiere dar a la información a ella referida. El consentimiento informado es un instituto que reviste especial trascendencia en el ámbito de las investigaciones clínicas, farmacológicas, y farmacogenéticas, y su exigencia es demostrativa del respeto por la autonomía y el derecho de las personas a disponer de su propio cuerpo. Cuando es requerido, la DNPDP revisa que los consentimientos informados a suscribir por los pacientes que se sometan a esas investigaciones respeten los principios de la Ley 25.326, y que el posterior tratamiento de los datos obtenidos por parte de los laboratorios y profesionales intervinientes se realice conforme a la normativa vigente.

Funciones del Centro de Asistencia a las Víctimas de Robo de Identidad

Por otra parte, la DNPDP cuenta con el Centro de Asistencia a las Víctimas de Robo de Identidad, cuya finalidad es orientar y asistir a las personas que hayan sido afectadas por este accionar fraudulento en cualquiera de sus variantes. En este Centro de Asistencia se encuentra el Registro Nacional de Documentos de Identidad Cuestionados, cuya función es organizar y mantener actualizado un registro informatizado donde consten el número, tipo y ejemplar de documentos de identidad que fueran denunciados por las autoridades públicas competentes y/o sus propios titulares con motivo de pérdida, hurto, robo o cualquier otra alteración. A partir de enero de 2013, el Banco Central de la República Argentina consideró fundamental la consulta al Registro Nacional de Documentos de Identidad Cuestionados para otorgar seguridad a las operaciones que realizan las entidades financieras y bancarias, casas, agencias, oficinas y corredores de cambio, y empresas no financieras emisoras de tarjetas de crédito. Por ello, mediante la comunicación "A" 5387 dispuso la obligatoriedad de la consulta del mencionado registro por parte de dichas entidades. Para 2017 la DNPDP planifica llevar el Centro de Asistencia al programa "El estado en tu barrio", iniciativa del Gobierno nacional que permite acceder a los vecinos de manera inmediata y en un solo lugar a servicios de asistencia, asesoramiento y colaboración en los trámites.

Procedimientos destacados en 2016

En 2016 cabe destacar los siguientes procedimientos iniciados:

– Ley 25.326, Protección de Datos Personales. Ingresaron 138 nuevas denuncias por supuesta infracción a la Ley 25.326 y su Decreto Reglamentario 1.558/01, de las cuales aproximada-

mente un sesenta y sies por ciento (66%) corresponde a reclamos por derecho de supresión; un veintidos por ciento (22%) a derecho de rectificación; uno por ciento (1%) a derecho de actualización; siete por ciento (7%), por derecho de acceso; y un cuatro por ciento (4%), de expedientes iniciados por control de observancia de la Ley 25.326.

- Ley 26.951, Registro Nacional "No Llame". Ingresaron treinta y dos mil seis (32.006) denuncias por presuntas infracciones a la Ley 26.951 y su Decreto Reglamentario 2.501/14, de las cuales veintiún mil ciento veinticinco (21.125) forman parte de expedientes en trámite, tres mil novecientos cincuenta y nueve (3.959) se encuentran a la espera de la apertura de sumarios conforme el criterio establecido por la Disposición DNPDP 17/16. El resto de las denuncias han sido desestimadas por improcedentes.
- Asimismo, se respondieron unas 900 consultas en el año, efectuadas principalmente por mail, y en algunos casos personalmente.
- Registro Nacional de Documentos de Identidad Cuestionados. Desde el inicio de su funcionamiento (4 de octubre de 2010), se encuentran incorporados cerca de ochenta y cinco mil seiscientos ochenta y un (85.661) registros relativos a documentos de identidad nacionales (DNI, DNI-Tarjeta, CI-PFA, Pasaporte, LC, LE) denunciados como robados, hurtados o extraviados.

Durante 2016, el volumen de carga fue de doce mil seiscientos treinta y ocho (12.638) registros, y el nivel de consultas telefónicas y en forma personal asciende a ciento cincuenta (150) mensuales.

En función de algunas solicitudes por parte de las entidades descriptas en el punto anterior, respecto de poder contar con un mecanismo ágil de la consulta de la información, se estableció un procedimiento de envío de la información por medios electrónicos, previa registración de aquellas entidades que así lo solicitaran, a través de formularios que fueron comunicados por el BCRA a través de la Comunicación "B" 10550. Al día de la fecha, se han inscripto ochenta entidades de todas partes del país.

5. PROCEDIMIENTOS DE INSPECCIÓN Y SANCIÓN

Potestad sancionadora de la Autoridad

La Dirección Nacional de Protección de Datos Personales tiene la facultad de aplicar sanciones administrativas por violación a las normas a las Leyes 25.326 y 26.951 y las reglamentaciones que se dicten en su consecuencia. Conforme lo establece la Disposición 7/05 y sus modificatorias Disposición 9/15, cada infracción constatada, debe ser sancionada en forma independiente.

Asimismo, la DNPDP cuenta con un área de inspecciones que tiene a su cargo el análisis y control de cumplimiento de los principios establecidos por la Ley 25.326, su decreto reglamentario y disposiciones emanadas del órgano de control. Para llevar a cabo su tarea notifica la apertura del procedimiento de inspección, analiza la documentación remitida por las empresas y, posteriormente realiza la visita a las

empresas. Las visitas pueden ser una o varias, conforme los requerimientos que se realicen a cada inspeccionado. Durante la visita se establece un acta que es suscripta por los inspectores actuantes y quien represente a la empresa.

Nuevo procedimiento de control de los de responsables del tratamiento de datos

El 7 de noviembre se publicó en el Boletín Oficial el nuevo procedimiento de inspección y control para la fiscalización de las actividades de responsables del tratamiento de datos y su administración, en el marco del proceso de revisión de los procedimientos existentes con la finalidad de hacerlos más eficientes y fortalecer el rol de órgano de control. En este sentido, como consecuencia de la sanción de la Ley 2.6951 que crea el Registro Nacional No Llame, se impone la fiscalización del cumplimiento de dicha norma. Se iniciaron 6 Procedimientos de inspección a empresas con sede en el interior del país, en las localidades de Mar del Plata, San Miguel de Tucumán y Bahía Blanca. Como resultado de ello, tres se remitieron casos al área de Sanciones por no contestar la notificación de inicio del procedimiento con sus requerimientos, encontrándose debidamente notificados, el resto aún se encuentran en trámite.

Las inspecciones abarcarán los siguientes aspectos, sin perjuicio de otros que puedan contemplarse al momento de llevarse a cabo:

- Licitud de las bases de datos (arts. 3, 21 y 24, Ley 25.326).
- Calidad de los datos tratados (arts. 4, Ley 25.326).
- Consentimiento del titular del dato e información (arts. 5 y 6, Ley 25.326).
- Cumplimento de los principios de categorías de datos, seguridad y confidencialidad (arts. 7, 9 y 10, Ley 25.326).
- Requisitos de la cesión de datos y transferencia internacional de datos (arts. 11 y 12, Ley 25.326).
- Ejercicio de los derechos de los titulares del dato (arts. 14, 15, 16 y 19, Ley 25.326).
- Prestación de servicios de información crediticia (art. 25, Ley 25.326).
- Tratamiento de datos con fines de publicidad (art. 27, Ley 25.326 y Ley 26.951).

De las sanciones aplicadas durante 2016, cabe destacar:

Sanción por obstrucción

- La DI-2016-48-E-APN-DNPDP#MJ a través de la cual se impuso a la firma "Compañía Argentina de Marketing Directo SA." a sanción pecuniaria de 105.200 pesos, por obstruir el ejercicio de la función de inspección y fiscalización a cargo de la Dirección Nacional de Protección de Datos Personales, de conformidad con lo previsto en el punto 2, inciso l) del Anexo I a la Disposición DNPDP 7/05 y sus modificatorias referido específicamente a la falta de presentación del formulario de inspección y la remisión de la documentación allí requerida y, la falta de inscripción de sus bases de datos de carácter personal en el registro correspondiente, cuando haya sido requerido para ello por la Dirección Nacional de Protección de Datos Personales, con encuadre en el punto 3, inciso a) del Anexo I a la disposición citada.

Sanción por no atender la solicitud de acceso, rectificación o supresión

– La DI-2016-53-E-APN-DNPDP#MJ aplica al Banco Columbia S.A. la sanción pecuniaria de 60.000 pesos por una denuncia de un ciudadano en atención a que recibía reclamos de la entidad bancaria por una deuda cuyo titular no era el denunciante, sino una persona de sexo femenino con el mismo número de Documento Nacional de Identidad. La conducta del denunciado se encuadró en "no proporcionar la información que solicite la Dirección Nacional de Protección de Datos Personales, en el ejercicio de las competencias que tiene atribuidas", y por "no atender en tiempo y forma la solicitud de acceso, rectificación, o supresión de los datos personales objeto de tratamiento cuando legalmente proceda", infracciones leve y grave respectivamente. La Ley 25.326 establece en su Capítulo III que el titular del dato tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados; el responsable debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley (conforme artículo 14 -derecho de acceso). La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado. Por su parte el artículo 16 de la Ley 25.326 referido al derecho de rectificación, actualización o supresión, dispone que toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad. El incumplimiento de esta obligación dentro del término acordado, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data. De las actuaciones se desprende que el denunciante procedió a intimar al Banco Columbia SA y al no recibir respuesta alguna y haciendo uso del derecho que le confiere la norma, formuló el pertinente reclamo. La afirmación efectuada por la firma denunciada en relación a que procedió a rectificar el dato, sólo puede ser tomada como una afirmación sin sustento probatorio por cuanto no se acompaña copia de la notificación que debió haber enviado a la denunciante en relación al pedido de rectificación satisfecho.

Sanción por no inscribir la base de datos en el Registro

– La DI-2016-68-E-APN-DNPDP#MJ aplica a la empresa la firma "UPG Comercial SRL" la sanción pecuniaria de pesos 100.000 pesos por no proporcionar en tiempo y forma la información que solicite la Dirección Nacional de Protección de Datos Personales, en el ejercicio de las competencias que tiene atribuidas" y por "no inscribir la base de datos de carácter personal en el Registro correspondiente, cuando haya sido requerido para ello por la DNPDP", infracciones leve y grave respectivamente.

Sanción por contactar telefónicamente para publicidad, oferta, venta o regalo

– La DI-2016-3-E-APN-DNPDP#MJ aplica a la empresa "TELECOM PERSONAL SA" la sanción de 60.000 pesos por contactar con el objeto de publicidad, oferta, venta o regalo de bienes o servicios utilizando los servicios de telefonía en cualquiera de sus modalidades a quienes se encontraren debidamente inscriptos ante el Registro Nacional "No Llame". La omisión del denunciado de no haber justificado la calidad de clientes, se asimila a la ausencia de la infractora de aportar el registro de llamadas salientes, en cuanto aporte de pruebas se refiere. En relación a la infracción constatada ésta encuentra su causa en el artículo 7 de la Ley 26.951 que dispone que quienes publiciten, oferten, vendan o regalen bienes o servicios utilizando como medio de contacto los servicios de telefonía en cualquiera de sus modalidades, no podrán dirigirse a ninguno de los inscriptos en el Registro Nacional "No Llame" y deberán consultar las inscripciones y bajas producidas en el citado registro, con una periodicidad de treinta días corridos a partir de su implementación, en la forma que disponga la autoridad de aplicación. Las denuncias recibidas indican que "TELECOM PERSONAL S.A." efectuó contactos ofreciendo promociones, beneficios y publicidades de productos y servicios, entre otras, lo que inexorablemente conduce a la configuración de la infracción del artículo 7 de la citada norma legal. Respecto a los números telefónicos reconocidos por la empresa que fueran contactados, cabe señalar que la denunciada informa que el motivo del contacto fue el ofrecimiento de planes de telefonía y promociones. Cabe considerar que lo expresado por la firma no prueba que los contactos hayan sido efectuados dentro del vínculo contractual que los une a los clientes, toda vez que mediante esos sistemas se ofrecen productos y servicios que no siempre constituyen el objeto estricto del vínculo. Es más, en algunos casos se promocionan productos y servicios de otras empresas, violando así el artículo 7 de la Ley 26.951.

Sanción por no proporcionar la información a la Autoridad

– La DI-2016-86-E-APN-DNPDP#MJ aplica a la firma "Telefónica de Argentina SA" la sanción pecuniaria de 70.000 pesos por "no proporcionar la información que solicite la Dirección Nacional de Protección de Datos Personales, en el ejercicio de las competencias que tiene atribuidas", y por "no atender en tiempo y forma la solicitud de acceso, rectificación, o supresión de los datos personales objeto de tratamiento cuando legalmente proceda", infracciones leve y grave respectivamente. La presentación efectuada por la firma en su descargo, en la

cual pretende probar que contestó el pedido del denunciante y suprimió el dato, sólo puede ser tomada como una afirmación sin sustento probatorio, por cuanto no se acompaña copia de la notificación que debió haber enviado a la denunciante en relación al pedido de supresión y por otro lado la supresión de la información, según la constancia emanada por "Organización Veraz SA". Se produjo casi seis meses después. La Ley 25.326 en el artículo 16 referido al derecho de rectificación, actualización o supresión, dispone que toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.

6. COOPERACIÓN CON OTRAS INSTITUCIONES

Participación en la Conferencia Internacional de Autoridades de Protección de Datos

Por otro lado, luego de 10 años de ausencia de la Dirección Nacional, la Argentina, a través de Eduardo Bertoni, participó de la 38ª Conferencia Internacional de Autoridades de Protección de Datos, llevada a cabo en la ciudad de Marrakech, Marruecos, durante el mes de octubre. En esta conferencia, nuestro país fue co-sponsor de 2 resoluciones.

Comité Ejecutivo de la Red Iberoamericana

Otra cuestión a resaltar fue la designación de la DNPDP como miembro del Comité Ejecutivo de la Red Iberoamericana de Protección de Datos (RIPD), hecho acontecido en el mes de noviembre durante la realización del seminario "Europa-Iberoamérica: una visión común de la protección de datos. El nuevo marco europeo y su incidencia en Iberoamérica", dictado por la RIPD en la ciudad de Montevideo, Uruguay.

Participación en otros eventos

De igual forma, durante 2016 la DNPDP participó en los siguientes eventos:

- International Associations of Privacy Professional como Autoridad de Protección de Datos Personales a la Conferencia Anual "Privacy Summit" llevada a cabo en Washington DC, donde se expuso en el panel "Latin America Regulatory Update" junto con distintas autoridades de la región (abril).
- XIV Encuentro Iberoamericano de Protección de Datos y del 4º Congreso Internacional en la materia en la ciudad de Santa Marta, Colombia. Bertoni expuso en los paneles referidos con el desafío de la protección de datos en las políticas de seguridad nacional y la importancia de establecer mecanismos de cooperación entre las autoridades de protección de datos de la región mientras que también brindó una conferencia titulada "Rol y Responsabilidad de los Intermediarios en el tratamiento de datos personales" (junio).

– Primera Semana Nacional de la Protección de Datos Personales, realizada en las ciudades de Montevideo y de Maldonado, en la República Oriental del Uruguay, participó del Panel 5, titulado "Desafíos de la protección de datos según sus autoridades" (agosto).
– 38ª Conferencia Internacional de Autoridades de Protección de Datos, llevada a cabo en la ciudad de Marrakech, Marruecos. El evento reunió a organismos públicos reguladores provenientes de diversos países, organizaciones no gubernamentales, expertos y universitarios, así como representantes del sector privado. La DNPDP fue co-sponsor de dos resoluciones (octubre)
– Seminario "Europa-Iberoamérica: una visión común de la protección de datos. El nuevo marco europeo y su incidencia en Iberoamérica", dictado por la Red Iberoamericana de Protección de Datos (RIPD) en la ciudad de Montevideo, Uruguay.

7. COOPERACIÓN CON LA SOCIEDAD

Sistematización de disposiciones en el portal institucional

Con el objetivo de brindarle a la comunidad mejores servicios, la DNPDP implementó un ordenamiento temático de disposiciones a través de su portal de internet. La plataforma ahora permite a los usuarios efectuar búsquedas de las disposiciones por tema o por número, sin necesidad de concurrir a la sede de la Dirección, pudiendo descargar y consultar todas las disposiciones regulatorias de diversos temas de interés para la adecuada protección de datos personales.

8. OTRAS ACTIVIDADES

Presencia de la DNPDP en la web y en los medios

En cuanto a la presencia de la DNPDP en la web, es importante resaltar que se mantuvo el flujo de accesos a la página oficial del organismo, contabilizando 1.933.577 visitas a lo largo de 2016, cifra que superó levemente a las consultas del año anterior, con lo que los ciudadanos pudieron informarse, asesorarse, realizar denuncias y/o reclamos y aportar sugerencias referentes a la protección de datos personales.

Por otra parte, los medios de comunicación abordaron el trabajo de la DNPDP. Por ejemplo, se dio a conocer las investigaciones iniciadas contra UBER, Facebook, WhatsApp, Club Tigre, entre otros.

Centro de Capacitación, Investigación y Difusión

Cabe señalar que el 15 de septiembre de 2014 se creó el Centro de Capacitación, Investigación y Difusión de la Dirección Nacional de Protección de los Datos Personales mediante Resolución 1645/14. Consiste en un espacio de capacitación y difusión de las distintas temáticas involucradas con las tareas de la DNPDP: seguridad de la información, niños/ adolescentes y sus relaciones con las nuevas tecnologías, el resguardo del derecho de privacidad e intimidad ante el avance de Internet, las amenazas y los riesgos en el uso de las TIC: cómo evitarlos, la reputación online, los delitos informáticos, protección de datos personales para abogados, etc. La cantidad de inscriptos

respecto a 2015 ascendió un 118% en relación al 2016. En ese marco, los Cursos dictados durante 2016 fueron:

– Claves para la Protección de los Datos Personales.
– Mecanismos de Inscripción de bases de datos.
– Protección de Datos Personales en Internet.
– Robo de Identidad.

9. DATOS ESTADÍSTICOS

140% más consultas que el año anterior

En comparación con años anteriores, han aumentado las consultas de los ciudadanos respecto de los alcances de la Ley 25.326 y el ejercicio de sus derechos. Durante 2016 las consultas llegaron aproximadamente a unas 2500 significando un 140% más comparada con el año anterior. Ello revela una mayor concientización sobre la importancia de proteger los datos personales y la privacidad, y un mayor conocimiento sobre la existencia de la Ley y sus alcances. De igual forma, se recibieron 351 denuncias siendo ello una cifra similar a la recibida en 2015. En algunos servicios concretos podemos señalar las siguientes cifras:

Registro Nacional "No Llame": 32.759 denuncias

– Registro Nacional "No Llame": Durante el año 2016 se recibieron un total de 32.759 denuncias que motivaron la instrucción de 71 actuaciones administrativas. Cabe destacar que en el año 2016 se recibieron un 35% menos de denuncias que el año anterior, que podría indicar un mayor cumplimiento de la Ley. Para ello pudieron haber contribuido tanto las exposiciones públicas del Director Nacional advirtiendo que se impondría mayor dureza en la aplicación de las multas, como el aumento de las multas impuestas. Las cifras son las siguientes:
  - 32.759 denuncias recibidas 2016 de un total de más de 83.000 desde el inicio del "No Llame".
  - 193.003 usuarios inscriptos durante 2016 ascendiendo a un total de más de 767.000.
  - 71 sumarios administrativos iniciados durante 2016 correspondientes a 21.283 denuncias, conformando un total de 407 sumarios iniciados.
  - 111 empresas intimadas en 2016.
  - Propusimos un total de 11.004.600 pesos en multas a 38 empresas infractoras.
  - 59 disposiciones firmadas por un total en multas de 1.218.600 pesos.
  - Propusimos apercibimientos a 8 empresas.
  - 73 empresas inscriptas en el RNNLL.
  - 35 empresas en proceso de inscripción.
  - 95.700 pesos recaudados en la habilitación de empresas obligadas.
  - 346.194 visitas al sitio web www.nollame.gob.ar.

Consentimiento informado: 2.463 formularios recibidos

– Consentimiento informado: En se han aprobado 322 formularios sobre un total de 2.463 formularios.

Procedimientos de inspección y sanción: 62 inspecciones con visita ocular

– Procedimientos de inspección y sanción: Durante el año 2016 se efectuaron 62 inspecciones con visita ocular, realizándose en cada caso su respectiva acta con los requerimientos para su cumplimiento. Con las respuestas obtenidas a partir de los requerimientos se elaboraron los Informes Finales, en los que se estableció el grado de cumplimiento de la Ley 25.326 y normas reglamentarias. Aquellos casos que no dieron respuesta adecuada a los requerimientos efectuados en el Acta elaborada durante la visita ocular y que no tienen un porcentaje de cumplimiento del 100% a las obligaciones que la Ley requiere, se derivaron a seguimiento y fueron un total de 32 empresas. Se derivaron a Sanciones 22 expedientes por incumplimientos previos a la inspección ocular. Se iniciaron las reuniones para la discusión de la modificación a la Disposición DNPDP 11/06 sobre "Medidas de Seguridad para el tratamiento y Conservación de los datos personales" y la capacitación a los inspectores.

Multas y apercibimientos: 24 sanciones de multa por un total de 569.601 pesos y 5 sanciones de apercibimiento

– Multas y apercibimientos 2016: Por incumplimientos a la Ley 25.326, se aplicaron 24 sanciones de multa por un total de 569.601 pesos y 5 sanciones de apercibimiento, representando un 412% más que el año 2015. Por incumplimientos a la Ley 26.951, se aplicaron 59 sanciones de multa por un total de 1.138.400 pesos y 36 apercibimientos superando lo aplicado en 2015 en un 3.900%.

Centro de Asistencia a las Víctimas de Robo de Identidad

– Centro de Asistencia a las Víctimas de Robo de Identidad: Se registraron 12.680 documentos cuestionados, manteniéndose la misma cantidad de registros con respecto al año anterior. Desde la creación del Registro a la fecha, el total asciende a 84.734 documentos cuestionados registrados.

III. CHILE

1. INTRODUCCIÓN

Legislación chilena de protección de datos

La legislación en Chile en materia de protección de datos personales se circunscribe, principalmente, a lo regulado por la Ley 19.628, sobre Protección de la Vida Privada, publicada en el Diario Oficial el 28 de agosto de 1999, que regula el tratamiento de datos de carácter personal. El ordenamiento jurídico chileno no contempla la existencia de un órgano garante en la materia, o autoridad especializada encargada del cumplimiento de la legislación que protege los datos personales. La Ley se limita a regular la utilización de los datos personales; los derechos de los titulares de los datos; la utilización de los datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial; el tratamiento de datos por parte de los organismos públicos; y, la responsabilidad por las infracciones a la Ley. Por lo tanto, existe un importante vacío en esta materia, ya que la legislación existente no tiene la institucionalidad necesaria para, en primer lugar, efectuar una adecuada difusión del derecho y, en segundo lugar, resguardar los derechos de los titulares de los datos, al no otorgarle los mecanismos adecuados para ejercer una correcta y efectiva defensa de su derecho.

Funciones del Consejo para la Transparencia

El Consejo para la Transparencia, cuya función principal consiste en promover la transparencia de la función pública, tiene también algunas limitadas atribuciones en materia de protección de datos. En efecto, de acuerdo a lo dispuesto por el artículo 33. m), de la Ley de Transparencia, aprobada por el artículo primero de la Ley 20.285, sobre Acceso a la Información Pública, publicada en el Diario Oficial el 20 de agosto de 2008, el Consejo para la Transparencia tiene la función de "velar por el adecuado cumplimiento de la Ley 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado". Por lo demás, la estrecha interrelación que existe entre los temas vinculados a transparencia y acceso a la información pública, por un lado, con la protección de datos personales, por el otro, ha hecho que este Consejo deba armonizar los deberes de protección de datos con los de transparencia. Esto último se ha dado, especialmente, por el gran número de datos personales, incluso sensibles, tratados por los órganos de la Administración del Estado, por ejemplo, para desarrollar e implementar políticas públicas, tales como entrega de beneficios, planificación, orden público, entre otras, y que, a efectos del control social, han sido requeridos bajo el amparo de la Ley 20.285.

Necesidad de ajustar la legislación nacional a los estándares internacionales

Las normas de la Ley 19.628, vigente desde el año 1999, han sido sometidas a distintos análisis, con el objeto de ser adecuadas a las necesidades contemporáneas. Los intentos de modificación sustancial de dicho cuerpo normativo, no han sido exitosos a la fecha. Los proyectos de reforma integral, que buscaban enfrentar la situación actual y ajustar la legislación conforme a los estándares internacionales, aún no han sido aprobados por el Congreso Nacional. De este modo, la estructura básica sobre la cual se regulan los datos personales en Chile sigue siendo la misma desde 1999. El miércoles 15 de marzo de 2017, el Ejecutivo ingresó en el Congreso Nacional un proyecto de ley relativo a la protección de datos personales.

2. PLANIFICACIÓN

Plan Operativo del Consejo para la Transparencia

El Consejo para la Transparencia, a efectos de ejercer su atribución conferida por el artículo 33 m) de la Ley de Transparencia, planifica actividades de protección de datos, tendientes a la promoción del derecho, actividades que son permanentemente evaluadas y de las que se rinde cuenta ante la sociedad civil. En este sentido, dentro del Plan Operativo del Consejo para la Transparencia, en materia de protección de datos personales, se han contemplado acciones tendientes a implementar, entre otras actividades, una semana de la protección de datos, desayunos realizados con la industria y expertos en la materia, la elaboración y envío de propuestas normativas a los órganos colegisladores (Ejecutivo y Congreso Nacional), recomendaciones enviadas a distintos órganos de la Administración del Estado y órganos públicos en general.

3. ACCIÓN NORMATIVA

Directrices para la ejecución y aplicación de la legislación

En base a la facultad legal otorgada al Consejo para la Transparencia, de velar por el adecuado cumplimiento de la Ley de protección de datos de carácter personal, este organismo ha dictado directrices que orientan la ejecución y aplicación de la Ley, de alcance general, o focalizado a determinados organismos obligados, tendientes a recomendar una correcta aplicación de la legislación de protección de datos. Al no existir un órgano garante propiamente tal, no hay organismo con potestad normativas, distinta del Ejecutivo, con competencia para dictar reglas de aplicación general en materia de protección de datos. Sin embargo, y en base a la facultad otorgada por la Ley al Consejo, se han elaborado, entre otros, los siguientes cuerpos normativos en materia de protección de datos personales:

Recomendaciones sobre protección de datos por la Administración del Estado

– Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado. En agosto de 2011, este Consejo dictó un texto de recomendaciones sobre protección de datos personales por parte de los órganos de la Administración del Estado, las que tienen por objeto "establecer orientaciones respecto de los

criterios jurídicos aplicables por los órganos de la Administración del Estado en el tratamiento de datos de carácter personal que obren en su poder, a fin de dar cumplimiento a las obligaciones y limitaciones dispuestas por la Ley 19.628, garantizar a las personas el derecho a la protección de los datos de carácter personal y asegurar el debido manejo de los registros o bancos de datos personales que sean necesarios para el ejercicio de sus competencias".

Propuestas de mejora normativa enviadas al Ejecutivo

– Recomendaciones de propuestas de mejoras normativas, enviadas al Ejecutivo (en su calidad de colegislador), para un eventual proyecto que regule la protección de datos personales. Mediante oficio de marzo de 2016, este Consejo remitió al Ministro de Hacienda un documento que contiene una "Propuesta general de perfeccionamientos normativos en materia de protección de datos personales y comentarios al anteproyecto de ley que modifica la Ley N° 19.628, sobre Protección de la Vida Privada". A través de dicho documento, se dieron a conocer al citado Ministerio diez propuestas elaboradas por este Consejo, para perfeccionar la protección de datos personales en Chile. Dichas propuesta fueron las siguientes:
  - Consagrar la autodeterminación informativa como derecho fundamental y objeto de protección de la Ley 19.628.
  - Incorporación de los principios rectores en materia de protección de datos.
  - Revisar el catálogo de definiciones y, en especial, la categoría de "datos sensibles".
  - Reforzamiento de la regulación del consentimiento expreso e informado y de los derechos asociados a los titulares de los datos.
  - Territorialidad de la ley y regulación del flujo transfronterizo de datos.
  - Establecer un registro nacional de bases de datos.
  - Tratamiento de datos personales por organismos públicos.
  - Incorporación de un régimen de infracciones y sanciones.
  - Implementación gradual de la normativa.
  - Consagración de un órgano garante.

Oficios para garantizar un adecuado tratamiento de datos por parte de los órganos públicos

– Oficios dirigidos a distintos órganos de la Administración del Estado, entregando recomendaciones a fin de efectuar un adecuado tratamiento de los datos personales en las materias respectivas de que se trate. Este Consejo ha elaborado diversos oficios, dirigidos a distintos órganos de la Administración del Estado, que contienen recomendaciones, requiriendo entrega de información y antecedentes y, en general, abordando diversas materias tendientes a garantizar un adecuado tratamiento de datos por parte de los órganos públicos. Asimismo, se ha ofrecido la colaboración técnica para la ejecución y correcta aplicación de la normativa que regula la protección de datos personales. Entre los principales oficios enviados, se destacan los siguientes:
  - En septiembre de 2015, y luego de conocerse la noticia de que los municipios de Las Condes y Lo Barnechea habían

implementado globos aerostáticos, dotados de cámaras de alta tecnología, que vigilaban sectores de dichas comunas, como una medida de prevención del delito, este Consejo requirió a dichas municipalidades que informes la forma en que se ha dado cumplimiento a las disposiciones de la Ley 19.628 de protección de datos de carácter personal.

- En febrero de 2016 se ofició a la Subsecretaría de Telecomunicaciones, para que informe sobre el cumplimiento de la Ley 19.628, a propósito de un software diseñado para dispositivos móviles, que ayudaban a los usuarios a efectuar los cambios de numeración telefónica.
- A propósito de una falla en la red del Ministerio de Salud, que dejó expuesta información confidencial, que contenía datos sensibles de pacientes del sistema de salud, en marzo de 2016, este Consejo ofició a dicho ministerio, a fin de que informara sobre el cumplimiento de la Ley 19.628, en materia de datos sensibles de pacientes.
- En junio de 2016, y durante el proceso constituyente impulsado por el gobierno, este Consejo ofició a los organismos encargados de llevar adelante el proceso, formulando recomendaciones en materia de protección de datos personales para la Fase Participativa del proceso denominado "Una Constitución para Chile".
- En noviembre del año pasado, este Consejo tomó conocimiento que el Estado, a través de la Subsecretaría del Interior, en conjunto con la Intendencia Metropolitana de Santiago, adquiriría un software de reconocimiento facial, que sería utilizado en los estadios y en distintas manifestaciones, y que funcionaría con la base fotográfica del Servicio de Registro Civil. En virtud de lo anterior, se ofició a los órganos de la Administración del Estado involucrados para que informaran sobre el cumplimiento de la Ley 19.628, en materia de datos personales y sensibles, a propósito del software de reconocimiento facial.

4. PROCEDIMIENTOS DE GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS Y DE INSPECCIÓN Y SANCIÓN

No existe autoridad de control que garantice la protección de datos

Como se describió más arriba, en Chile no existe autoridad de control que garantice la protección de los datos personales, ni tampoco existe un procedimiento especial que asegure una rápida y eficaz protección ante la vulneración de los derechos reconocidos a los titulares de los datos. Por lo tanto, al no existir un procedimiento especial para exigir el cumplimiento de estos derechos, se debe iniciar una acción judicial ante los tribunales civiles, distinguiéndose en la Ley dos tipos de procedimientos, según se trate de exigir el cumplimiento de los derechos ante el responsable de la base de datos, o se persiga obtener una indemnización por el daño ocasionado como conse-

cuencia del tratamiento indebido de los datos. Lo anterior trae como consecuencia, entre otras cosas, que en la práctica los derechos reconocidos a los titulares de los datos personales queden desprotegidos. Por un lado, quien debe resolver estas cuestiones se trata de un juez no especializado en la materia y, por otro, el asunto queda sometido a la tramitación de procedimientos que no resolverán el asunto en plazos breves.

Asimismo, la inexistencia de autoridad de control, impide que algún organismo ejerza facultades fiscalizadoras y de inspección que, por una parte, promuevan el derecho y, por la otra, aseguren el debido cumplimiento y respeto de los mismos.

Inexistencia de sanciones en la actual legislación

En materia de sanciones tampoco se contemplan en la actual legislación, limitándose ésta a señalar que el responsable de un banco de datos, que cause perjuicio por el tratamiento indebido de los datos, deberá indemnizar el daño patrimonial y moral que causare. Sin embargo, no se contempla ninguna sanción específica a quien, haciendo mal uso de los datos de que es responsable, causare algún tipo de perjuicio, no respete los derechos, o no se someta a las obligaciones establecidas por la Ley.

5. COOPERACIÓN CON OTRAS INSTITUCIONES PÚBLICAS

En cumplimiento del mandato dispuesto por el artículo 33, letra m), de la Ley de Transparencia, el Consejo, a través de diversas acciones, ha estado en constante preocupación por el adecuado cumplimiento de las disposiciones de la Ley de protección de datos personales, por parte de los órganos de la Administración del Estado. En este sentido, en reiteradas oportunidades el Consejo ha ofrecido cooperación a los organismos públicos, en materia de alcanzar una adecuada protección en el tratamiento de los datos que éstos deben efectuar. Así, por ejemplo, destacan, entre otras, las siguientes:

Asistencia para la elaboración del protocolo del software de reconocimiento facial

– A propósito del software de reconocimiento facial, que se implementaría por el Ministerio del Interior, en conjunto con la Intendencia Metropolitana de Santiago y Carabineros de Chile, este Consejo ofició al Departamento Estadio Seguro de la Subsecretaría del Interior. Por medio de ese oficio se ofreció a dicho órgano de la Administración del Estado asistencia técnica en la confección del protocolo de tratamiento de datos personales que se está elaborando.

Participación en el proceso "Una Constitución para Chile"

– Asimismo, en las recomendaciones formuladas en materia de protección de datos personales para la Fase Participativa del proceso "Una Constitución para Chile", este Consejo ofreció a los organismos involucrados, con el fin de contribuir en el perfeccionamiento de dicho proceso, la disposición para colaborar y participar en las instancias que se estimen pertinentes, a fin de avanzar en estas materias.

6. COOPERACIÓN CON LA SOCIEDAD

Mesas de trabajo con la sociedad civil

Entre enero y abril de 2016, el Consejo para la Transparencia inició la discusión con distintos actores involucrados con el tratamiento de los datos personales en Chile. Se constituyeron mesas de trabajo en materia de Protección de Datos Personales, invitándose a expertos, tanto de la sociedad civil, como académicos vinculados con el tema. En ese marco, se desarrolló una primera mesa de trabajo, el 25 de enero de 2016, en la cual se presentó la propuesta del Consejo para la Transparencia y se acordó recibir comentarios en una futura reunión. La segunda mesa de trabajo, se efectúo el 4 de marzo de 2016, en la cual los expertos plantearon la necesidad de incorporar nuevas temáticas como propuestas normativas. Finalmente, una tercera reunión se llevó a cabo el 8 de abril de 2016, en donde, entre otras cosas, los expertos plantearon la necesidad de que los estándares recogidos en un futuro Proyecto de Ley aseguren que Chile se convierta en un Puerto Seguro a efectos de protección y transferencia internacional de datos, como también se señaló la necesidad de generar urgencia política para tramitar una reforma a la Ley actual. De igual manera, se desarrolló una mesa de trabajo con representantes de la industria, a efectos de que éstos expongan sus planteamientos respecto a la manera en que la regulación de protección de datos afecta o influye en su sector.

7. OTRAS ACTIVIDADES

Sensibilización en redes sociales

El Consejo para la Transparencia ha desarrollado una constante y permanente actividad durante todo el año, a través principalmente de redes sociales, a fin de promover entre la ciudadanía un mayor conocimiento de sus derechos en la materia. También se han implementado acciones con el fin de ejemplificar con situaciones concretas y cotidianas, aquellos casos en los que los ciudadanos permanentemente entregan sus datos a terceros, sin tomar conocimiento de los diversos tratamientos de que estos son objeto.

El Consejo para la Transparencia impulsó la campaña denominada "Cuida tus datos", la que por medio de distintas acciones de incidencia por Twitter, Facebook, y redes sociales, busca, por una parte, dar a conocer los derechos que en materia de protección de datos tienen todos los ciudadanos. Por otra parte, se entregan distintas recomendaciones, a efectos de que la ciudadanía, de forma consiente e informada, sepa qué hacer, por ejemplo, cuando al comprar en el retail se le pida su número nacional de identificación.

Todas estas acciones desarrolladas por el Consejo para la Transparencia han tenido por objeto difundir los derechos entre la ciudadanía, explicando detalladamente en qué consisten y qué son los datos personales. Igualmente, a través de campañas más focalizadas, se ha apuntado hacia sectores más específicos como los trabajadores y la protección de datos, los niños, niñas y adolescentes y la protección de datos, y el consumo (en épocas, por ejemplo, de navidad) y su vinculación con la protección de los datos personales.

IV. COLOMBIA

1. INTRODUCCIÓN

La Superintendencia de Industria y Comercio, a través de la Delegatura para la Protección de Datos Personales, es en Colombia la Autoridad encargada de la protección del derecho fundamental de todos los ciudadanos a conocer, actualizar y rectificar la información personal que de ellos se haya recogido en una base de datos, consagrado en el artículo 15 de la Constitución Política de Colombia, es decir, de la facultad de todas las personas de controlar las actividades que realizan con su información personal.

Legislación colombiana de protección de datos

En Colombia, el derecho fundamental mencionado consagrado en el artículo 15 de la Constitución Política ha sido desarrollado en dos leyes estatutarias: la Ley 1.266 de 2008 que regula en particular el tratamiento de información financiera, comercial, crediticia o de servicios destinada al cálculo del riesgo crediticio y dispuso que la Superintendencia de Industria y Comercio (SIC) ejercería la vigilancia de los operadores, fuentes y usuarios de información financiera y crediticia, y la Ley 1.581 de 2012 considerada como el Régimen General de Protección de Datos Personales, aplicable al tratamiento de otros datos personales, diferentes a los financieros, comerciales, crediticios y de servicios, mantenidos en cualquier base de datos, bien sea de entidades de naturaleza pública o privada; esta Ley designó a la SIC como Autoridad de Protección de Datos para garantizar que en el tratamiento de esos datos se respeten los principios, derechos y procedimientos dispuestos en la Ley y, por supuesto, para imponer las sanciones por el incumplimiento a esa disposición.

La Ley 1.266/2008, enfocada únicamente en la protección de la información financiera, comercial, crediticia y de servicios, destinada al cálculo del riesgo crediticio, consagra dentro de su articulado los principios que rigen el tratamiento de información personal, los derechos para los titulares, los deberes para los sujetos que intervienen en la actividad de tratamiento y las funciones de la Autoridad. En tal virtud, la SIC ha llevado a cabo investigaciones administrativas que han finalizado con sanciones de tipo pecuniario a aquellas fuentes, operadores y usuarios de información financiera, en su mayoría empresas del sector privado, que incumplen sus obligaciones y afectan el derecho de hábeas data de los titulares.

La SIC fue dotada de competencia para ejercer funciones de inspección y vigilancia y, entre ellas, impartir sanciones pecuniarias o

Funciones de la Superintendencia de Industria y Comercio y de la Delegatura para la Protección de Datos Personales

no pecuniarias desde la expedición de la Ley 1.266/2008, que fue la primera ley que desarrolló el derecho fundamental de hábeas data contenido en la Carta Política Colombiana dentro del listado de derechos fundamentales dentro de los que se encuentran la vida, la libertad, la igualdad, la intimidad, el libre desarrollo de la personalidad y la libertad de expresión, entre otros.

Dentro de las funciones asignadas a la SIC por la Ley 1.266/2008, se encuentran las siguientes:

- Impartir instrucciones y órdenes sobre la manera como deben cumplirse las disposiciones de la presente ley relacionadas con la administración de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países fijar los criterios que faciliten su cumplimiento y señalar procedimientos para su cabal aplicación.
- Velar por el cumplimiento de las disposiciones de la presente ley, de las normas que la reglamenten y de las instrucciones impartidas por la respectiva Superintendencia.
- Velar porque los operadores y fuentes cuenten con un sistema de seguridad y con las demás condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme lo previsto en la presente ley.
- Ordenar a cargo del operador, la fuente o usuario la realización de auditorías externas de sistemas para verificar el cumplimiento de las disposiciones de la presente ley.
- Ordenar de oficio o a petición de parte la corrección, actualización o retiro de datos personales cuando ello sea procedente, conforme con lo establecido en la presente ley. Cuando sea a petición de parte, se deberá acreditar ante la Superintendencia que se surtió el trámite de un reclamo por los mismos hechos ante el operador o la fuente, y que el mismo no fue atendido o fue atendido desfavorablemente.
- Iniciar de oficio o a petición de parte investigaciones administrativas contra los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, con el fin de establecer si existe responsabilidad administrativa derivada del incumplimiento de las disposiciones de la presente ley o de las órdenes o instrucciones impartidas por el organismo de vigilancia respectivo, y si es del caso imponer sanciones u ordenar las medidas que resulten pertinentes.

Por su parte, la Ley 1.581 de 2012, conocida como el Régimen General de Protección de Datos Personales, contempla la protección de la información personal de todo tipo, diferente a la financiera, comercial y crediticia, igualmente incluye un catálogo de derechos para los titulares, unos principios fundamentales, unos deberes y unas facultades para la Autoridad en cuyo ejercicio también ha impartido sanciones de tipo pecuniario a empresas del sector privado que efectúan el tratamiento de información de las personas incumpliendo lo previsto en dicha disposición legal.

Las funciones establecidas para la Delegatura en la Ley 1.581 /2012, son las siguientes:

a) Velar por el cumplimiento de la legislación en materia de protección de datos personales;
b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;
c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva;
d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementará campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos;
e) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley;
f) Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.
g) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos;
h) Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento;
i) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional;
j) Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personajes;
k) Las demás que le sean asignadas por ley.

2. PLANIFICACIÓN

Plan de Acción 2016: líneas de acción y productos estratégicos

Dentro del ejercicio anual de Planeación Estratégica efectuado por la Superintendencia de Industria y Comercio, se realizó la programación de los productos propuestos para el 2016 por la Delegatura para la Protección de Datos Personales y de las actividades a desarrollar para la ejecución de esos productos. Así mismo, en el Plan de Acción

de 2016 se identificó la meta, la unidad de medida y los indicadores de cada producto, con el fin de controlar la gestión, la eficiencia y la eficacia de los productos y actividades propuestos. En desarrollo de los compromisos asumidos es necesario:

- Dar estricto cumplimiento a las actividades previstas en la programación institucional a términos legales o internos previamente establecidos y al incremento de los niveles de oportunidad, eficiencia y calidad.
- La concertación de los objetivos de cada uno de los funcionarios vinculados a la dependencia, debe estar fundamentada en el plan de acción institucional, el cual hace parte constitutiva de los acuerdos de gestión suscritos entre el Superintendente de Industria y Comercio y los funcionarios del nivel directivo de la institución.
- Las modificaciones a la programación de actividades que puedan ser requeridas por circunstancias excepcionales, deben ser solicitadas con anterioridad a la fecha límite de terminación prevista y son aprobadas por el Jefe de la Oficina Asesora de Planeación o por el Superintendente de Industria y Comercio en caso de requerirlo. La solicitud deberá siempre incluir la justificación del jefe de la dependencia respectiva así como la autorización del superior inmediato.
- El sistema de planeación institucional es administrado por la Oficina Asesora de Planeación.

Para el 2016, la Delegatura para la Protección de Datos Personales propuso los siguientes productos estratégicos:

- Implementar el Sistema de Supervisión Inteligente basado en riesgos, como herramienta de supervisión para identificar de manera eficiente las bases de datos que ofrecen mayores niveles de riesgo y así adelantar investigaciones que deriven en decisiones de sanción por incumplimiento a las leyes de protección de datos personales o en órdenes de adecuación a las especificaciones de esas disposiciones normativas.
- Proferir sanciones de alto impacto y relevancia para el país por incumplimientos y afectaciones graves al derecho a la protección de datos personales de las personas.
- Publicar la guía para la protección de datos personales en sistemas de videovigilancia.
- Realizar el Cuarto Congreso Internacional de Protección de Datos Personales.
- Desarrollar una estrategia de protección de datos personales de niños, niñas y adolescentes realizando campañas de divulgación y adelantando capacitaciones en materia de protección de datos personales a personal administrativo y docente de algunas instituciones educativas país.

3. ACCIÓN NORMATIVA

Instrucciones a los Responsables del tratamiento para el registro de sus bases de datos

Dentro de las funciones otorgadas a la Superintendencia de Industria y Comercio por la Ley 1.581 de 2012, se encuentra la de "Impartir instrucciones y órdenes sobre la manera como deben cumplirse las disposiciones de la presente ley relacionadas con la administración de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países fijar los criterios que faciliten su cumplimiento y señalar procedimientos para su cabal aplicación". En tal virtud expidió la Circular Externa Núm. 01 de 2016, mediante la cual impartió instrucciones a los Responsables del tratamiento para llevar a cabo el registro de sus bases de datos ante el Registro Nacional de Bases de Datos.

4. PROCEDIMIENTOS DE GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS

Procedimientos de consulta y reclamo para el ejercicio del derecho de hábeas data

Las Leyes 1.266/2008 y 1.581/2012 incluyen los procedimientos de consultas y reclamos para el ejercicio del derecho de hábeas data de los titulares ante los responsables y encargados del tratamiento, estableciendo requisitos para su presentación y los términos de respuesta que deben cumplir los sujetos obligados.

Si una vez agotado el procedimiento de consulta o reclamo, según corresponda, el titular no ve satisfecho su derecho, puede presentar una queja ante la SIC, como Autoridad de Protección de Datos Personales, que se rige por procedimiento administrativos general establecido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo (Ley 1.437 de 2011). Así, una vez recibida la queja, esta entidad solicita información adicional o explicaciones a la fuente, operador o fuente de información (cuando hay una posible vulneración del derecho de hábeas data financiero) o al Responsable o Encargado del tratamiento (en los demás casos), con el fin de que este presente sus argumentos de defensa y las pruebas que se encuentren en su poder para proceder a esclarecer la situación relacionada con la posible vulneración del derecho del titular. Una vez analizada toda la información recolectada, la SIC procede a tomar una decisión que puede consistir en una orden de corrección, actualización, rectificación o supresión en defensa del derecho de los titulares.

En ese sentido, la Dirección de Investigación de Protección de Datos Personales de la Superintendencia de Industria y Comercio profirió durante 2016 resoluciones que ponen fin a actuaciones administrativas en las que se ordena a las investigadas tomar acciones en procura de la protección del derecho fundamental de hábeas data o del derecho a la protección de datos personales de los ciudadanos. Uno de los casos más relevantes de 2016 se señala a continuación:

– Resolución 47.868, de 26 de julio de 2016, relacionada con la rectificación de datos en el sistema de información de an-

Caso relevante: rectificación de antecedentes judiciales

tecedentes judiciales que lleva la policía nacional. En ejercicio del derecho de hábeas data un titular solicita rectificar la información alojada en el sistema de información sobre antecedentes y anotaciones (SIAN) administrado por la Dirección de Investigación Criminal e Interpol de la Policía Nacional, puesto que en dicho registro se encuentra vinculado su número de identificación como perteneciente a un procesado por los delitos de tráfico de armas y estupefacientes, y que pese a solicitar la corrección de la información, su petición no fue atendida.

Una vez se requirió a la entidad en comento, para que se pronunciara sobre los hechos y aportara las pruebas que pretendiera hacer valer, ésta guardó silencio, por lo que la Superintendencia procede a ordenar que, con fundamento en la aplicación del principio de veracidad consagrado en el artículo 4 b) de la Ley 1.581/2012, se actualice la información que se encontraba registrada en la base de datos del sistema de información sobre antecedentes y anotaciones (SIAN) de la policía nacional de Colombia.

5. PROCEDIMIENTOS DE INSPECCIÓN Y SANCIÓN

Etapas del procedimiento administrativo sancionatorio

El procedimiento utilizado por la SIC en el caso de las investigaciones administrativas de carácter sancionatorio es el procedimiento administrativo sancionatorio descrito en la Ley 1.437 de 2011 o Código de Procedimiento Administrativo y de lo Contencioso Administrativo, que establece una etapa de averiguación preliminar, la formulación de cargos, la presentación de descargos, el período probatorio, la presentación de alegatos y la toma de decisión, que puede consistir en una archivo de la investigación o en la imposición de multas o sanciones e incluso la impartición de órdenes.

Tipos de sanciones

Las leyes de protección de datos personales incluyen los siguientes tipos de sanciones que puede imponer la SIC:

a) Multas de carácter personal e institucional hasta por el equivalente de mil quinientos o dos mil salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;
b) Suspensión de las actividades relacionadas con el tratamiento de datos personales hasta por un término de seis meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;
c) Cierre temporal de las operaciones relacionadas con el tratamiento de datos personales una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la SIC;
d) Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos personales sensibles.

En aplicación del procedimiento descrito, la Dirección de Investigación de Protección de Datos Personales de la Superintendencia

de Industria y Comercio profirió las siguientes decisiones de carácter sancionatorio:

Sanciones relevantes impuestas en 2016

- Resolución 7.883 del 24 de febrero de 2016 por incumplimiento por parte de una empresa de giros postales de dinero al deber de solicitar y conservar copia de la autorización previa expresa e informada para el tratamiento de datos personales y de informar previamente y de manera clara expresa e inequívoca al titular acerca del tratamiento al cual serían sometidos sus datos y la finalidad de los mismos. Por este incumplimiento se dispuso una sanción de aproximadamente 79.100 €.
- Resolución 13.681, de 29 de marzo de 2016, por el tratamiento inadecuado por parte de una persona natural de datos sensibles relacionados con la orientación política de las personas debido a la exposición de datos personales sensibles relacionados con la firma de la iniciativa de revocatoria al Alcalde de Bogotá (Colombia) en una página de internet. Se encontró una violación al deber de requerir consentimiento explícito por parte del titular para incluir sus firmas en la página web abierta a consulta pública al incluir allí una opinión política de las personas considerada dato sensible. Por incurrir en esta conducta se impuso una sanción de más de 1.000 €.
- Resolución 15.339, de 31 de marzo de 2016, por incumplimiento por parte de una persona natural al deber de solicitar y conservar copia de la autorización previa expresa e informada en virtud de la venta de bases de datos con información personal (direcciones electrónicas) sin autorización previa, expresa e informada del titular. Por incurrir en esta conducta se impuso una sanción de más de 1.000 €.
- Resolución 16.308, de 6 de abril de 2016, por violación por parte de una empresa de cobranza de cartera al principio de circulación restringida y deber de seguridad al remitir mensajes electrónicos de datos con exposición injustificada de datos personales semiprivados de ciudadanos. Por esta conducta se impuso una sanción de más de 22.000 €.
- Resolución 39.298, de 21 de junio de 2016, por violación al principio de circulación restringida, al deber de seguridad y al deber de comunicar un incidente de seguridad por la exposición injustificada y masiva de datos sensibles de salud en internet. En el curso de la investigación se estableció que estuvieron visibles y sin ningún tipo de control en un portal web de una entidad prestadora de servicios de salud, datos personales relativos a la salud de treinta titulares, usuarios de esa entidad, los cuales claramente son catalogados por la Ley 1.581 de 2012 como de naturaleza sensible. Este incumplimiento generó una multa de más de 271.000 €.
- Resolución 85.323, de 26 de diciembre de 2016, por violación del régimen de protección de datos personales por parte una institución educativa por el incumplimiento de los deberes deber de solicitar y conservar copia de la autorización previa expresa e informada, no conservar la información bajo condi-

ciones de seguridad y garantizar la reserva de la información, entre otros. Por estos incumplimientos la institución educativa fue sancionada con la suma aproximada de 6.500 €.

– Resolución 85.653, de 27 de diciembre de 2016, por incumplimiento al deber de conservar la información de los titulares bajo las condiciones de seguridad necesarias en virtud de la exposición injustificada de datos de ubicación de un titular en la red social twitter por una empresa encargada de prestar servicios públicos domiciliarios en el país. Esta conducta generó una sanción de aproximadamente 79.000 €.
– Resolución 85.654, de 13 de diciembre de 2016, por incumplimiento por parte de una empresa dedicada a la venta de productos por internet del deber de garantizar al titular el pleno y efectivo ejercicio del derecho de hábeas data que se viola cuando no se atiende en debida forma la solicitud de supresión del dato de un titular que afirma que a pesar de haber autorizado el envío de publicidad a su correo electrónico no aceptó el envío de la misma mediante mensajes de texto a su teléfono móvil y a pesar de ejercer su derecho se supresión sigue recibiendo esos mensajes publicitarios. En este caso la sanción fue por 79.000 € aproximadamente.

6. COOPERACIÓN CON OTRAS INSTITUCIONES PÚBLICAS

Implementación de buenas prácticas

La SIC ha tenido acercamientos con varias entidades nacionales del sector central, como la Presidencia de la República y, específicamente, la Secretaría de Transparencia, la Procuraduría General de la Nación, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Comercio Industria y Turismo, el Departamento Administrativo de la Función Pública, el Centro de Documentación Judicial de la Rama Judicial, la Registraduría Nacional del Estado Civil, la Fiscalía General de la Nación, la Policía Nacional, la Unidad para la Atención y Reparación de Víctimas del Conflicto Armado, entre otras, con el fin de acompañar y capacitar a las diferentes entidades en la implementación de buenas prácticas en materia de protección de datos personales y para lograr convenios colaborativos que permitan mejorar la labor investigativa de la SIC como Autoridad de Protección de Datos Personales.

Participación en encuentros internacionales

A nivel internacional, la SIC participó en el Taller sobre Protección de Datos y Acción Internacional Humanitaria celebrado el 16 y 17 de junio de 2016 en Ciudad de Guatemala, que surgió como parte del compromiso adquirido por la Red Iberoamericana de Protección de Datos Personales, en el marco de la Resolución sobre Protección de Datos y Acción Internacional Humanitaria adoptada por la Conferencia Internacional de Autoridades de Protección de Datos Personales de 2015. En el mencionado taller participaron representantes de autoridades de protección de datos de México, España y Colombia, observadores de Chile y Guatemala y repre-

sentantes de la Cruz Roja Internacional y ACNUR. La SIC, por intermedio del Director de Investigación de Protección de Datos Personales, participó con una ponencia en la que se expuso el trabajo de acompañamiento que está adelantando la SIC, como Autoridad de Protección de Datos en Colombia, y la Unidad para la Atención y Reparación de Victimas del Conflicto Armado en la implementación de los protocolos y lineamientos que deben aplicar las entidades que hacen parte de la Red Nacional de Información y la Unidad de Víctimas para compartir información respetando el Régimen de Protección de Datos Personales así como de los nuevos retos que representa la protección de datos personales en el post-conflicto.

Barrido Global de Privacidad

En mayo de 2016, por tercer año consecutivo, la SIC se unió a 24 autoridades de privacidad y protección de datos personales en el Barrido Global de Privacidad organizado por GPEN, con el fin de examinar más de 300 dispositivos que captan información personal como, por ejemplo, relojes que monitorizan la salud, consolas de videojuegos, lavadoras y neveras; con el fin de establecer si los productores y fabricantes de dichos artefactos cumplen a cabalidad las disposiciones de protección de datos personales con un enfoque de responsabilidad demostrada, para identificar las tendencias del mercado que puedan orientar las actuaciones de las autoridades en el sentido de brindar capacitación y divulgación a los consumidores o adelantar investigaciones por posibles vulneraciones al régimen de protección de datos personales.

7. COOPERACIÓN CON LA SOCIEDAD

Capacitaciones a empresas y gremios

La SIC realiza frecuentemente capacitaciones a comerciantes, empresas y gremios o agrupaciones de empresas en las que da a conocer y explica de manera práctica la metodología sugerida por esta Autoridad para la implementación de las normas de protección de datos personales al interior de esas organizaciones. En ese sentido, y con fundamento en lo señalado en la "Guía para la implementación del Principio de Responsabilidad demostrada" publicada por esta entidad en el 2015, los funcionarios de la SIC acuden a las organizaciones que lo solicitan a difundir y explicar las medidas incluidas en esa guía como sugerencias para la correcta aplicación de la Ley 1581 de 2012.

Congreso Internacional de Protección de Datos

Adicionalmente, cada año se organiza el Congreso Internacional de Protección de Datos Personales, como un evento en el que se exponen temas de alto impacto, novedosos y de interés para la comunidad, con el fin de abrir un espacio para que tanto la SIC, los sujetos obligados y los consultores interesados se actualicen en los diferentes temas relacionados con la protección de datos personales a nivel mundial y se compartan experiencias con Autoridades y organizaciones privadas de otros países que le permitan a los empresarios colombianos, a la academia y a los consultores desarrollar sus objetivos y funciones de manera actualizada y competitiva.

Guía sobre videovigilancia

Además, en el 2016 la SIC realizó la publicación de la guía para la protección de datos personales en sistemas de videovigilancia, con el fin de orientar a aquellos que implementan estos sistemas para que adecúen el uso de los mismos a las disposiciones que regulan la protección de datos personales. En esta guía se precisan algunos aspectos que se deben tener en cuenta para garantizar la protección de los derechos de los titulares de información cuyas imágenes son captadas mediante esos sistemas.

8. OTRAS ACTIVIDADES

Programa de divulgación masiva

En cumplimiento de la función de promover y divulgar los derechos de las personas en relación con el tratamiento de sus datos personales, la SIC continúa desarrollando el programa de divulgación masiva del Régimen General de Protección de Datos Personales y del Registro Nacional de Bases de Datos, el cual incluye entidades del sector público y privado, universidades, gremios empresariales y cámaras de comercio. En total, en el 2016 se capacitaron más de 5204 personas en más de treinta eventos realizados en varias ciudades del país. Igualmente, continuando con la realización del Curso Virtual Introducción a la Protección de Datos Personales, durante el período se llevó a cabo cinco cursos externos con un total de 1.042 participantes, un curso interno con un total de 275 participantes y seis cursos para las empresas que lo solicitaron, con un total de 88 participantes.

9. DATOS ESTADÍSTICOS SOBRE LAS ACTIVIDADES DESCRITAS EN LOS APARTADOS ANTERIORES

Quejas recibidas y sanciones impuestas

Durante el 2016, la SIC recibió más de seis mil quejas de titulares de información que consideraron vulnerado su derecho de hábeas data y finalizó más de cincuenta casos imponiendo sanciones a los sujetos obligados por el incumplimiento de sus deberes en el tratamiento de información personal, por la suma aproximada de 5.564.000.000 pesos, esto es, más de 1.700.000 €.

Los motivos principales de las multas impuestas están relacionados con el incumplimiento de los siguientes deberes: veracidad y calidad de la información, no atención de reclamaciones presentadas, no contar con la autorización para el tratamiento por parte del titular no conservar la información personal con medidas de seguridad adecuadas y no contar con políticas para el tratamiento de la información.

Sumado a lo anterior, durante el 2016 se cerraron 2.430 casos iniciados con fundamento en quejas recibidas de los titulares de la información personal exigiendo la protección de sus datos personales. De los casos cerrados, 343 concluyeron con una orden proferida por esta Autoridad en la que se exige a los sujetos obligados tomar medidas para que cese la vulneración del derecho del titular, como por ejemplo, rectificar, actualizar o eliminar su información personal.

Bases de Datos inscritas en el Registro Nacional

Finalmente, a finales de 2015 se habilitó el Registro Nacional de Bases de Datos, administrado por la SIC para que las personas jurídicas de naturaleza privada cumplieran con este deber. A corte del 30 de diciembre de 2016 se habían inscrito ya 146.775 bases de datos de 103.877 responsables del tratamiento. Cabe anotar que a finales de 2016 se habilitó el Registro para las personas naturales y las entidades públicas.

V. ESPAÑA: AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

1. INTRODUCCIÓN

Creación de la Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos (AEPD) es la autoridad estatal de control encargada de velar por el cumplimiento de la normativa sobre el derecho fundamental a la protección de los datos personales, que nace en 1992 con la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal e inicia sus actividades en 1994. Se trata de un ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada. La existencia de una autoridad de control independiente que vele por este derecho fundamental está prevista en el Convenio 108 del Consejo de Europa, de 1981, el primer texto internacional sobre la materia, y obtiene su configuración más acabada en la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. Esta Directiva ha sido sustituida por el Reglamento (UE) 2016/679, de 27 de abril de 2016, del Parlamento Europeo y del Consejo, 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 (RGPD), que entrará en vigor en vigor el 25 de mayo de 2018. El estatuto de Autoridades de Control independientes en materia de protección de datos personales está regulado en el capítulo VI del RGPD. Uno de los rasgos característicos de la AEPD es que actúa con independencia para el desempeño de sus funciones. En términos generales, la misión de la AEPD es velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de acceso, rectificación, cancelación y oposición de datos (ARCO).

Funciones de la AEPD

Las funciones de la AEPD se establecen en el artículo 37 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD). Estas funciones se pueden concretar como sigue:

- En relación con los ciudadanos:
  - Atender a sus peticiones, denuncias y reclamaciones de tutela de derechos.
  - Informar de los derechos reconocidos en la Ley.
  - Promover campañas de difusión a través de los medios.
  - Velar por la publicidad de los ficheros de datos de carácter personal.
- En relación con quienes tratan datos (responsables y encargados):

- Emitir las autorizaciones previstas en la Ley.
- Requerir medidas de corrección.
- Ordenar, en caso de ilegalidad, el cese en el tratamiento de los datos y la cancelación de los mismos.
- Ejercer la potestad sancionadora, en los términos previstos en el Título VII de la LOPD.
- Recabar de los responsables de los ficheros la ayuda e información que precise para el ejercicio de sus funciones.
- Autorizar las transferencias internacionales de datos.

– En la elaboración de normas: Informar preceptivamente los Proyectos de normas de desarrollo de la LOPD.

Evolución de la AEPD

Desde sus inicios, la AEPD ha desarrollado un notable esfuerzo en la normalización de la cultura de protección de datos, participando en múltiples acciones de divulgación a través de distintas herramientas, materiales y recursos (guías, videos, blog, web, etc.), participación en actos sectoriales, celebración de una sesión abierta anual dirigida fundamentalmente a los profesionales de la privacidad y a los responsables, así como mediante una presencia continua en los medios de comunicación. Asimismo, se ha incrementado considerablemente la transparencia en la actuación de la AEPD, como pone de manifiesto la publicación de sus resoluciones y la creación de una página web informativa sobre sus actividades. Es destacable el considerable aumento de la participación internacional de la AEPD, especialmente en los ámbitos europeo y latinoamericano. En el ámbito europeo, se subraya la intervención de la AEPD en las actividades del Grupo de Trabajo del artículo 29 de la Directiva 95/46, que es el organismo consultivo de la Comisión Europea en lo referente a la protección de Datos Personales. La AEPD también forma parte de las Autoridades de control de Europol a raíz de la puesta en marcha del fichero informatizado común, en términos que, sin afectar a su finalidad, se tenga en cuenta el derecho a la protección de datos personales. Además, ejerce las funciones de Secretaría Permanente de la Red Iberoamericana de Protección de Datos.

2. PLANIFICACIÓN

Plan Estratégico 2015–2019

Una parte importante de la actividad de la AEPD durante 2016 se encuadra dentro de los objetivos de su Plan Estratégico de Actuación 2015–2019, que se aprobó en noviembre de 2015 con la finalidad de afrontar de forma ordenada e integral los nuevos retos en materia de protección de datos, y especialmente los desafíos derivados de la adaptación al nuevo Reglamento Europeo en 2018. Dicho Plan Estratégico también tiene como meta reforzar la identidad y cohesión interna de la Institución y su imagen exterior, afianzándola como Autoridad de referencia en los contextos europeo e iberoamericano. Otra de las metas esenciales del Plan Estratégico es continuar avanzando en facilitar la mayor participación posible de ciudadanos, responsables y profesionales de la privacidad, en la gestión cotidiana de

la Agencia. A fin de alcanzar dichas metas, se han configurado los siguientes cinco ejes estratégicos del Plan:

Prevención para una protección más eficaz

– Eje estratégico 1: Prevención para una protección más eficaz, especialmente en ámbitos socialmente sensibles como la protección de menores, la educación y la sanidad. Con esta línea estratégica se pretende avanzar en un enfoque más preventivo que reactivo en la defensa de los derechos. En este sentido, ocupa un lugar destacado todo lo relacionado con los menores como grupo en situación vulnerable. En este ámbito, se han establecido distintas líneas de trabajo para fomentar la privacidad entre alumnos, padres y profesores, como por ejemplo mediante un canal específico (teléfono y servicio de WhatsApp) orientado a la resolución de dudas; donde se han atendido en 2016 más de 700 consultas.. Otro campo que ha merecido especial atención en las políticas de prevención de la AEPD en 2016 es la contratación irregular de servicios y la inclusión indebida en los ficheros de morosidad. En colaboración con la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD) y los organismos en materia de consumo, se ha previsto la elaboración de materiales prácticos y guías para que los ciudadanos puedan conocer con claridad a quién deben acudir en defensa de sus derechos. Entre estos materiales, hay que destacar, sin duda, la "Guía sobre privacidad y seguridad en internet", elaborada conjuntamente entre la AEPD y el INCIBE. En ella, los interesados pueden encontrar una respuesta rápida y sencilla a cuestiones como: información para proteger dispositivos portátiles, generar y gestionar contraseñas o como ejercitar el derecho al olvido. Por último, en el ámbito sanitario, hay que resaltar el plan de inspección sectorial de oficio que se ha llevado a cabo en relación con los Hospitales. .

Innovación y protección

– Eje estratégico 2: Innovación y protección, que incida en la mejora de la confianza. La iniciativa más relevante en 2016 es la creación de la Unidad de Evaluación y Estudios Tecnológicos cuyo fin es detectar y analizar tendencias, productos o servicios que puedan tener un impacto en la privacidad de los ciudadanos, favoreciendo la introducción de políticas de protección de datos desde el diseño, para garantizar que estén presentes en todas las fases de concepción, análisis e implantación de dichos desarrollos tecnológicos. Entre los cometidos principales de esta Unidad está la realización de estudios y análisis de los productos y servicios para conocer de primera mano sus funcionalidades y la forma en que se almacenan, tratan y comunican los datos personales que recogen, así como la transparencia con la que se llevan a cabo los tratamientos. Además, se han llevado a cabo dos estudios sobre *big data*: uno centrado en las soluciones que se aplican en el entorno comercial y empresarial; y, el otro en la reutilización de información clínica y análisis masivos de datos en el sector sanitario, con el que se pretende conocer la situación española en este campo en los ámbitos asistencial, de investigación, epidemiológico y de salud pública, público y privado.

Una Agencia más colaboradora, transparente y participativa

– Eje estratégico 3: Se incluyen en este eje todas aquellas actuaciones que contribuyan a configurar una AEPD más colaboradora, transparente y participativa, que favorezca la comunicación con la sociedad y establezca relaciones estables con los profesionales de la privacidad, facilitando su acceso a los servicios de la Agencia. En este eje destaca la puesta en marcha del blog de la Agencia y la atención personalizada a los medios de comunicación, con objeto de fomentar la sensibilización y el conocimiento de los ciudadanos en materia de protección de datos. Ello se ha concretado en casi 400 consultas de medios atendidas y en la gestión y coordinación, por el personal directivo de la AEPD, de más de 60 entrevistas y tribunas a diferentes medios. De cara a la próxima entrada en vigor del nuevo Reglamento Europeo de Protección de Datos (mayo de 2018), se está diseñando un conjunto de guías y herramientas prácticas. Además, se han seguido manteniendo colaboraciones fluidas con los profesionales de la privacidad, a través de sus asociaciones, con el objetivo de conocer sus problemas y sus propuestas de solución. Por otro lado, ante la aparición de la figura del Delegado de Protección de Datos, en aquellos casos en que sea exigible, se han puesto en marcha por parte de la AEPD los trabajos para la elaboración de un esquema de acreditación y certificación de las entidades de certificación, así como de los profesionales que van a llevar a cabo estas tareas.

Simplificar los procedimientos de la Agencia

– Eje estratégico 4: Simplificar los procedimientos de la AEPD, para hacerla más cercana a los responsables y profesionales de la privacidad. Este eje trata de todas las iniciativas encaminadas a conseguir una AEPD más cercana a los responsables y profesionales de la privacidad, así como a las empresas. El eje se centra en la preparación para la entrada en vigor del nuevo Reglamento General de Protección de Datos, ya que este hecho va a requerir un importante esfuerzo de adaptación, no sólo en el ámbito normativo sino también por parte de los principales implicados (ciudadanos, responsables y profesionales de la privacidad). La AEPD durante 2016 ha realizado un importante esfuerzo para dotar a las empresas de un conjunto de herramientas y de materiales que faciliten su adaptación al Reglamento. En este sentido, cabe mencionar la presentación en enero de 2017 de la Guía para Responsables; las Directrices sobre modelos de cláusulas informativas y contrato responsable-encargado, así como herramientas de autoevaluación para micropymes que realicen tratamientos con bajo riesgo. Todos estos materiales están reunidos en un *site* específico creado en la web de la AEPD. En cuanto a las Administraciones públicas, también se están poniendo en marcha distintas iniciativas, de manera especial en los municipios pequeños. Un ejemplo de estas iniciativas fue la creación de un Grupo de Trabajo con representantes de la Secretaría General de Administración Digital, del Centro Criptológico Nacional y de la AEPD, para la identificación de las particularidades que la aplicación del Reglamento supone para el Sector Público.

Incrementar la agilidad y eficiencia de la Agencia

– Eje estratégico 5: Incrementar la agilidad y eficiencia de la AEPD, reduciendo los tiempos de los trámites y optimizando la utilización de los recursos disponibles. En este eje una de las más emblemáticas iniciativas fue la creación de la Unidad de Admisión, que ha permitido dar una respuesta rápida a un alto número de denuncias y reclamaciones sobre cuestiones que no son competencia de la AEPD. Otras iniciativas llevadas a cabo fueron: la puesta en marcha de la Plataforma "Cl@ve", que permite a los ciudadanos identificarse de la misma forma ante todos los organismos de la Administración; el impulso del registro electrónico, como canal de presentación de documentos ante la AEPD; y, la integración de la AEPD en el Sistema de Interconexión de Registros (SIR).

3. PROCEDIMIENTOS DE GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS

Resoluciones estimatorias destacadas

En 2016, entre las Resoluciones estimatorias de tutela de derechos, podemos subrayar los criterios referentes a los derechos ARCO y el derecho al olvido, que fueron establecidos en las siguientes seis Resoluciones:

Derecho de oposición

– R/02382/2016. Resolución que se formula ante una reclamación, de 5 de abril de 2016, contra la versión digital de un periódico, por no haber atendido el derecho de oposición (art. 6.4 LOPD) de la persona reclamante, donde se estimó que: "la publicación de la información, conteniendo los datos personales del reclamante, por la versión digital de (…), es conforme con las libertades de opinión e información recogidas en el artículo 20 CE bajo la denominación genérica de "libertad de expresión". El derecho a "recibir libremente información veraz por cualquier medio de difusión" prevalece frente a otros derechos constitucionales, atendiendo a la Jurisprudencia del Tribunal Constitucional, que reconoce esta posición preferente a la libertad de expresión siempre y cuando los hechos comunicados se consideren de relevancia pública (Sentencias 105/1983 y 107/1988) y la información facilitada sea veraz (Sentencias 6/1988, 105/1990 y 240/1992)". Sin embargo, la AEPD agregó que en este caso no se solicitaba la cancelación de los datos personales del reclamante en la web del Periódico, sino que se adopten las medidas para que la web de la noticia no sea indexada por los motores de búsqueda de Internet. Sobre ese tema, luego de analizar sentencias pertinentes, se estimó que: "A la vista de lo dictaminado en las dos Sentencias citadas, teniendo en consideración que la noticia es del año AA, que el reclamante no es una persona de relevancia pública, y que los hechos carecen de interés histórico, esta Agencia concluye que el tratamiento de los datos personales del reclamante resulta inadecuado, no pertinente y excesivo para la finalidad inicial que lo justificaba".

Derecho a la cancelación y derecho al olvido

– R/02170/2016. En este caso se trata el derecho a la cancelación y el derecho al olvido y se señala que: "Por lo que se refiere a la naturaleza del buscador como responsable de tratamiento, […] el Tribunal de Justicia considera que el gestor del motor de búsqueda es el responsable del tratamiento de los datos al determinar los fines y los medios de su actividad. […] En relación a la posibilidad de ejercer el derecho de cancelación ante el buscador de Internet sin acudir al responsable del sitio web, […] una vez que el interesado ha presentado su solicitud de cancelación de sus datos personales ante el motor de búsqueda, deberá examinarla y proceder, en su caso, a la supresión de los enlaces concretos de la lista de resultados, sin que previa o simultáneamente se tenga que acudir al responsable del sitio web […]. Respecto a su petición de eliminación del aviso que ofrece el buscador al pie de los resultados al realizar un consulta por su nombre y apellidos, hay que recordar que el Grupo de Trabajo de Autoridades europeas de protección de datos (GT29), sobre la aplicación de la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) del 13 de mayo de 2014, relativa al denominado derecho al olvido, expone que la práctica de algunos buscadores de informar a los usuarios de que la lista de resultados puede no estar completa como consecuencia de la aplicación del derecho europeo no encuentra fundamento en ninguna exigencia normativa. El GT29 ha manifestado que esta práctica solo puede ser aceptable si de la información que se ofrece a los usuarios no se deduzca que una persona concreta, ha solicitado la retirada de ciertos resultados asociados a su nombre. Se recomienda que estas informaciones se proporcionen a través de una declaración general que figure de forma permanente en las páginas del buscador".

Interpretación del derecho a la cancelación

– R/03262/2016. En esta Resolución se interpreta el derecho a la cancelación: "A la vista de lo manifestado por la reclamante en su solicitud ante Google y en su reclamación ante esta Agencia, de que la dirección postal que se publica en dicha página es su domicilio particular junto con su nombre y apellidos y un teléfono que desconoce, que en ningún momento autorizó la publicación de sus datos personales y su dirección, y teniendo en consideración que la reclamante no es una persona de relevancia pública, y que los datos carecen de interés público al no referirse a datos profesionales, esta Agencia concluye que el tratamiento de los datos personales de la reclamante resulta inadecuado, no pertinente y excesivo".

Derecho de acceso a datos personales

– R/03419/2015. En este caso sobre el derecho de acceso a datos personales se estimó que: "la Entidad reclamada está obligada a elaborar la documentación que debe incorporarse a la historia clínica de los pacientes y a conservar dicha historia en las condiciones y con las finalidades previstas en la normativa de aplicación, así como a favorecer y posibilitar el ejercicio del derecho de acceso a los datos de carácter personal que consten en sus ficheros y, en particular, el acceso a la historia clínica de las personas que hayan recibido asistencia médica en dicho centro".

Cancelación de datos de solvencia patrimonial

– R/03418/2015. En referencia a la cancelación de datos de solvencia patrimonial: "el artículo 29.2 de la LOPD, que regula la prestación de servicios de información sobre solvencia patrimonial y crédito, determina que el acreedor o quien actúe por su cuenta e interés está legitimado para aportar datos al fichero de solvencia patrimonial y crédito al ser el único que conoce si la deuda realmente existe o si ha sido saldada o no, y por lo tanto tiene la potestad de la inclusión o cancelación de los datos personales del reclamante siempre y cuando cumplan los requisitos recogidos en la normativa de protección de datos, por consiguiente, para llevar a cabo dicha inclusión, la deuda tiene que ser cierta, vencida, exigible, que haya resultado impagada y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, por lo tanto, el acreedor puede inscribir al reclamante en un fichero de solvencia patrimonial y crédito cuando exista una deuda previa, vencida y exigible".

Datos publicados en una sentencia del Tribunal Constitucional

– R/01015/2016. En esta Resolución se atiende una solicitud presentada por un reclamante cuyos datos personales aparecen publicados en una sentencia del Tribunal Constitucional. La reclamación es formulada contra Google Inc., el TC y la Agencia Estatal del Boletín Oficial del Estado, por no haber sido atendido debidamente el derecho de cancelación. Concretamente solicitaba la retirada de la publicación en sus páginas web de una sentencia del TC o la eliminación de sus datos personales de dicha sentencia, para evitar que fuera accesible a través del buscador al realizar una búsqueda de su nombre. La AEPD estima parcialmente la solicitud contra Google y reitera criterios semejantes a los antes descritos en la R/02170/2016. En ese sentido, a partir de algunas sentencias la AEDP reitera que: "el gestor del motor de búsqueda es el responsable del tratamiento de los datos al determinar los fines y los medios de su actividad". En relación a la posibilidad de ejercer el derecho de cancelación ante el buscador de Internet sin acudir al responsable del sitio web: "Una vez que el interesado ha presentado su solicitud de cancelación de sus datos personales ante el motor de búsqueda, deberá examinarla y proceder, en su caso, a la supresión de los enlaces concretos de la lista de resultados, sin que previa o simultáneamente se tenga que acudir al responsable del sitio web". En cuanto a que la solicitud de su nombre no se vincule a determinados resultados: "La lista de resultados obtenida en una búsqueda a partir de un nombre, página web o información relativa a una persona, facilita la accesibilidad y difusión de la información a cualquier internauta que realice una búsqueda sobre el interesado, constituyendo una injerencia en el derecho fundamental al respeto de la vida privada del interesado". En este caso, la AEPD comprobó que el TC había determinado sustituir por iniciales los datos del reclamante, pero Google continuaba asociando el nombre del afectado a la URL de la Sentencia y para la AEPD: "prevalece el derecho del reclamante y procede la exclusión de sus datos personales, al tratarse de

datos obsoletos dado que la información pertenece al año 2001; por haberse anonimizado sus datos en la web de origen; y por no concurrir interés preponderante del público en tener acceso a esta información a través de una búsqueda en Internet que verse sobre el nombre de esa persona".

Infracción de las Administraciones públicas

De igual manera, entre los procedimientos de declaración de infracción de las Administraciones públicas podemos destacar las siguientes tres Resoluciones en las que se determinan criterios trascendentes sobre la ponderación entre las obligaciones de transparencia de las Administraciones públicas y el derecho a la protección de datos; el manejo de los datos sanitarios y el principio de seguridad de los datos:

Publicación de la relación de puestos de trabajo de empleados públicos

– R/00401/2016. Que trata sobre la publicación de la relación de puestos de trabajo de empleados públicos en el Boletín Oficial de Aragón (BOA) con información excesiva. Esta Resolución fue emitida en un procedimiento instruido en contra de la Consejería de Hacienda y Administraciones Públicas del Gobierno de Aragón porque se había publicado en el BOA la relación de puestos de trabajo (RPT) de todos sus trabajadores. Probados los hechos la AEPD se refirió a la Ley 8/2015, de Transparencia de la Actividad Pública y Participación Ciudadana de Aragón y a las obligaciones de publicidad activa de las Administraciones públicas, pero también a los límites a la transparencia y consideró que se incumplió el deber de secreto por la revelación de datos personales a terceros en esa publicación (art. 10 LOPD). Para la AEDP: "la publicación en la página web de la Consejería de los datos personales de los solicitantes relativos a su nombre, apellidos y DNI, asociados al resto de información contenida en la RPT se deduce información excesiva cuya publicación no está prevista en la citada Ley 8/2015 […]. Por tanto, no existe habilitación legal y aunque existiera el informe requiere la adopción de una serie de medidas para garantizar la protección de datos de carácter personal, tales como la notificación previa a los interesados dando plazo con posibilidad de oposición" y resolvió: "PRIMERO: DECLARAR que la CONSEJERÍA DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DEL GOBIERNO DE ARAGÓN ha infringido lo dispuesto en el artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.b) de la citada Ley Orgánica. SEGUNDO: REQUERIR a la CONSEJERÍA DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DEL GOBIERNO DE ARAGÓN, de acuerdo con lo establecido en el apartado 3 del artículo 46 de la Ley 15/1999, para que acredite en el plazo de un mes desde este acto de notificación las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del artículo 10 de la LOPD, para lo que se abre expediente de actuaciones previas E/01043/2016. En concreto: deberá proceder a retirar de la página web la publicación de las RPT denunciadas, procediendo, en todo caso, a la anonimización de los datos personales de los empleados públicos. TERCERO: NOTIFICAR la presente resolución a la CONSEJERÍA DE HACIENDA

Y ADMINISTRACIONES PÚBLICAS DEL GOBIERNO DE ARAGÓN y a Don A.A.A. CUARTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 46.4 de la LOPD".

Datos sanitarios de internos en la aplicación informática SANIT

– R/00711/2016. Dictada en el marco de un procedimiento de declaración de infracción de Administraciones públicas contra el Centro Penitenciario Sevilla de la Secretaría General de Instituciones Penitenciarias. En el cual se analiza el manejo de los datos sanitarios de internos en la aplicación informática SANIT, que también es un fichero de nivel de seguridad alto por tratar datos de salud y sexuales de personas en los centros de privación de la libertad (el programa dispone de varias bases de datos como Datos VIH, Serología, mantenimiento con metadona, etc.). Una vez comprobados los hechos y realizadas las inspecciones, la AEDP, entre otros puntos, señaló que: "la asignación de contraseñas conociéndose por el Administrador al ser el mismo el que las asigna, infringe la confidencialidad del acceso a los datos y contraria el principio de uso por su titular, ya que la misma tiene como función la identificación de forma inequívoca y personalizada del usuario" y resolvió: "PRIMERO: DECLARAR que el Centro Penitenciario Sevilla, (Secretaría General de Instituciones Penitenciarias) ha infringido lo dispuesto en el artículo 9.1 de la LOPD, en relación con los artículos 88, 93.3, 96, 99, 104 y 111 del RLOPD tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica. SEGUNDO: REQUERIR al Centro Penitenciario Sevilla, de acuerdo con lo establecido en el apartado 3 del artículo 46 de la LOPD, para que acredite en el plazo de un mes desde este acto de notificación las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del artículo 9.1 de la LOPD, para lo que se abre expediente de actuaciones previas E/01970/2016. En concreto deberá implementar el documento de seguridad del fichero que figura creado, inscrito y en funcionamiento desde 2005, informando de los extremos que afecten al personal que opera con datos. Deberá proceder a realizar una auditoría del fichero y remitirla a esta Agencia. Deberá acreditar que cumple las medidas de seguridad de control de acceso físico de ficheros, sean equipos de información o sean documentos en papel. En idéntico sentido, respecto al almacenamiento de soportes que contengan datos. Deberá informar del sistema de tratamiento de información que realiza a través de correo electrónico si lo utiliza o del registro y envío de historias clínicas a otros centros".

Omisión de medidas de seguridad en expedientes con datos de salud

– R/00814/2016. Al igual que la anterior, esta Resolución trata de la falta de medidas de seguridad sobre expedientes que contienen datos de salud y es instruida contra el Instituto Nacional de Toxicología y Ciencias Forenses. En este caso, entre otros puntos, la AEDP señala que el "artículo 9 de la LOPD establece el "principio de seguridad de los datos" imponiendo la obligación de adoptar las medidas de índole técnica y organiza-

tiva que garanticen aquella, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos a título de ejemplo, entre otros de "acceso no autorizado" por parte de terceros. Así, aun cuando el artículo 9 de la LOPD establece una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos, también es un mecanismo de garantía la seguridad" y resuelve: "PRIMERO: DECLARAR que el INSTITUTO NACIONAL DE TOXICOLOGIA Y CIENCIAS FORENSES ha infringido lo dispuesto en el artículo 9.1 de la LOPD, en relación con los artículos 88. 89.2, 93, 96, 99, 111 y 113 del RLOPD tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica. SEGUNDO: NO REQUERIR al INSTITUTO NACIONAL DE TOXICOLOGIA Y CIENCIAS FORENSES, sede de BARCELONA, la adopción de medidas de seguridad al haber constatado que se han adoptado las necesarias para garantizar la seguridad de los datos de carácter personal".

Comunicación de infracciones al Defensor del Pueblo

En este tipo de Resoluciones se debe subrayar que cuando se producen infracciones de las Administraciones públicas, por disposición legal, la AEPD debe comunicarlas al Defensor del Pueblo (art. 46.4 LOPD).

4. PROCEDIMIENTOS DE INSPECCIÓN Y SANCIÓN

Procedimientos de sanción destacados en 2016

De los procedimientos de sanción, instruidos en 2016, cabe subrayar los siguientes seis:

- PS/00149/2016. Instruido a Google Inc., donde se resuelve: PRIMERO: IMPONER a la entidad Google Inc., por una infracción del artículo 10 de la LOPD, tipificada como grave en el artículo 44.3.d) LOPD, una multa 150.000 euros, de conformidad con lo establecido en el artículo 45.2, 4 y 5 de la citada LOPD. SEGUNDO: REQUERIR a Google Inc. para que adopte sin dilación las medidas necesarias para poner fin a la vulneración del artículo 10 de la LOPD declarada en esta Resolución […]. TERCERO: ACORDAR la apertura de Actuaciones Previas de Investigación para verificar la existencia de comunicaciones con información no anonimizada efectuadas por Google Inc. a la organización Lumen. CUARTO: ACORDAR la apertura de Actuaciones Previas de Investigación que permitan determinar las posibles responsabilidades que pudieran derivarse de la práctica de Google Inc. de informar a los usuarios, en las páginas de resultados de búsquedas por nombre, que la lista de resultados puede no estar completa".
- PS/00047/2016 y PS/00053/2016. A partir de la investigación de dos casos muy similares en los que los reclamantes señalaban que había recibido una carta publicitaria remitida por Sistemas Médicos Profesionales S.L. (PLENISAN), que no tenían ninguna relación con esa entidad y que sus datos personales no

estaban en ninguna fuente de acceso público y que al pie de las cartas figura que el origen de los datos eran los ficheros de la entidad Macro Select Print S.L. (MSP). En los dos casos, la Directora de la AEPD, luego de un arduo proceso de investigación y de dos extensas fundamentaciones a las Resoluciones (en las cuales se realizan juicios de ponderación del nivel de responsabilidad de cada entidad) consideró que las conductas de esas entidades implicaron una infracción grave de la obligación de contar con el consentimiento de la persona afectada por el tratamiento de datos y resolvió en ambos casos: PRIMERO: IMPONER a la entidad MSL, por una infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 44.3 b) de la LOPD, una multa de 60.000 € de conformidad con lo establecido en el artículo 45 de la citada LOPD. SEGUNDO: IMPONER a la entidad MEYDIS, S.L., por una infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 44.3 b) de la LOPD, una multa de 60.000 € de conformidad con lo establecido en el artículo 45 de la citada LOPD. TERCERO: IMPONER a la entidad PLENISAN SL, por una infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 44.3 b) de la LOPD, una multa de 60.000 € de conformidad con lo establecido en el artículo 45 de la citada LOPD".

– PS/00005/2016. Esta Resolución es en relación con un escrito recibido por la AEPD en el que se señalaba que Telefónica de España-Movistar emplea "supercookies" en el acceso a Internet utilizando terminales móviles, sin informar debidamente al usuario y sin que este preste su consentimiento. En este caso se resuelve: "PRIMERO: IMPONER a la entidad TELEFONICA MOVILES ESPAÑA, S.A.U., por una infracción del artículo 22.2 de la LSSI, tipificada como leve en el artículo 38.4 g) de la LSSI, una multa de 20.000 € (veinte mil euros) de conformidad con lo establecido en los artículos 39 y 40 de la citada LSSI".
– PS/00691/2015. En este caso la Asociación 11 M Afectados de Terrorismo había puesto de manifiesto que en la dirección de internet www.peonesnegros.info aparecían publicados 392 documentos de carácter personal de las víctimas del atentado del 11 M de 2004. La AEPD realizó una investigación del caso y al concluir el procedimiento resolvió: PRIMERO: IMPONER a la entidad Asociación Peones Negros de Madrid, por una infracción del artículo 7.3 de la LOPD, tipificada como muy grave en el artículo 44.4.b) de la misma norma, una multa de 100.000 € (cien mil euros), de conformidad con lo establecido en el artículo 45.3, 4 y 5 de la citada Ley Orgánica. SEGUNDO: REQUERIR a la entidad Asociación Peones Negros de Madrid para que adopte sin dilación las medidas necesarias para poner fin a la vulneración del artículo 7.3 de la LOPD declarada en esta Resolución. En concreto se insta a dicha entidad para que, en el plazo de mes contado desde la notificación de este acto, cese en el tratamiento de los datos de carácter perso-

nal que constituyen el objeto de las presentes actuaciones. En el mismo plazo deberá comunicar a esta Agencia Española de Protección de Datos las medidas y actuaciones adoptadas para el cumplimiento de lo requerido, justificando haber eliminado de sus ficheros los datos de carácter personal reseñados".

5. COOPERACIÓN CON OTRAS INSTITUCIONES PÚBLICAS

Subgrupo de "Enforcement" del GT 29

La AEPD ha llevado en 2016 un número significativo de actividades en colaboración con distintas instituciones públicas. En el ámbito internacional, la AEPD se ha incorporado al Subgrupo de "*Enforcement*" del GT 29, cuyo objetivo es permitir la coordinación de la actuaciones de sus miembros en relación con problemas de protección de datos en tratamientos desarrollados por grandes compañías transnacionales, los cuales afectan a la mayor parte de los Estados miembros.

Actuaciones significativas en Iberoamérica

En lo referente a Iberoamérica, durante 2016, las actuaciones más significativas de la Agencia Española de Protección de Datos, en su condición de Secretaría Permanente de la Red Iberoamericana de Protección de Datos (RIPD), han sido las siguientes: 1) XIV Encuentro Iberoamericano de Protección de Datos, 8, 9 y 10 junio, Santa Marta, Colombia. 2) Taller "Privacidad y Acción Internacional Humanitaria", 16 y 17 de junio, Centro de la Cooperación Española en La Antigua, Guatemala. 3) Seminario "Europa-Iberoamérica: una visión común de la protección de datos. El nuevo marco europeo y su incidencia en Iberoamérica", 8 y 9 de noviembre, Centro de la Cooperación Española en Montevideo.

Otros ámbitos de colaboración institucional

En el ámbito interno, la AEPD también ha emprendido una estrecha colaboración con la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN) y con el Instituto Nacional de Ciberseguridad (INCIBE) para la elaboración y presentación de la "Guía de Privacidad y Seguridad en Internet", que ha tenido una amplia difusión ciudadana. Además, se han llevado a cabo colaboraciones con las Autoridades Autonómicas de Protección de Datos, creándose Grupos de Trabajo con la Agencia Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos, en relación con la aplicación del nuevo Reglamento Europeo de Protección de Datos.. En el marco de colaboración con el Poder Judicial, la AEPD ha participado como ponente en el Seminario organizado por el CGPJ sobre "Seguridad y Protección de Datos en los procedimientos judiciales". Asimismo, se ha impulsado la colaboración con la Secretaría General de Administración Digital (SGAD), dependiente del Ministerio de Hacienda y Función Pública, y con el Centro Criptológico Nacional (CCN), cuyo objetivo es evaluar el impacto en las Administraciones Públicas del nuevo Reglamento Europeo y redactar un conjunto de guías o directrices que ayuden en su implantación.

6. COOPERACIÓN CON LA SOCIEDAD

Cooperación con empresas, grupos sociales y profesionales de la privacidad

La AEPD ha celebrado durante 2016 varias actuaciones de cooperación y colaboración, tanto con empresas como con grupos sociales o profesionales de la privacidad. Así, en el marco de las relaciones periódicas que se mantienen con los principales prestadores de servicios en internet, se han celebrado diversas reuniones con representantes de Google en las que se informó las nuevas opciones de configuración de la privacidad de esa entidad. La AEPD también mantuvo reuniones con directivos de Facebook Spain, en la que éstos informaron a la AEPD sobre cambios en el tratamiento de la información recopilada. Con las PYMES, se ha promovido la elaboración de una herramienta de ayuda a las mismas para facilitar su gestión de la protección de datos en el marco del nuevo Reglamento Europeo.

Colaboración con Universidades y Consumidores y Usuarios

La AEPD también ha colaborado con grupos sociales y Universidades. En este marco se sitúa el Acuerdo suscrito con el Consejo de Consumidores y Usuarios. En el ámbito de promoción de la investigación, en 2016 se han establecido contactos preliminares con diversas Universidades españolas de perfil tecnológico para explorar posibilidades de colaboración en este sentido. También se están impulsando mecanismos de autorregulación en el ámbito de las telecomunicaciones y la publicidad, para favorecer los derechos de los usuarios de estos servicios y mejorar la calidad de los mismos.

Colaboración con profesionales de la privacidad

En el contexto de la colaboración con los profesionales de la privacidad, y sus asociaciones, han sido diversas las actuaciones de la AEPD a lo largo de 2016, entre las cuales cabe mencionar la participación de la AEPD en los Congresos de ENATIC (abogados digitales) y de la APEP (Asociación Profesional Española de Privacidad), o en la Jornada organizada por la APEP sobre habeas data y delitos informáticos. Asimismo, hay que reseñar las reuniones celebradas con la APEP, ISMS Fórum y ENATIC para recoger sus opiniones y sugerencias sobre el Reglamento Europeo de Protección de Datos.

7. OTRAS ACTIVIDADES DE INFORMACIÓN Y SENSIBILIZACIÓN CIUDADANA

En cuanto a la divulgación de información práctica para los ciudadanos, la AEPD ha desarrollado una intensa labor de información y sensibilización ciudadana. En este contexto se sitúa la ya citada "Guía sobre privacidad y seguridad en internet", compuesta por 18 fichas ampliables, que abordan distintos riesgos y problemas que pueden surgir en internet.

También cabe mencionar la elaboración de sendas guías con orientaciones sobre la protección de datos personales en los ámbitos de la reutilización de la información en el sector público y de la anonimización. Del mismo modo, la AEPD imparte anualmente cursos de formación para empleados públicos de la Administración General del Estado, dentro de la programación del Instituto Nacional de Administraciones Públicas. Igualmente, se han publicado en la sede

electrónica las nuevas FAQS, que en total tratan 25 temáticas y, a finales del 2016, se puso en marcha el blog de la AEPD.

8. DATOS ESTADÍSTICOS

En 2016, el número de denuncias registradas en la Agencia ha sido de 7.935, y el de reclamaciones de tutela de 2.588, haciendo un total de 10.523 escritos formulados por los ciudadanos en garantía de sus derechos. Se ha producido una ligera disminución de las denuncias registradas respecto a 2015, que fue de 8.489, mientras que, por el contrario, se mantiene la tendencia del incremento de las reclamaciones de tutelas de derechos, que fue en 2.015 de 2.082.

De la lectura de estas cifras, cabe destacar lo siguiente:

Denuncias

En paralelo con la bajada en el número de denuncias registradas, se ha producido una reducción del número de resoluciones sancionadoras en comparación con años anteriores que, sin embargo no ha afectado en la misma proporción al importe económico global de las sanciones impuestas que repunta levemente.

Un dato destacable es el crecimiento de los apercibimientos (un 43% sobre 2015) frente a la imposición de sanciones. Se trata de un mecanismo, el del apercibimiento, más rápido y más eficaz a la hora de conseguir la adecuación de los comportamientos infractores o en riesgo de serlo y, con ello, más eficiente a la hora de garantizar los derechos ciudadanos en esta materia.

En cuanto a la naturaleza de las denuncias tramitadas, cabe destacar el notable aumento de los casos de morosidad y de contratación fraudulenta. Ambas modalidades suponen el grueso de las quejas que recibe cotidianamente la Agencia. A continuación, figuran las denuncias recibidas en materia de videovigilancia y SPAM, supuestos ambos que, cuando las circunstancias legales y reglamentarias lo permiten, están siendo objeto, en lugar de sanciones, del correspondiente apercibimiento al sujeto infractor con las connotaciones anteriormente mencionadas. En consonancia con lo anterior, el mayor número y porcentaje de sanciones impuestas han recaído en infracciones cometidas por la inclusión indebida en los llamados "ficheros de morosos" y en segundo lugar en supuestos de contratación fraudulenta.

Reclamaciones de tutela

El aumento tan relevante producido en 2016 en este tipo de reclamaciones se debe en primer término a las reclamaciones frente a ficheros de solvencia patrimonial. El derecho de cancelación ha sido de nuevo el derecho más reclamado, refiriéndose a ficheros de solvencia patrimonial casi el 25 % de las reclamaciones planteadas. Dentro de las reclamaciones por la denegación del derecho de cancelación ante los ficheros de solvencia patrimonial, la mayoría de los casos se producen por negar el reclamante la existencia de la deuda que ha sido inscrita en los citados ficheros por parte, sobre todo, de las compañías de telecomunicaciones o de empresas que compran créditos.

Otro grupo de reclamaciones muy relevante es el referido al derecho de cancelación frente a los buscadores de internet, el llamado "derecho al olvido". En el entorno de los buscadores, foros sociales,

blogs y páginas web en general es donde se observa un incremento de las reclamaciones derivadas de los constantes tratamientos de datos que se producen en una sociedad digital. En ese entorno digital, que proporciona innumerables ventajas a los ciudadanos, se producen con frecuencia importantes violaciones en el ámbito de la privacidad. El anonimato con que se participa en muchas ocasiones dificulta extraordinariamente la posibilidad de dar una respuesta eficaz para impedir infracciones a la normativa de Protección de Datos.

Otros problemas añadidos en un mundo globalizado como el actual es la dificultad para tutelar los derechos ARCO frente a entidades que radican fuera de España y carecen de establecimientos en España o bien en las que las filiales en nuestro país no tienen ninguna participación en la determinación de los fines y medios del tratamiento. También representa una dificultad el hecho de que los servidores se encuentren en el extranjero, y en el caso de los foros, que no sea posible identificar a los administradores.

Por último, se observa una mayor preocupación de los afectados en el tratamiento de sus datos en los historiales clínicos. Como se aprecia por el número de reclamaciones referidas al derecho de acceso y a los derechos de rectificación y cancelación. Destacan los casos en que la Agencia ha tutelado el derecho de acceso, por la no entrega o entrega incompleta de la historia clínica por parte del responsable del fichero a los pacientes.

VI. ESPAÑA: AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS

1. INTRODUCCIÓN

Independencia de las Agencias autonómicas en el ejercicio de sus funciones

Conforme se señaló anteriormente, en España la protección de datos de carácter personal está desarrollada en la LOPD que regula los aspectos básicos del régimen jurídico de la AEPD. En la misma LOPD se establece que la mayor parte de las funciones asignadas a la AEPD, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas (CCAA) y por la Administración Local de su ámbito territorial, serán ejercidas por los órganos correspondientes de las CCAA. Las autoridades de control de las CCAA tienen plena independencia en el ejercicio de sus funciones (art. 41.1 LOPD); además, se determina que las CCAA pueden crear y mantener sus propios registros de ficheros para el ejercicio de sus competencias (art. 41.2 LOPD) y que el Director de la AEPD puede convocar regularmente a los órganos correspondientes de las CCAA a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. De igual manera, el Director de la AEPD y los órganos correspondientes de las CCAA pueden solicitarse mutuamente la información que sea necesaria para el cumplimiento de sus funciones (art. 41.3 LOPD).

Normativa reguladora de la Autoridad Catalana de Protección de Datos

A nivel autonómico, la normativa reguladora de la Autoridad Catalana de Protección de Datos (APDCAT) es el Estatuto de Autonomía de Cataluña (arts. 4.1, 15, 20, 23, 27, 28, 30, 31, 76, 78, 156, 182.3); la Ley 32/2010, de la Autoridad Catalana de Protección de Datos; y el Decreto 48/2003, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos. La APDCAT es una autoridad independiente, creada por la Ley 5/2002, de la Agencia Catalana de Protección de Datos, que desde su creación ha tenido una destacada evolución para garantizar el derecho a la protección de datos en el ámbito de las Administraciones públicas catalanas. Con la aprobación del Estatuto de Autonomía de 2006 se reconoce por primera en esa norma el derecho a la protección de datos y se fortalece el rol de la Autoridad catalana de control en materia de protección de datos. Entre las varias medidas adoptadas destaca que se establece su designación parlamentaria y que se cambia su denominación por la de Autoridad, con el objetivo de evitar la confusión de su naturaleza con el de otras entidades administrativas más instrumentales, que son conocidas como agencias.

Ámbito de actuación de la APDCAT

El ámbito de actuación de la APDCAT se determina en el artículo 3 de la Ley 32/2010 e incluye los ficheros y los tratamientos

de datos que se realizan en Cataluña por: a) Instituciones públicas. b) Administración de la Generalidad. c) Entes locales. d) Entidades autónomas, consorcios y demás entidades de derecho público vinculadas a la Administración de la Generalidad o a los entes locales, o que dependen de ellos. e) Entidades de derecho privado que cumplan los requisitos señalados en la Ley. f) Otras entidades de derecho privado que prestan servicios públicos en los ficheros y tratamientos vinculados a la prestación de esos servicios. g) Universidades públicas y privadas que integran el sistema universitario catalán, y los entes que de ellas dependen. h) Las personas físicas o jurídicas que cumplen funciones públicas con relación a materias que son competencia de la Generalidad o de los entes locales. Por último, i) Las corporaciones de Derecho público que cumplen sus funciones exclusivamente en el ámbito territorial de Cataluña.

Competencias de la APDCAT

En la misma Ley se establecen las competencias a la APDCAT que incluyen: registro, control, inspección, sanción, resolución y aprobación de propuestas, recomendaciones e instrucciones (art. 4). De igual forma, las funciones de la Autoridad catalana se regulan en el artículo 5 de la Ley 32/2010 y se pueden resumir en:

- Velar por el cumplimiento de la legislación de protección de datos y de la Ley 23/1998, de estadística de Cataluña, en lo referente a la recogida de datos estadísticos y al secreto estadístico, y adoptar las medidas correspondientes para garantizar las condiciones de seguridad de los ficheros constituidos con finalidades exclusivamente estadísticas, sin perjuicio de las competencias atribuidas al Instituto de Estadística de Cataluña.
- Resolver las reclamaciones de tutela respecto al ejercicio de los derechos ARCO.
- Promover la divulgación de los derechos de las personas con relación a la protección de datos y el acceso a la información, y la evaluación del impacto sobre la privacidad".
- Dictar las instrucciones y las recomendaciones en materia de protección de datos de carácter personal y de acceso a la información.
- Requerir (a los responsables del fichero o del tratamiento y a los encargados del tratamiento) la adopción de las medidas necesarias para la adecuación del tratamiento de los datos personales objeto de investigación a la legislación vigente en materia de protección de datos de carácter personal y, en su caso, ordenar el cese de los tratamientos y la supresión de los ficheros.
- Proporcionar información sobre los derechos de las personas en materia de tratamiento de datos personales.
- Atender las peticiones de información, las quejas y las denuncias.
- Decidir sobre las inscripciones de ficheros y el tratamiento de datos de carácter personal en el Registro de Protección de Datos de Cataluña; así como, tener conocimiento de los demás ficheros en que, a pesar de estar exentos del deber de inscripción en el Registro, la legislación vigente establezca un deber de comunicación a la autoridad de protección de datos.

– Ejercer las potestades de inspección y sanción.
– Elaborar planes de auditoría.
– Emitir informe, con carácter preceptivo, sobre los proyectos de disposiciones de carácter general de la Generalidad de creación, modificación o supresión de ficheros de datos de carácter personal, y sobre las disposiciones que afecten a la protección de datos de carácter personal.
– Emitir informe, con carácter potestativo, sobre los proyectos de disposiciones de carácter general de los entes locales de creación, modificación o supresión de ficheros, y sobre las disposiciones que tengan impacto en materia de protección de datos de carácter personal que los entes locales le sometan.
– Responder a las consultas que formulen las entidades de su ámbito de actuación sobre la protección de datos de carácter personal.
– Otorgar las autorizaciones para la exención del deber de información en la recogida de datos y para el mantenimiento íntegro de determinados datos, entre otras.
– Colaborar con la AEPD y con las demás agencias autonómicas.

2. ACCIÓN NORMATIVA

Instrucciones, recomendaciones y resoluciones

La acción normativa de la APDCAT se ha desarrollado en tres tipos de actuaciones: Instrucciones, Recomendaciones y Resoluciones. Entre las que destacan las siguientes: A) Instrucción 1/2009, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de video-vigilancia. B) Recomendaciones: 1. Recomendación 1/2008 sobre la difusión de información que contenga datos de carácter personal a través de Internet. 2. Recomendación 1/2010 sobre el encargado del tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña. 3. Recomendación 1/2011 sobre la creación, modificación y supresión de ficheros de datos de carácter personal de titularidad pública. 4. Recomendación 1/2013 sobre el uso del correo electrónico en el ámbito laboral. C. Resoluciones: 1. Resolución de 4 de abril de 2011, por la que se aprueba la modificación de los soportes normalizados para formalizar las inscripciones de los ficheros en el Registro de Protección de Datos de Cataluña y por la Resolución, de 6 de junio de 2016, por la que se modifican soportes normalizados para formalizar inscripciones en el Registro de Protección de Datos de Cataluña. 2. Resoluciones de aprobación de los ficheros de la Autoridad: 2.1. Resolución de 2 de noviembre de 2010, por la que se regulan los ficheros de datos de carácter personal de la Autoridad Catalana de Protección de Datos. 2.2. Resolución de 30 de enero de 2013, per la que se crea el fichero de datos de carácter personal; 2.3. Resolución de 18 de mayo de 2016, por la que se modifican ficheros de datos de carácter personal de la Autoridad Catalana de Protección de Datos. 3. Resolución de 26 de junio de 2015, por la que se crea la sede electrónica y el registro electrónico de la Autoridad Catalana de Protección de Datos.

3. PROCEDIMIENTOS DE GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS Y DE INSPECCIÓN Y SANCIÓN

Resoluciones de procedimientos sancionadores: infracciones leves, graves y muy graves

En 2016 la APDCAT realizó 44 Resoluciones de procedimientos sancionadores, con las que la APDCAT busca garantizar el derecho a la protección de datos. A continuación se relacionan estas resoluciones, en las que se declaró la comisión de una infracción (leve, grave o muy grave). El contenido íntegro de estas resoluciones está disponible en la web de la APDCAT.

RESOLUCIÓN del procedimiento sancionador núm. PS 21/2016, referente al Instituto de Seguridad Pública de Cataluña.	*Incorporar el NIF completo en la tarjeta identificativa que el alumnado debe llevar en un lugar visible mientras permanece dentro de las instalaciones y en las listas de calificaciones, cuando las personas afectadas ya están identificadas a través de otro dato personal, es un tratamiento excesivo que constituye una infracción grave. No informar debidamente a las personas afectadas en la recogida de sus datos constituye una infracción leve.*
RESOLUCIÓN del procedimiento sancionador núm. PS 14/2016, referente a una concejala del Ayuntamiento de…	*Una concejala no adscrita a ningún grupo de un Ayuntamiento accedió a un documento en ejercicio de sus funciones, y con posterioridad entregó una copia del documento a una tercera persona, sin consentimiento de la persona afectada -de quien constaban sus datos el documento- ni habilitación legal. Este hecho se considera una cesión ilegítima constitutiva de una infracción grave.*
RESOLUCIÓN del procedimiento sancionador núm. PS 15/2016, referente a la empresa Servicio de Enseñanza y Asesoramiento Deportivo, SA.	*El envío de correos electrónicos a múltiples destinatarios sin utilizar la herramienta de copia oculta, por parte de una empresa privada que gestiona instalaciones deportivas municipales, supone una infracción grave, en concreto la vulneración del deber de secreto. Al tratarse de un fichero/tratamiento de titularidad privada, resulta de aplicación el régimen sancionador general previsto en el art. 45 LOPD, si bien en el caso presente se dan las circunstancias que permiten la aplicación de la advertencia.*
RESOLUCIÓN del procedimiento sancionador núm. PS 16/2016, referente a Servicio de Enseñanza y Asesoramiento Deportivo, SA	*El envío por parte de una empresa privada que gestiona instalaciones deportivas municipales, de un correo electrónico que contiene datos de carácter personal relativos a terceras personas, sin el consentimiento de sus titulares y sin habilitación legal, supone una infracción grave, concretamente por vulneración del deber de secreto. Sin embargo, procede aplicar la rebaja de un grado en la multa impuesta, conforme al art. 45.5 LOPD.*
RESOLUCIÓN del procedimiento sancionador núm. PS 12/2016, referente al Instituto Catalán de la salud.	*No atender los requerimientos de medidas correctoras de la Autoridad formulados en el marco de un procedimiento sancionador es constitutivo de una infracción de carácter grave.*
RESOLUCIÓN del procedimiento sancionador núm. PS 13/2016, referente al Ayuntamiento de Cabrera de Mar.	*La difusión en Internet de fotografías de menores sin el consentimiento específico de los padres / madres o representantes legales de dichos menores a tal efecto, constituye una comunicación ilícita de datos personales. Las figuras de advertencia y rebaja de un grado del art. 45 LOPD no son aplicables a las infracciones cometidas en tratamientos de titularidad pública, a los que se aplica el régimen específico del art. 46 LOPD.*
RESOLUCIÓN del procedimiento sancionador núm. PS 6/2016, referente al Ayuntamiento de Santpedor.	*El Ayuntamiento recogió el teléfono móvil y la información sobre una queja que se había formulado por whatsapp sobre las molestias ocasionadas por unos vehículos presuntamente mal estacionados. El dato del número de teléfono y la queja las incluyó después la Policía Local en un acta que levantó por unos hechos detectados antes de la queja efectuada por whatsapp, todo ello sin informar al respecto de los extremos del art. 5 LOPD.*

RESOLUCIÓN del procedimiento sancionador núm. PS 9/2016, referente a la Corporación Sanitaria Parc Taulí.	*Facilitar a una tercera persona documentación que contiene datos relativos a la salud sin el consentimiento expreso y sin la concurrencia de una habilitación legal, es constitutiva de una infracción muy grave. Respecto la alegación de error en la comisión de los hechos, se recuerda la doctrina jurisprudencial sobre el principio de culpabilidad, y al respecto es suficiente que se haya actuado sin la diligencia necesaria.*
RESOLUCIÓN del procedimiento sancionador núm. PS 10/2016, referente a Parés Seixas, SL.	*Se declara la comisión de dos infracciones (1 leve y 1 grave), cometidas por una empresa que actuaba como encargada del tratamiento en el servicio de gestión de recobro de deudas, respecto al servicio de suministro de agua prestado por la entidad responsable del tratamiento. Por un lado, dicha empresa subcontrató a un tercero sin la autorización del responsable del tratamiento. Por otro, trató los datos del denunciante (que era el hijo del deudor, pero no el titular del contrato de suministro) sin su consentimiento y sin habilitación legal.*
RESOLUCIÓN del procedimiento sancionador núm. PS 7/2015, referente a la Dirección General de la Policía del Departamento de Interior de la Generalidad de Cataluña.	*Por un lado, con motivo de la notificación de un acto de un expediente disciplinario, se permitió al personal al que se encomendó la práctica de tal notificación el acceso al contenido del acto a notificar, lo cual se considera innecesaria para llevar a cabo simplemente la notificación. Por ello se declara que se produjo un tratamiento ilícito de datos especialmente protegidos, lo que constituye una infracción muy grave. Por otra parte, también en el mismo expediente disciplinario se intentó practicar la notificación de un acto en el domicilio de una persona diferente, que tenía los mismos apellidos que la persona expedientada y figuraba en un registro que se había consultado. Esta actuación constituye una vulneración del principio de calidad, en su vertiente de exactitud, lo cual está prevista como infracción grave.*
RESOLUCIÓN del procedimiento sancionador núm. PS 11/2016, referente al Ayuntamiento de Girona.	*El Ayuntamiento de Girona contrató a una empresa externa la gestión del cobro de las zonas reguladas de aparcamiento, lo que supone el acceso por parte de la empresa concesionaria a datos de carácter personal incluidos en ficheros del Ayuntamiento. En la documentación que rige la contratación administrativa no se contempla la totalidad de los extremos del artículo 12 de la LOPD, en concreto, no se detallan las medidas de seguridad que la concesionaria debe implementar, lo que es constitutivo de una infracción leve por falta de contrato de encargado. La matrícula de los vehículos tiene la consideración de dato de carácter personal. La empresa concesionaria tiene la condición de encargado del tratamiento, no sólo cuando accede a determinados datos que se encuentran previamente en poder del responsable del fichero, sino también en aquellos casos en que en cumplimiento del encargo realizado, los datos son recogidos por la concesionaria*
RESOLUCIÓN del procedimiento sancionador núm. PS 8/2016, referente al Ayuntamiento de Perafort.	*El Ayuntamiento notificó una resolución de alcaldía con su contenido íntegro a dos trabajadoras a las que se extinguía la relación laboral que tenían con esta entidad, revelando datos de las dos personas (nombre y apellidos, fecha extinción contrato trabajo, inicio preaviso y cuantía de indemnización), sin su consentimiento ni habilitación legal. Es por ello que se considera que se ha cometido una comunicación de datos ilícita, lo que está tipificada como infracción grave. Respecto de la alegación de error involuntario y falta de intencionalidad del Ayuntamiento, se recuerda la doctrina jurisprudencial sobre el principio de culpabilidad, y al respecto es suficiente que se haya actuado sin la diligencia necesaria.*
RESOLUCIÓN del procedimiento sancionador núm. PS 5/2016, referente a la Federación Catalana de Fútbol Sala.	*La difusión de datos personales en una asamblea / Pleno sin el consentimiento de los afectados ni habilitación legal, se califica como una comunicación de datos ilícita, constitutiva de infracción grave. Ante la alegación de falta de competencia de la Autoridad, se argumenta que a pesar de ser una entidad privada, el tratamiento de datos personales imputado efectuó en el marco del ejercicio de funciones públicas, y por lo tanto es competencia de esta Autoridad.*
RESOLUCIÓN del procedimiento sancionador núm. PS 2/2016, referente al Instituto Catalán de la salud.	*La pérdida de documentación que debería formar parte de la historia clínica constituye una vulneración de las medidas de seguridad necesarias y, por lo tanto una infracción grave. En la tramitación del procedimiento se ha evidenciado que en un momento determinado no se localizó la documentación, y el propio responsable manifestó que se había extraviado.*

RESOLUCIÓN del procedimiento sancionador núm. PS 3/2016, referente al Hospital Arnau de Vilanova, dependiente del Instituto Catalán de la Salud.	*La destrucción precipitada de parte de la Historia Clínica sin respetar los plazos de conservación de la documentación, constituye un tratamiento ilícito y, por tanto, una infracción grave. La entidad denunciada pone de manifiesto que al proceder a digitalizar la documentación física, sólo se hizo con respecto a una parte de esta documentación, habiendo eliminado el resto, por error.*
RESOLUCIÓN del procedimiento sancionador núm. PS 67/2015, referente al Instituto Manuel de Cabañas, del Departamento de Enseñanza.	*La publicación en el tablón de anuncios de un centro escolar de forma que queden accesibles a una pluralidad de personas, de un listado de alumnos identificados con su nombre y apellidos, con indicación de datos referentes a la salud, constituye un tratamiento ilícito de datos especialmente protegidos, y por lo tanto se declara la comisión de una infracción muy grave.*
RESOLUCIÓN del procedimiento sancionador núm. PS 58/2015, referente al Ayuntamiento de Vilagrassa.	*Permitir el acceso a un expediente administrativo en materia urbanística en el trámite de información pública es lícito, pero una vez finalizado el período correspondiente a este trámite ya no se debe permitir el acceso, porque de lo contrario se vulnera el principio de calidad en su vertiente de proporcionalidad -temporalidad-. Es por ello que se declara aquí una infracción grave, por vulneración del principio mencionado.*
RESOLUCIÓN del procedimiento sancionador núm. PS 60/2015, referente al Ayuntamiento de Manresa.	*La captación de imágenes mediante cámaras de personas en la vía pública es constitutiva de una infracción grave, al considerarse excesiva en relación a los fines perseguidos. No informar debidamente de la existencia de las cámaras mediante carteles colocados antes de entrar en el campo de visión de la cámara, es constitutivo de una infracción leve.*
RESOLUCIÓN del procedimiento sancionador núm. PS 61/2015. referente al Ayuntamiento de Manresa.	*Es necesaria la creación del archivo cuando se registran imágenes captadas a través de cámaras de videovigilancia con fines de control del tráfico, lo que es constitutivo de una infracción grave.*
RESOLUCIÓN del procedimiento sancionador núm. PS 53/2015, referente al Ayuntamiento de Torredembarra.	*La recogida y tratamiento de datos personales (geolocalización) a través de un sistema GPS incorporado a los aparatos de radiofrecuencia que utilizan los agentes de la Policía Local de un municipio, sin haber creado el fichero correspondiente, constituye una infracción de carácter grave. La recogida y tratamiento de dichos datos sin haber informado previamente a las personas afectadas, supone una vulneración del deber de informar. La no inclusión en el documento de seguridad de la recogida de los datos mediante el sistema referido, supone una infracción del principio de seguridad de los datos.*
RESOLUCIÓN del procedimiento sancionador núm. PS 59/2015, referente al Ayuntamiento de Torredembarra.	*El acceso por parte del personal administrativo adscrito a la concejalía de Gobernación de un Ayuntamiento, a todos los datos incluidos en el documento "novedades policiales" (que recoge todas las actuaciones diarias que lleva a cabo la Policía Local), supone una vulneración del principio de seguridad, dado que no se ha acreditado la necesidad de que el citado personal administrativo tenga que acceder a todo el documento íntegro para realizar sus funciones. 2) El envío mediante red pública de telecomunicaciones del documento de "novedades policiales" (que contiene datos que exigen un nivel alto de medidas de seguridad), sin cifrar, supone una vulneración al principio de seguridad. 3) El almacenamiento del documento "novedades policiales" en formato papel, en salas no dotadas de sistemas de cierre adecuados, supone una vulneración del principio de seguridad.*
RESOLUCIÓN del procedimiento sancionador núm. PS 44/2015, referente a Ferrocarril Metropolitano de Barcelona, SA.	*Se declara la infracción grave de vulneración del deber de secreto, para remitir a una pluralidad de trabajadores un correo electrónico con datos sobre una persona trabajadora concreta, sin que estuviera justificado. Por otra parte, se declara también la infracción grave de vulneración del principio de seguridad, porque la configuración de una herramienta informática permitía que todos los usuarios accedieran a datos personales que no eran necesarios para el ejercicio de sus funciones.*

RESOLUCIÓN del procedimiento sancionador núm. PS 54/2015, referente al Ayuntamiento de...	*El acceso por parte de un agente a datos personales que figuran en los archivos de la Dirección General de la Policía -al que tiene acceso dada su condición de agente- constituye un tratamiento ilícito cuando este acceso no tiene relación con las actuaciones policiales.*
RESOLUCIÓN del procedimiento sancionador núm. PS 56/2015, referente a la Escuela Oficial de Idiomas Barcelona-Vall d'Hebron.	*La difusión por internet -sin ningún tipo de restricción- de datos personales sobre las que recae el deber de secreto constituye una infracción de la LOPD aunque la difusión por parte del órgano responsable no haya sido producida intencionadamente.*
RESOLUCIÓN del procedimiento sancionador núm. PS 40/2015.	*Permitir el acceso a un documento con datos personales a terceros no autorizados vulnera el deber de secreto, la cual constituye una infracción grave.*
RESOLUCIÓN del procedimiento sancionador núm. PS 50/2015, referente al Ayuntamiento de Castell-Platja d'Aro.	*Se imputa comunicación ilícita porque policía local levantó formulario denuncia por infracción ordenanza con datos de 2 personas que según la denunciante no tienen nada que ver, de tal manera que al dar copia del acto a ambas están revelando datos personales a un tercero.*
RESOLUCIÓN del procedimiento sancionador núm. PS 47/2015, referente al Ayuntamiento de Torredembarra.	*Se declaran tres infracciones, todas ellas relacionadas con la instalación de un sistema de videovigilancia en la sede de la Policía Local del municipio. En primer lugar, se declara una infracción por falta de creación de archivo, ya que aunque se había aprobado la disposición de creación del fichero de videovigilancia, esta no se había publicado en el boletín oficial correspondiente. En segundo lugar, se declara una vulneración del deber de informar dado que, por una parte, se habían captado imágenes sin haber instalado los preceptivos carteles informativos, y, por otra parte, no se había informado mediante otros canales explicitados la instrucción 1/2009. Y, en tercer lugar, se declara una vulneración principio proporcionalidad para la captación ininterrumpida -y posterior almacenamiento- de imágenes del interior de las celdas de detenidos.*
RESOLUCIÓN del procedimiento sancionador núm. PS 42/2015, referente a Seguridad Profesional Mediterránea, SA.	*Procede el sobreseimiento cuando no se puede descartar que la captación ilícita de las imágenes se hubiera producido una vez la infracción ya estuviera prescrita cuando se notificó el acuerdo de inicio del presente procedimiento sancionador; y cuando no se puede acreditar de manera suficiente la comisión de los hechos imputados, relativos a la modificación del campo de visión de una de las cámaras para captar imágenes de personas en la vía pública.*
RESOLUCIÓN del procedimiento sancionador núm. PS 45/2015, referente al Instituto Catalán de la Salud.	*En primer lugar, se considera que la entidad imputada habría vulnerado el principio de confidencialidad de los datos, ya que varias personas que prestaban servicio a la entidad accedieron a la historia clínica de la persona denunciante sin que este acceso estuviera justificado por ninguna razón asistencial. En segundo lugar, la entidad vulneró la medida de seguridad relativa al registro de accesos, por falta de auditorías periódicas en relación con dicho registro.*
RESOLUCIÓN del procedimiento sancionador núm. PS 52/2015, referente al ALTHAIA Red Asistencial Universitaria de Manresa.	*El acceso a la historia clínica de una persona, sin su consentimiento y sin que este acceso esté justificado por ninguna razón asistencial, supone una vulneración del principio de confidencialidad de los datos. No se aplica en este caso la figura del advertencia dadas las circunstancias concurrentes.*
RESOLUCIÓN del procedimiento sancionador núm. PS 51/2015, referente al Ayuntamiento de Salou.	*No atender los requerimientos de la Autoridad es constitutivo de una infracción de carácter grave.*
RESOLUCIÓN del procedimiento sancionador núm. PS 62/2015, referente al Ayuntamiento de L'Ametlla del Vallès.	*Facilitar el acceso a datos personales a una persona no autorizada vulnera el deber de secreto y es constitutivo de una infracción grave. La falta de notificación de la inscripción y supresión de ficheros en el Registro de Protección de Datos de Cataluña, dependiente de la Autoridad, es constitutivo de una infracción leve.*

RESOLUCIÓN del procedimiento sancionador núm. PS 4/2016, referente al Ayuntamiento de Gavà.	*La publicación de datos personales de dos agentes policiales sobre infracciones disciplinarias en anuncio en el BOE (en un caso después de haberse notificado personalmente el acto publicado) se considera un tratamiento ilícito de datos personales del art. 7.5 de la LOPD.*
RESOLUCIÓN del procedimiento sancionador núm. PS 46/2015, referente al Centro Educativo de Infantil y Primaria Escuela San Jorge de Bonmatí, del Departamento de Enseñanza de la Generalidad de Cataluña.	*La difusión en Internet de vídeos de los alumnos sin el consentimiento específico de los progenitores para la difusión de la voz, constituye una comunicación ilícita de datos personales. Por otra parte, el hecho de mantener publicado durante el curso escolar 2015-2016 material gráfico relativos a los cursos de 2011 a 2014, constituye una vulneración del principio de calidad de datos personales.*
RESOLUCIÓN del procedimiento sancionador núm. PS 64/2015, referente al Ayuntamiento de Barcelona.	*Permitir el acceso al expediente durante el trámite de información pública es lícito, pero no si se permite el acceso una vez ya había finalizado el trámite de información pública, lo que vulnera el principio de calidad en su vertiente de proporcionalidad -temporalidad-, y por tanto se imputa infracción grave.*
RESOLUCIÓN del procedimiento sancionador núm. PS 48/2015, referente al Organismo de Gestión Tributaria de la Diputación de Barcelona.	*La notificación en sobre abierto, dejada en el local del destinatario constituye una vulneración del deber de secreto.*
RESOLUCIÓN del procedimiento sancionador núm. PS 49/2015, referente al Consejo Comarcal del Baix Empordà.	*El intento de notificación en un domicilio incorrecto, así como la notificación edictal indicando nombre, apellidos y NIF completo de la persona afectada, constituyen un tratamiento de datos con conculcación de los principios y garantías del artículo 4 de la LOPD una vulneración del deber de secreto.*
RESOLUCIÓN del procedimiento sancionador núm. PS 55/2015, referente al Ayuntamiento de Cardedeu.	*Se imputa al Ayuntamiento una infracción grave por la comunicación de la identidad relativa a una persona, al titular del establecimiento respecto el que había formulado una queja, acción que no dio lugar al procedimiento en que se efectuó dicha revelación, el cual se había iniciado a instancia del propio establecimiento. Dicha comunicación de datos no estaría habilitada para la LRJPAC. Se imputa también la vulneración del deber de información en la recogida de datos de la persona que hizo la queja.*
RESOLUCIÓN del procedimiento sancionador núm. PS 57/2015, referente al Instituto Catalán de la salud.	*Incluir en el calendario laboral una anotación del motivo por el que un empleado no presta servicios en un determinado turno es un tratamiento de datos personales no adecuado, no pertinente y excesivo en relación a la finalidad para las que se han recogido y constituye una infracción grave.*
RESOLUCIÓN del procedimiento sancionador núm. PS 43/2015, referente a la Diputación de Barcelona.	*La publicación por edictos, tanto en el BOP como en el tablón de edictos, de una resolución íntegra que contara datos excesivos, es constitutivo de una infracción grave.*
RESOLUCIÓN del procedimiento sancionador núm. PS 41/2015, referente al Instituto Municipal de Hacienda del Ayuntamiento de Barcelona.	*Comunicar datos especialmente protegidos relativos a la comisión de infracciones es constitutivo de una infracción grave. El consentimiento tácito también debe ser inequívoco.*
RESOLUCIÓN del procedimiento sancionador núm. PS 38/2015, referente al Ayuntamiento de Sallent.	*Vulneración del principio de seguridad, dado que mediante el aplicativo que gestiona la correspondencia que registra el Ayuntamiento, se posibilita que todas las personas que son usuarias puedan acceder a documentación que no es necesaria para ejercer sus funciones.*

RESOLUCIÓN del procedimiento sancionador núm. PS 39/2015, referente al Ayuntamiento de Lleida.	*El acceso a una sentencia no anonimizada enviada por correo electrónico y expuesto en un mostrador por parte de usuarios del responsable del fichero no autorizado, vulnera el deber de secreto y es constitutivo de una infracción grave.*
RESOLUCIÓN del procedimiento sancionador núm. PS 27/2016.	*El hospital cedió datos especialmente protegides (salud) a un tercero (Centro de ortopéida), sin acreditar la existència del consentimiento expreso de la paciente ni habilitación legal suficiente, lo que se considera una infracción muy graves por tratamiento ilícito (cesión) de datos especialmente protegides. La persona afectada tuvo conocimiento de los hechos cuando en la habitación en la que estaba hospitalizada se personó una empleada del Centro de Ortopedia para ofrecerle sus productos, con una hoja en la que constaban datos personales de la paciente.*

4. COOPERACIÓN CON OTRAS INSTITUCIONES PÚBLICAS Y CON LA SOCIEDAD

Dictámenes e informes

Una de las principales actividades de cooperación de la ADPCAT para con otras instituciones públicas y con la sociedad civil se realiza a través de sus Dictámenes e Informes (134 en 2016) con los cuales, al resolver las consultas que recibe, la ADPCAT contribuye al fomento de la autorregulación y facilita el debido cumplimiento de la Ley. En 2016 la Autoridad emitió 83 dictámenes en relación a cuestiones como las comunicaciones de datos, difusión de imágenes o implantación de sistemas de videovigilancia. A continuación se señalan algunos de especial interés.

Videovigilancia en centro residencial

– CNS 77/2016. Videovigilancia en un centro residencial de acción educativa. La memoria del sistema de videovigilancia del CRAE sometida a análisis no contiene elementos de juicio suficientes que permitan establecer si el tratamiento de imágenes pretendido en el presente caso resultaría proporcionado a la finalidad de seguridad perseguida. La utilización de este sistema, en su vertiente de control laboral, podría resultar adecuada al principio de proporcionalidad, siempre que se reunieran los requisitos expuestos en el dictamen.

Notificación edictal de expedientes sancionadores de menores

– CNS 71/2016. Notificaciones por edictos en expedientes sancionadores relativos a menores de edad. La publicación por edicto de un anuncio en el boletín oficial correspondiente (BOP), relativo a un expediente sancionador, sin consentimiento de la persona afectada, especialmente si ésta es menor de edad, resultaría ajustada a la normativa de protección de datos si incluye, únicamente, la información mínima necesaria (art. 46 LPAC y art. 58.5 Ley 26/2010). En concreto, el anuncio podría incluir el nombre y apellidos de las personas afectadas y las cuatro últimas cifras del DNI, evitando indicar que la notificación se refiere a un expediente sancionador, a las Ordenanzas relacionadas con la infracción, y a la concreta infracción cometida.

Utilización de Microsoft Office 365 en la universidad

– CNS 60/2016. Utilización del producto Microsoft Office 365 con los colectivos de una universidad. Teniendo en cuenta la Decisión de la Comisión de 5 de febrero de 2010, la Resolución de la AEPD de 9 de mayo de 2014, así como la adhesión de Microsoft al Escudo de Privacidad (Privacy Shield), se pue-

de considerar que el contrato de encargo del tratamiento que podría suscribir la universidad con Microsoft en relación con los servicios "Microsoft 365" y "Microsoft Azure", seguiría en principio ajustándose a las exigencias de la normativa de protección de datos (LOPD, RLOPD y RGPD). En cuanto a las medidas de seguridad técnicas y organizativas para garantizar la seguridad de los datos, se puede considerar que las previsiones de Microsoft en relación con los servicios "Microsoft 365" y "Microsoft Azure" pueden ser, a priori, adecuadas a lo que prevé la normativa de protección de datos teniendo en cuenta que la implantación de las medidas previstas es objeto de certificación y auditoría por parte de un tercero independiente.

Sistemas de mensajería instantánea

– CNS 55/2016. Uso de los sistemas de mensajería instantánea. Las administraciones públicas deben asegurarse de que los terceros prestadores de servicios y de sistemas de comunicación cumplen sus responsabilidades, ya sea como encargados del tratamiento o, en su caso, como responsables del tratamiento de los datos de los usuarios (en el caso los SMI), dado que el tratamiento se encuentra sometido a las exigencias de los principios y garantías de la normativa europea de la protección de datos (LOPD, RLOPD, y RGPD). Cuando consideren la elección de un determinado sistema de mensajería instantánea (SMI) deberían tener en cuenta, especialmente, el fin de la comunicación, la información personal que hay que tratar; el consentimiento de los afectados; el modelo de seguridad y la evaluación de impacto y las concretas medidas de seguridad aplicadas; los mecanismos de certificación; las transferencias internacionales de datos y la ubicación de los servidores; el derecho de información y la transparencia, en atención a las previsiones de la normativa europea de protección de datos.

Whatsapp y Spotbros en las comunicaciones abogado-cliente

– CNS 24/2013. Utilización de Whatsapp y Spotbros en las comunicaciones abogado-cliente. En relación con el tratamiento de datos de los usuarios de Whatsapp y de Spotbros situados en España, resultan aplicables los principios y garantías de la LOPD. Sin perjuicio de la responsabilidad sobre el tratamiento de los datos de los usuarios de las apps que pueda corresponder a las respectivas empresas (Whatsapp y Spotbros), el abogado tiene un grado de responsabilidad específico respecto al tratamiento de los datos de sus clientes, que incluye la elección de los canales de comunicación más adecuados con sus clientes. Tanto Whatsapp como Spotbros explicitan en la información de las respectivas páginas web que no pueden garantizar la seguridad de la información enviada utilizando las respectivas apps. Teniendo en cuenta esto, junto con varias vulnerabilidades detectadas, y dado que en el contexto de la relación entre abogado y clientes puede ser habitual la comunicación y tratamiento de datos sensibles (artículo 7 LOPD), la utilización de las aplicaciones de Whatsapp y de Spotbros no resulta recomendable, en relación con la seguridad exigida por la LOPD y el RLOPD.

– CNS 53/2016. Adecuación a la normativa de protección de datos de un modelo de consentimiento informado relativo a la participación en un programa de identificación genética. Se valora positivamente la formalización del consentimiento, expreso y por escrito, previo e informado de las personas que decidan participar en el programa de identificación genética, a través de la cumplimentación del documento de consentimiento informado, sin perjuicio de algunas consideraciones.

Modelo de consentimiento informado

– CNS 51/2016. Posibilidad de poner en funcionamiento un sistema de alarma de personas asociadas a determinados comportamientos. Desde el punto de vista del derecho a la protección de datos de carácter personal, la configuración del sistema de alarma descrito en la Memoria no se adecua a los principios de proporcionalidad y de minimización, por lo que sería recomendable implantar sistemas alternativos que pueden dar respuesta adecuada a la finalidad pretendida, sin poner en riesgo el correcto cumplimiento de los principios y garantías de la normativa de protección de datos personales.

Sistema de alarma de personas asociado a determinados comportamientos

– CNS 48/2016. Uso de dispositivos GPS en los vehículos policiales del Ayuntamiento. El uso de dispositivos GPS en los vehículos policiales conlleva el tratamiento de datos personales y, por tanto, está sometido a la normativa de protección de datos personales. Si el tratamiento se lleva a cabo para asegurar el normal funcionamiento del servicio, el Ayuntamiento no necesitaría disponer del consentimiento previo de los afectados, pero sí que debería cumplir el deber de información y la obligación de creación (o modificación) y notificación del archivo que contenga los datos de geolocalización.

Dispositivos GPS en vehículos de la policía local

– CNS 44/2016. Solicitud de un certificado en el Registro Central de Delincuentes Sexuales presumiendo el consentimiento de los afectados. Es necesario el consentimiento expreso de los afectados (como se desprende del artículo 9.2 RD 1110/2015, en conexión con el artículo 7.3 LOPD) para que una Administración pública, en este caso, la Institución sanitaria que formula la consulta, pueda solicitar al RCDS el certificado por delitos de naturaleza sexual, de modo que no se puede considerar que el artículo 28.2 de la LPACAP habilite la solicitud de certificación al RCDS presumiendo el consentimiento de los afectados.

Certificados del Registro Central de Delincuentes Sexuales

– CNS 31/2016. Donación y conservación del fondo documental de una asociación. En atención al régimen de comunicación de datos (art. 11.2.a) LOPD), a la normativa archivística (LA) y en la normativa reguladora de colegios profesionales (Ley 2/1974, y Estatutos del Colegio), hay suficiente habilitación para comunicar el fondo documental al colegio que, como responsable, deberá determinar qué datos pueden ser conservados para la finalidad histórica, estadística o científica prevista. En cuanto a la exención del deber de informar (artículo 5.5 LOPD), en relación con el traspaso del fondo documental, esta Autoridad deberá valorar las circunstancias del caso en el momento que el colegio solicite la autorización correspondiente.

Fondo documental de una asociación

Resultados de controles sanitarios en restaurantes y bares

– CNS 27/2016. Denegación de acceso a información sobre los resultados de las inspecciones y controles sanitarios y de higiene realizados en restaurantes y bares de una ciudad. La normativa de protección de datos no impediría el acceso a la información desglosada por nombre y dirección de establecimiento relativa a la puntuación o nivel obtenido en los controles e inspecciones en materia sanitaria y de higiene realizadas en bares y restaurantes, sin perjuicio de que puedan concurrir otros límites que imposibiliten el acceso a esta información. En cambio, el acceso a los datos relacionados con incumplimientos, infracciones o sanciones administrativas la responsabilidad recaiga en las personas físicas titulares de los establecimientos, no resultaría respetuoso con el derecho a la protección de datos.

Borrado de datos de teléfono móvil

– CNS 19/2016. Entrega de un teléfono móvil a la persona que lo encontró. La entrega de un teléfono móvil a la persona que lo encontró, transcurrido el plazo legal establecido para que su propietario lo reclame, sólo podría efectuarse previo borrado definitivo de los datos que pudiera conservar y siempre que se garantizara que no es posible acceder a los datos almacenados remotamente.

Acceso a la historia clínica

– CNS 15/2016. Posibilidad de conocer la identidad de las personas que han accedido a la historia clínica. Dada la configuración del derecho de acceso en la normativa de protección de datos (arts. 15 LOPD y 27 RLOPD), el responsable tiene la obligación de informar al afectado, entre otros, de las "comunicaciones efectuadas o que se prevén hacer". Por lo tanto, el derecho de acceso no incluye la información sobre los accesos que se hayan podido producir por parte del personal propio de la entidad. Facilitar la información referida a los accesos del personal propio del centro a la HC, cuando así lo reclama el afectado, puede suponer un ejercicio de transparencia, que estaría amparado por la legislación de autonomía del paciente, y que puede conllevar el efecto positivo de transmitir al afectado un mayor grado de confianza en la buena praxis del centro, respecto al tratamiento que este ha realizado de los datos de la HC.

Localización de viviendas vacías e identificación de los propietarios

– CNS 14/2016. Localización de viviendas vacías e identificación de los propietarios a partir del consumo de agua. El artículo 41 de la LDH sólo habilita, a falta del consentimiento de los afectados, la comunicación al Ayuntamiento de los datos de los consumos de agua a los efectos de constatar la situación de desempleo (artículo 41.5 LDH), si el Ayuntamiento ya ha detectado previamente la existencia de determinados viviendas desocupadas en el municipio a través de los sistemas explicitados en el artículo 41.4 LDH, o a través de otros mecanismos que se hayan podido establecer.

Disociación de datos personales en documentos en la web municipal

– CNS 10/2016. Criterios de disociación de datos personales de los documentos que se publican en la web municipal. Para anonimizar o disociar la información hay que eliminar aquellos datos que permitan identificar a la persona afectada, directa o indirectamente, en términos razonables, es decir, sin esfuerzos

desproporcionados. Al mismo tiempo, la disociación no debería eliminar elementos o información que hagan inviable la comprensión de la información de conjunto. Esta doble condición conllevará que el Ayuntamiento tenga que hacer una valoración o ponderación respecto qué sistema de disociación puede ser más efectivo en cada caso, en los términos que se apuntan en este dictamen.

Fotografías de actos organizados en el municipio

– CNS 9/2016. Captación y posterior publicación de fotografías de diferentes actos organizados en el municipio. La LO 1/1982 habilita la captación, a través de fotografías, de la imagen de personas identificables que aparece como meramente accesoria en diferentes actos organizados en el municipio para su posterior difusión en una revista, con fines divulgativos o informativos del acto público en cuestión. En atención al superior interés del menor, la difusión legítima en Internet de fotografías de menores efectuadas durante la celebración de actos realizados en la guardería municipal debería limitarse a las personas de la comunidad educativa, a través de la implantación de mecanismos de identificación y autenticación.

Grabación de las conversaciones del equipo de gobierno municipal

– CNS 2/2016. Grabación por parte de los ciudadanos de las conversaciones mantenidas con miembros del equipo de gobierno municipal. La grabación de la conversación de un miembro del equipo de gobierno por un ciudadano en principio requiere el consentimiento previo del afectado. Ahora bien, podría estar legitimado si se hace con el fin de utilizarlo con ocasión de la exigencia de responsabilidades. La difusión, sin consentimiento, de esta conversación podría estar legitimada cuando la información registrada sea veraz, tenga relevancia pública dada la materia objeto de la información o bien la persona implicada, y resulte proporcionada al interés general que justifica su difusión.

Guías básicas

Por otra parte, esta Autoridad también elaboró tres documentos que se deben subrayar: a) Guía básica de protección de datos para los entes locales (2012); b) Guía básica de protección de datos para los colegios profesionales (2014); y, c) Guía básica de protección de datos para los centros educativos (2015). De igual manera, la ADPCAT mantiene abierto un foro de debate sobre el desarrollo de las ciudades inteligentes (Smart cities) y sus implicaciones sobre la información de carácter personal de la ciudadanía, desde el que se pretende apoyar a las Administraciones públicas de Cataluña que quieren implantar los servicios de las Smart Cities y a las empresas que llevan a cabo el diseño y la implantación de esas tecnologías.

5. OTRAS ACTIVIDADES

Promoción y sensibilización

En actividades de promoción y sensibilización sobre el derecho a la protección de datos personales, en 2016 la APDCAT organizó las siguientes jornadas y eventos: "El nuevo papel de los responsables del tratamiento: hacia un nuevo modelo basado en la responsabilidad"; "Foro de la Seguridad: La seguridad de la información en el Regla-

mento Europeo de Protección de Datos"; "La revisión de los principios de la protección de datos en un entorno sin fronteras"; "Principales novedades del Reglamento General de Protección de Datos"; "El nuevo Reglamento: un reto para las empresas"; "Internet y los menores"; Proyecto ARCADES: mejores prácticas de educación en protección de datos y privacidad; "Jornada: Privacidad y Geolocalización"; "La protección de la privacidad a través de las decisiones del Tribunal Europeo de Derechos Humanos y de la APDCAT"; "Festival de la infancia".

Ciclo de conferencias con el Colegio de la Abogacía de Barcelona

Por otra parte, es destacable, el Ciclo de Conferencias organizado por la APDCAT, en colaboración con el Ilustre Colegio de la Abogacía de Barcelona, con el fin de acercar el RGPD a las entidades y facilitar su adaptación al mismo. Este ciclo se inició en 2016 y ha finalizado en el 2017 realizándose un análisis de las principales novedades del Reglamento. En concreto ha estado formado por las siguientes conferencias: Principales novedades del Reglamento General de Protección de Datos, La revisión de los principios de la protección de datos en un entorno sin fronteras, El nuevo papel de los responsables del tratamiento: Hacia un nuevo modelo basado en la responsabilidad, Los derechos de las personas en el nuevo Reglamento General de Protección de Datos y, la última que trató sobre las Garantías para una protección efectiva del derecho a la protección de datos.

Premio de Protección de Datos en el Diseño

Con el objetivo de potenciar el compromiso de las entidades públicas y privadas con la privacidad, la APDCAT concede anualmente (desde 2013) el Premio de Protección de Datos en el Diseño. Este premio reconoce las aplicaciones y las soluciones tecnológicas que suponen una aportación relevante para la protección de la privacidad en el momento de diseñar las aplicaciones. En definitiva, se trata de premiar las aplicaciones o sistemas que mejoren la implementación de las medidas de seguridad, faciliten el cumplimiento de las obligaciones legales en materia de protección de datos, refuercen el control de las personas sobre su propia información y en general, faciliten la gestión de la privacidad. En este sentido, para dotar de un mayor reconocimiento a dichas aplicaciones y soluciones tecnológicas, la convocatoria vigente de la quinta edición del Premio de Protección de Datos en el Diseño incluye una dotación económica.

VII. ESPAÑA: AGENCIA VASCA DE PROTECCIÓN DE DATOS

1. INTRODUCCIÓN

Creación de la Agencia Vasca de Protección de Datos

Conforme se señaló anteriormente, en España la protección de datos de carácter personal está desarrollada en la LOPD que regula los aspectos básicos del régimen jurídico de la AEPD. La Agencia Vasca de Protección de Datos (AVPD), se crea mediante la Ley 2/2004, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, que posteriormente es desarrollada en el Decreto 308/2005 donde se regulan los procedimientos que se tramitan por la AVPD. El mismo año, se aprueba el Estatuto de la Agencia Vasca de Protección de Datos en el Decreto 309/2005. La AVPD tiene competencia sobre los ficheros de datos de carácter personal creados o gestionados, para el ejercicio de potestades de derecho público, por: "a) La Administración General de la Comunidad Autónoma, los órganos forales de los territorios históricos y las administraciones locales del ámbito territorial de la Comunidad Autónoma del País Vasco, así como los entes públicos de cualquier tipo, dependientes o vinculados a las respectivas administraciones públicas, en tanto que los mismos hayan sido creados para el ejercicio de potestades de derecho público. b) El Parlamento Vasco. c) El Tribunal Vasco de Cuentas Públicas. d) El Ararteko. e) El Consejo de Relaciones Laborales. f) El Consejo Económico y Social. g) El Consejo Superior de Cooperativas. h) La Agencia Vasca de Protección de Datos. i) La Comisión Arbitral. j) Las corporaciones de derecho público, representativas de intereses económicos y profesionales, de la Comunidad Autónoma del País Vasco. k) Cualesquiera otros organismos o instituciones, con o sin personalidad jurídica, creados por ley del Parlamento Vasco, salvo que ésta disponga lo contrario" (art. 2.1 Ley 2/2004).

Funciones de la AVPD

Las funciones de la AVPD, como autoridad de control de los ficheros antes señalados, están establecidas en el artículo 17.1 de su Ley de creación y se pueden resumir en:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación.
b) Emitir las autorizaciones previstas en las leyes y reglamentos.
c) Dictar las instrucciones precisas para adecuar los tratamientos a la legislación vigente.
d) Atender las peticiones y reclamaciones formuladas por los afectados.
e) Proporcionar información a los titulares de derechos sobre el tratamiento de los datos de carácter personal.

f) Requerir a los responsables y a los encargados de los tratamientos la adecuación del tratamiento de datos a la legislación y ordenar la cesación de los tratamientos y la cancelación de los ficheros cuando no se ajuste a la legislación.
g) Ejercer la potestad sancionadora; proponer la iniciación de procedimientos disciplinarios; y, adoptar las medidas cautelares que procedan.
h) Informar los proyectos de disposiciones generales que desarrollen la Ley 2/2004.

Funciones de la AVPD

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.
j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal.
k) Redactar una memoria anual y remitirla a la Vicepresidencia del Gobierno Vasco.
l) Velar por el cumplimiento de las disposiciones que la legislación sobre la función estadística pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos.
m) Colaborar con la AEPD y entidades similares de otras CCAA para una mejor protección de la seguridad de los ficheros de datos de carácter personal y de los derechos de los ciudadanos en relación con los mismos.
n) Atender a las consultas que en materia de protección de datos de carácter personal de su competencia.

2. PLANIFICACIÓN

Plan Estratégico de la AVPD

La actividad anual de la AVPD está concebida en su Plan Estratégico donde se identifican las metas y los objetivos estratégicos que anualmente se aprueban en el Plan de Gestión. El Plan Estratégico de la AVPD fue reelaborado en 2012 y se aplicó hasta 2015, estando prevista su revisión desde 2016. Con la revisión del Plan Estratégico de la AVPD en 2016 se busca fortalecer el trabajo de la AVPD en torno a los siguientes cuatro ejes y sus respectivos objetivos:

Ciudadanía

– Eje: Ciudadanía. Lograr que la ciudadanía pueda ejercer su derecho a la protección de los datos y que conozca su derecho, para lo cual se propone los siguientes objetivos: 1. Aumentar el grado de conocimiento del derecho a la protección de datos personales. 2. Facilitar ejercicio del derecho de forma sencilla y práctica. 3. Aumentar el grado de conocimiento de la labor de la AVPD como garante de la protección de datos personales.

Administraciones públicas

– Eje: Administraciones públicas. Lograr que las Administraciones den cumplimiento al derecho. Objetivos: 1. Mejorar la garantía del derecho por parte de las Administraciones públicas. 2. Fomentar acciones preventivas de la AVPD, en colabo-

ración con las Administraciones públicas en proyectos emergentes. 3. Difundir el conocimiento de Buenas Prácticas en las Administraciones y enfoque proactivo en concienciación y capacitación.

Aliados estratégicos

– Eje: Aliados estratégicos. Disponer de alianzas estratégicas que ayuden en la consecución de los objetivos de la AVPD para lo cual se pretende: 1. Definir y revisar el marco de alianzas estratégicas. 2. Establecer y mantener las alianzas estratégicas necesarias.

Organización interna

– Eje: Organización interna. Mejorar e innovar en la gestión y el desarrollo profesional de la personas de la AVPD: 1. Mejorar la actividad permanente de la AVPD. 2. Aumentar el uso eficiente de los recursos económicos y materiales de la AVPD. 3. Consolidar una plantilla satisfecha, capacitada e implicada en la AVPD.

3. ACCIÓN NORMATIVA

Resoluciones principales

En cuanto a la acción normativa de la AVPD son cuatro sus Resoluciones principales. Dos de ellas tratan de su organización interna: Resolución de 28 de noviembre de 2005, del Director, por la que se desarrolla la estructura orgánica de la AVPD y, Resolución de 17 de junio de 2013, de modificación de la anterior. Otras dos Resoluciones establecen los procedimientos para los ficheros en el Registro de Protección de Datos y sobre los procedimientos sancionadores: Resolución de 31 de octubre de 2014, del Director de la AVPD, por la que se establecen los modelos normalizados y los medios por los que debe procederse a la solicitud de las inscripciones de creación, modificación o supresión de ficheros en el Registro de Protección de Datos de la Agencia Vasca de Protección de Datos y, Resolución del mismo Director, por la que se fija el sistema objetivo de turno para la designación de instructor en los procedimientos de infracción o sancionadores que tramite esta Agencia.

4. PROCEDIMIENTOS DE GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS

Dictámenes para la garantía del derecho a la protección de datos

En el período comprendido entre el 1 de enero de 2016 y el 31 de diciembre del mismo año, la AVPD emitió varios Dictámenes para la garantía del derecho a la protección de datos. En la mayoría de los casos los Dictámenes fueron previamente solicitados en consultas realizadas por las Administraciones públicas y son los siguientes:

Datos de personas fallecidas

– Acceso a expedientes de colegiados fallecidos del Colegio Oficial de Enfermería, de 21 de diciembre de 2016. En el cual la AVPD estableció que: "las normas de la Ley Orgánica 15/1999 no serían directamente aplicables a los tratamientos de datos de carácter personal referidos exclusivamente a personas fallecidas, de las que no puede predicarse el derecho fundamental a la protección de datos".

Huella digital como medio de fichaje

– Implantación de la huella digital como medio de fichaje, de 19 de diciembre de 2016. Dictamen en el que la AVPD consideró que el tratamiento de los datos biométricos de los trabajadores, con la finalidad de control de acceso, era adecuado a la normativa en materia de protección de datos.

Cesión de datos en ficheros de la policía local

– Cesión de datos obrantes en ficheros de la policía local a un tercero perjudicado, de 22 de noviembre de 2016. En este caso se determinó que: "cuando proceda la comunicación solicitada deberá realizarse el juicio ponderativo correspondiente, de tal modo que únicamente se cedan los datos adecuados, pertinentes y no excesivos, teniendo en cuenta la finalidad perseguida con ese tratamiento".

Cancelación de datos por revocación del consentimiento

– Cancelación de datos personales por revocación del consentimiento, de 16 de septiembre de 2016. En este Dictamen se debe subrayar que la AVPD estableció que "al igual que el consentimiento del interesado ha de ser una manifestación de voluntad, libre, inequívoca, específica e informada mediante la que el mismo consienta el tratamiento de datos que le conciernen [art. 3 h) LOPD], la revocación del consentimiento ha de tener esos mismos atributos, de forma que el interesado sea consciente de las consecuencias que la revocación del consentimiento pueda tener en su esfera jurídica".

Cesión a grupo político de copia nominal de la plantilla de entes forales

– Cesión al grupo juntero del PP de la copia nominal de la plantilla de diversos entes forales, de 8 de septiembre de 2016. En este caso la AVPD señaló que: "la cesión de la información requerida por el Grupo Juntero estará legitimada siempre que sea adecuada para el efectivo cumplimiento de su labor parlamentaria. Por el contrario, el tratamiento de esa información para finalidades ajenas al ejercicio de esa función legítima contravendría el derecho fundamental a la privacidad de las personas afectadas".

Cámaras en vehículos privados

– Instalación de cámaras en vehículos privados, de 29 de julio de 2016. En este Dictamen se determinó que: "la utilización de cámaras por particulares con fines de vigilancia en la vía pública, con independencia de que se realice desde un vehículo, una bicicleta, un dron, corriendo o caminando, no tiene encaje en la tan citada excepción; la vigilancia de la conducta ajena mediante cámaras no es algo subsumible en el ámbito particular, familiar o de amistad, tanto es así, que cuando se realiza afectando a la vía pública compete a las Fuerzas y Cuerpos de Seguridad. La realización en vía pública de tratamientos domésticos, como captación o grabación de imágenes, es perfectamente posible, así, muchas actividades particulares, familiares o de amistad tienen lugar en la misma, sin embargo estos actos no tienen ni pueden tener por finalidad la vigilancia".

Estudio genealógico

– Estudio genealógico de Azkoitia y cómo compatibilizarlo con la protección de datos, de 26 de julio de 2016. En referencia a la publicación de ese estudio la AVPD realizó un amplio análisis de la normativa aplicable y concluyó que: "analizada la normativa sectorial, en lo referente a información obrante en los archivos históricos, la legitimidad del tratamiento de datos de perso-

nas vivas vendrá dada por el transcurso de los plazos previstos en la respectiva normativa reguladora, concretamente el de 50 años contenido en el artículo 19.1 b) ahora citado, así como en el artículo 57 de la Ley de Patrimonio Histórico Español. No obstante, la información relativa a la ideología, religión, creencias o afiliación sindical, dotada de especial protección en el artículo 7.2 de la LOPD al exigirse para su cesión consentimiento expreso y escrito, no debiera ser objeto de publicación. Igual cautela debiera adoptarse a nuestro juicio respecto de la información relativa a infracciones penales o administrativas a que se refiere el artículo 7.5 de la LOPD. En cuanto a otro tipo de información personal, el responsable de la divulgación del estudio, (a tenor de la consulta parece que será el Ayuntamiento), a la vista del texto, debiera realizar una ponderación entre el interés general perseguido y el derecho a la privacidad de las personas afectadas, a fin de ofrecer únicamente aquella información que supere dicho juicio. Por último, aun cuando la difusión de la información pueda estar legalmente amparada, ha de recordase el derecho de los afectados a oponerse al tratamiento de la información, debiendo por ello el Ayuntamiento con carácter previo y con la debida difusión, establecer mecanismos que permitan a los interesados la consulta del texto para el posterior ejercicio de este derecho regulado en el artículo 34 del Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD. Igualmente la tutela por parte de los familiares del honor, intimidad personal y propia imagen de los fallecidos exige el establecimiento de los mecanismos de difusión y consulta citados".

Publicación de compatibilidad de empleados públicos

– Publicación de las Resoluciones de compatibilidad de empleados públicos, de 26 de julio de 2016. En el cual la AVPD resolvió: "la previsión contenida en el artículo 8.1 g) de la LTAIBG [Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno] constituye la norma habilitante para publicar con nombres y apellidos las resoluciones de autorización de compatibilidad de empleados públicos sin necesidad de consentimiento de éstos".

Cesión de datos de salud para proyectos de investigación

– Cesión de datos por el Departamento de Salud para diversos proyectos de investigación, de 19 de julio de 2016. En este Dictamen la AVPD señala las distintas medidas que se deben adoptar para garantizar el anonimato en los datos de salud y dictamina que "es obligatorio preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de forma que quede asegurado el anonimato. Esta obligación sólo cede en el caso de que el paciente haya dado su consentimiento expreso para no separar dichos datos (artículo 16.3 Ley 41/2002). […] Además de asegurar el anonimato, habrá que tener presente que la cesión de datos relativos a la salud deberá ser congruente con los principios de protección de datos y, en particular, con los consagrados en el artículo 4 de la LOPD […]. De este modo la comunicación de datos deberá limitarse

a aquéllos estrictamente necesarios para la finalidad pretendida (principio de calidad de los datos). Asimismo, en el tratamiento de datos de salud, deberán observarse las medidas de seguridad que deberán ser, además de las de nivel medio y básico, las de nivel alto, conforme señala el artículo 81.3 a) del Reglamento de desarrollo de la LOPD, y que se concretan en sus artículos 89 y siguientes. Las cesiones de datos de salud para la realización de estudios de investigación epidemiológica serán conformes a la normativa de protección de datos siempre y cuando las mismas se ajusten a lo dispuesto en el cuerpo de este dictamen".

Datos en aplicación informática de necesidades educativas especiales

– Cancelación de datos de una alumna incluida en una aplicación informática de necesidades educativas especiales de la Administración educativa, de 30 de mayo de 2016. En este caso la AVPD responde a una consulta de consulta de la Dirección de Innovación Educativa del Departamento de Educación, Política Lingüística y Cultura del Gobierno Vasco y luego de realizar un detallado repaso de la normativa de educación aplicable establece que "será la Administración educativa la que tendrá que determinar el plazo de conservación de los datos personales, y por tanto, fijar los límites al derecho de cancelación ejercido por la representante legal del alumno, en cumplimiento con la normativa educativa y de protección de datos personales citadas en el cuerpo de este dictamen".

Comunicación de datos a la policía municipal

– Comunicación a la policía municipal de datos personales para la incoación de una infracción administrativa en materia de seguridad ciudadana, de 16 de mayo de 2016. En este Dictamen se resuelve una consulta de la Osakidetza-Servicio Vasco de Salud y la AVPD dictamina que "las autoridades y órganos de las administraciones públicas competentes para imponer sanciones de acuerdo con la LO 4/2015 estarán legitimadas para solicitar del Ayuntamiento correspondiente los datos de domicilio y número de documento nacional de identidad de la persona presuntamente infractora obrantes en el padrón municipal. Además, en el caso de que estas autoridades y órganos desconozcan el municipio de residencia del presunto infractor, estarían igualmente legitimadas para recabar esos datos personales del Instituto Vasco de Estadística (EUSTAT) o, en su caso, del Instituto Nacional de Estadística (INE)".

Datos de asociación para justificar una subvención

– Cesión al Ayuntamiento de datos solicitados a una asociación para la justificación de la subvención percibida, de 10 de mayo de 2016. En este caso la AVPD sostiene que "existe habilitación legal para la cesión de la información pretendida, ajustándose por ello dicho tratamiento a la normativa en materia de protección de datos de carácter personal, si bien los datos deberán tratarse exclusivamente para la finalidad de control, tal y como exige el principio de calidad proclamado en el artículo 4 de la LOPD".

– Cesión de datos sobre el importe de la deuda por impago del impuesto de vehículos de tracción mecánica, de 5 de mayo de 2016. A partir de una consulta presentada por un Ayuntamien-

Cesión de datos sobre el importe de la deuda por impago de impuesto

to, la AVPD resolvió que cuando: "el interesado en participar en una subasta pública que tenga por objeto un vehículo embargado por la Seguridad Social, no puede acceder a la información concreta de la deuda contraída por el impago del impuesto, se le estaría privando de conocer de antemano el coste total que supone la adquisición del vehículo, puesto que en el caso de que el transmitente no haga frente a la citada deuda, tendrá que ser el futuro adquirente el que tendrá que abonar la misma para obtener de la Dirección General de Tráfico la renovación del permiso de circulación a su nombre. Por lo tanto, a falta de más información, esta Agencia entiende que solamente en este último supuesto estaría justificado que el Ayuntamiento cediese a un tercero que alegue tener interés en la adquisición de un vehículo, el dato concreto de la deuda contraída por el impago del impuesto sobre vehículos de tracción mecánica correspondiente al año inmediatamente anterior a la realización del trámite (artículo 99 del Texto Refundido de la Ley Reguladora de las Haciendas Locales), sin proporcionar datos relativos a la titularidad del vehículo, ni otros datos personales, todo ello en base al principio de calidad de los datos recogido en el artículo 4 de la LOPD".

Cesión de datos a sindicatos sobre integrantes de bolsas de trabajo

– Cesión de datos a sindicatos sobre integrantes de bolsas de trabajo, de 2 de mayo de 2016. Ante una consulta planteada por el Departamento de Justicia y Administración pública del Gobierno Vasco, sobre la adecuación a la normativa de protección de datos de una solicitud de información relativa a bolsas de trabajo planteada por un sindicato, la AVPD señaló: "el control de las bolsas de trabajo a que se refiere la consulta, justificaría conocer sus integrantes, y también los resultados del proceso seguido para su dotación, pudiendo comprobar así el cumplimiento de la legalidad del procedimiento".

Cesión de datos sobre consumos de agua en viviendas

– Cesión de datos sobre consumos de agua en viviendas, de 22 de abril de 2016. En referencia a la consulta planteada por una Sociedad Pública Municipal, sobre cesión al Gobierno Vasco de datos de consumo de agua en determinadas viviendas, la AVPD consideró que "dado que este artículo 64 y otros de la Ley 3/2015 de Vivienda han sido suspendidos por el Tribunal Constitucional con ocasión del recurso de inconstitucionalidad promovido por la Presidenta del Gobierno en funciones, debe concluirse que en tanto no se levante la suspensión o se resuelva la constitucionalidad de este precepto, no existe título legal que ampare la cesión de datos pretendida sin consentimiento de las personas afectadas".

Cesión de datos padronales

– Cesión de datos padronales de los Ayuntamientos a Correos y Telégrafos, de 20 de abril de 2016. En este tema la AVPD concluyó que "La cesión a Correos y Telégrafos de datos relativos a la dirección de una persona sin el previo consentimiento de la misma, resulta contrario a la normativa de protección de datos de carácter personal".
– Cesión de datos del padrón municipal, de información tributaria y acceso a expedientes por un Concejal, de 18 de abril de

2016. En este caso, la respuesta a la consulta presentada por un Ayuntamiento contiene varios temas: 1. Por una parte, se analiza la licitud de la comunicación de los datos del padrón municipal de habitantes a personas distintas de sus titulares. En este tema la AVPD determinó que "la cesión de datos del padrón está prevista fundamentalmente con destino a las Administraciones Públicas y al propio interesado. El vecino del municipio es, por tanto, el titular de los datos personales contenidos en el padrón municipal, y por ello, será el vecino el que podrá acudir al Ayuntamiento correspondiente a solicitar el acceso a los mismos. Será necesaria, pues, autorización expresa del interesado para que una tercera persona pueda solicitar y obtener el volante de empadronamiento del mismo, no siendo suficiente con la presentación ante el Ayuntamiento de copia del documento nacional de identidad del interesado y la comprobación del que el mismo y el que lo solicita en su nombre figuran empadronados en el mismo domicilio. De conformidad con el artículo 12.3 del Reglamento de desarrollo de la LOPD, al tener el responsable del tratamiento, en este caso, el Ayuntamiento, la carga de la prueba de la existencia del consentimiento, sería conveniente que la autorización expresa del interesado quede en poder de la entidad local para poder acreditar en cualquier momento la existencia del mismo". 2. En este Dictamen se resolvió además una cuestión referente a la cesión por dicha entidad local de un dato personal que figura en el padrón a una empresa adjudicataria de un contrato municipal, cuyo objeto es el sondeo o encuestas de opinión y para ese supuesto la AVPD sostuvo que: "para que la empresa adjudicataria del contrato pueda acceder a datos de carácter personal obrantes en el padrón municipal, necesarios para la realización del servicio contratado, y que obran en poder del Ayuntamiento como responsable del tratamiento, será necesario que se cumplan las previsiones de los apartados 2 y 3 del artículo 12 de la LOPD anteriormente transcritas. Siendo necesario en todo caso que consten por escrito las previsiones contenidas en el apartado 2 de dicho artículo 12, ello con independencia de que la formalización del contrato se materialice o no a través de un contrato menor". 3. Igualmente, sobre la consulta realizada por el Ayuntamiento para la cesión de información tributaria la AVPD resolvió que: "Será necesaria, pues, autorización expresa del interesado para que una tercera persona pueda solicitar y obtener la liquidación del impuesto municipal […] sería conveniente que la autorización expresa del interesado quede en poder de la entidad local para poder acreditar en cualquier momento la existencia del consentimiento del mismo". 4. Por último, el Ayuntamiento plantea en su consulta el tema del acceso de un concejal, miembro de la comisión de bienestar social, a copias de los expedientes de ayudas de emergencia social resueltos por otro concejal, ante lo cual la AVPD señaló que: "la cesión masiva e indiscriminada de los expedientes de ayudas de emergencia social al concejal al

que se refiere la consulta vulneraría la normativa de protección de datos".

– Cesión de datos del padrón municipal a una asociación de comerciantes, de 14/04/2016. En este Dictamen se concluyó que "la cesión de datos a la Confederación Vasca de Comercio, en los términos que contempla el proyecto de convenio, sin el consentimiento de los afectados, resulta contrario a la normativa de protección de datos de carácter personal".

Acceso de los concejales al registro de entradas y salidas del Ayuntamiento

– Acceso de los concejales al registro de entradas y salidas del Ayuntamiento, de 31 de marzo de 2016. En este caso se estableció que "la aplicación del principio de calidad de datos impide claramente el acceso directo (bien de forma tradicional o telemática) por los Concejales al fichero de Registro de entradas y salidas, debiendo existir en todo caso una ponderación previa por parte del responsable del tratamiento […]. Es cierto que el derecho de los corporativos de acceder a la información es un derecho cualificado respecto al de los ciudadanos en general, no obstante, esta facultad no puede implicar un acceso automático a la información. Tampoco resulta ocioso recordar que en numerosas ocasiones el deber de información puede ser cumplido mediante el ofrecimiento de información disociada, práctica más respetuosa con el derecho fundamental y que deberá observarse siempre que ello sea posible. Por último, también deben ser conscientes los corporativos del deber de secreto al que están sujetos por el artículo 10 de la LOPD, sin que la información que obtengan pueda ser utilizadas para finalidades distintas de las que motivaron su tratamiento".

Publicación del sorteo para la formación de mesas electorales

– Publicación en página web del resultado del sorteo para la formación de mesas electorales, de 10 de marzo de 2016. Ante la consulta presentada por un Ayuntamiento sobre ese tema, la AVPD dictaminó que "La publicación en la página web del Ayuntamiento del resultado del sorteo para la formación de las mesas electorales sin consentimiento de los afectados ni habilitación legal, resulta contraria a la normativa de protección de datos de carácter personal".

Publicación de resoluciones judiciales en la web municipal

– Publicación de resoluciones judiciales en la web municipal, de 7 de marzo de 2016. El primer tema tratado en esta resolución fue el alcance la publicidad de las sentencias; en referencia a ello la AVPD sostuvo que "no cabe una publicidad general de las resoluciones judiciales, hallándose este tratamiento de datos limitado a supuestos antes citados, sin que ello suponga una contradicción con el principio de publicidad de las actuaciones judiciales". De igual forma, en este Dictamen se analizó si el deber disociar las sentencias se extiende a los nombres de los jueces, magistrados, abogados y procuradores, en este punto la AVPD consideró que no puede ofrecer una respuesta única porque "en ocasiones será suficiente con la supresión del nombre y los apellidos, pero en otras, puede resultar necesario suprimir aquellas informaciones que, sin ser de por sí identificativas, permitan al lector de la sentencia identificar a las partes, a alguna de ellas o

a personas intervinientes en el proceso, bien por la localización geográfica citada, por las descripciones contenidas en el relato de hechos, o por las circunstancias concurrentes en el caso. Por ello, habrá de estarse al supuesto concreto para determinar la forma más adecuada de conciliar la publicidad de las resoluciones judiciales con el derecho a la privacidad".

Cesión al ayuntamiento de vida laboral para tramitar una jubilación

– Cesión al ayuntamiento de vida laboral para tramitar de oficio una jubilación, de 24 de febrero de 2016. Dictamen que se emite en relación a la consulta planteada por una persona sobre el requerimiento por la Administración de información de la Seguridad Social con el objeto de tramitar de oficio su jubilación forzosa, siendo la respuesta de la AVPD que: "si para determinar la edad de acceso a la pensión de jubilación del consultante es suficiente con conocer sus periodos de cotización a la Seguridad Social, esa información sería la única exigible por la Administración, en cumplimiento del artículo 4 de la LOPD".

Identidad de los beneficiarios de ayudas concedidas por una mancomunidad

– Cesión de datos sobre identidad de los beneficiarios de ayudas concedidas por una mancomunidad a los ayuntamientos integrados en la misma, de 19 de febrero de 2016. En este Dictamen la AVPD concluyó que: "La indicación de la persona física perceptora de ayudas de servicios sociales, así como la información sobre el servicio que han recibido o reciben estas personas, son datos de carácter personal protegidos por la LOPD. Cualquier comunicación de dichos datos personales por parte de la mancomunidad, en tanto que responsable y cedente, al ayuntamiento del municipio donde reside la persona beneficiaria, y que forme parte integrante de la mancomunidad, se deberá someter al régimen general previsto en los artículos 11 y 21 de la LOPD. Aplicando el régimen de los citados artículos 11 y 21 de la LOPD, sería legítima la comunicación al Ayuntamiento de la identidad y de la ayuda concedida por la mancomunidad a sus vecinos siempre y cuando ese ayuntamiento se haya reservado funciones en materia de servicios sociales para cuyo ejercicio resultase imprescindible conocer dichos datos. En los demás casos, la comunicación de dicha información habrá de efectuarse previo procedimiento de disociación que impida asociar la misma a una persona identificada o identificable".

Asistencia jurídica gratuita, certificado de convivencia colectivo y consentimiento

– Asistencia jurídica gratuita, certificado de convivencia colectivo y consentimiento, de 19 de febrero de 2016. En este Dictamen se puede destacar que la AVPD subrayó que: "De conformidad con la regulación jurídica del padrón municipal, para poder obtener el certificado o volante de empadronamiento colectivo será necesario el consentimiento de todas las personas inscritas en el domicilio. En el caso de que se encuentren inscritos hijos menores o mayores incapacitados judicialmente sujetos a patria potestad prorrogada o rehabilitada, será necesario el consentimiento de los padres. En el caso de que no se disponga de dichos consentimientos, bien por parte de alguno de los miembros de la unidad familiar del solicitante o de otras personas que aun estando inscritas en el domicilio no pertenezcan a la

misma, el Ayuntamiento correspondiente sólo podrá expedir certificados o volantes de empadronamiento individuales de las personas que efectivamente lo hayan prestado, con indicación en los mismos del número total de personas inscritas en el domicilio".

Acceso a expedientes desde el portal web del Ayuntamiento

– Acceso a expedientes desde el portal web del Ayuntamiento, de 16 de febrero de 2016. Se trata de un Dictamen que se emite en relación a una consulta planteada por una Administración local sobre el acceso telemático a expedientes obrantes en la misma y sobre publicaciones de actos administrativos. En el cual la AVPD resolvió que "en aquellos supuestos en que a través de la publicación pudieran divulgarse datos especialmente protegidos, infracciones administrativas o situaciones personales de vulnerabilidad, debiera optarse por publicar una indicación del contenido del acto y del lugar donde pueda ser consultado por los interesados para su conocimiento. En cuanto al segundo supuesto expresado en el escrito de consulta, acceso a testamento en el que consta el mejor derecho a un bien inmueble por parte de uno de los hermanos, parece clara la habilitación legal para el acceso del resto de hermanos a dicho documento (art. 35 a de la Ley 30/92 en relación con el art.11.2.a) de la LOPD), si bien debiera omitirse aquella información que no resultase adecuada o pertinente para la finalidad perseguida. Por último, debe recordarse asimismo que el acceso telemático deberá realizarse cumpliendo las medidas de seguridad detalladas en los artículos 89 a 104 del Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, garantizándose la observancia del principio de seguridad de datos consagrado en el artículo 9 de la Ley Orgánica".

Solicitud de consentimiento en certificados de convivencia

– Solicitud de consentimiento en certificados de convivencia, de 28 de enero de 2016. En este caso, la AVPD dictaminó que "la necesidad de consentimiento constituye un requisito común para la verificación de datos de residencia. Por otro lado, y respondiendo a la última de las cuestiones planteadas en el escrito, cuando los volantes de convivencia sean objeto de interoperabilidad, el consentimiento a solicitar, será, al igual que hemos mantenido con carácter general, el de todos, no sólo el del solicitante, sino también el del resto de personas que convivan con él. La única salvedad sería la de aquellas personas respecto de las cuales, el solicitante ejerza la tutela o patria potestad. Quiere con ello decirse que el medio utilizado para la comunicación de los datos no afecta al principio básico del derecho fundamental como es la necesidad de consentimiento de los interesados".

Datos en el portal municipal de transparencia

– Publicación de datos en el portal de transparencia de la web municipal, de 25 de enero de 2016. En este Dictamen la AVPD realiza un análisis con amplias consideraciones del que se puede extraer la conclusión final: "No debe confundirse la publicidad activa, que, insistimos, es la información a que esta consulta se refiere, con el derecho de acceso a la información pública o publicidad pasiva. La publicidad activa, realizada motu propio y

sin necesidad de petición alguna, implica una mayor afectación a la privacidad de las personas en la medida en que supone una publicación en el portal de transparencia o página web, y por ende, una accesibilidad total, lo que no ocurre al ejercitar el derecho de acceso a la información pública, sometido a la necesidad de petición y limitado al propio peticionario. Por ello, debe recordarse que aun cuando determinada información no pueda ser objeto de publicidad activa al no contar con habilitación legal suficiente, o consentimiento de los interesados, esa misma información, solicitada en el ejercicio del derecho de acceso a la información pública, y tras la oportuna ponderación de intereses, podría ser entregada al peticionario. En este supuesto, sería conveniente informar expresamente a los solicitantes que la normativa en materia de protección de datos de carácter personal se aplicará en todo caso al tratamiento posterior de la información entregada".

Acceso y uso de datos por una Sociedad Pública Municipal para un censo de vivienda vacía

– Acceso y uso de datos personales por una Sociedad Pública Municipal para realizar un censo de vivienda vacía, de 25 de enero de 2016. En este Dictamen la AVPD concluye: "Como el procedimiento de declaración de vivienda deshabitada puede iniciarse y resolverse por el ayuntamiento respectivo, ello exigirá a la entidad local recoger y tratar datos personales (datos de padrón relativos a viviendas desocupadas, datos de titularidad de dichas viviendas, etc.). Y con carácter obligatorio y previo a dicha recogida y tratamiento, el ayuntamiento respectivo tendrá que crear un fichero de datos de carácter personal de titularidad pública, en el que se contengan dichos datos personales de conformidad con la LOPD y la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la AVPD".

Cesión de datos a concejales sobre deudores a la hacienda municipal en vía ejecutiva

– Cesión de datos a concejales sobre deudores a la hacienda municipal en vía ejecutiva, de 18 de enero de 2016. En este caso la AVPD señala que: "La cesión de los datos de naturaleza tributaria por parte de un Ayuntamiento a un grupo de concejales no estaría contemplada en los supuestos que reconoce la Normativa Foral Tributaria, no tendría amparo en lo dispuesto en el art. 11 de la LOPD, resultando su comunicación contraria a la protección de datos de carácter personal".

Cesión al Ayuntamiento de los datos de los empleados de la empresa de limpieza

– Cesión al Ayuntamiento de los datos de los empleados de la empresa adjudicataria del servicio de limpieza, de 12 de enero de 2016. En este Dictamen se señaló que "la Administración sólo podrá acceder a la información personal adecuada, pertinente y necesaria para comprobar que el contrato se está cumpliendo en sus justos términos. En relación con este extremo, en el escrito de consulta se plantea, porque así lo recoge el pliego de cláusulas administrativas, la cesión al Ayuntamiento de los documentos contractuales que haya otorgado la empresa adjudicataria con el personal que emplee para la ejecución del contrato, cualquiera que sea la nacionalidad de los mismos. A este respecto habría que decir que el contrato de trabajo puede

contener información personal de diversa índole (retribución, número de afiliación a la seguridad social, DNI, información merecedora de especial protección en los términos del artículo 7 LOPD), y que en atención a la finalidad que justificaría en el presente caso la cesión de datos, facilitar al Ayuntamiento copia íntegra de los contratos de trabajo de los trabajadores de la empresa adjudicataria adscritos a la ejecución del contrato podría resultar no adecuado al principio de calidad de los datos (artículo 4.1 de la LOPD). Así, podría resultar adecuada al principio de calidad la comunicación de la información personal relativa al nombre y apellido del trabajador, su categoría profesional o nivel funcional del mismo, y su jornada laboral. En cuanto a la solicitud del Ayuntamiento a la empresa adjudicataria del calendario de presencia y que se prevé en el Pliego de condiciones técnicas, la comunicación de los datos personales en él contenido no vulneraría el principio de calidad de los datos, ya que en dicho calendario tan solo se detalla el nombre de los trabajadores y los horarios de trabajo".

Cesión de información sobre licencias de obras a vecinos del municipio

– Cesión de información sobre licencias de obras a vecinos del municipio, de 12 de enero de 2016. En este Dictamen se concluye: "1.- La cesión de los datos contenidos en los expedientes administrativos tramitados con ocasión de la licencia de obras no es contraria al derecho fundamental a la protección de datos de carácter personal en los términos expresados en el Considerando II del presente. 2.- La comunicación de los datos debe ser respetuosa con el principio de calidad recogido en el artículo 4 LOPD en los términos expresados en el Considerando III del presente".

5. COOPERACIÓN CON OTRAS INSTITUCIONES PÚBLICAS

Actividad Parlamentaria y Protección de Datos: Doctrina de la Agencia

En 2016 la AVPD publicó un Informe titulado "Actividad Parlamentaria y Protección de Datos Personales: Doctrina de la Agencia Vasca de Protección de Datos", que analiza los distintos Dictámenes emitidos en las preguntas formuladas por el Parlamento Vasco y el Gobierno Vasco sobre la posibilidad de entrega de documentación que contiene datos personales desde el Ejecutivo al Parlamento Vasco (Doctrina que está disponible electrónicamente[1]). El Informe trata, principalmente, sobre la competencia del Parlamento de control político al Ejecutivo cuando ese control está vinculado a las solicitudes de información de datos personales. Desde del análisis de varios Dictámenes, la AVPD sienta doctrina en referencia a la pregunta de si ¿Existe una habilitación legal para la entrega de documentación con datos personales cuando dicha documentación es requerida por el Parlamento? Siendo la respuesta afirmativa.

Convenios firmados por la AVPD

La AVPD se ha caracterizado por la cooperación con otras Administraciones públicas más allá de sus Dictámenes, para lo cual ha

[1] http://www.avpd.euskadi.eus/contenidos/informacion/publicaciones_avpd/es_def/adjuntos/Dictamenes2016_web-es.pdf

celebrado diversos convenios. Por ejemplo con: los Centros asociados de la UNED en la Comunidad Autónoma del País Vasco para realizar actividades para la promoción y difusión del derecho de la protección de datos personales; el Departamento de Administración Local y Equilibrio Territorial de la Diputación Foral de Álava y la Asociación de Municipios Vascos para el desarrollo de un programa para facilitar a las entidades locales del TH de Álava la realización de los planes de implantación en materia de protección de datos de carácter personal; la Diputación Foral de Gipuzkoa y la Asociación de Municipios Vascos (EUDEL) para el desarrollo de un programa para facilitar a las entidades locales del TH de Gipuzkoa la realización de los planes de implantación en materia de protección de datos de carácter personal; el Gobierno Vasco para la realización de estudios sociológicos relacionados con el derecho fundamental a la protección de datos personales en la realidad social vasca; el Instituto Vasco de Administración Pública en orden a colaborar en las áreas de la capacitación y normalización lingüística; el Instituto Vasco de Administración Pública para desarrollar estrategias conducentes al cumplimiento de la Misión y retos de ambas instituciones, así como al eficaz funcionamiento de los procesos en que basan su gestión, mediante la puesta en marcha de proyectos de carácter colaborativo orientados a la mejora de los servicios prestados; la Universidad del País Vasco en materia Practicum de la licenciatura de Derecho para mejorar la formación práctica de los alumnos de dicha institución.

Convenios con otras Autoridades de Protección de Datos

Por otra parte, la AVPD cuenta con un conjunto de convenios de cooperación con otras agencias de protección de datos anteriores a 2016, pero que vale la pena mencionar en este primer informe y son con: la Comisión Estatal para el Acceso a la Información Pública de Zacatecas para la realización de actividades conjuntas de cooperación, formación, desarrollo de programas y proyectos específicos en las áreas que se determine de mutuo acuerdo; la Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León (México) para promover la difusión del derecho a la protección de datos de carácter personal, el fomento de estudios e investigaciones al respecto, así como el intercambio de experiencias de mutuo interés; la Comisión para el Acceso a la Información Pública de Puebla (México) para promoción, información y estudio de la gestión de protección de datos; la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires para colaborar en la promoción del uso seguro de las tecnologías de la información y comunicación en todo lo relacionado con la protección de la privacidad y los datos personales de niñas, niños y adolescentes; el Instituto Federal de Acceso a la Información y Protección de Datos de los Estados Unidos Mexicanos para realizar actividades conjuntas de cooperación, de formación, de capacitación, de desarrollo de programas y proyectos específicos; Protocolo de colaboración, entre las cuatro Agencias de Protección de Datos (AEPD, AVPD, APD-CAT, APD-CM), para la puesta en marcha del Sistema de Información de Intercambio Registral (SIDIR).

6. COOPERACIÓN CON LA SOCIEDAD CIVIL

Convenios con organizaciones de la sociedad civil

En 2016 no se registran Convenios de cooperación con instituciones y organizaciones de la sociedad civil. Sin embargo, se debe señalar que este tipo de cooperación con la sociedad civil, para el fomento de la autorregulación y el cumplimiento de la Ley, ha estado presente en la actividad de la AVPD desde su creación. Así, además de los Dictámenes antes señalados, se pueden subrayar los siguientes Convenios que fueron suscritos en años anteriores, pero que aún están vigentes con: la Asociación Internet&Euskadi para el fomento del derecho fundamental a la protección de datos personales en aspectos relacionados con las TIC; la Asociación Profesional Española de Privacidad con la finalidad de fomentar y promover el respeto y debida tutela del derecho fundamental a la protección de los datos personales; la Asociación Vasca de Privacidad y Seguridad de la Información (Pribatua) para realizar actividades conjuntas de cooperación, de formación, de capacitación, de desarrollo de programas y proyectos específicos; la Comisión de Libertades e Informática; con el Colegio Oficial de Ingenieros de Telecomunicación y Asociación de Ingenieros de Telecomunicación del País Vasco para promover la divulgación, sensibilización y formación en protección de datos personales y seguridad de las telecomunicaciones; el Colegio Oficial de Ingenieros en Informática del País Vasco para el establecimiento de un cauce de colaboración en el ámbito de la protección de datos de carácter personal; la Universidad de la Rioja con el fin de establecer un acuerdo de cooperación bibliotecaria en el marco del proyecto Dialnet para, por un lado, poder incluir el mayor número de títulos de revistas existentes en las bibliotecas de ambas instituciones y, por otro, sentar las bases para la prestación de nuevos servicios documentales de interés para ambas instituciones; con la Fundación Vasca para la calidad; el Consorcio HAURRESKOLAK para la gestión de las escuelas infantiles y la atención asistencial y educativa a los menores de tres años; con la sociedad "IZENPE, S.A., Ziurtapen eta Zerbitzu Enpresa - Empresa de certificación y Servicios", para colaborar en materia de protección de datos personales y de desarrollo de firma electrónica; la Sociedad Informática de la Salud.

7. OTRAS ACTIVIDADES

Carta de Servicios a la Ciudadanía y otras actividades de sensibilización

Entre las actividades de difusión se debe destacar que en 2016 la AVPD publicó una Carta de Servicios a la Ciudadanía que está disponible en su web. Además, la AVPD realizó un tríptico informativo para la sensibilización social sobre el manejo de datos privados en internet y redes sociales, titulado: "La Agencia Vasca de Protección de Datos presenta… Asuntos privados". De igual manera, se realizaron dos videos de sensibilización en el marco de la campaña "La protección de datos con humor", uno sobre el uso del teléfono y otro sobre Whatsapp. En las actividades de sensibilización social podemos subrayar que en 2016 se realizó la "IV Edición de Premios a la Protección

de Datos". En los cuales la AVPD reconoce la labor de quienes promueven el conocimiento, la investigación, la divulgación de la cultura de protección de datos y la difusión de la misma en la sociedad. Asimismo, se destacan los proyectos que implican una mejora de los tratamientos de datos de carácter personal por las Administraciones públicas vascas.

Jornadas y seminarios

En este ámbito de actuaciones la AVPD participó en las siguientes jornadas: "VIII Jornadas de Seguridad y Protección de Datos"; "VII Jornada Pribatua: Primera Aproximación al nuevo Reglamento Europeo de Protección de Datos"; "Transferencias internacionales de datos: del Safe Harbor al Privacy Shield"; "XIII Foro de Seguridad y Protección de Datos en Salud"; y, "Evolución de la protección de datos en los últimos tiempos y a futuro" en la que se realizó la entrega de los III Premios a la Protección de Datos.

VIII. MÉXICO

1. INTRODUCCIÓN

Creación del Instituto Federal de Acceso a la Información Pública

El Instituto Federal de Acceso a la Información Pública (IFAI) se creó en el marco de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), expedida por el Congreso de la Unión de los Estados Unidos Mexicanos y publicada en el Diario Oficial de la Federación (DOF) el 11 de junio de 2002[1]. Por Decreto de 24 de diciembre de 2002, se precisa la naturaleza jurídica del Instituto y se establece que "es un organismo descentralizado, no sectorizado, con personalidad jurídica y patrimonio propios, con domicilio legal en la Ciudad de México; y que contará con autonomía operativa, presupuestaria y de decisión en términos de la Ley que lo crea y del Decreto al que se hace referencia" (art. 1). Asimismo, "El Instituto tendrá por objeto promover y difundir el ejercicio del derecho de acceso a la información; resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades" (art. 2)[2].

Derechos de acceso a la información y a la protección de datos: evolución y reformas constitucionales

Ambos derechos, el derecho de acceso a la información y el derecho a la protección de datos personales son de gran importancia para el Estado mexicano. A través del derecho de acceso a la información se garantiza una gestión pública transparente, sujeta a la supervisión de la sociedad mediante la apertura de los asuntos de dominio público. Por medio del ejercicio de este derecho, la población puede evaluar y conocer las acciones de las instituciones públicas, y así fortalecer la rendición de cuentas en México. La protección de datos personales es el derecho que tiene toda persona a conocer y decidir quiénes, cómo y de qué manera recaban, utilizan y comparten su información. Como parte de este derecho fundamental se encuentran los derechos de acceso, rectificación, cancelación y oposición de datos personales (ARCO).

El 20 de julio de 2007 se publicó en el DOF el Decreto por el que se adiciona un segundo párrafo con siete fracciones al artículo 6 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM). Dos de estas fracciones hacen referencia a la protección de los datos personales: "la información que se refiere a la vida privada y los datos

[1] Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, disponible en http://www.dof.gob.mx/nota_detalle.php?codigo=727870&fecha=11/06/2002

[2] Decreto del Instituto Federal de Acceso a la Información Pública, disponible en: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/Decreto_del_IFAI.pdf

personales será protegida en los términos y con las excepciones que fijen las leyes" (fracción II) y "toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos" (fracción III).[3]

El 30 de abril de 2009 se publicó en el DOF el Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la CPEUM, en el que se faculta al Congreso de la Unión para legislar en materia de datos personales en posesión de los particulares[4].

El 1 de junio de 2009, se publicó en el DOF el Decreto por el que se adiciona un párrafo al artículo 16 de la CPEUM, el cual establece que: "toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros"[5].

Más adelante, el 7 de febrero de 2014, mediante Decreto publicado en el DOF, se reformaron y aprobaron diversas disposiciones de la CPEUM, entre ellas el artículo 6, apartado A. Esta reforma fue resultado de atender una demanda social por conocer ámbitos de interés público antes no contemplados, tales como partidos políticos, fideicomisos y fondos públicos así como cualquier persona física o moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal[6].

La reforma al artículo 6 señala que la Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica y de gestión, con capacidad para el ejercicio de su presupuesto y para determinar su organización interna, responsable de garantizar el cumplimiento de los derechos de acceso a la información y protección de datos personales. La conducción del organismo autónomo es encomendada a siete comisionados, el cual estará encabezado por una o un Comisionado Presidente.[7]

Posteriormente, el 4 de mayo de 2015, se publicó en el DOF el Decreto por el que se expide la Ley General de Transparencia y Acce-

---

[3] Decreto por el que se adiciona un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, disponible en http://inicio.ifai.org.mx/Articulo6/PublicacionDOF20Jul_2007.pdf

[4] Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5089047&fecha=30/04/2009

[5] Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, disponible en http://www.dof.gob.mx/nota_detalle.php?codigo=5092143&fecha=01/06/2009

[6] Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, disponible en http://www.dof.gob.mx/nota_detalle.php?codigo=5332003&fecha=07/02/2014

[7] *Ibíd.*

Ley General de Transparencia y Acceso a la Información Pública

so a la Información Pública (LGTAIP) por la cual el IFAI se convierte en el organismo autónomo a que se refiere el artículo 6 constitucional y cambia de denominación al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), con nuevas facultades como la resolución de recursos de inconformidad y el ejercicio de la facultad de atracción de los recursos de revisión que se encuentren en los organismos garantes locales, así como el ser coordinador del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (SNT). Lo anterior significa un incremento importante en las responsabilidades del Instituto[8].

La misión del INAI es "garantizar en el Estado mexicano los derechos de las personas a la información pública y a la protección de sus datos personales, así como promover una cultura de transparencia, rendición de cuentas y debido tratamiento de datos personales para el fortalecimiento de una sociedad incluyente y participativa". Su visión es "ser una institución nacional eficaz y eficiente en la consolidación de una cultura de transparencia, rendición de cuentas y debido tratamiento de datos personales, reconocida por garantizar el cumplimiento de la normativa en la materia y promover el ejercicio de los derechos de acceso a la información y protección de datos personales como base para la participación democrática y un gobierno abierto"[9].

Objetivos estratégicos INAI

El INAI tiene cuatro objetivos estratégicos que describen el conjunto de fines ulteriores de la institución, pues hacen referencia al mandato constitucional conferido al Instituto:

- Garantizar el óptimo cumplimiento de los derechos de acceso a la información pública y la protección de datos personales.
- Promover el pleno ejercicio de los derechos de acceso a la información pública y de protección de datos personales, así como la transparencia y apertura de las instituciones públicas.
- Coordinar el Sistema Nacional de Transparencia y de Protección de Datos Personales, para que los órganos garantes establezcan, apliquen y evalúen acciones de acceso a la información pública, protección y debido tratamiento de datos personales.
- Impulsar el desempeño organizacional y promover un modelo institucional de servicio público orientado a resultados con un enfoque de derechos humanos y perspectiva de género.

Atribuciones del INAI

Con el propósito de que el INAI cumpla su misión como organismo autónomo de carácter nacional, es decir, garantizar el derecho de los ciudadanos a la privacidad de sus datos personales y promover en la sociedad y en el gobierno la cultura del derecho a la privacidad, la legislación vigente lo dota de las siguientes atribuciones:

- Atribuciones normativas: interpreta la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

[8] Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública, disponible en http://www.dof.gob.mx/nota_detalle.php?codigo=5391143&fecha=04/05/2015

[9] Misión, Visión y Objetivos, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, disponible en http://inicio.ifai.org.mx/SitePages/misionViosionObjetivos.aspx

(LFPDPPP), la LGTAIP y la Ley General de Protección de Datos en Posesión de Sujetos Obligados (LGPDPPSO) conforme a la CPEUM y Tratados Internacionales; emite sus reglamentos; criterios, lineamientos y recomendaciones para garantizar el pleno derecho a la protección de datos personales; y, divulga estándares y buenas prácticas internacionales en la materia.
- Atribuciones informativas: proporciona apoyo técnico a los sujetos obligados de dichas leyes que lo solicitan, para apoyarlos en el cumplimiento de sus obligaciones; desarrolla y difunde análisis, estudios e investigaciones en la materia. Por ley, está obligado a presentar un informe anual de actividades al Congreso.
- Atribuciones de verificación: vigila y verifica el cumplimiento de las disposiciones contenidas en la normatividad aplicable.
- Atribuciones preventivas: elabora estudios de impacto sobre la privacidad previos a implementar una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes.
- Atribuciones resolutorias: en el sector privado, conoce y resuelve procedimientos de protección de derechos y de verificación e impone las sanciones según corresponda. Asimismo, en el sector público, conoce y resuelve recursos de revisión e inconformidad, así como procedimientos de verificación.
- Atribuciones sancionadoras: la LFPDPPP prevé una serie de conductas consideradas como infracciones y sus sanciones correspondientes, que van desde el apercibimiento hasta la imposición de multas máximas, bajo un sistema de modulación de la penalidad, de acuerdo con la gravedad de las conductas. En el caso particular del sector público, la recién publicada LGPDPPSO aplicable al sector público, establece causales de sanción por incumplimiento de las obligaciones establecidas en dicha Ley; por otro lado, faculta al Instituto y a los Organismos garantes para imponer medidas de apremio para asegurar el cumplimiento de sus determinaciones, consistentes en multa o amonestación pública. Además, la referida Ley, precisa que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

2. PLANIFICACIÓN

Programa 2016-2019 del Instituto

El Programa Institucional 2016-2019 del Instituto fue integrado con el objetivo de lograr el cabal cumplimiento de acciones que contribuyan a la consecución de los objetivos estratégicos institucionales, con miras a garantizar la plena observancia de los derechos humanos de acceso a la información y protección de datos personales, la gestión documental, el fortalecimiento del SNT y el impulso de acciones que fomenten la construcción de capacidades en los sujetos obligados. Esto con el fin de mejorar la transparencia y la apertura de las instituciones públicas, a partir de un modelo institucional de servicio público orientado a resultados con un enfoque de derechos humanos y

perspectiva de género que garantice un manejo más eficaz y eficiente de los recursos públicos del INAI[10].

El Programa Institucional es resultado de un esfuerzo plural de las áreas que integran el INAI. En éste se definen objetivos específicos, estrategias y líneas de acción que en el corto y mediano plazo permitirán acercar a la sociedad al conocimiento, ejercicio y tutela de los derechos de acceso a la información y protección de datos personales. Para la definición de estos elementos, se partió de una perspectiva tripartita inherente a las atribuciones y al quehacer del INAI (como coordinador del SNT, como órgano garante nacional y como sujeto obligado a otorgar acceso a la información y a proteger los datos personales en su posesión).

El INAI incluye como parte de su Programa Institucional diversos instrumentos de medición, tales como, encuestas, indicadores e índices, los cuales miden diferentes aspectos de los derechos que tutela el Instituto, a los que ha denominado Indicadores de Impacto. Estos buscan crear un marco de referencia que permita advertir los cambios sociales a los que contribuye el quehacer institucional a mediano y largo plazo.

Acciones estratégicas durante 2016: evaluación del cumplimiento del marco jurídico y otras

Las acciones estratégicas durante 2016 fueron:

- Evaluación del cumplimiento al marco jurídico en materia de acceso a la información de los sujetos obligados: acciones de vigilancia, acciones de acompañamiento y de seguimiento para el cumplimiento de la LGTAIP y Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) con los sujetos obligados, elaboración de estudios sectorizados y de carácter transversal.
- Desarrollo del ejercicio del derecho de protección de datos personales en el sector público a través de solicitudes de acceso y corrección de datos personales.
- Temas sustantivos del derecho a la protección de datos personales: desarrollo de herramientas para facilitar el cumplimiento de la normativa, monitoreo, seguimiento y análisis de ordenamientos, iniciativas o dictámenes con incidencia en el tema de protección de datos personales.
- Sistema Nacional de Transparencia: armonización legislativa de las entidades federativas y actividades conjuntas del INAI y los organismos garantes de los Estados; desarrollo e integración de la Plataforma Nacional de Transparencia.
- Capacitación en materia de derechos de acceso a la información y la protección de datos personales dirigida a sujetos obligados.
- Acciones de vinculación y de promoción de la cultura de la transparencia, del derecho de acceso a la información pública y de la protección de datos personales con la sociedad.
- Desarrollo de políticas de acceso a la información y de gobierno abierto.

[10] Acuerdo mediante el cual se aprueban los lineamientos para conformar el Programa Institucional 2016-2019 del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Acuerdo ACT-PUB/15/09/2015.04, disponible en http://inicio.ifai.org.mx/MarcoNormativo-Documentos/ACT-PUB-15-09-2015.04.pdf

– Foros, congresos y seminarios del INAI en materia de protección de datos personales, acceso a la información y gestión documental.
– Acciones estratégicas en materia de acceso a la información, protección de datos personales, gobierno abierto, archivos y lucha contra la corrupción a nivel internacional: cooperación internacional, promoción y vinculación internacional.

3. ACCIÓN NORMATIVA

Leyes de protección de datos en México

El Congreso mexicano ha promulgado tres instrumentos jurídicos de orden público y de observancia general en toda la República que tienen por objeto la protección de los datos personales, a saber:

– Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) de 2010: regula el tratamiento de los datos personales que están en posesión de personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de las sociedades de información crediticia y las personas que lleven a cabo la recolección y almacenamiento de datos personales para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.
– Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) de 2015: esta ley crea el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales y tiene por objeto establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las Entidades Federativas y los municipios. En ese orden de ideas, también establece que los Sujetos Obligados serán responsables de los datos personales en su posesión y, en relación con éstos dispone directrices a las que debe sujetarse el tratamiento, por ejemplo: adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso, rectificación, corrección y oposición al tratamiento de datos; tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos; procurar que los datos personales sean exactos y actualizados, entre otros.
– Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) de 2017: regula la Protección de los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la Federación, las Entidades Federativas y los municipios, con la finalidad de vigilar su debido tratamiento. Es importante señalar que a nivel estatal, los órganos legislativos locales emiten sus propias leyes, mismas que deben

apegarse a la normativa Constitucional. Existen once entidades federativas que tienen leyes de protección de datos personales en el sector público.

Atribuciones normativas del INAI

Desde su constitución como órgano constitucional autónomo el Instituto ha realizado las siguientes actividades para cumplir con sus atribuciones normativas e informativas:

– El 4 de marzo de 2014 se publicó en el Diario Oficial de la Federación un Acuerdo en el que se facultó al Secretario de Protección de Datos Personales junto con los Directores Generales competentes para dictar diversos acuerdos en los procedimientos de verificación, protección de derechos e imposición de sanciones. Asimismo, se le atribuyeron facultades en materia de autorregulación. Por otra parte, se han publicado los siguientes materiales informativos de enero de 2013 a la fecha:
  - Directrices para el Aviso de Privacidad.
  - Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante.
  - Reglas de Operación del Registro de Esquemas de Autorregulación Vinculantes.
  - Recomendaciones sobre seguridad de datos personales.
  - El ABC de los avisos de privacidad.
  - Modelo de aviso de privacidad para videovigilancia.
  - Formularios de autoevaluación del aviso de privacidad.
  - Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales
  - Metodología de Análisis de Riesgo BAA.
  - Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas.
  - Modelos de avisos de privacidad para migrantes.
  - Guía para Instrumentar Medidas Compensatorias.
  - Guía para prevenir el robo de identidad.
  - Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
  - Guía para orientar el debido tratamiento de datos personales en la actividad de cobranza extrajudicial.
  - Guía de Borrado Seguro.

4. PROCEDIMIENTOS DE GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS

El procedimiento de protección de derechos

El INAI tiene atribuciones para sustanciar el procedimiento de protección de derechos, a través del cual el titular de los datos personales o su representante legal acude a la Institución en virtud de la falta de respuesta del responsable o por inconformidad con la respuesta proporcionada por éste, a su solicitud por la que ejerció su derecho de acceso, rectificación, cancelación u oposición al tratamiento de sus datos. El procedimiento de protección de derechos es un procedimiento administrativo que se sigue en forma de juicio, por lo cual, las partes gozan

de igualdad procesal entre otros derechos. En ese sentido, se reporta la actividad durante el periodo del 2016, respecto a los asuntos sustanciados en el sector privado mediante ese procedimiento:

Se recibieron 243 asuntos, adicionados a los 40 asuntos en trámite derivados del 2015. Fueron concluidos en el mismo año 2016, 243 expedientes de la siguiente manera:

Conciliados	16
Sobreseídos	50
Resueltos por el Pleno del Instituto: Confirmando	24
Resueltos por el Pleno del Instituto: Revocando	9
Resueltos por el Pleno del Instituto: Modificando	9
Ordenando hacer efectivo el derecho del Titular (Artículo 48 de la LFPDPPP)	5
Desechados	40
Por reconducción a otras áreas	3
Por acuerdo de no presentado	71
Concluidos por acuerdo de Conclusión del Expediente	16

Etapa de conciliación

Es importante señalar que el procedimiento de protección de derechos contiene una etapa de conciliación, cuya característica fundamental estriba en que las partes manifiestan su voluntad para sujetarse a dicho medio alternativo de solución de controversias. En el 2016, fueron 44 los casos en los que las partes decidieron sujetarse a la conciliación y en 16 las partes lograron avenir sus intereses suscribiendo un acuerdo conciliatorio, es decir en el 36% de los casos.

Casos de incompetencia del Instituto

Otro dato importante por destacar es que de los 40 asuntos desechados, 15 corresponden a la incompetencia del Instituto y ello es debido a que el titular de los datos personales considera responsable a medios de comunicación por las notas periodísticas publicadas, en cuyo contenido se advierten datos personales. En este sentido, se considera que los datos personales que contienen dichas notas son producto del ejercicio de actividad periodística; del derecho a la información y, por lo tanto, es procedente una acción distinta a la de la protección de datos personales en términos de la LFPDPPP.

Casos destacados de protección de derechos: acceso al expediente clínico

Un caso que se puede destacar dentro del ejercicio que se informa es el del derecho de acceso a los datos personales de los titulares a su expediente clínico y en el que el Responsable manifestó que no contaba con el mismo toda vez que había sido destruido con base en la norma oficial mexicana que determina mantener la información durante un plazo de 5 años. Lo significativo del caso es que el Instituto resolvió que dicho plazo no había transcurrido, pues aun faltando unos días para el vencimiento del plazo señalado le asistía al Responsable la obligación de mantener la información disponible para sus titulares, puesto que dicho plazo contemplado por la norma es un mínimo. Se argumenta en la resolución del Instituto la importancia del derecho de acceso a los datos personales contenidos en un expe-

diente clínico como una puerta de entrada de otros derechos humanos de los titulares como el derecho a la salud y en el caso específico motivado por el interés superior del menor. Por lo tanto, el Instituto resolvió que el Responsable debía dar cumplimiento al derecho solicitado por los titulares y determinó el inicio del procedimiento de imposición de sanciones.

5. PROCEDIMIENTO DE INSPECCIÓN Y SANCIÓN

Dentro de las actividades de inspección que lleva a cabo el INAI se encuentra la sustanciación y resolución de los procedimientos de investigación y de verificación, a saber:

Procedimiento de investigación

– Procedimiento de investigación. El procedimiento de investigación es definido como el conjunto de actos que lleva a cabo la Dirección General de Investigación y Verificación del INAI con la finalidad de allegarse de elementos suficientes a efecto de dilucidar los hechos denunciados, de forma previa al procedimiento de verificación. En ese sentido, el procedimiento de investigación se podrá iniciar, según sea el caso: i) de oficio, cuando se presuma de manera fundada y motivada alguna violación a la normatividad aplicable en materia de protección de datos personales; o ii) a petición de parte, a través de la presentación de una denuncia. Cuando se hayan cumplido con los requisitos legales para la presentación de una denuncia, se formularán los requerimientos que se estimen necesarios al denunciante, al denunciado y/o a cualquier tercero, para que se proporcione la información necesaria. Una vez que se cuente con elementos suficientes para resolver lo que en derecho corresponda, la Dirección General de Investigación y Verificación podrá emitir lo siguiente:

  - Acuerdo de determinación. Se expedirá, de manera fundada y motivada, cuando el Instituto no cuente con elementos suficientes para acreditar la comisión de actos contrarios a lo establecido por la ley de la materia.
  - Acuerdo de Inicio de Procedimiento de Verificación. Se dictará cuando, de manera fundada y motivada, se presuma que el Responsable incurrió en acciones u omisiones que constituyen un probable incumplimiento a la ley de la materia.

Procedimiento de investigación: duración máxima

El Procedimiento de investigación tendrá una duración máxima de noventa días hábiles, contados a partir de la fecha en que se haya emitido el acuse de recibo de la denuncia correspondiente, o bien, a partir de la fecha en que se haya dictado el acuerdo de inicio de Procedimiento de Investigación; dicho plazo podrá ser ampliado por una vez y hasta por un periodo igual, cuando exista causa justificada.

Procedimientos de investigación durante 2016:

Tipo de expediente	2016		
	Iniciados	Concluidos	En trámite
Investigaciones Preliminares Sector Privado	279	212	67
Investigaciones Preliminares Sector Público	4	0	4
Investigaciones Preliminares Mixtas	3	2	1
TOTAL	286	214	72

Procedimiento de verificación

– Procedimiento de verificación. El procedimiento de verificación es el conjunto de actos mediante los cuales el INAI, a través de la Dirección General de Investigación y Verificación, vigila el cumplimiento de la normatividad en materia de protección de datos personales. El Procedimiento de Verificación tendrá una duración máxima de ciento ochenta días hábiles, en el caso del sector privado, y de cincuenta días hábiles, tratándose del sector público; dichos plazos comenzarán a contar a partir de la fecha en que se haya dictado el Acuerdo de Inicio. En el caso del sector privado, el Pleno del Instituto podrá ampliar por una vez y hasta por un periodo igual dicho plazo. En esa tesitura, el Procedimiento de Verificación se podrá iniciar: a) de oficio, si se presume de manera, fundada y motivada la existencia de un probable incumplimiento a la normatividad en la materia; b) a petición de parte, derivado de una denuncia que haya dado origen a un procedimiento de investigación. El desarrollo del Procedimiento de Verificación se podrá llevar a cabo mediante requerimientos de información, o bien, a través de visitas de verificación con la finalidad de allegarse de elementos de convicción sobre el tratamiento otorgado a los datos personales materia del procedimiento. El procedimiento de verificación concluirá con la resolución que emita el Pleno del Instituto, en la cual, en su caso, se podrán establecer las medidas que deberá adoptar el Responsable en el plazo que la misma establezca; asimismo, la resolución del Pleno podrá instruir el inicio del procedimiento de imposición de sanciones o establecer un plazo para su inicio. Finalmente, cabe señalar que en contra de la resolución al procedimiento de verificación, se podrá interponer el juicio de nulidad ante el Tribunal Federal de Justicia Administrativa.
Procedimientos de verificación durante 2016:

Tipo de expediente	2016		
	Iniciados	Concluidos	En trámite
Verificaciones Sector Privado	92	72	20
TOTAL	92	72	20

Entre los procedimientos de verificación instruidos por el INAI durante 2016, cabe destacar los siguientes:

- Iniciado a partir de una denuncia por probables incumplimientos a la LFPDPPP por parte de una persona física, deri-

vado de la presunta divulgación de datos personales. En ese sentido, se requirió al Responsable diversa información, sin embargo, transcurrido el plazo legal otorgado fue omiso en emitir pronunciamiento alguno, por lo que obstruyó los actos de verificación de la autoridad. Ahora bien, el Responsable reconoció expresamente que pegó en la parte interior del inmueble en el que se desempeña como Administrador Condómino un documento que contiene el nombre y domicilio de la denunciante, por lo que divulgó ante terceros dichos datos personales, vulnerando así el deber de confidencialidad al que se encuentra sujeto y cambió sustancialmente la finalidad originaria del tratamiento por la que obtuvo los datos personales, sin que se haya advertido que obtuvo el consentimiento de la titular para tal efecto. De igual manera, el Responsable incumplió los principios de consentimiento, información, responsabilidad y licitud, ya que fue omiso en dar respuesta al requerimiento formulado, y por lo tanto, en proporcionar la evidencia documental que acreditara que recabó el consentimiento y que puso a disposición de la denunciante su Aviso de Privacidad, dejando de garantizar que se diera debido tratamiento a los datos personales bajo su cuidado y custodia, de conformidad con los principios establecidos en la normatividad aplicable; en contravención a las disposiciones de la LFPDPPP y la normatividad que de ella deriva; por tal motivo se ordenó iniciar el procedimiento de imposición de sanciones.

- Iniciado con motivo de una denuncia por presuntos incumplimientos a la LFPDPPP por parte de una institución educativa, debido a que la Responsable recabó datos personales de dos menores sin consentimiento de los padres, para enviarles una carta en las que les ofrece una beca. Con base en las constancias integradas en el expediente, se advirtió que la Responsable recabó y dio tratamiento a los datos personales de las menores hijas de los denunciantes sin obtener previamente el consentimiento expreso de quienes ejercen la patria potestad. Asimismo, se consideró que la Responsable incumplió los principios de información, responsabilidad y licitud, ya que omitió hacer del conocimiento de los denunciantes las finalidades para las que se tratarían los datos personales recabados, a través de la puesta a disposición del aviso de privacidad, y tampoco adoptó las medidas necesarias para privilegiar los intereses de las menores de edad, sujetando el tratamiento al consentimiento previo de sus padres, incumpliendo lo establecido en el marco jurídico de la materia; por tal motivo, se ordenó iniciar el procedimiento de imposición de sanciones.
- Se inició por una denuncia en la que se manifestó que una institución bancaria utilizó datos personales para fines de publicidad y mercadotecnia a pesar de que el denunciante le solicitó que no fueran empleados para ningún propósito de

promoción comercial y oferta de servicios financieros. De tal forma, se acreditó que la Responsable envió diversos correos electrónicos con fines de publicidad y mercadotecnia aún y cuando le fue solicitado el cese en el tratamiento de los datos personales del titular, por lo que se concluyó que continuó con su uso ilegítimo. Además, se apreció un presunto incumplimiento a los principios de responsabilidad y licitud, al haber sido omiso en implementar las medidas necesarias y adecuadas para garantizar el debido tratamiento de los datos personales que se encuentran bajo su custodia y posesión, con el objeto de velar y responder debidamente por el cumplimiento de los principios de protección de los datos personales establecidos por la ley de la materia, dejando de apegar su actuación a las disposiciones de la LFPDPPP; motivo por el cual, se ordenó el inicio del procedimiento de imposición de sanciones.

- Este asunto fue iniciado a partir de una denuncia en la que se manifestó que después de abrir una cuenta de nómina, el ejecutivo de una institución bancaria que atendió a la titular le envió mensajes de texto vía "WhatsApp" para tratar asuntos personales. En ese sentido, se acreditó que la Responsable cambió sustancialmente la finalidad inicial del tratamiento de los datos personales de la denunciante, ya que reconoció expresamente que su empleado aceptó que hizo un uso indebido de la información confidencial de la titular. Del mismo modo, al no haber demostrado que recabó nuevamente el consentimiento de la denunciante al tratar sus datos personales para una finalidad distinta a la que dio origen la recolección de los mismos, la Responsable incumplió el principio de consentimiento. Finalmente, se advirtió un presunto incumplimiento a los principios de responsabilidad y licitud, pues la Responsable no adoptó las medidas necesarias y adecuadas para garantizar el debido tratamiento de los datos personales que se encuentran bajo su custodia y posesión, con el objeto de velar y responder debidamente por el cumplimiento de los principios de protección de los datos personales establecidos por la ley de la materia, en contravención a las disposiciones de la LFPDPPP; por lo que se ordenó iniciar el procedimiento de imposición de sanciones.

Procedimiento de imposición de sanciones

– Procedimiento de imposición de sanciones. El procedimiento de imposición de sanciones es un procedimiento administrativo que procede a la conclusión de un procedimiento de verificación o de un procedimiento de protección de derechos cuya resolución determine el inicio de aquél. Durante el periodo de 2016, se dieron las siguientes actividades con respecto a los asuntos sustanciados. Se iniciaron 84 procedimientos de imposición de sanciones, aunados a 21 en trámite de los años anteriores. De ellos 53 fueron concluidos y 52 quedaron en trámite. Durante el año 2016, se impusieron multas por un monto total de 93 millones, 135 pesos, con 88 centavos a los

responsables por infracciones a la LFPDPPP y a los principios que ella contempla.

Principios transgredidos

Es importante destacar de las resoluciones emitidas por el Instituto, los principios que fueron transgredidos y que fueron el sustento de las sanciones impuestas: Principio de licitud, en 34 veces; Principio de consentimiento, 7 veces; Principio de información, 16 ocasiones; Principio de calidad, 4 ocasiones; Principio de lealtad, 2 veces; Principio de responsabilidad, 28 veces.

La multa más elevada

En cuanto a un caso concreto que vale la pena resaltar, es que la multa más elevada del ejercicio que se informa, fue de 8 millones, 949 mil 274 pesos, impuesta a la infractora por transgredir los principios de lealtad, responsabilidad y licitud al tratar los datos de los titulares con fines distintos para los cuales le fueron proporcionados, así como divulgar información patrimonial sin el consentimiento de sus suscriptores ya que su objeto social consiste prestar servicios de actividades deportivas.

6. COOPERACIÓN CON OTRAS INSTITUCIONES PÚBLICAS

Ámbito nacional: información, capacitación y sensibilización

Ámbito nacional. Una tarea central del INAI es extender el conocimiento de la LFTAIP, de la LGTAIP y de la LFPDPPP entre público en general, así como abordar los matices fundamentales de los derechos que resguardan esas leyes, entre especialistas y servidores públicos que se ocupan de la realización y operación del ejercicio de ese derecho. De esta manera, a través de eventos como foros y seminarios, se crean las condiciones ideales para que población abierta y servidores públicos accedan a conocimientos especializados y académicos en las materias de las que es garante el INAI.[11]

Día Internacional de Protección de Datos

El Día Internacional de Protección de Datos se celebró el 28 y 29 de enero con dos jornadas en la Ciudad de México y en siete ciudades del país. Las jornadas tuvieron como objetivos principales promover el ejercicio del derecho a la protección de datos personales y generar conocimiento para un pleno ejercicio de este derecho.

Convenios de colaboración

Otro aspecto importante del quehacer institucional es el acercamiento del Instituto con instituciones nacionales a través de mecanismos de colaboración. Durante 2016, el INAI suscribió convenios de colaboración con diversas instituciones con el objeto de llevar a cabo actividades y estrategias para fortalecer la cultura de la transparencia, acceso a la información y protección de datos personales. Se destacan los convenios de colaboración con sindicatos, con la Auditoría Superior de la Nación, Banco de México, Partidos Políticos, Cámara de Diputados, Barra Mexicana Colegio de Abogados, Procuraduría Federal del Consumidor.

El Instituto ha firmado convenios de colaboración con distintas cámaras y asociaciones, siendo uno de los propósitos la realización de acciones de capacitación a fin de incrementar el conocimiento de sus

[11] Informe de Labores 2016, p. 309, disponible en http://inicio.ifai.org.mx/Informes%202016/Informe%20de%20labores%202016.pdf

afiliados en materia de protección de datos personales. En este Programa se realizaron 41 acciones de capacitación en las que participaron 859 integrantes de las asociaciones y cámaras nacionales siguientes[12]: Asociación Mexicana de Instituciones de Seguros (AMIS); Confederación Patronal de la República Mexicana (COPARMEX); Asociación Mexicana de la Industria Automotriz, A.C. (AMIA); Asociación Mexicana de Proveedores Autorizados de Certificación (AMEXIPAC); Asociación de Bancos de México (ABM).

Ámbito internacional: estándares

Ámbito internacional. La labor internacional del INAI tiene como objetivo primordial acreditarlo como un órgano garante eficaz en la tutela del derecho de la protección de datos personales en México, así como allegarse las mejores prácticas para generar una política idónea ajustada a los más altos estándares internacionales en materia de protección de datos personales e impulsar la creación de un sistema normativo regional que permita, eventualmente, el desarrollo de un órgano que dictamine, evalúe y establezca los niveles adecuados de confianza de los mecanismos nacionales de protección de datos personales.

Fortalecimiento de la imagen internacional de México

El fortalecimiento de la imagen internacional de México, como actor responsable en el escenario mundial debe sustentarse en la certidumbre de que los asuntos públicos se conducen con transparencia, garantizando el acceso a la información pública, la protección de datos personales y la rendición de cuentas.

Participación del INAI en foros internacionales

Durante 2016 se reforzó la participación del INAI en diversos foros internacionales, se mantuvo la presencia en grupos de regiones económicas a las que pertenece México y en grupos *ad hoc* enfocados a la defensa y promoción de los derechos que el Instituto tutela, de los cuales destacan los siguientes en materia de protección de datos13:

- En su calidad de presidente de la Red Iberoamericana de Protección de Datos (RIPD), el INAI participó en el XIV Encuentro Iberoamericano de Protección de Datos y en la 4° Conferencia Internacional sobre Protección de Datos, en Santa Marta, Colombia. El INAI planteó la posibilidad de construir un acuerdo regional que busque maximizar el ejercicio y respeto del derecho a la protección de datos personales en toda la región iberoamericana, que sirva de referente normativo.
- Participación en el Taller sobre Protección de Datos y Acción Internacional Humanitaria, en La Antigua Guatemala.
- Participación en la VI Jornada Iberoamericana de Derecho del Trabajo y Seguridad Social, en Santo Domingo, República Dominicana. El INAI destacó la importancia de contribuir a una conciencia social sobre el valor de la protección de datos personales en las relaciones laborales, como un derecho fundamental.
- Participación en la Reunión Única del Comité Ad-Hoc sobre Protección de Datos (CAHDATA)-Convenio 108 y en la 33° Reunión Plenaria del Comité Consultivo del Convenio 108, en Estrasburgo, Francia. En ambas comisiones, el INAI se enfocó al fortalecimiento institucional.

[12] *Ibíd.*, p.235.
[13] *Ibíd.*, pp. 323-325.

– Participación en el 45° de Autoridades de Privacidad de Asia-Pacífico (APPA Forum) en Singapur. Este espacio sirvió para posicionar al INAI como un referente en la materia ante diversas autoridades de Privacidad.
– Participación en la 39ª Reunión de la Mesa Directiva Del Comité Consultivo Del Convenio 108 en París, Francia.
– Participación en la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP) en Marruecos.
– Organización del 46° Foro APPA en la Ciudad de Manzanillo, Colima. En este foro, representantes de países integrantes del Foro e invitados se dieron cita por primera vez en un país de América Latina.

7. COOPERACIÓN CON LA SOCIEDAD

El INAI se ha caracterizado por ser una institución pública con un importante vínculo con la ciudadanía y la población en general. Sus atribuciones lo distinguen como un actor clave en el fortalecimiento de la confianza ciudadana en las autoridades así como en la conformación de una sociedad más activa, informada y que exige cuentas a los entes públicos. El Instituto busca robustecer la vida democrática nacional e incentivar en la población el uso de los derechos de acceso a la información y protección de datos personales.

Herramientas a disposición de la ciudadanía

Desde el 2013, el INAI ha desarrollado y puesto a disposición de la ciudadanía diversas herramientas que tienen como objetivo orientar a los responsables y encargados del tratamiento de datos personales en cumplimiento de las obligaciones establecidas por la LFPDPPP. A continuación se enlistan las principales acciones que realizó el INAI durante 2016 para promover y facilitar el cumplimiento de la normativa en materia protección de datos personales[14]:

Aplicación para dispositivos móviles

– Lanzamiento de la aplicación para dispositivos móviles Protección INAI, desarrollada por cuatro jóvenes emprendedores de la ciudad de Puebla, en el marco del Día Internacional de Protección de Datos Personales, celebrado el 28 de enero. Esta aplicación cumple con el objetivo de crear conciencia acerca del valor intrínseco que poseen los datos de las personas y de la necesidad de protegerlos.

Guía para el Borrado Seguro de Datos

– Elaboración de la Guía para el Borrado Seguro de Datos Personales la cual proporciona a los responsables del tratamiento de estos datos, los métodos y técnicas recomendados para la eliminación segura de los mismos, que impidan la recuperación no autorizada y mal uso de datos personales.

Lineamientos para el uso de hiperenlaces o hipervínculos

– Publicación de los Lineamientos para el uso de hiperenlaces o hipervínculos en una página de Internet del INAI, para dar a conocer avisos de privacidad a través de medidas compensatorias.
– Otras actividades relevantes en materia de facilitación y autorregulación: estudio para fortalecer la estrategia de educación

[14] *Ibíd.*, pp.142-146.

cívica y cultura para el ejercicio del derecho a la protección de los datos personales por parte de los titulares.

8. OTRAS ACTIVIDADES

Colaboración interinstitucional y con la sociedad civil

El INAI ha creado mecanismos de colaboración interinstitucional en los tres órdenes de gobierno, órganos garantes y con la sociedad civil, con el propósito de capacitar, asesorar y promover el conocimiento y el ejercicio del derecho de acceso a la información y de protección de datos personales. Estas iniciativas se reflejan en la colaboración de organizaciones de la sociedad civil, instituciones académicas y órganos garantes locales, lo que ha fortalecido la promoción del ejercicio de los derechos que tutela el INAI y de vinculación de esta Institución con el resto de la sociedad, los órganos garantes y las instituciones estatales[15].

Las estrategias del INAI de vinculación con la sociedad han permitido crear y reforzar alianzas, por medio de las cuales se ha logrado transmitir conocimientos prácticos del ejercicio de acceso a la información y protección de datos personales entre instituciones académicas y organizaciones de la sociedad civil (OSC).

Algunas de las actividades de vinculación con la sociedad civil durante 2016 son:[16]

Proyecto de Transparencia en Red

– Proyecto de Transparencia en Red: busca promover la vinculación y fomentar alianzas estratégicas entre el Instituto y organizaciones de la sociedad civil. Se realizaron 10 eventos de sensibilización, en los cuales se impartieron 22 talleres, con la asistencia de 510 personas integrantes de organizaciones de la sociedad civil, de comunidades académicas y población en general.

Mesas de diálogo

– Mecanismos de Diálogo por la Transparencia y por la Protección de Datos Personales (Mesas de Diálogo): acercamiento con los titulares de 13 instituciones públicas, con representantes de organizaciones de la sociedad civil y de instituciones académicas, así como de organismos multilaterales.

Programa de Sensibilización de Derechos

– Programa de Sensibilización de Derechos (PROSEDE): Programa de Sensibilización de Derechos con el objetivo de fomentar la cultura de la transparencia y rendición de cuentas por medio de la vinculación con la sociedad civil organizada como aliado estratégico y promotor de los derechos tutelados por el INAI. Los temas centrales de los proyectos financiados con el PROSEDE son: promoción y ejercicio de los derechos a la información pública y la protección de datos personales, promoción del derecho a saber, el ejercicio de los derechos ARCO, transparencia, entre otros.

– Talleres de sensibilización: se impartieron en materia del derecho de acceso a la información y de protección de datos personales; adicionalmente, se realizaron pláticas y conferencias en universidades y preparatorias en esta materia en la Ciudad de México y en algunas entidades federativas.

---

[15] *Ibíd.*, p. 254.

[16] *Ibíd.*, pp. 254-261.

Centro de Atención a la Sociedad

– Atención ciudadana: el Centro de Atención a la Sociedad (CAS) orienta, asesora, recibe y responde consultas que formulan los particulares al INAI, las cuales se registran mediante un sistema que administra la respuesta otorgada por los canales de atención establecidos en los lineamientos que rigen su operación, ello bajo un marco normativo cuyo objeto constituye la observancia obligatoria de procedimientos vinculantes para el personal del Instituto que permita brindar una correcta y oportuna asesoría respecto de los diversos servicios que son prestados.

Actividades de capacitación

La capacitación es considerada por el Instituto como uno de los procesos prioritarios que contribuye al cumplimiento del segundo objetivo estratégico: promover el pleno ejercicio de los derechos de acceso a la información pública y de protección de datos personales, así como la transparencia y apertura de las instituciones públicas[17]. Las acciones de capacitación forman parte de un proceso que acompaña la generación de cambios en los patrones de actuación de los sujetos obligados, de los servidores públicos y de la ciudadanía en general en favor de una cultura basada en la transparencia, la apertura de la información, el respeto a la autodeterminación informativa y la rendición de cuentas. Durante el 2016 se impartieron capacitaciones dirigidas a:

– Sujetos obligados (Ciudad de México y entidades federativas): las modalidades de capacitación que se utilizan para lograr la mayor cobertura posible son presencial y en línea a través del Centro Virtual de Capacitación del INAI. Las capacitaciones fueron en materia de transparencia, acceso a la información y protección de datos personales, LGTAIP, LFTAIP.
– Sujetos Regulados por la LFPDPPP (micro, pequeñas y medianas empresas, emprendedores, así como a integrantes de cámaras de comercio y asociaciones): el INAI mantiene un programa permanente de capacitación en las modalidades presencial y en línea en materia de protección de datos personales. Algunas de las actividades de capacitación se realizaron en coordinación con la Secretaría de Economía, por conducto del Instituto Nacional del Emprendedor.
– Estudiantes: se dio continuidad a las actividades de formación educativa dirigida a estudiantes de licenciatura y posgrado, todo lo anterior a partir de la alianza del INAI con instituciones de educación superior de reconocido prestigio en el ámbito nacional. Estas actividades incluyeron el desarrollo del proyecto denominado "Aula de Protección de Datos Personales" en coordinación con la Benemérita Universidad Autónoma de Puebla, el Diplomado en línea en Protección de Datos Personales coordinado con la Universidad Autónoma de Guadalajara y la Maestría en Derecho en el Campo del Conocimiento del Derecho a la Información mediante Convenio con la Universidad Nacional Autónoma de México.

[17] *Ibíd*. p. 215.

9. DATOS ESTADÍSTICOS

Procedimiento de Protección de Derechos: 243 solicitudes

Procedimiento de Protección de Derechos (LFPDPPP) al 31 de diciembre de 2016[18]. El número total de asuntos sustanciados en el ejercicio 2016 se incrementó en 69.7% con respecto a los sustanciados en el ejercicio 2015:

- Total de solicitudes de protección de derechos (En una solicitud puede pedirse más de un derecho ARCO): 243.
- Total de asuntos sustanciados: 112.
- Total de asuntos no sustanciados: 131.

Sectores con mayor número de verificaciones: servicios financieros y seguros

Procedimientos de verificación en materia de Datos Personales (sector privado): sectores con mayor número de verificaciones durante 2016[19]:

- Servicios financieros y de seguros: 32.
- Servicios profesionales, científicos y técnicos: 11.
- Información en medios masivos: 9.
- Comercio al por menor: 5.
- Otros servicios excepto actividades gubernamentales: 7.
- Servicios de apoyo a los negocios: 4.
- Servicios de salud y de asistencia social: 3.
- Servicios educativos: 7.
- Industrias manufactureras: 4.
- Servicios de esparcimiento culturales y deportivos, y otros servicios recreativos: 1.
- Comercio al por mayor: 1.
- Servicios inmobiliarios y de alquiler de bienes muebles e intangibles: 4.
- Construcción: 2.
- Transportes, correos y almacenamiento: 0.
- Servicios de alojamiento temporal y de preparación de alimentos y bebidas: 2.

Procedimientos de verificación en materia de Datos Personales al 31 de diciembre de 2016[20] (Verificaciones sector privado):

- Iniciadas: 92.
- Concluidas: 85.
- En trámite: 7.

Procedimiento de imposición de sanciones: 84 procedimientos instaurados

Procedimiento de imposición de sanciones en 2016 (LFPDPPP)[21]:

- Procedimientos instaurados: 84.
- Procedimientos concluidos en 2016: 53.

---

[18] Procedimiento de Protección de Derechos, disponible en http://inicio.inai.org.mx/SitePages/proteccionDeDatosPersonalesEstadisticas.aspx, seleccionar "4. Procedimiento de Protección de Derechos".

[19] Procedimientos de verificación en materia de Datos Personales (sector privado), disponible en http://inicio.inai.org.mx/SitePages/proteccionDeDatosPersonalesEstadisticas.aspx, seleccionar "2. Estadísticas verificaciones por sectores".

[20] Procedimientos de verificación en materia de Datos Personales al 31 de diciembre de 2016, disponible en http://inicio.inai.org.mx/SitePages/proteccionDeDatosPersonalesEstadisticas.aspx, seleccionar "3. Estadísticas verificaciones con gráfico".

[21] Procedimiento de imposición de sanciones, disponible en http://inicio.inai.org.mx/SitePages/proteccionDeDatosPersonalesEstadisticas.aspx, seleccionar "5. Procedimiento de Imposición de Sanciones".

– Importe de las multas: 93.000.135,88 pesos.

Desarrollo del ejercicio del derecho de protección de datos personales en el sector público durante 2016:

– Solicitudes de acceso y corrección a datos personales: 41.887.
– Respuestas a solicitudes de acceso y corrección a datos personales: 32.682.
– Recursos de revisión sobre solicitudes de acceso y corrección a datos personales interpuestos ante el INAI: 1.134.
– Recursos de revisión sobre solicitudes de acceso y corrección a datos personales resueltos: 1.134.

Datos del Sector público

Los 5 sujetos obligados con más solicitudes de acceso y corrección de datos personales:

– Instituto Mexicano del Seguro Social: 24.069.
– Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado: 3.040.
– Hospital Regional de Alta Especialidad de Ixtapaluca: 1.799.
– Instituto Nacional de Cardiología Ignacio Chávez: 1.401.
– Instituto del Fondo Nacional de la Vivienda para los Trabajadores: 1.155.

IX. PERÚ

1. INTRODUCCIÓN

El derecho de Habeas Data en la Constitución

La Constitución Política del Perú de 1993 recoge como un derecho fundamental en el artículo 2.6 el derecho de toda persona "a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar, de forma que la protección de los datos personales ha existido, con rango constitucional desde 1993, aun sin autoridad administrativa y sin legislación propia y ha estado, además, acompañada de la correspondiente acción de garantía, a través del Habeas Data que, conforme al artículo 200, de la propia Constitución "procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5 y 6 de la Constitución".

Esta figura se legisló, se interpretó y se desarrolló, principalmente, como herramienta de acceso a la información y así puede apreciarse del contenido de la Ley 26.301, Ley de Habeas Data, de mayo de 1994, pero es con la entrada en vigencia del Código Procesal Constitucional en diciembre de 2004, que reguló de forma unificada el Habeas Corpus, el Amparo, la Acción de Cumplimiento, la Acción Popular, la Acción de Inconstitucionalidad y el Habeas Data, que esta última se describe como una acción de garantía en protección del derecho de "acceso" a la información que incluye los derechos a conocer, actualizar, incluir, suprimir o rectificar información o datos personales.

Ley de Protección de Datos Personales y creación de la Autoridad Nacional de Protección de Datos Personales

La Ley 29.733, de Protección de Datos Personales (LPDP), publicada en el Diario Oficial El Peruano el 3 de julio de 2011, desarrolla el derecho fundamental a la protección de los datos personales y crea la Autoridad Nacional de Protección de Datos Personales, a cargo del Ministerio de Justicia, a través de la Dirección Nacional de Justicia, órgano de línea del mencionado Ministerio. Posteriormente, con la Ley 29.809, de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, publicada el 8 de diciembre de 2011, se crea el Despacho Viceministerial de Derechos Humanos y Acceso a la Justicia, que tiene entre sus funciones la de supervisar a la Autoridad Nacional de Protección de Datos Personales. En ese sentido, el 20 de abril de 2012 se publicó el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado mediante Decreto Supremo 011-2012-JUS, situando a la Autoridad Nacional de Protección de Datos Personales en el nivel de dirección general individual (órgano de línea), denominada Dirección General

de Protección de Datos Personales, bajo la esfera del Despacho Viceministerial de Derechos Humanos.

Funciones de la Autoridad Nacional

La Autoridad Nacional de Protección de Datos Personales (APDP) tiene funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras. La Autoridad Nacional de Protección tiene a su cargo también el Registro Nacional de Protección de Datos Personales, donde los titulares de los bancos de datos de las entidades públicas y privadas inscriben sus bancos de datos personales.

Las funciones de la Autoridad Nacional de Protección de Datos Personales son las siguientes:

- Representar al país ante las instancias internacionales en materia de protección de datos personales.
- Cooperar con las autoridades extranjeras de protección de datos personales para el cumplimiento de sus competencias y generar mecanismos de cooperación bilateral y multilateral para asistirse entre sí y prestarse debido auxilio mutuo cuando se requiera.
- Administrar y mantener actualizado el Registro Nacional de Protección de Datos Personales.
- Publicitar, a través del portal institucional, la relación actualizada de bancos de datos personales de administración pública y privada.
- Promover campañas de difusión y promoción sobre la protección de datos personales.
- Promover y fortalecer una cultura de protección de los datos personales de los niños y de los adolescentes.
- Coordinar la inclusión de información sobre la importancia de la vida privada y de la protección de datos personales en los planes de estudios de todos los niveles educativos y fomentar, asimismo, la capacitación de los docentes en estos temas.
- Supervisar el cumplimiento de las exigencias previstas en la LPDP, para el flujo transfronterizo de datos personales.
- Emitir autorizaciones, cuando corresponda, conforme al reglamento de la LPDP
- Absolver consultas sobre protección de datos personales y el sentido de las normas vigentes en la materia, particularmente sobre las que ella hubiera emitido.
- Emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, la que es vinculante.
- Emitir las directivas que correspondan para la mejor aplicación de lo previsto en esta Ley y en su reglamento, especialmente en materia de seguridad de los bancos de datos personales, así como supervisar su cumplimiento, en coordinación con los sectores involucrados.
- Promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales.
- Celebrar convenios de cooperación interinstitucional o internacional con la finalidad de velar por los derechos de las personas en materia de protección de datos personales que son tratados dentro y fuera del territorio nacional.

– Atender solicitudes de interés particular del administrado o general de la colectividad, así como solicitudes de información.
– Conocer, instruir y resolver las reclamaciones formuladas por los titulares de datos personales por la vulneración de los derechos que les conciernen y dictar las medidas cautelares o correctivas.
– Velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores.
– En el marco de un procedimiento administrativo en curso, solicitado por la parte afectada, obtener de los titulares de los bancos de datos personales la información que estime necesaria para el cumplimiento de las normas sobre protección de datos personales y el desempeño de sus funciones.
– Supervisar la sujeción del tratamiento de los datos personales que efectúen el titular y el encargado del banco de datos personales a las disposiciones técnicas que ella emita y, en caso de contravención, disponer las acciones que correspondan conforme a la LPDP.
– Iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la LPDP y en su reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento.
– Las demás funciones que le asignen la LPDP y su reglamento.

Para cumplir con las funciones mencionadas, la Dirección General de Protección de Datos Personales cuenta con cuatro unidades orgánicas: La Dirección de Normatividad y Asistencia Legal, la Dirección de Supervisión y Control, la Dirección de Sanciones y la Dirección de Registro Nacional de Protección de Datos Personales.

2. PLANIFICACIÓN

Planes del Ministerio de Justicia y Derechos Humanos

El Ministerio de Justicia y Derechos Humanos cuenta con planes estratégicos, los que responden a los siguientes planes:

– Plan Estratégico Institucional 2016-2018, cuyo objetivo estratégico institucional 2 es "Garantizar la protección de datos personales de la población."
– Plan Estratégico Sectorial Multianual 2015-2021, cuyo objetivo estratégico q es "Fomentar el respeto irrestricto de los Derechos Humanos por parte de la sociedad civil y el Estado", incluyendo dentro de las acciones estratégicas la de "Promover el respeto del Derecho a la Protección de Datos Personales y garantizar su cumplimiento".

En ese marco, en el Plan Operativo Institucional del Ministerio de Justicia y Derechos Humanos del año 2016 se contemplaron actividades específicas que debía cumplir la Dirección General de Protección de Datos Personales y sus unidades orgánicas. Cabe señalar que, entre las actividades contempladas se encuentra la elaboración de un

Plan de Difusión y un Plan de Supervisión, sobre los cuales se debe rendir cuenta de forma trimestral.

3. ACCIÓN NORMATIVA

Directivas dictadas por la Autoridad peruana

Como se señaló líneas arriba, la APDP tiene entre sus funciones emitir las directivas que correspondan para la mejor aplicación de lo previsto en esta Ley y en su reglamento, especialmente en materia de seguridad de los bancos de datos personales, así como supervisar su cumplimiento, en coordinación con los sectores involucrados. En ese marco, la APDP ha aprobado dos directivas:

- La Directiva sobre Protección de Datos Personales y Programas Sociales, aprobada en el año 2014, mediante la Resolución Directoral 60-2014-JUS/DGPDP, que tiene como objetivo establecer las disposiciones para la protección de datos personales en el marco de los procedimientos para la construcción, administración, sistematización y actualización del Padrón General de Hogares y el Registro Nacional de Usuarios, a cargo del Ministerio de Desarrollo e Inclusión Social.
- Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales, aprobada en el año 2013, mediante la Resolución Directoral 19-2013-JUS/DGPDP que orienta sobre las condiciones, los requisitos y las medidas técnicas que se deben tener en cuenta para el cumplimiento de la Ley 29.733, de Protección de Datos Personales, y su reglamento, aprobado a través del Decreto Supremo 003-2013-JUS. Esta última, ha permitido que los titulares de bancos de datos personales y encargados de tratamiento adecuen las medidas de seguridad de sus bancos de datos personales.

Opiniones técnicas vinculantes

Por otro lado, la APDP tiene la función de emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, la que es vinculante. En ese marco, en el año 2016 la Dirección General de Protección de Datos Personales ha emitido siete opiniones técnicas sobre proyectos normativos referidos parcial o totalmente a datos personales.

Propuesta normativa para la creación de una Autoridad Nacional de Transparencia

La Autoridad Nacional de Protección de Datos Personales participó en el Grupo de Trabajo encargado de elaborar un informe técnico que contenga una propuesta normativa para la creación de una Autoridad Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, que se encargue de desarrollar ambos derechos fundamentales. El 12 de setiembre de 2016 se aprobó la Resolución Ministerial 0268-2016-JUS, a través de la cual se creó el Grupo de Trabajo encargado de elaborar un informe técnico que contenga una propuesta normativa para la creación de una Autoridad Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. En ese sentido, el 19 de setiembre se instaló el grupo de trabajo mencionado y se llevaron a cabo trece sesiones de trabajo. El Director General de Protección de Datos Personales tuvo a cargo la presidencia de dicho Grupo de Trabajo.

Como producto de las sesiones, el Grupo de Trabajo culminó con la elaboración de la Exposición de Motivos, así como de la fórmula normativa del Proyecto de Decreto Legislativo que propone la creación del Sistema Nacional para la Transparencia, Acceso a la Información Pública y Protección de Datos Personales; así como la Autoridad para la Transparencia, Acceso a la Información Pública y Protección de Datos Personales y regular su funcionamiento. Dicho proyecto fue presentado a la Ministra el 22 de noviembre de 2016. Sin embargo, la propuesta no fue aprobada en su totalidad, ya que a través del Decreto Legislativo 1.353, publicado el 7 de enero de 2017, se creó la Autoridad Nacional de Transparencia y Acceso a la Información Pública, a cargo del Ministerio de Justicia y Derechos Humanos, sin incluir el tema de protección de datos personales.

4. PROCEDIMIENTOS DE GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS

32 procedimientos trilaterales de tutela en 2016

La APDP tiene entre sus funciones la de conocer, instruir y resolver las reclamaciones formuladas por los titulares de datos personales por la vulneración de los derechos que le conciernen. En esa línea, en el Reglamento de la LPDP, aprobado a través del Decreto Supremo 003-2013-JUS, se desarrolló el procedimiento trilateral de tutela para la atención de las reclamaciones de tutela de los denominados derechos ARCO. En ese marco, en el 2016 se iniciaron 32 procedimientos trilaterales de tutela, de los cuales: 13 procedimientos ya concluyeron y 19 procedimientos se encuentran en trámite dentro del plazo para resolver al 31 de diciembre de 2016.

5. PROCEDIMIENTOS DE INSPECCIÓN Y SANCIÓN

65 fiscalizaciones en 2016

La APDP puede realizar fiscalizaciones de oficio o por denuncia, para supervisar el tratamiento de datos personales realizado por responsables de tratamiento. Dichas fiscalizaciones culminan en un informe que indica si existen circunstancias o no que justifiquen el inicio de un procedimiento sancionador.

Las fiscalizaciones son realizadas por la Dirección de Supervisión y Control y de encontrar indicios que justifiquen el inicio de un procedimiento sancionador informa a la Dirección de Sanciones para el inicio del mencionado procedimiento. En el año 2016 se han concluido 65 fiscalizaciones, A través de las cuales se han fiscalizado a 77 responsables de tratamiento de datos personales (titulares de bancos de datos personales o encargados de tratamiento). De las 65 fiscalizaciones concluidas, en 60 de ellas se encontraron indicios de infracción de las disposiciones de la LPDP y su reglamento, por lo que se informó de los mismos a la Dirección de Sanciones.

Tipos de infracciones

La LPDP contempla infracciones leves graves y muy graves en el artículo 38 de la LPDP de la siguiente manera:

– Son infracciones leves:

- Dar tratamiento a datos personales sin recabar el consentimiento de sus titulares, cuando el mismo sea necesario conforme a lo dispuesto en la LPDP.
- No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales (derechos ARCO) cuando legalmente proceda.
- Obstruir el ejercicio de la función fiscalizadora de la Autoridad Nacional de Protección de Datos Personales.

– Son infracciones graves:
- Dar tratamiento a los datos personales contraviniendo los principios establecidos en la LPDP o incumpliendo sus demás disposiciones o las de su Reglamento.
- Incumplir la obligación de confidencialidad.
- No atender, impedir u obstaculizar, en forma sistemática, el ejercicio de los derechos del titular de datos personales (Derechos ARCO), cuando legalmente proceda.
- Obstruir, en forma sistemática, el ejercicio de la función fiscalizadora de la Autoridad Nacional de Protección de Datos Personales.
- No inscribir el banco de datos personales en el Registro Nacional de Protección de Datos Personales.

– Son infracciones muy graves:
- Dar tratamiento a los datos personales contraviniendo los principios establecidos en la LPDP o incumpliendo sus demás disposiciones o las de su Reglamento, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
- Crear, modificar, cancelar o mantener bancos de datos personales sin cumplir con lo establecido por la LPDP o su reglamento.
- Suministrar documentos o información falsa o incompleta a la Autoridad Nacional de Protección de Datos Personales.
- No cesar en el tratamiento ilícito de datos personales, cuando existiese un previo requerimiento de la Autoridad Nacional de Protección de Datos Personales para ello.
- No inscribir el banco de datos personales en el Registro Nacional de Protección de Datos Personales, no obstante haber sido requerido para ello por la Autoridad Nacional de Protección de Datos Personales.

Es preciso señalar que, el Decreto Legislativo 1.353, publicado en el Diario Oficial El Peruano, modifica algunas disposiciones de la LPDP, señalando que el artículo 38 de la misma, a través del cual se establecen las infracciones señaladas estará vigente hasta que se apruebe el Reglamento del mencionado Decreto, que deberá tipificar las infracciones en materia de protección de datos personales.

Sanciones: las multas y su graduación

Las sanciones establecidas en la LPDP son multas se encuentran tipificadas en unidades impositivas tributarias (UIT)[1], de acuerdo a la gravedad de la sanción se han considerado las siguientes:

[1] En el año 2016 el valor de una UIT era de Tres mil novecientos cincuenta soles (S/ 3.950) y en el año 2017 es de cuatro mil cincuenta soles (S/. 4050).

– Las infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).
– Las infracciones graves son sancionadas con multa desde más de cinco UIT hasta cincuenta UIT.
– Las infracciones muy graves son sancionadas con multa desde más de cincuenta UIT hasta cien UIT.

La LPDP establece que en ningún caso la multa impuesta puede exceder del diez por ciento de los ingresos brutos anuales que hubiera percibido el presunto infractor durante el ejercicio anterior.

6. COOPERACIÓN CON OTRAS INSTITUCIONES PÚBLICAS

Orientación a la Administración

La Autoridad Nacional de Protección de Datos Personales ha realizado en el año 2016 cuatro campañas a nivel nacional, a través de las cuales orientó a entidades públicas sobre las obligaciones respecto a la protección de datos personales. Asimismo, ha resuelto consultas realizadas por las entidades públicas, tanto de forma presencial, por escrito como por teléfono.

7. COOPERACIÓN CON LA SOCIEDAD

Campañas nacionales

La Autoridad Nacional de Protección de Datos Personales ha realizado en el año 2016 cuatro campañas a nivel nacional, a través de las cuales orientó a entidades privadas sobre las obligaciones respecto a la protección de datos personales. Asimismo, ha resuelto consultas realizadas por personas naturales y personas jurídicas, tanto de forma presencial, por escrito como por teléfono. Además de ello, ha realizado 38 charlas informativas a nivel nacional en la que se informó sobre las obligaciones señaladas en la LPDP y su reglamento.

8. DATOS ESTADÍSTICOS

Datos sobre la actividad de la Autoridad

Se iniciaron 32 procedimientos trilaterales de tutela, de los cuales, al 31 de diciembre de 2016, 13 procedimientos ya concluyeron y 19 procedimientos se encuentran en trámite dentro del plazo para resolver.

– Se emitieron 2 opiniones de flujo transfronterizo, a solicitud de titulares de bancos de datos personales, las cuales consideraron que los flujos sobre los que se había solicitado opinión no estaban adecuados a la LPDP y su reglamento.
– La Dirección General de Protección de Datos Personales ha emitido 7 opiniones técnicas sobre proyectos normativos referidos parcial o totalmente a datos personales.
– La Dirección de Registro Nacional de Protección de Datos Personales recibió dos mil novecientos veinte (2920) solicitudes de inscripción de bancos de datos personales. Luego del trámite

correspondiente, en el año 2016 se inscribieron en el RNPDP dos mil ochocientos once (2811) bancos de datos personales.
– Se han inscrito 232 comunicaciones de flujo transfronterizo en el Registro Nacional de Protección de Datos Personales.
– Se han iniciado 89 fiscalizaciones, las cuales pueden incluir a más de una entidad de diversos rubros, y se concluyeron 65 fiscalizaciones, a través de las cuales se han fiscalizado a 77 responsables de tratamiento de datos personales (titulares de bancos de datos personales o encargados de tratamiento). De las 65 fiscalizaciones concluidas, en 60 de ellas se encontraron indicios de infracción de las disposiciones de la LPDP y su reglamento, por lo que se informó de los mismos a la Dirección de Sanciones.
– En el marco de las fiscalizaciones realizadas, con la finalidad de obtener elementos que evidencien la existencia o no de circunstancias que justifiquen el inicio de un procedimiento sancionador, se realizaron 148 visitas de fiscalización.
– En atención a los informes de fiscalización recibidos, durante 2016, la Dirección de Sanciones emitió un total de 90 resoluciones directorales de inicio de procedimiento administrativo sancionador, así como 48 resoluciones directorales que culminan la primera instancia del procedimiento sancionador, en 41 de ellas se sancionó con multa a los administrados por infracciones a la LPDP.
– Durante el año 2016 se realizaron 38 charlas informativas sobre protección de datos personales en Lima y provincias.
– En el año 2016, se atendieron 1836 consultas sobre las disposiciones de la LPDP y su Reglamento, tanto de forma presencial, por teléfono, correo electrónico, por escrito.

X. URUGUAY

1. INTRODUCCIÓN

Gobierno electrónico y protección de datos

Bajo la concepción de que se trata de derechos fundamentos para el ejercicio de una ciudadanía plena, sobre todo en la consideración de la era de las tecnologías de la información y la comunicación, es que desde la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) se avanzó en la formulación y propuesta de normativa legal y reglamentaria que diera sustento al marco jurídico necesario para el desarrollo y avance del Gobierno Electrónico en el país.

Creación de la Unidad Reguladora y de Control de Datos Personales

En la lógica de funcionamiento y concepción de cómo y hacia dónde deberían dirigirse los esfuerzos en materia de gobierno electrónico, es que se consideró fundamental avanzar en la consolidación de institucionalidades autónomas desde el punto de vista técnico, que funcionaran bajo la figura de la desconcentración. Así, se crearon sucesivamente: la Unidad Reguladora y de Control de Datos Personales (Ley 18.331, de 11 de agosto de 2008, en adelante URCDP), la Unidad de Acceso a la Información Pública (Ley 18.381, de 17 de octubre de 2008) y la Unidad de Certificación Electrónica (Ley 18.600, de 21 de setiembre de 2009) a los efectos de otorgar resguardo de efectividad a los derechos constitucionalmente consagrados tal el caso de la protección de datos personales, el acceso a la información pública y la seguridad de la información mediante la firma electrónica avanzada.

Todas revisten las mismas características, desde el punto de vista jurídico, habiendo sido su creación en términos de unidad desconcentrada en forma privativa la que opera como un mecanismo de atribución de competencia al subordinado que implica en el caso, la privación de ésta al jerarca, de forma tal que el o los actos de que se trate solo podrán ser dictados por el subordinado y no por el jerarca. Se trata de un poder propio y privativo de decisión, según establece la doctrina nacional en la materia, que se atribuye al subordinado quitándolo de la esfera de atribuciones de quien sería el superior. Es una forma excepcional de distribución de competencias que se basa en la especialización técnica del subordinado. Ahora bien, desde el punto de vista estructural, el sistema no se modifica por lo que solamente el ejercicio de la función desconcentrada estará por fuera de los poderes que se atribuyen al superior. A lo anterior debe agregarse que la atribución de competencia solo puede tener su origen en una norma general y abstracta, esto es en el caso una ley y solo podrá darse cumplimiento a aquellas competencias que ésta determine sin posi-

bilidades de ampliación por otra vía que una norma con igual rango que la que las otorgara en su formulación original. Sin embargo, esta desconcentración no obsta a la existencia de un sustancial carácter autonómico desde el punto de vista técnico. Así, la formación de la voluntad del órgano es, en todos los casos, con absoluta independencia técnica.

A efecto de garantizar la verificación de alineamiento para con los objetivos de AGESIC y asegurar un funcionamiento desde el punto de vista de los recursos humanos y económicos sustanciales para sus actividades, se cuenta en el Consejo Ejecutivo de cada una de estas Unidades con la presencia de quien ostenta la calidad de Director Ejecutivo de AGESIC.

Estructura de la Autoridad

En cuanto a la estructura orgánica, podemos decir que la Unidad Reguladora y de Control de Datos Personales está compuesta de dos órganos: uno de conducción ejecutiva, el Consejo Ejecutivo (integrado por tres miembros, dos designados por Resolución del Presidente de la República, entre personas que por sus características personales y de conocimiento aseguren la independencia en el funcionamiento, más el Director Ejecutivo de AGESIC) y uno de consulta, el Consejo Consultivo (integrado por cinco miembros designados en representación del Poder Judicial, el Poder Legislativo, el Ministerio de Público, la academia y el sector privado).

Competencias y funciones de la Unidad Reguladora

En lo que hace referencia a los cometidos, competencias y funciones, responden a lo que son las especificidades de su materia particular. La Unidad Reguladora y de Control de Datos Personales, tiene sus competencias asignadas a través de lo preceptuado por el artículo 34 de la Ley 18.331, que señala:

> "A) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente ley y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza.
>
> B) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley.
>
> C) Realizar un censo de las bases de datos alcanzadas por la ley y mantener el registro permanente de los mismos.
>
> D) Controlar la observancia de las normas sobre integridad, veracidad y seguridad de datos por parte de los responsables de las bases de datos, pudiendo a tales efectos realizar las actuaciones de inspección pertinentes.
>
> E) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, las autoridades deberán garantizar la seguridad y confidencialidad de la información y elementos suministrados.
>
> F) Emitir opinión toda vez que le sea requerida por las autoridades competentes, incluyendo solicitudes relacionadas con el dictado de sanciones administrativas que correspondan por la violación a las disposiciones de esta ley, de los reglamentos o de las resoluciones que regulan el tratamiento de datos personales comprendidos en ésta.
>
> G) Asesorar en forma necesaria al Poder Ejecutivo en la consideración de los proyecto de ley que refieran total o parcialmente a protección de datos personales.

> H) Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables, en forma gratuita."

El presupuesto de las Unidades se rige por el artículo 214 de la Constitución de la República, traduciéndose en su integración a al presupuesto general de AGESIC. Desde el punto de vista de la infraestructura física y humana, la Unidad funciona con el soporte de AGESIC la que provee de los recursos técnicos informáticos, profesionales y estructura edilicia para efectivizar sus actividades.

Cabe señalar que en de mayo de 2009 se puso efectivamente en funcionamiento la Unidad Reguladora y de Control de Datos Personales, contando a la fecha con experiencias, lecciones aprendidas y un cúmulo importante de resoluciones y dictámenes. En efecto, luego de nueve años de funcionamiento, ha incrementado notablemente su actividad vinculada con la sustanciación de denuncias presentadas por ciudadanos que sienten vulnerados sus datos por causa de las injustificadas intromisiones que se producen.

Desde la perspectiva de que la protección de datos es un derecho fundamental que plantea desafíos derivados de la expansión de internet y las tecnologías, el tratamiento masivo de datos personales y la internacionalización inevitable de las transferencias de información, la Unidad comenzó un trabajo intenso a efectos de procurar que las transferencias internacionales aseguraran niveles adecuados de protección, redundando en beneficios para todos los titulares, responsables, encargados e interesados en general.

Ratificación del Convenio 108

Gracias a ese enfoque y al trabajo realizado, mediante la Decisión del Parlamento y del Consejo Europeo número 2012/484/EU, de 21 de agosto de 2012, Uruguay fue declarado país adecuado. Posteriormente, por Ley 19.030, de 27 de diciembre de 2012, Uruguay ratificó el Convenio Núm. 108 sobre tratamiento automatizado de datos personales y su Protocolo Adicional, convirtiéndose en el primer país no europeo en ser parte de dicho Convenio.

2. PLANIFICACIÓN

Plan Estratégico para 2016

La URCDP planifica anualmente sus actividades, las que se alinean a los diferentes niveles de política pública nacional que se plantean como ejes centrales. Como ha sido la tradición de la URCDP desde su creación, el fortalecimiento del conocimiento del derecho y sus implicancias entre las personas, las empresas y las entidades públicas continuó siendo un pilar fundamental de su accionar. En este sentido, el Plan Estratégico para 2016 contempló una serie de iniciativas, algunas de las cuales pretendieron dar continuidad a acciones ya realizadas y que se consideraron positivamente así como otras iniciativas nuevas para avanzar en diferentes productos aprehensibles por la sociedad. Las grandes áreas de desarrollo de la Unidad pueden dividirse de la siguiente manera:

a) Fortalecimiento y posicionamiento de la Unidad como referente nacional en la materia.
b) Gobernanza y fortalecimiento de sujetos obligados.
c) Promoción del derecho en la ciudadanía.
d) Investigación.
e) Actividad administrativa.
f) Posicionamiento y liderazgo a nivel internacional.

Cada una de estas áreas verifica una serie de proyectos y actividades operativas asociadas. Para este Informe se han elegido únicamente, de manera ilustrativa, las siguientes:

Capacitación

– Capacitación. Se proyectaron una serie de acciones y actividades que involucraron a los diferentes sectores y áreas de actividad, así como a personas de los diversos ámbitos y ubicación territorial del país. En efecto, la Unidad se ha planteado avanzar con su plan de capacitación sectorial en un doble sentido. Por un lado, se continuó un proceso de formación a través de charlas y talleres con funcionarios de entidades públicas; y por otro lado, se hizo lo propio con personas que tienen responsabilidades en diferentes empresas, de forma tal de colaborar con el conocimiento del derecho para su adecuada aplicación no solo en la esfera personal, sino también en el ejercicio de las funciones que cada uno debe ejecutar en la vida social. Asimismo, se continuaron las capacitaciones a nivel virtual a través del sitio web de la Unidad y el curso que se desarrolla mediante la plataforma de Educantel.

Charlas de café

– Charlas de café de Protección de Datos Personales. Las Charlas de Café son una iniciativa de la URCDP iniciada como proyecto piloto durante 2015 y que dado su éxito se extendió a 2016. Estas charlas se instrumentaron 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. Se ha planteado como un mecanismo de acercamiento de una temática especializada y concreta a los distintos grupos de interés, de forma tal de plantear, a través de expertos especialmente convocados al efecto, inquietudes, experiencias, consultas, problemáticas de ineludible análisis. Durante 2016 se concretaron charlas acerca de educación, identidad digital, innovaciones tecnológicas: ciudades inteligentes e internet de las cosas, el nuevo Reglamento Europeo. También se proyectó la película del Director alemán David Bernet "Democracy".

Primera Semana Nacional de la Protección de Datos

– Primera Semana Nacional de la Protección de Datos Personales. En oportunidad de celebrarse los ocho años de aprobación de Ley 18.331, se realizó una semana de actividades coordinadas entre los días 8 y 12 de agosto tanto en Montevideo como en el interior del país. En esta semana se realizó la premiación del concurso "Tus Datos Valen" y varias conferencias y talleres con destacados profesionales nacionales y extranjeros comprometidos con el derecho a la protección de datos personales, en esta primera experiencia en dos ciudades del país: Montevideo

y Maldonado. Se debatió a propósito de los nuevos temas que involucran al derecho y a las autoridades que tienen las obligaciones de su resguardo y protección. Se contó con la presencia de especialistas provenientes de Argentina, Brasil y México, así como de especialistas nacionales además de la participación de más de dos centenares de personas.

Revista de Protección de Datos Personales

– Primera revista de Protección de Datos Personales. Este emprendimiento tuvo por finalidad reunir el pensamiento nacional e internacional en materia de datos personales y se aunaron los conocimientos de los autores referentes y las autoridades de diferentes países. Se trata de un esfuerzo que pretende tener continuidad a los efectos de presentar un conocimiento unificado de las principales tendencias que se verifican en relación con el derecho a la protección de datos personales. Asimismo, incluye espacios para entrevistas, normatividad y decisiones judiciales y administrativas que se consideran de relevancia.

Relaciones internacionales

– Relacionamiento internacional. Convencidos de la necesidad de estar en contacto y comunicación con los desarrollos que se ejecutan en diferentes partes del mundo y en el entendido que Uruguay tiene experiencia para compartir con quienes están interesados en el avance en materia de protección de datos personales, se continuaron desarrollando acciones de vinculación y colaboración en las diferentes redes que se integran. En ese sentido, se continuó trabajando con compromiso en el marco de la Red Iberoamericana de Protección de Datos, habiéndose asumido a finales de año su Presidencia. Se participó en las reuniones tendientes a modificar el Convenio Núm. 108 y la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en Marruecos, así como en diferentes foros, conferencias y seminarios en donde fue requerida la presencia de la Unidad.

3. ACCIÓN NORMATIVA

Potestad regulatoria: criterios para la aplicación de la normativa

De acuerdo con lo establecido en las disposiciones normativas vigentes, la URCDP posee potestad regulatoria, mas no reglamentaria, la que ha sido atribuida al Poder Ejecutivo. En ese marco, la URCDP dictamina especificando criterios, en función de sus competencias, los que se transforman en especificidades de la aplicación normativa. Si bien se ha establecido el pronunciamiento de la Unidad (no con carácter vinculante, pero sí como asesor del Poder Ejecutivo) frente a disposiciones normativas referentes a protección de datos, no fue requerido este tipo de asesoramiento durante 2016. Por su parte, el Poder Legislativo sí ha requerido asesoramientos que han sido puntualmente respondidos, sea con la presencia de las autoridades del Consejo Ejecutivo en las comisiones parlamentarias solicitantes, sea con la redacción de informes de asesoramiento.

4. PROCEDIMIENTOS DE GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS

Tramitación de denuncias

La URCDP tiene un importante caudal de actividad asociado a garantizar el ejercicio del derecho a la protección de datos. De hecho, la mayor parte de la tramitación administrativa que debe cumplimentar refiere a la sustanciación de procedimientos administrativos en el marco de denuncias que efectúan las personas en relación con inconvenientes suscitados en el ejercicio de su derecho. En este punto, corresponde destacar las siguientes Resoluciones vinculadas a denuncias presentadas por titulares de datos contra responsables que dificultaron, o no cumplieron con permitirles el ejercicio de sus derechos:

Ejercicio del derecho de actualización

– Resolución 1/016, de 17 de febrero de 2016. Se resuelve una denuncia presentada por no permitir el ejercicio del derecho de actualización. En el caso concreto, se trató de una refinanciación de adeudos no comunicada dentro de los plazos legales a la empresa que brinda informes de créditos, ya que se demoraron 8 meses en la mencionada comunicación. En este caso, la Unidad entendió que correspondía la aplicación de una sanción por la vulneración de las normas previstas en la LPDP.

Ponderación con el derecho de información pública

– Resolución 6/016, de 9 de marzo de 2016. Se resuelve una denuncia presentada por la publicación de un acta taquigráfica, con referencia a la persona del denunciante en el sitio web de una entidad pública. En este caso el denunciante procuró la supresión de la información contenida en el sitio por entenderla vulneratoria de su derecho a la intimidad, al trabajo, a la igualdad y a la protección de datos. El denunciado manifestó que las actas publicadas, tienen el carácter de fuentes de acceso al público y que no existe solución legal, para la eliminación de los datos contenidos en ella. La Unidad en el caso, mantuvo el criterio sostenido en Dictamen 16/12, de 9 de agosto de 2012, señalando, especialmente, que en las situaciones de simultánea aplicación de los derechos a la protección de los datos personales y el derecho de información, comprensivo del derecho de acceso a la información pública, la competencia resolutiva es de la autoridad responsable de la difusión de que se trate. Ésta deberá interpretar de manera armónica ambos derechos y, en su caso, procurar el menor sacrificio posible de aquéllos. Asimismo, señaló que la entidad pública de marras posee atribuciones para retirar todo o parte de la versión incorporada al sitio web, cuando se advierta que este tipo de difusión afecta algún valor esencial, o un derecho fundamental como es el de la protección de los datos personales, señalando que "en el ejercicio de esas atribuciones se estima pertinente prevenir tal circunstancia, evitando la publicación total o parcial en dicho medio".

Derecho de cancelación

– Resolución 32/016, de 8 de junio de 2016. Se resuelve una denuncia presentada por una persona por el alegado incumplimiento a su derecho de supresión por parte de un responsable. En el caso se había asegurado por el responsable que se había eliminado la información del titular de los datos, pese a lo cual

fue nuevamente contactado por el primero. La Unidad impuso sanciones al responsable por vulneración de la Ley de PDP.

Consentimiento previo

– Resolución 54/016, de 8 de setiembre de 2016. Se resuelve la denuncia presentada por una persona por la publicación en una página web oficial de determinada información que se encuentra exceptuada del consentimiento previo, conforme lo dispuesto por la LPDP (nombres y apellidos, documento de identidad y dirección). En este caso, la Unidad manifestó que el uso creciente de las tecnologías de la información y comunicación por las entidades públicas arroja múltiples beneficios, entre otros, la sustantiva ampliación y diversificación de los modos de relación entre gobernantes y gobernados, los que se deben procurar sin desmedro de los principios que caracterizan el derecho fundamental a la protección de datos personales. En este caso, y sin perjuicio de que los datos de la denunciante, publicados en la página web no vulneran la normativa vigente de protección de datos personales, sin perjuicio de recomendar a la denunciada, publicar contenidos en su sitio web, en función de la adopción de alguno de los criterios establecidos en la Resolución de esta Unidad 1.040/012, de 20 de diciembre de 2012 y su anexo.

Publicidad no deseada

– Resolución 92/016, de 29 de diciembre de 2016. Se resuelva la denuncia presentada por reiteración de envío de publicidad no deseada, a través de correo electrónico. En este caso, el denunciante manifestó recibir por tercera vez, publicidad no deseada, habiendo sido la conducta de la denunciada, objeto de pronunciamientos anteriores por la Unidad. De hecho, por Resolución 39/014, de 27 de marzo de 2014, ya se había exhortado al denunciado a ajustar sus sistemas y a capacitar a sus recursos, y por Resolución 18/015, de 8 de abril de 2015, se le impuso sanción de observación. En este caso, el incumplimiento a la LPDP, la reiteración de la conducta y la existencia de sanciones previas fueron considerados por la Unidad, para la ponderación de la sanción pecuniaria, que finalmente se impuso.

5. PROCEDIMIENTOS DE INSPECCIÓN Y SANCIÓN

Práctica de la auditoría e inspección

En caso de entenderse pertinente, la URCDP puede determinar la realización de procedimientos de auditoría e inspección, lo que se ha instrumentado en contadas ocasiones. La filosofía imperante en la estrategia de la Unidad es la colaboración activa, procurando trabajar en conjunto con entidades públicas y privadas; de forma tal que incluyan a la protección de datos personales como un elemento que les aporta valor a su actividad profesional y no procurando avanzar desde los mecanismos sancionadores, salvo que sean de imprescindible aplicación. A pesar de lo indicado en el párrafo anterior, en múltiples ocasiones se impone la determinación de sanciones, las que han sido específicamente establecidas en la Resolución 105/005, de 15 de diciembre de 2015 dictada por el Consejo Ejecutivo de la Unidad. En

ella, se establece una graduación de sanciones, que oscila entre aquéllas leves a muy graves, con multas de hasta 500.000 unidades indexadas.

A modo de ejemplo, se citan Resoluciones conteniendo los criterios aplicados y las sanciones asociadas:

Sanción por no inscripción de bases de datos

– Resolución 20/016, de 27 de abril de 2016. En el caso la Unidad se pronuncia -al igual que en otras situaciones similares- por la imposición de sanción de multa de 12.001 Unidades Indexadas, por la no inscripción de Bases de Datos en plazo, pese a la intimación realizada por Resolución 65/2015. Ello, en el marco de las potestades sancionatorias consagradas en el artículo 35 de la Ley de PDP en la redacción dada por la Ley 18.719, de 27 de diciembre de 2010, y según lo previsto en la Resolución 105/015, de 23 de diciembre de 2015.

Uso de número telefónico para fines publicitarios

– Resolución 39/016, de 12 de julio de 2016. La Unidad resolvió la denuncia presentada por el uso del número telefónico obtenido de la guía telefónica, para contactar por cuestiones promocionales a la denunciante, sin que el número estuviera relacionado a su persona. Además, se impuso por las denunciadas, determinada formalidad a los titulares de los datos para el ejercicio del derecho de supresión, que en el caso, no corresponde, atento a lo dispuesto por el artículo 21 de la LPDP. Ello motivó la imposición multa de 12.001 Unidades Indexadas, por contravenir las normas en materia de protección de datos personales establecidas en los artículos 6°, 9°, 14, 15 y 21 de la Ley de PDP, intimando además, a las denunciadas a adecuar sus políticas vinculadas al ejercicio de los derechos explicitados en los artículos 14 y 15 de la Ley.

Cancelación con retraso y omisión de control previo al registro

– Resolución 91/016, de 22 de diciembre de 2016. En este caso se mantuvo indebidamente el Registro de incumplimiento del denunciante, pese a la cancelación realizada con atraso. Se visualizó la inexistencia de mecanismos de control previos al registro de información por parte de la institución de crédito, lo que genera comunicación de datos inexactos y desactualizados, capaces de perjudicar y entorpecer el acceso al crédito. Por estas razones, la Unidad sancionó al denunciado con multa de 3.001 Unidades Indexadas, por incumplimiento del principio de veracidad, exhortándose además, a la denunciada, a implementar mecanismos de control sobre la información que se registra en su base de referencias.

6. COOPERACIÓN CON OTRAS INSTITUCIONES PÚBLICAS

Capacitación a entidades públicas y reuniones de asesoramiento

La URCDP coopera y se interrelaciona con todas las entidades públicas que requieren de su colaboración. Anualmente en la planificación se prevé la realización de actividades de capacitación a entidades públicas y se llevan a cabo multiplicidad de reuniones de asesoramiento. En ese sentido, en materia de asesoramiento se ha cumplido con la respuesta, en tiempo y forma, a decenas de requerimientos plantea-

dos tanto por entidades públicas (particularmente se trabajó con CEIBAL, Oficina de Planeamiento y Presupuesto, Dirección Nacional de Aduanas, Ministerio de Salud Pública, Administración Nacional de Combustibles Alcohol y Portland, Ministerio de Desarrollo Social, entre otras) como por ciudadanos que han concurrido personalmente a plantear sus consultas o denuncias o enviado sus inquietudes por la vía electrónica.

Además, en materia de capacitación se avanzó en la formación y transferencia de conocimiento a cientos de funcionarios públicos, docentes y ciudadanos, a través de las diferentes actividades desarrolladas en conjunto con AGESIC. Se trabajó particularmente con entes autónomos y servicios descentralizados vinculados con los diferentes sectores, como: la industria, la banca, la educación, la seguridad social, la transparencia en la función pública, entre otros.

7. COOPERACIÓN CON LA SOCIEDAD

Promoción de mejores prácticas

En sentido similar al trabajo con las entidades públicas, la Unidad asesora a entidades privadas promoviendo mejores prácticas y procurando incidir de forma positiva en la adopción de criterios y mecanismos de inserción de la protección de datos en sus respectivos ámbitos. Así, la Unidad participó a través de 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). También ha participado a través de su vínculo con AGESIC en el Grupo de Investigación sobre Privacidad desde el diseño, generado en el marco del Centro Tecnológico ICT4V ("Information and Communication Technologies for Verticals").

Asimismo, se atiende a las personas que recurren a la Unidad a presentar sus inquietudes, las que en algunos casos podrán luego derivar en dictámenes o resoluciones.

8. OTRAS ACTIVIDADES

Acuerdo de *Privacy Shield*

La URCDP tiene competencia para autorizar transferencias internacionales de datos, frente a las dificultades planteadas debido a la invalidación del Acuerdo *Safe Harbor*, y en mérito a la necesidad de dar continuidad a la referida actividad, la Unidad trabajó con varias empresas a los efectos de la adecuación de las correspondientes cláusulas contractuales de forma tal de facilitar el flujo de datos sin vulnerar los derechos de las personas. En la misma línea, se continuó trabajando una vez aprobado el nuevo acuerdo de *Privacy Shield*.

Del mismo modo, se ha trabajado con diferentes núcleos profesionales (como asociaciones de carácter gremial, clubes deportivos, entre otras) que han requerido el asesoramiento para el desenvolvimiento de las actividades vinculadas con el tratamiento de sus datos.

Exposición Rural del Prado

En el marco de la Exposición Rural del Prado (exposición agrícola-ganadera nacional más importante del país) se participó en el stand organizado por la AGESIC entregando folletería, desarrollando actividades interactivas y materiales de promoción.

9. DATOS ESTADÍSTICOS

La URCDP realiza actividad cuantificable estadísticamente en relación con las inscripciones de bases de datos y denuncias y consultas que se formalizan a través de expedientes administrativos. De hecho, se tiene por criterio la resolución de las situaciones planteadas por las personas con la mayor celeridad posible, de ahí que solo en caso de ser imprescindible se formalizan los correspondientes expedientes administrativos. En caso contrario, se procura resolver las diferentes situaciones en plazos de entre 48 y 96 horas.

Número de personas atendidas

Durante 2016 se atendió a un total de 1990 personas en canal presencial, 685 personas vía correo electrónico y 822 personas en forma telefónica. Es decir, la Unidad atendió un total de 3.497 requerimientos por parte de los ciudadanos, entre consultas, solicitudes de información y denuncias.

200 Dictámenes y Resoluciones

En términos de expedientes, el Consejo Ejecutivo de la Unidad se ha pronunciado a través de Dictámenes y Resoluciones, que totalizan más de doscientas. En un 32% las denuncias presentadas refieren a temas vinculados con comunicaciones de datos, en un 16% implican situaciones vinculadas con empresas de crédito y finanzas, un 11% refieren a la denegación del derecho de supresión, un 11% implican denuncias por inclusión errónea o sin consentimiento en una base de datos, 10% verifica referencia a situaciones vinculadas con políticas o sistemas informáticos que se encuentran en instrumentación, 5% refieren a denegación de ejercicio de los derechos de rectificación y actualización, 5% se vinculan con publicidad no deseada y 10% implica una suma de múltiples consultas referidas a temas únicos.

El 42% de los mayores de 18 años conocen su derecho a la protección de datos

Cabe destacar que la URCDP ha realizado una importante tarea de promoción del derecho, que se puede constatar en el "Estudio de conocimientos, actitudes y prácticas de Ciudadanía Digital de 2016", elaborado por el Observatorio de la Ciudadanía de AGESIC y de donde se puede afirmar que el 42% de los mayores de 18 años conocen su derecho a la protección de datos.

XI. SÍNTESIS*

1. INTRODUCCIÓN

Creación, naturaleza y denominación de las Autoridades de Protección de Datos

En Europa las Autoridades de Protección de Datos fueron creadas mediante ley como instituciones independientes y de la siguiente manera: 1) La *Agència Andorrana de Protecció de Dades* se instituye en la Ley 15/2003, cualificada de protección de datos personales, desarrollada por el Reglamento de Desarrollo de 9 de junio de 2010; 2) La Agencia Española de Protección de Datos se crea en la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal; 3) En Cataluña la Institución está regulada en la Ley 32/2010, de la Autoridad Catalana de Protección de Datos, que tiene como antecedente la Ley 5/2002, de la Agencia Catalana de Protección de Datos; 4) En el País Vasco esta Autoridad se crea en la Ley 2/2004, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

En América Latina se han establecido diversas fórmulas para la institucionalización de la Autoridad de Protección de Datos en cada Estado: 1) En Argentina la Dirección Nacional de Protección de Datos Personales es una entidad dependiente de la Subsecretaría de Asuntos Registrales del Ministerio de Justicia y Derechos Humanos de la Nación (Ley 25.326); 2) En Colombia la Ley Estatutaria 1.581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, otorgó a la Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, competencias para garantizar que el tratamiento de datos personales se realice conforme a esa Ley; 3) En Chile el Consejo para la Transparencia ha asumido funciones para la protección de datos personales, que están reguladas en la Ley 19.628, sobre Protección de la Vida Privada y en la Ley 20.285, sobre Acceso a la Información Pública; 4) En México la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, de 11 de junio de 2002, y Ley General de Transparencia y Acceso a la Información Pública, de 4 de mayo de 2015, revistieron de competencia en esta materia al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; 5) En Perú la Ley de Protección de Datos Personales de 2011 desarrolla el derecho fundamental a la protección de los

* Esta síntesis se basa exclusivamente en las contribuciones nacionales que figuran en los apartados precedentes de este capítulo. La referencia a la actuación de determinadas Autoridades se realiza a título meramente ejemplificativo. El hecho de que, en relación con cada una de las materias tratadas, no se mencione a otras Autoridades, no implica, en modo alguno, que éstas no hayan intervenido activamente en las referidas materias.

datos personales y crea la Autoridad Nacional de Protección de Datos Personales, a cargo del Ministerio de Justicia y Derechos Humanos; 6) En Uruguay la Unidad Reguladora y de Control de Datos Personales, creada en la Ley 18.331, de 11 de agosto de 2008, es una unidad desconcentrada de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.

Autonomía de las Autoridades de Protección de Datos

Las Autoridades de Protección de Datos Personales son instituciones con autonomía para el desarrollo de sus funciones. Debido a la propia evolución de la sociedad de la información, en la cual la protección de los datos personales cada vez enfrenta mayores retos frente al desarrollo de las nuevas tecnologías, las competencias de las Autoridades que conforman esta Red han ido ampliándose desde su creación hasta la actualidad. Cabe señalar que el Registro de Ficheros de Protección de Datos es una de las principales funciones asumidas por estas Autoridades en la Región.

2. PLANIFICACIÓN

Planes estratégicos por períodos anuales y líneas operativas prioritarias de actuación para 2016

Para el buen desempeño de su labor algunas Autoridades de Protección de Datos reportan planes estratégicos institucionales por períodos anuales (España: AEPD y AVPD; México, Perú y Uruguay) y otras han optado por establecer líneas operativas prioritarias de actuación para 2016 que no se derivan necesariamente de un plan estratégico institucional (Andorra, Argentina, Colombia y Chile). En España el Plan Estratégico de Actuación 2015–2019, cuenta con cinco ejes: 1) Prevención para una protección más eficaz; 2) Innovación y protección que incida en la mejora de la confianza; 3) Colaboración, transparencia y participación, que favorezca la comunicación con la sociedad y establezca relaciones estables con los profesionales de la privacidad; 4) Simplificar los procedimientos de la AEPD para hacerla más cercana a los responsables y profesionales de la privacidad; 5) Incrementar la agilidad y eficiencia de la AEPD reduciendo los tiempos de los trámites y optimizando la utilización de los recursos disponibles. En México el Programa Institucional 2016-2019 incluyó acciones estratégicas como: 1) Evaluación del cumplimiento al marco jurídico en materia de acceso a la información de los sujetos obligados; 2) Desarrollo del ejercicio del derecho de protección de datos personales en el sector público a través de solicitudes de acceso y corrección de datos personales; 3) Desarrollo de herramientas para facilitar el cumplimiento de la normativa, monitoreo, seguimiento y análisis de ordenamientos, iniciativas o dictámenes con incidencia en el tema de protección de datos personales; 4) Sistema Nacional de Transparencia y armonización legislativa de las entidades federativas y actividades conjuntas del INAI y los organismos garantes de los Estados; 5) Capacitación en materia de derechos de acceso a la información y la protección de datos personales dirigida a sujetos obligados; 6) Acciones de vinculación y de promoción de la cultura de la transparencia, del derecho de acceso a la información pública y de la protección de datos personales con la sociedad; 7) Desarrollo de políticas de acceso

a la información y de gobierno abierto; 8) Cooperación internacional, promoción y vinculación internacional. Asimismo, en Uruguay el Plan Estratégico de 2016 se desarrolló en las siguientes áreas: 1) Fortalecimiento y posicionamiento de la Unidad como referente nacional en la materia; 2) Gobernanza y fortalecimiento de sujetos obligados; 3) Promoción del derecho en la ciudadanía; 4) Investigación; 5) Actividad administrativa; 6) Posicionamiento y liderazgo a nivel internacional.

Por otra parte, en Andorra para 2016 la Agencia diseñó su estrategia de actuación orientada al tratamiento de datos de los menores, al tratamiento de datos en el sector inmobiliario y en las comunidades de propietarios. En Argentina la Planificación Operativa de 2016 se centró en: 1) Difusión del Programa de concientización Con vos en la web; 2) Continuar con las Inspecciones al sector privado y aumentar la cantidad de inspecciones; 3) Modernizar el sistema informático del Registro Nacional de Bases de Datos; 4) El Centro de Capacitación, Investigación y Difusión de la Protección de los Datos Personales; 5) Difusión y desarrollo del Centro de Asistencia a las Víctimas de Robo de Identidad y del Registro Nacional de Documentos de Identidad Cuestionados; 6) Continuación de la implementación del Registro Nacional No Llame. Para el 2016 la Delegatura para la Protección de Datos Personales de Colombia se propuso: 1) Implementar el Sistema de Supervisión Inteligente basado en riesgos; 2) Proferir sanciones de alto impacto y relevancia para el país por incumplimientos y afectaciones graves al derecho a la protección de datos personales de las personas; 3) Publicar la guía para la protección de datos personales en sistemas de videovigilancia; 4) Realizar el Cuarto Congreso Internacional de Protección de Datos Personales; y, 5) Desarrollar una estrategia de protección de datos personales de niños, niñas y adolescentes.

3. ACCIÓN NORMATIVA

Las Autoridades de la Red cuentan con potestad reglamentaria y la ejercen

Las Autoridades que conforman la Red Iberoamericana de Protección de Datos han sido embestidas de potestad reglamentaria o regulatoria y desde su creación han aprobado diversas normas (reglamentos, instrucciones, disposiciones, directrices, resoluciones, circulares, etc.) en el marco de sus competencias (Andorra, Argentina, Chile, España, México, Perú y Uruguay).

Acción normativa destacada en 2016: Argentina, Colombia, Chile y Perú

En 2016 destacan en este punto Argentina, Colombia, Chile y Perú. En Argentina la Autoridad emitió la Disposición 17/2016 referente al Registro Nacional "No Llame" y la Disposición 56/2016 sobre los formularios de inscripción del Registro Nacional de Bases de Datos. Por su parte, en Colombia la Autoridad dictó la Circular Externa Núm. 01 de 2016, mediante la cual impartió instrucciones a los responsables del tratamiento para llevar a cabo el registro de sus bases de datos ante el Registro Nacional de Bases de Datos.

El Consejo para la Transparencia de Chile realizó una "Propuesta general de perfeccionamientos normativos en materia de protección

de datos personales y comentarios al anteproyecto de ley que modifica la Ley 9.628, sobre Protección de la Vida Privada" en la cual se establecieron varias propuestas para perfeccionar la protección de datos personales en Chile, como: 1) Consagrar la autodeterminación informativa como derecho fundamental y objeto de protección de la Ley 19.628; 2) Incorporar los principios rectores en materia de protección de datos; 3) Revisar el catálogo de definiciones y, en especial, la categoría de "datos sensibles"; 4) Reforzar la regulación del consentimiento expreso e informado y de los derechos asociados a los titulares de los datos; 5) Territorialidad de la Ley y regulación del flujo transfronterizo de datos; y, 6) Establecer un Registro Nacional de Bases de Datos. La Autoridad Nacional de Protección de Datos Personales de Perú participó en el Grupo de Trabajo encargado de elaborar una propuesta normativa para la creación de una Autoridad Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Informes sobre proyectos y propuestas de reforma normativa

Asimismo, desde su creación las Autoridades de Protección de Datos han emitido informes sobre proyectos de normas aprobadas por otros órganos y han realizado propuestas de reformas normativas para la protección de datos. Por ejemplo, en Andorra la Agencia emitió en 2016 un total de 21 Informes sobre la adecuación de proyectos legislativos y otras normas a las regulaciones de protección de datos. De igual manera, en Perú la Dirección General de Protección de Datos Personales realizó siete opiniones técnicas sobre proyectos normativos referidos parcial o totalmente a datos personales que son vinculantes.

4. PROCEDIMIENTOS DE GARANTÍA DEL DERECHO A LA PROTECCIÓN DE DATOS

Actuaciones para garantizar los derechos ARCO y el derecho al olvido: ponderación con el acceso a la información pública

En 2016 las Autoridades de Protección de Datos han desplegado vastas actuaciones para garantizar la tutela de derechos ARCO y el derecho al olvido en Internet. De igual modo, se han preocupado por la ponderación entre el derecho de acceso a la información pública, la transparencia y el derecho a la protección de datos personales. En Argentina la Autoridad subraya que en 2016 se duplicó número de dictámenes emitidos, siendo algunos de los temas más relevantes: el Contrato de Transferencia Internacional; el Acceso a la Información Pública en el Decreto 1172/03 y los videos vigilancia. En México el INAI recibió 243 asuntos en el marco de procedimientos de protección de derechos en 2016. Al respecto, algunas actuaciones que podemos subrayar en este punto por la doctrina que establecen son:

– Andorra: los procedimientos en 2016 se desarrollaron para garantizar el derecho de acceso a datos personales y son dos Resoluciones estimatorias las incluidas en este Informe: 1) la Resolución que se formula contra un centro deportivo privado por no atender demandas sobre el derecho de acceso en la que se impone una sanción de 2.000 euros; 2) la Resolución que se formula a la Seguridad Social.

– Colombia: la Dirección de Investigación de Protección de Datos Personales de la Superintendencia de Industria y Comercio señala que uno de los casos más relevantes en 2016 fue el correspondiente la Resolución 47.868, de 26 de julio, sobre la rectificación de datos en el sistema de información de antecedentes judiciales que lleva la policía nacional y en el que la Autoridad ordenó que se actualice la información que se encontraba registrada en la base de datos del sistema de información sobre antecedentes y anotaciones de la policía colombiana.
– España: de la AEPD las Resoluciones que destacamos son: 1) R/01015/2016 en esta Resolución se atiende una solicitud presentada por un reclamante cuyos datos personales aparecen publicados en una sentencia del Tribunal Constitucional (TC). La reclamación es formulada contra Google Inc., el TC y la Agencia Estatal del Boletín Oficial del Estado, por no haber sido atendido debidamente el derecho de cancelación. 2) R/00401/2016, que trata sobre la publicación de la relación de puestos de trabajo de empleados públicos en el Boletín Oficial de Aragón con información excesiva. 3) R/00711/2016, dictada en el marco de un procedimiento de declaración de infracción de Administraciones públicas contra un Centro Penitenciario por el manejo de los datos sanitarios de internos. 4) R/00814/2016, también sobre la falta de medidas de seguridad de los expedientes que contienen datos de salud. En este tipo de Resoluciones se debe subrayar que cuando se producen infracciones de las Administraciones públicas, por disposición legal, la AEPD debe comunicarlas al Defensor del Pueblo (art. 46.4 LOPD).
  De igual modo, en el País Vasco la AVPD ha emitido un conjunto de Dictámenes para la garantía del derecho a la protección de datos, que en la mayoría de los casos los fueron previamente solicitados en consultas realizadas por las Administraciones públicas. Entre los que podemos enunciar los referentes a: 1) la implantación de la huella digital como medio de fichaje, de 19 de diciembre de 2016, dictamen en el que la AVPD consideró que el tratamiento de los datos biométricos de los trabajadores, con la finalidad de control de acceso, era adecuado a la normativa en materia de protección de datos; 2) La instalación de cámaras en vehículos privados, de 29 de julio de 2016; 3) La cesión de datos sobre el importe de la deuda por impago del impuesto de vehículos de tracción mecánica, de 05/05/2016; 4) La cesión de datos padronales de los Ayuntamientos a Correos y Telégrafos, de 20 de abril de 2016; y, 5) La Publicación en página web del resultado del sorteo para la formación de mesas electorales, de 10 de marzo de 2016, en donde la AVPD dictaminó que: "La publicación en la página web del Ayuntamiento del resultado del sorteo para la formación de las mesas electorales sin consentimiento de los afectados ni habilitación legal, resulta contraria a la normativa de protección de datos de carácter personal".
– Uruguay: Entre las Resoluciones incluidas por la Autoridad es de especial importancia la Resolución 6/016, de 9 de marzo de

2016, en la que se analiza la necesaria ponderación del derechos a la protección de los datos personales y el derecho de acceso a la información pública. De igual manera la Resolución 92/016, de 29 de diciembre de 2016, que trata sobre el envío de publicidad no deseada.

5. PROCEDIMIENTOS DE INSPECCIÓN Y SANCIÓN

Actuaciones previas a la imposición de sanciones

Las Autoridades de Protección de Datos realizan diversos tipos de actividades de inspección, investigación y verificación, tanto de oficio como a petición de parte, previas a la imposición de sanciones.

Tipos de infracciones

En España, Perú y Uruguay las infracciones a la protección de datos se han clasificado en tres tipos (leves, graves y muy graves) y se establecen sanciones de multas de distinto monto y graduación según el tipo de infracción del que se trate. Es similar el sistema de Andorra, que también incluye una graduación de multas según la gravedad de la infracción a la protección de datos y la posibilidad de inmovilizar los ficheros a efecto de restaurar los derechos de las personas afectadas. Igualmente en México, en donde durante 2016 la Autoridad impuso multas por un monto aproximado de 93 millones de pesos a los responsables por infracciones a la normativa de protección de datos.

Casos destacados en 2016: España, Argentina, Colombia y Uruguay

Entre los casos destacados en 2016 en España la AEPD (PS/00149/2016) impuso a Google Inc. una multa 150.000 euros, por una infracción del artículo 10 de la LOPD, tipificada como grave en el artículo 44.3.d). Entre los procedimientos de sanción de la APDCAT en Cataluña, a modo de ejemplo, destacamos los siguientes en los que se señalan infracciones graves: 1) PS 3/2016, a un Hospital, dependiente del Instituto Catalán de la Salud, donde se establece que la destrucción de parte de la Historia Clínica, sin respetar los plazos de conservación de la documentación, constituye un tratamiento ilícito y, por tanto, una infracción grave; 2) PS 60/2015, a un Ayuntamiento que señala que la captación de imágenes mediante cámaras de personas en la vía pública es constitutiva de una infracción grave, al considerarse excesiva en relación a los fines perseguidos; 3) PS 53/2015, también a un Ayuntamiento sobre la recogida y tratamiento de datos personales (geolocalización) a través de un sistema GPS incorporado a los aparatos de radiofrecuencia que utilizan los agentes de la Policía Local de un municipio, sin haber creado el fichero correspondiente, constituye una infracción de carácter grave; 4) PS 43/2015, a la Diputación de Barcelona que establece que la publicación por edictos de una resolución íntegra que contara datos excesivos, es constitutivo de una infracción grave.

En Argentina, entre las sanciones aplicadas durante el año 2016, subrayamos la sanción pecuniaria de 105.200,00 pesos impuesta a compañía argentina de Marketing Directo S.A. por obstruir el ejercicio de la función de inspección y fiscalización a cargo de la Dirección Nacional de Protección de Datos Personales.

La Dirección de Investigación de Protección de Datos Personales de la Superintendencia de Industria y Comercio de Colombia también realizó en 2016 procedimientos en los que se imponen sanciones

de multas, suspensión y cierre de las actividades relacionadas con el tratamiento de datos personales. De los procedimientos enunciados en este Informe podemos recalcar el correspondiente a la Resolución 39.298, de 21 de junio de 2016, por violación al principio de circulación restringida, al deber de seguridad y al deber de comunicar un incidente de seguridad por la exposición injustificada y masiva de datos sensibles de salud en Internet. En este caso, la Autoridad verificó que una entidad prestadora de servicios de salud tuvo visibles en su página web datos personales relativos a la salud de 30 usuarios de esa entidad e impuso una multa de más de 271.000 euros.

Por otra parte, en Uruguay la Autoridad apunta que puede determinar la realización de procedimientos de auditoría, inspección y sanción, con una graduación de sanciones de leves a muy graves y multas de hasta 500.000 unidades indexadas. Sin embargo, la estrategia de la Autoridad uruguaya es la colaboración activa con las entidades controladas y solo en contadas ocasiones se han producido este tipo de procedimientos. No obstante, se incluyen algunos casos y entre ellos subrayamos el correspondiente a la Resolución 20/016, de 27 de abril de 2016, en el cual la Unidad se pronuncia sobre la no inscripción de Bases de Datos en plazo e impone una multa de 12.001 Unidades Indexadas.

En Chile no se contemplan sanciones específicas

Merece un comentario aparte el caso de Chile pues el Consejo para la Transparencia pone de manifiesto la inexistencia de una autoridad de control con competencias de inspección, fiscalización y sanción para el debido cumplimiento y garantía del derecho a la protección de datos. Asimismo, la Institución chilena agrega que tampoco se contemplan en la actual legislación sanciones específicas para el incumplimiento de las normas de protección de datos.

6. COOPERACIÓN CON OTRAS INSTITUCIONES PÚBLICAS

Cooperación con otras Administraciones: dictámenes e informes, doctrina para la aplicación de las normas

La actividad de todas las Autoridades de Protección de Datos de esta Red se ha caracterizado por su activa cooperación con otras Administraciones públicas para facilitar y promover la aplicación de la legislación de protección de datos y la garantía de los derechos de los sujetos titulares. Esta cooperación se lleva a cabo por distintos medios, ya sea a través de Dictámenes e Informes en los que se sienta doctrina para la aplicación de las normas que son formulados previa consulta de las Administraciones públicas o desde la celebración de convenios con estas Administraciones que constan enunciados en cada apartado nacional de este Informe. Por citar un ejemplo, en México se pueden subrayar los convenios de colaboración con: sindicatos, Auditoría Superior de la Nación, Banco de México, Partidos Políticos, Cámara de Diputados, Barra Mexicana Colegio de Abogados, Procuraduría Federal del Consumidor, entre otros.

Chile: Protocolo del software de reconocimiento facial

En este ámbito de actuaciones podemos subrayar que en Chile el Consejo para la Transparencia, debido a la implementación de software de reconocimiento facial por parte del Ministerio del Interior,

de la Intendencia Metropolitana de Santiago y de Carabineros de Chile, está realizando una asistencia técnica para la elaboración de un Protocolo de tratamiento de datos personales del software de reconocimiento facial.

España: nuevo Reglamento Europeo y guías para su implantación

Por su parte, la Agencia Española de Protección de Datos está colaborando con la Secretaría General de Administración Digital y el Centro Criptológico Nacional para evaluar el impacto en las Administraciones públicas del nuevo Reglamento Europeo y redactar un conjunto de guías o directrices que ayuden a su implantación. Además, mantiene canales de colaboración con el Consejo General del Poder Judicial para la fijación de criterios comunes y delimitación de competencias entre ambas autoridades.

En 2016 la Agencia Vasca de Protección de Datos publicó un Informe titulado "Actividad Parlamentaria y Protección de Datos Personales: Doctrina de la Agencia Vasca de Protección de Datos", que analiza los distintos Dictámenes emitidos en las preguntas formuladas por el Parlamento Vasco y el Gobierno Vasco sobre la posibilidad de entrega de documentación que contiene datos personales desde el Ejecutivo al Parlamento Vasco.

Cooperación entre Autoridades de Protección de Datos a nivel nacional e internacional

En el presente Informe también se constatan diversas actividades de cooperación entre Autoridades de Protección de Datos a nivel nacional e internacional. En España las Autoridades Estatal y Autonómicas de Protección de Datos participan en Grupos de Trabajo para analizar los desafíos que presenta la aplicación del nuevo Reglamento Europeo de Protección de Datos. A más de las actividades desarrolladas en el marco de esta Red, en España la Agencia Española de Protección de Datos se ha incorporado al Subgrupo de "*Enforcement*" del GT 29, cuyo objetivo es permitir la coordinación de las actuaciones de sus miembros en relación con problemas de protección de datos en tratamientos desarrollados por grandes compañías transnacionales. En el ámbito europeo, podemos señalar la intervención de la Autoridad Española en las actividades del Grupo de Trabajo del artículo 29 de la Directiva 95/46, que es el organismo consultivo de la Comisión Europea en lo referente a la protección de Datos Personales y, también, esta Institución forma parte de las Autoridades de control de Europol.

De igual manera, en Andorra la Autoridad es parte de la Asociación Francófona de Protección de Datos, de las conferencias de Primavera de Protección de Datos e Internacional de Protección de Datos y, además, representa al Principado de Andorra en el Grupo de Trabajo del Convenio 108 del Consejo de Europa.

7. COOPERACIÓN CON LA SOCIEDAD

Fomento de la autorregulación y la capacitación

Con el objetivo de facilitar el cumplimiento de la legislación de protección de datos se desarrollaron actividades de cooperación con la sociedad civil destinadas al fomento de la autorregulación y la capacitación. Para ello, la mayoría de las Autoridades de esta Red han suscrito un importante número de convenios con organizaciones de la

sociedad civil y con empresas, que pueden verse en los respectivos apartados nacionales.

Guías para facilitar la aplicación de las normas: México, Colombia y España

Además, algunas de estas Instituciones en 2016 han elaborado guías para facilitar la aplicación de las disposiciones normativas. Es el caso de la Autoridad de Protección de Datos de México que ha desarrollado diversas herramientas para orientar a los responsables y encargados del tratamiento de datos personales en cumplimiento de sus obligaciones legales, como: la Guía para el Borrado Seguro de Datos Personales; los Lineamientos para el uso de hiperenlaces o hipervínculos en una página de Internet; un estudio para fortalecer la estrategia de educación cívica y cultura para el ejercicio del derecho a la protección de los datos personales por parte de los titulares; y una aplicación para dispositivos móviles para crear conciencia acerca del valor de los datos personales.

Del mismo modo, la Autoridad colombiana en el 2016 elaboró una Guía para la protección de datos personales en sistemas de videovigilancia, con el objetivo de orientar a quienes implementan estos sistemas para que apliquen las disposiciones que regulan la protección de datos personales. Previamente, en 2015 esta Autoridad publicó la Guía para la implementación del Principio de Responsabilidad demostrada.

En España la Agencia Española de Protección de Datos, en colaboración con la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición y con el Instituto Nacional de Ciberseguridad, elaboró la "Guía de Privacidad y Seguridad en Internet".

Mesas de diálogo sobre reforma normativa en Chile

Cabe señalar que el Consejo para la Transparencia de Chile realizó varios encuentros con representantes de la sociedad civil en los que se establecieron mesas de trabajo en materia de protección de datos personales a fin de analizar los retos pendientes de ese Estado de cara a las reformas normativas que se requieren para garantizar este derecho.

Foros sobre Smart Cities: Andorra y Cataluña

La ADPCAT mantiene abierto un foro de debate sobre el desarrollo de las ciudades inteligentes (*Smart Cities*) y sus implicaciones sobre la información de carácter personal de la ciudadanía, desde el que se pretende apoyar a las Administraciones públicas de Cataluña que quieren implantar los servicios de las *Smart Cities* y también a las empresas que llevan a cabo el diseño y la implantación de esas tecnologías. También en Andorra la Autoridad colaboró con empresas y otras organizaciones para la protección de datos en el marco de las *Smart Cities*.

8. OTRAS ACTIVIDADES

Promoción, sensibilización y capacitación

En 2016 una amplia variedad de acciones de promoción, sensibilización y capacitación ha sido desarrollada por las Autoridades de Protección de Datos iberoamericanas, principalmente desde la organización de congresos, seminarios y cursos cortos. Asimismo, con motivo del Día Internacional de Protección de Datos, el 28 de enero se realizaron algunas actividades de promoción y jornadas de capacitación en la Región.

Participación internacional de las Autoridades de Protección de Datos

Es destacable también el considerable incremento de la participación internacional de las Autoridades de Protección de Datos en los ámbitos europeo y latinoamericano. Debemos resaltar que la Red Iberoamericana de Protección de Datos llevó a cabo en 2016 el "XIV Encuentro Iberoamericano de Protección de Datos y la 4° Conferencia Internacional sobre Protección de Datos", en Santa Marta, Colombia; y, el "Seminario Europa-Iberoamérica: una visión común de la protección de datos. El nuevo marco europeo y su incidencia en Iberoamérica", en Montevideo, Uruguay.

Las Autoridades que conforman la Red señalan que han participado en diversos foros internacionales como: la Reunión Única del Comité Ad-Hoc sobre Protección de Datos (CAHDATA)-Convenio 108; la Reunión Plenaria del Comité Consultivo del Convenio 108, en Estrasburgo, Francia; el Encuentro de Autoridades de Privacidad de Asia-Pacífico (APPA Fórum) en Singapur; la 39ª Reunión de la Mesa Directiva Del Comité Consultivo del Convenio 108 en París, Francia; la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP) en Marruecos; la Conferencia Anual "*Privacy Summit*" llevada a cabo en Washington DC, en el marco de *International Associations of Privacy Professional*, entre otros.

Campañas en redes sociales

Por otra parte, los miembros de esta Red también han realizado campañas en redes sociales (Twitter y Facebook) para dar a conocer los derechos de la ciudadanía en materia de protección de datos. La Agencia Vasca de Protección de Datos realizó dos videos de sensibilización en el marco de la campaña "La protección de datos con humor", uno sobre el uso del teléfono y otro sobre Whatsapp.

Conclusión: progresos y retos en la protección de datos en la Región

Finalmente, como conclusión podemos señalar que las Autoridades que conforman la Red Iberoamericana de Protección de Datos cuentan con amplias competencias para la protección de los derechos ARCO en sus respectivos territorios, que han ido ampliándose desde su creación. Estas Instituciones han desarrollado una labor trascendente para la garantía del derecho a la protección de datos personales en 2016, tanto desde actividades de sensibilización y promoción como con el ejercicio de sus funciones de inspección y sanción. No obstante, las Autoridades de la Red aún se enfrentan a varios retos para la protección de los datos personales en la Región, que en algunos casos incluye su propio fortalecimiento institucional al no estar dotadas de suficientes medios y facultades de inspección, sanción y acción normativa.

PARTE SEGUNDA (TEMA MONOGRÁFICO):
LA PROTECCIÓN DE DATOS DE LOS MENORES DE EDAD

I. PANORAMA INTERNACIONAL

Problemática de la protección de datos de los menores

Los avances tecnológicos y el uso de Internet favorecen una mayor conexión entre los ciudadanos y que éstos puedan recoger, almacenar, compartir y difundir, cada vez con mayor intensidad, ingentes cantidades de información sobre sí mismos o terceros. Pero esta ventaja se puede convertir también en un peligro para la vida privada. Esto es más evidente y preocupante en el caso de los menores de edad. Los menores de edad o niños y adolescentes (entendiendo como tales a los sujetos menores de 18 años) son participantes activos de la tecnología y de Internet, lo que les hace vivir su vida privada y desear compartirla para ser socialmente reconocidos y admitidos, sin ser conscientes, por regla general, de los peligros que esa información puede provocar en sus vidas y en su futuro desarrollo personal y profesional.

Pero el tratamiento de datos personales de los menores no se va a producir sólo en la Red y por parte de los mismos, sino que su información personal va a ser tratada en todos los ámbitos en los que el menor se desarrolle y participe. Cuestiones relacionadas con su falta de capacidad para consentir (en íntima conexión con su grado de madurez y las reglas civiles de la representación), con el grado de disposición de sus datos personales y con el ejercicio de su derecho, así como el papel de sus padres o tutores, de los centros escolares y sanitarios, de los medios de comunicación o, incluso, de los órganos judiciales y administrativos, a la hora de tratar sus datos personales deben ser analizadas con detalle. Todo ello con el fin de evitar un uso incorrecto o ilícito de los datos de los menores, para que éstos puedan disfrutar plenamente de su derecho a la protección de datos.

Ausencia generalizada de normas generales y remisión a normas sectoriales

Antes de adentrarnos en las citadas cuestiones, creemos conveniente realizar aquí dos observaciones. En primer lugar, en relación con el tratamiento de los datos personales de los menores de edad, ya sea a nivel internacional, latinoamericano o europeo, no vamos a encontrar una norma específica sobre la materia[1], sino que las normas o disposiciones que regulan el tratamiento de datos personales serán las que contengan los requisitos generales para dichos tratamientos y, en contadas ocasiones y de forma tangencial, se refieran a los casos en que los tratamientos tienen como sujetos a los menores de edad. Además, no podemos olvidar tampoco que, por regla general, la normativa que regula el tratamiento de datos personales es una norma de mínimos, de criterios generales, debiendo acudir en todo caso para tener una visión completa y adaptada al caso planteado a la normativa sectorial corres-

[1] Tenemos que citar aquí, por ser una excepción a la regla en esta materia la conocida como COPPA, la *Children´s Online Privacy Protection Act*, promulgada en 1998 en Estados Unidos (15 USC 6501-6505).

pondiente. Así, sucederá, por ejemplo, en el ámbito educativo, en el sanitario o en el judicial, aunque esto tampoco implica que en dichos ámbitos existan normas que reconozcan de forma expresa a los menores como destinatarios de las mismas, incluyéndolos en su régimen general.

Aplicación de las garantías de los derechos fundamentales

En segundo lugar, debemos diferenciar lo que es el reconocimiento y garantía del derecho fundamental a la protección de datos personales, vinculado estrechamente a la privacidad, dignidad y desarrollo personal del individuo, de lo que es la regulación jurídica del tratamiento de dichos datos. Si bien puede haber situaciones en las que no exista una norma que regule el tratamiento de datos personales, en último término estamos hablando de la garantía de un derecho fundamental que está reconocido a todos los niveles (ya sea como vida privada, intimidad, desarrollo personal o, expresamente, como protección de datos personales) y como tal debe ser protegido, ya sea su titular un mayor o un menor de edad. De ahí la necesaria referencia no sólo a la normativa específica, sino a los textos de derechos fundamentales correspondientes.

Sujetos obligados a respetar los derechos de los menores

El peligro que un mal uso de los datos personales de los menores puede producir no va a tener origen sólo en su comportamiento, sino también en el uso que de su información personal hagan quienes deben protegerles y representarles (familia y poderes públicos, más directamente), así como la sociedad en la que se integran. Por todos estos motivos es realmente importante que los menores reconozcan (y se les reconozca de forma expresa) su derecho a la protección de datos personales, y que este reconocimiento vaya acompañado de unas directrices universales y uniformes de la postura que los poderes públicos, sus representantes y el resto de la sociedad deben adoptar a la hora de tratar la información relativa a los mismos, pues de su control o, mejor dicho, de su falta de control, van a derivarse consecuencias que acabarán afectando a su desarrollo personal y, en último término, al desarrollo de la sociedad que queramos tener. La necesidad de garantizar la vida privada de los sujetos, especialmente de los más vulnerables, sigue siendo una constante en toda sociedad que se califique de democrática.

1. ÁMBITO INTERNACIONAL

1.1. Marco normativo

Tratados sobre derechos humanos y sobre derechos del niño: la Convención de 1989

A nivel internacional no existe una norma específica que regule el tratamiento de datos de los menores de edad o su derecho como tal. En relación con la protección de los derechos humanos en este ámbito es la Organización de Naciones Unidas (ONU) el organismo que ha creado los instrumentos legislativos más importantes, así como sus mecanismos de vigilancia y protección. Con el fin de garantizar los derechos del niño, se aprobó en su seno la Convención sobre los Derechos del Niño (CDN)[2], y se erigió como mecanismo de garantía de

[2] Convención sobre los Derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas, el 20 de noviembre de 1989. Disponible *on line*: http://www.ohchr.org/SP/ProfessionalInterest/Pages/CRC.aspx.

la citada norma, el Comité de los Derechos del Niño (art. 43 CDN)[3]. Aunque no con la intensidad, como es lógico, del Comité de los Derechos del Niño, el Comité de Derechos Humanos de las Naciones Unidas se va a encargar de interpretar el grado de cumplimiento de los instrumentos jurídicos aprobados por dicha Organización, y así lo ha hecho también cuando los titulares de los derechos en ellos reconocidos eran los menores de edad[4]. Asimismo, teniendo como objeto la garantía y vigilancia del cumplimiento de la CDN, destaca la creación de la Red Internacional de los Derechos del Niño (conocida por sus siglas en inglés, CRIN (*Child Rights International Network*)[5].

Tanto la CDN, con referencia expresa a los menores, como el resto de instrumentos jurídicos internacionales, si bien no garantizan de forma expresa un derecho a la protección de datos personales, reconocen el derecho a la vida privada. El artículo 16 CDN garantiza que "1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación. 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques". Dicho artículo se inspira, a su vez, en otros catálogos de derechos internacionales, concretamente, en el artículo 12 de la Declaración Universal de los Derechos del Hombre (DUDH) de 1948, y en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP) de 1966, que son aplicables igualmente a los menores, en tanto que son instrumentos jurídicos que garantizan derechos para todas las personas.

Comité de Derechos del Niño y UNICEF

Serán especialmente los órganos de garantía e interpretación de la CDN, como el Comité de los Derechos del Niño, los que al hilo de analizar los cambios que está experimentando la sociedad (fruto, a su vez, de la tecnología, de los medios digitales e Internet y de su efecto en los menores) se pronuncien sobre las consecuencias que el tratamiento incorrecto o ilícito de datos de los menores puede provocar en los mismos. Cuestiones como la monitorización de la actividad de los menores en la Red, de sus comunicaciones electrónicas y, especialmente, los casos de delitos cometidos a través de Internet tales como la distribución de pornografía infantil, el *grooming*, o el *cyberbullying*, serán temas a los que se les prestará una especial atención.

Por último, con carácter general, debemos recordar que en relación con la protección de los derechos del niño a nivel internacional existe de fondo una importante labor llevada a cabo por Organizacio-

[3] Sobre dicho Comité, vid. http://www.ohchr.org/EN/HRBodies/CRC/Pages/CRCIndex.aspx.

[4] Sobre el citado Comité, vid.: http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIndex.aspx. Y como un ejemplo de sus Dictámenes, vid. el Dictamen del Comité de Derechos Humanos, al caso *D.T. y A.A. contra Canadá*, aprobado en su sesión del 20 de junio al 15 de julio de 2016, y publicado el 29 de septiembre de 2016 (CCPR/C/117/D/20181(2011). Y, más en concreto, la Observación general nº 17, del Comité de Derechos Humanos, de 29 de septiembre de 1989, sobre *Los derechos del niño* (Disponible en http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6623&Lang=en).

[5] Más información sobre la CRIN en su web https://www.crin.org/es. En 2011, CRIN lanzó la *Wiki de los Derechos del Niño* (Wiki), herramienta en línea que reúne todos los datos sobre los derechos de los niños país por país (vid. https://www.crin.org/es/biblioteca/publicaciones/la-wiki-de-los-derechos-del-nino).

nes no gubernamentales y especializadas. Así, por ejemplo, destaca el papel llevado a cabo por UNICEF, que en 1953 fue reconocida por la Asamblea General de la Naciones Unidas como una organización permanente de ayuda a la infancia[6]. UNICEF ha tenido ocasión de pronunciarse a través de diversos informes y publicaciones sobre los derechos de los niños e Internet.

Más allá de los citados instrumentos internacionales de derechos humanos, como ha quedado dicho, a nivel internacional no existe una norma que regule específicamente el tratamiento de datos personales de los menores. Lo que sí que vamos a encontrar serán normas y directrices encargadas de establecer los principios generales de todo tratamiento de datos personales, en las que debemos entender incluidos los casos en los que se traten datos personales de menores de edad. No obstante, en algunas de estas normas y directrices se contendrán referencias expresas a cuestiones o aspectos concretos en los que habrá que tener en consideración el hecho de que el titular de los datos sea un niño o un adolescente.

Podemos citar como ejemplos de directrices generales sobre el tratamiento de datos personales a nivel internacional, la Resolución 45/95, de la Asamblea General de las Naciones Unidas, de 14 de diciembre de 1990, sobre los Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales[7], donde se establecieron unas garantías mínimas que debían observar las legislaciones nacionales a la hora de tratar datos personales. En esta misma línea se han aprobado otras Resoluciones y Observaciones Generales, sin que ninguna haya realizado referencia expresa al caso de los menores de edad. Así, podemos citar aquí también la Observación General nº 16, del Comité de Derechos Humanos, donde al hilo de analizar la interpretación del art. 17 PIDCP y la conexión del derecho a la vida privada y la familia, se refiere expresamente al tratamiento de datos personales[8]; o más directamente en relación con el derecho a la privacidad, las Resoluciones 68/167 y 69/166 sobre *El derecho a la privacidad en la era digital*, adoptadas por la Asamblea General de las Naciones Unidas[9], donde se manifiesta el carácter abierto y global de Internet y la necesidad de garantizar el valor del derecho a la privacidad de las comunicaciones, expresando preocupación por los efectos negativos que para el ejercicio de los derechos humanos puede tener su vigilancia.

En todas estas Resoluciones y Observaciones o Directrices se contienen las recomendaciones relativas a los principios esenciales a la

---

[6] Más información sobre UNICEF, en su web: https://www.unicef.org/es.

[7] Resolución disponible *on line*: http://www.un.org/es/comun/docs/?symbol=%20A/RES/45/95&Lang=S.

[8] Observación General nº 16, del Comité de Derechos Humanos, aprobada durante su 32º Periodo de Sesiones (abril 1988), sobre el "Derecho a la intimidad (artículo 17)", Apdos. 10 y 11.

[9] Resoluciones 68/167, de 18 de diciembre de 2013, y 69/166 del 18 de diciembre de 2014, de la Asamblea General de las Naciones Unidas, sobre "El derecho a la privacidad en la era digital". Disponibles *on line*: http://www.un.org/es/comun/docs/?symbol=A/RES/68/167; y http://www.un.org/es/comun/docs/?symbol=A/RES/69/166, respectivamente.

hora de tratar datos personales y se indica que tanto las autoridades públicas como privadas que traten datos personales deberán cumplirlos. Así, se recogen las necesarias medidas de seguridad que protejan la información personal, los principios de calidad y finalidad de la información que legitiman su tratamiento, así como los derechos de sus titulares al acceso, rectificación e, incluso, cancelación de la misma[10].

Labor de la OCDE

A nivel internacional, junto al papel desarrollado por la ONU y sus organismos, debemos destacar la labor llevada a cabo por la Organización para la Cooperación y el Desarrollo Económico (OCDE)[11]. A pesar de su objetivo marcadamente económico, con sus pronunciamientos ha venido a establecer unos principios generales en materia de tratamiento de datos personales. La OCDE publicó en 1980 unas Directrices que se convirtieron en el germen de la normativa comunitaria y latinoamericana en la materia. Nos referimos, concretamente, a las Directrices sobre Protección de la Privacidad y el Flujo trasfronterizo de Datos personales[12]. Pero entre sus principios no existe referencia alguna a los datos personales de los menores. No obstante, estas Directrices han sido revisadas en 2013, buscando establecer un nuevo marco para la privacidad. En este proceso de revisión se ha indicado que sería conveniente educar a los menores para que adquieran las competencias necesarias para proteger su privacidad, sin hacer mayor referencia al tratamiento de sus datos personales, a pesar de resaltarse el hecho de que los mismos se consideran sujetos vulnerables[13]. En el contexto de la OCDE, a diferencia de lo que ha sucedido con carácter general en el marco de la ONU (aunque de forma puntual), esta Organización se ha manifestado sobre cuestiones concretas del tratamiento de datos de los menores cuando éstos actúan en la Red[14]. En cualquier caso, no hay que olvidar que el principal objetivo de la OCDE es económico y, que los citados pronunciamientos no

---

[10] Observación General nº 16, del Comité de Derechos Humanos, Apdos. 10 y 11.

[11] Sobre la OCDE, vid. http://www.oecd.org/.

[12] El texto completo de estas Directrices lo podemos encontrar en: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[13] Sobre este procedimiento, vid. "*The OCDE Privacy Framework*" (http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf), pp. 31-32.

[14] Así, por ejemplo, vid. "Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security, Privacy and the Protection of Children Online", OCDE, 20 de diciembre de 2012 (http://dx.doi.org/10.1787/5k4dq3rkb19n-en). O, con carácter previo, "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", OCDE, 2 de mayo de 2011 (http://dx.doi.org/10.1787/5kgcjf71pl28-en), donde se identifican los riesgos para los menores en la Red como consumidores y usuarios de la misma. Todo ello, siguiendo la estela de la conocida como Declaración de Seúl sobre "El futuro de la economía en Internet", aprobada en la Reunión ministerial de 18 de junio de 2008 (http://www.oecd.org/sti/ieconomy/40839436.pdf), y reiterada en la Declaración ministerial sobre "La Economía digital: innovación, crecimiento y prosperidad social", aprobada en México el 23 de junio de 2016, donde se reconoce y declara, entre otras cosas contribuir a "*la protección de la privacidad, de la seguridad, de la propiedad intelectual y de los menores de edad en Internet, así como el fortalecimiento de la confianza en el Internet*".

son jurídicamente vinculantes, sino que son meras disposiciones de mínimos que recomiendan a los Estados seguir una serie de principios generales en materia de tratamiento de datos personales (limitación de recogida; calidad de los datos; especificación de los fines; limitación del uso; salvaguarda de la seguridad; transparencia; participación individual (o derechos de acceso, rectificación y cancelación); y responsabilidad).

La Conferencia Internacional de Autoridades y la Resolución de Madrid de 2009

En este plano internacional, y con un objetivo universal, debemos citar aquí las Conclusiones a las que llegaron las Autoridades Internacionales de Protección en la XXXI Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Madrid el 5 de noviembre de 2009, y que se recogieron en la denominada Resolución Madrid. En dicha Resolución se proponía la elaboración de unos estándares internacionales en materia de tratamiento de datos personales teniendo en cuenta el mundo globalizado en el que nos movemos. En la misma, la única referencia expresa a los menores se realizó al recomendar la implantación del principio de transparencia en la información facilitada relativa a los tratamientos de datos efectuados, exigiéndose que en el caso de los menores, dicha información fuera sencilla[15].

El principio del interés superior del niño

Así las cosas, no debemos olvidar que por mandato de la CDN (que en protección de datos no es una excepción) debe regir el principio del interés superior del niño (art. 3.1). Como la propia CDN nos recuerda, fruto de la falta de madurez física y mental del menor, hay que tener presente "la necesidad de proporcionar al niño una protección especial" y, por lo tanto, en todas las medidas que se adopten respecto de los mismos se deberá atender al "interés superior del niño". Así lo ha reiterado el Comité de los Derechos del Niño en su Observación General nº 14[16]. Cuando nos encontremos ante un tratamiento de datos de menores, a la hora de valorar su legitimidad y licitud, en primer y último lugar deberemos tener presente este principio. Cuando el derecho a la protección de datos del menor colisione con otros derechos fundamentales, especialmente con los de sus progenitores, tutores o instituciones, servicios o establecimientos encargados de sus cuidados, deberán ponderarse los intereses en juego, cobrando los del menor una especial consideración.

Escasez de normas vinculantes e inseguridad jurídica

En resumen, podemos concluir que en materia de protección de datos personales, las normas internacionales con carácter vinculante brillan por su ausencia y los pocos instrumentos jurídicos que existen brillan por su falta de precisión y su carácter de "mínimos", con las consecuencias que esta inseguridad jurídica provoca especialmente cuando los datos pertenecen a los menores de edad. Si bien es cierto que la OCDE marcó unos principios orientadores y unos criterios

[15] Sobre los estándares de privacidad a nivel internacional, vid. la Resolución Madrid: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/09-11-05_Madrid_Int_standards_ES.pdf.

[16] Observación General nº 14, del Comité de los Derechos del Niño, de 29 de mayo de 2013, sobre *El derecho del niño a que su interés superior sea una consideración primordial (artículo 3, párrafo 1)* (CRC/C/GC/14). Disponible on line: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CRC%2fC%2fGC%2f14&Lang=en.

que podríamos denominar "tecnológicamente neutros", se echan en falta unos criterios universales vinculantes que protejan la privacidad de los sujetos, especialmente, de los más vulnerables.

1.2. El consentimiento del menor para el tratamiento de sus datos personales

El consentimiento en la CDN; remisión al Derecho interno

En materia de protección de datos personales el consentimiento es el criterio legitimador de todo tratamiento de datos personales que se realice, siendo el titular de los datos el que debe prestarlo. La cuestión aquí es si el menor puede prestar por sí sólo el consentimiento a que se traten sus datos personales.

Dicho esto, debemos tener en cuenta que la CDN define al niño como al menor de 18 años (art. 1), indicándose también que el menor estará bajo la protección de la familia y del Estado. Asimismo, la CDN también señala que el Estado tiene que garantizar que el niño pueda formarse un juicio propio y expresar su opinión (y que se tenga en cuenta) en todos los asuntos que le afectan "en función de la edad y madurez del niño" (art. 12). En esta misma línea, la CDN añade que los Estados reconocen y respetan la obligación de padres o representantes respecto de los menores "en consonancia con la evolución de sus facultades" (art. 5), lo que reitera en el art. 14.2, aunque en relación con la libertad de pensamiento, conciencia y religión del menor a la hora de "guiar al niño en el ejercicio de su derecho". A más abundamiento, la propia CDN señala que los Estados garantizarán la responsabilidad de los padres de "la crianza y el desarrollo del niño" con pleno respeto al "*interés superior*" del menor (art. 18.1).

En este sentido debemos acudir a la normativa estatal correspondiente con el fin de comprobar las reglas que existen sobre la capacidad jurídica y de obrar de los menores. Si bien la regla general será que el consentimiento del menor deberá verse prestado o "ratificado" por sus representantes, habrá que estar a lo dispuesto por los diferentes ordenamientos jurídicos estatales con el fin de comprobar si existe alguna previsión específica que rebaje dicha edad y considere que el menor de edad es "mayor" para prestar el consentimiento a que se traten sus datos personales. El problema aquí es que no existe ningún instrumento que regule la edad de "madurez" del menor.

Directrices de la OCDE

En los instrumentos internacionales citados que regulan el tratamiento de datos personales, la regla general, como se deriva de las Directrices de la OCDE, es el principio de limitación tanto en la recogida como en el uso de los datos personales, exigiéndose el consentimiento del "sujeto de los datos" para su tratamiento (Principios 7 y 10, respectivamente)[17], sin referencia alguna a la edad del mismo. No obstante, en los Comentarios pormenorizados realizados de estas Directrices, se indicaba que "no se deberían aplicar las Directrices mecánicamente sin tener en cuenta el tipo de datos y las actividades de

[17] Directrices adoptadas el 23 de septiembre de 1980. Disponibles *on line*: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf.

proceso de los mismos"[18], lo que ofrece la posibilidad de adecuar el requisito del consentimiento a la edad de su titular. De hecho, en la revisión de dichas Directrices en 2013 se indicó expresamente que las Directrices no impedían la posibilidad de que el titular de los datos fuera representado por otro sujeto, mencionándose los casos de discapacitados y de los menores de edad[19].

El caso Pollock

Como ejemplo del consentimiento prestado por menores de edad para el tratamiento de sus datos personales y la necesidad de representante, desde la CRIN se resaltó la sentencia estadounidense *Pollock contra Pollock*, de 1 de septiembre de 1998 (154 F.3d 601 (6th Cir. 1998), donde se analizaba el caso de una menor de 14 años, de padres separados, y que había sido grabada telefónicamente sin su consentimiento por su madre bajo la sospecha de que el padre abusaba de ella. La cuestión de fondo que se planteaba en este asunto era si un padre podía grabar la conversación telefónica de su hijo (esto es, el dato personal de la voz y la información personal recogida en la conversación) sin el consentimiento real del niño. En este caso, la Corte haciendo valer el interés superior del menor concluyó que un progenitor podía consentir el tratamiento y grabación de los datos personales de su hijo siempre que la grabación se hiciera de buena fe y con la finalidad de proteger el interés superior del menor. No obstante, el Tribunal matizó que la capacidad del progenitor no podía interpretarse de manera extensiva y mucho menos considerar que un padre podía grabar siempre a su hijo bajo el argumento de velar por su interés, pues estaría lesionando su vida privada.

1.3. Ámbitos problemáticos

a) En las relaciones familiares

Conflictos intrafamiliares

Teniendo en cuenta que la CDN considera que la familia es el "grupo fundamental de la sociedad y medio natural para que el crecimiento y bienestar" de los niños (Preámbulo CDN), que el PIDCP la garantiza y protege (art. 23.1), y que los padres o representantes de los menores buscarán su desarrollo personal, observando siempre el interés superior del menor, el consentimiento para el tratamiento de sus datos personales en el entorno familiar no debería suponer un problema. Pero la cuestión es que los niños son titulares de derechos (como es el derecho a la protección de datos) que deben ser respetados incluso en el marco familiar y no verse diluidos o arrastrados por los derechos de sus padres o tutores, dado que el entorno familiar y las relaciones familiares pueden ser, también, un foco de conflictos sobre quién decide por el menor, así como el grado de decisión sobre sus derechos. Y ello, incluso, desde el mismo momento del nacimiento del niño.

---

[18] Véanse los Comentarios en: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf, Apdo. 3.45 sobre "Diferentes grados de sensibilidad".

[19] Al respecto, vid. "*The OCDE Privacy Framework*" (http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf), p. 56.

Derecho a conocer datos de los padres

Nos referimos, por ejemplo, al derecho del menor a conocer los datos de sus padres, no sólo como un acceso a datos de éstos como terceros, sino en el sentido de que son datos personales del menor que definen su identidad y marcan su desarrollo. En este punto, la CDN reconoce el derecho de los niños a conocer a sus padres, "en la medida de los posible" (art. 7). Con esta matización se deberá estar a lo que disponga la legislación nacional y a la interpretación que, en interés superior del menor, ofrezcan los Tribunales. La tónica general a nivel internacional hace prevalecer el derecho del menor a conocer sus orígenes frente al derecho a permanecer en el anonimato de sus padres. Y lo mismo sucederá con el derecho a tener un nombre y ser inscrito con tal identificación inmediatamente después de su nacimiento (art. 7 CDN).

Problemática del control parental

Durante la convivencia familiar, podemos encontrarnos los conflictos derivados del control parental que los padres pueden, y deben, ejercer sobre sus hijos y, por lo tanto sobre la información personal de los mismos. A pesar de esta obligación, no podemos olvidar las previsiones recogidas en las normas internacionales y debemos tener en cuenta el interés del menor, el respeto de sus derechos y el grado de madurez del mismo. Así, por ejemplo, a la hora de vigilar la correspondencia de los menores, la Observación General nº 16 del Comité de Derechos Humanos relativa al "Derecho a la vida privada y de familia" establece que en el entorno familiar también debería exigirse la integridad y confidencialidad de la correspondencia, que debería ser "entregada a su destinatario sin ser interceptada ni abierta o leída de otro modo", de la misma forma que debía garantizarse el secreto de las comunicaciones y debía evitarse la grabación de conversaciones o incluso los registros domiciliarios o médicos salvo previsión legal y por personal autorizado[20]. Pero matizando esta apreciación, ya vimos con en el citado caso *Pollock contra Pollock* (y como comprobaremos en otros ámbitos en los que los padres puedan controlar la información de sus hijos), que la regla general será respetar la vida privada del menor atendiendo a su grado de madurez, salvo que el interés superior del mismo requiera otra cosa.

Problemas derivados de la ruptura del vínculo familiar

En el seno familiar también se han planteado problemas respecto del tratamiento de datos de los menores cuando se produce la ruptura del vínculo familiar con los conflictos aparejados. La complejidad del problema de cómo tratar los datos de los menores involucrados en el proceso dependerá de los pronunciamientos judiciales estatales sobre la custodia y representación del menor y, en los casos más conflictivos en los que se produzca la sustracción de los menores, se tendrá que acudir a otras normas internacionales como el Convenio de La Haya donde se prevé el tratamiento de información relativa al menor con el fin de facilitar su localización, así como la colaboración en el intercambio de la misma (que en más de una ocasión conllevará un flujo transfronterizo de datos personales)[21]. Con la misma idea de

[20] Observación General nº 16, del Comité de Derechos Humanos, Apdo. 8.

[21] Arts. 7.d) y 8.d) Convenio de la Haya nº XXVIII, de 25 de octubre 1980, sobre *Aspectos civiles de la sustracción internacional de menores*. Disponible *on line*: http://www.oas.org/dil/esp/convenio_de_la_haya_sobre_los_aspectos_civiles_de_la_sustraccion_internacional_de_menores.pdf.

mantener al menor en el seno familiar, si el mismo se rompiera por la detención o encarcelamiento o incluso muerte de uno de los padres del niño, o de ambos, o del niño, el Estado correspondiente "proporcionará, cuando se le pida, a los padres, al niño o, si procede, a otro familiar, información básica acerca del paradero del familiar o familiares ausentes, a no ser que ello resultase perjudicial para el bienestar del niño" (art. 9.4 CDN).

Niños refugiados

Más allá de los casos en los que se produce la ruptura "voluntaria" del vínculo familiar, cuando la misma se produce por otros motivos como en el caso de los refugiados, además de las normas sectoriales correspondientes, la CDN también prevé que a los niños refugiados se le facilitará toda la información necesaria para que puedan "localizar a sus padres o a otros miembros de su familia" y reunirse con ella (art. 22.2), para lo cual deberá producirse un tratamiento de sus datos personales por parte de las instituciones implicadas.

En cualquier caso en este ámbito, todo tratamiento de datos personales del menor deberá estar al estricto cumplimiento de las Directrices de la OCDE, tener presentes las reglas de la representación y el grado de madurez del menor y, por otro lado, garantizar el principio del interés superior del mismo.

b) En el entorno escolar

Problemática del tratamiento de datos en la escuela

El entorno escolar, junto al familiar, es el ámbito donde el menor va a desarrollarse como persona. El centro educativo es donde el niño pasa más horas y adquiere conocimientos y destrezas a la par que valores (así lo reconoce el art. 29 CDN). La CDN reconoce en su artículo 28 el derecho a la educación del niño, pero no se indica nada respecto de la información relativa al mismo durante su proceso y periodo de escolarización. En este contexto, el tratamiento de datos personales del menor comienza desde el mismo momento de su matriculación en el centro (a veces incluso antes). La cuestión será determinar si el menor puede decidir personalmente sobre el uso de sus datos personales sin necesidad de ningún adulto y si el centro puede decidir sobre la conservación o sobre la comunicación de los mismos.

En este ámbito educativo internacional rigen, con carácter general, las Directrices sobre tratamiento de datos personales, debiendo aplicarse las medidas de seguridad correspondientes, así como las reglas generales sobre los principios de calidad y finalidad y los derechos del titular de los datos. Sólo en caso de conflicto entre las decisiones tomadas y el derecho del menor a la protección de sus datos personales se hará valer el principio del interés superior del menor. Habrá que tener en cuenta también lo dispuesto por los ordenamientos jurídicos estatales sobre el ámbito educativo y la forma en la que éstos pueden tratar datos de menores de edad. Nuevamente aquí, la regla general será contar con el consentimiento de los padres o representantes legales.

El caso G. C. contra Owensboro Public Schools

Por citar un ejemplo, la CRIN analiza la violación del derecho a la vida privada de un menor por parte de un centro escolar en el caso *G.C. contra Owensboro Public Schools*, de 28 de marzo de 2013 (711

F.3d 623, 6th Cir. 2013). En este caso, con motivo de una sanción disciplinaria, la Directora del centro leyó los mensajes del teléfono móvil de un estudiante de secundaria que tenía un comportamiento conflictivo bajo el argumento de evitar que el menor quisiera dañar a alguien o a sí mismo. El Tribunal consideró que el mal comportamiento o las tendencias depresivas de un estudiante no justificaban el registro de su teléfono móvil, sin el consentimiento paterno y si el incidente por el que había sido sancionado no se relacionaba con el comportamiento anterior del estudiante. Esto es, al no ser existir una causa justificada, la medida llevada a cabo por el centro había sido desproporcionada, lesionándose la vida privada del menor.

c) En el ámbito sanitario

El derecho a la salud en la CDN

La CDN reconoce el derecho del niño a acceder a los servicios sanitarios, la obligación del Estado de asegurar la prestación de la asistencia médica, así como la abolición de las prácticas tradicionales que sean perjudiciales para la salud de los niños (art. 24), pero no dice nada del tratamiento de sus datos o información clínica.

A pesar de esto, la propia CDN reconoce la responsabilidad que en este ámbito recae en los padres o tutores de los menores en función de la evolución de las facultades del menor (art. 5), esto es, en función de su madurez. Así, el Comité de los Derechos del Niño en este contexto ha establecido que "los padres o cualesquiera otras personas legalmente responsables del niño están obligadas a cumplir cuidadosamente con sus derechos y obligaciones de proporcionar dirección y orientación al niño en el ejercicio por estos últimos de sus derechos"[22].

Derechos y obligaciones en el ámbito sanitario según el Comité de Derechos del Niño

Como ocurría en el entorno docente, en este caso los centros médicos deberán respetar los principios generales para todo tratamiento de datos personales fijados internacionalmente por las Directrices de la OCDE. Asimismo, en relación con el consentimiento informado de los pacientes, cuando éstos sean menores de edad, la regla general derivada de la representación parental será el necesitar del consentimiento de sus padres o tutores. A juicio de la CRIN, esta regla general en este ámbito perpetúa las violaciones de sus derechos[23]. Por este motivo, aunque dejando margen de actuación a los Estados, el Comité de los Derechos del Niño ha reconocido la necesidad de que los menores puedan prestar su consentimiento en relación con sus datos médicos en función de su grado de madurez. Se les ha reconocido la capacidad para prestar un "consentimiento con conocimiento de causa", y se ha indicado que "De conformidad con la evolución de sus capacidades, los niños deben tener acceso a terapia y asesoramiento

[22] Observación General nº 4, del Comité de los Derechos del Niño, de 21 de julio de 2003, sobre "La salud y el desarrollo de los adolescentes en el contexto de la Convención sobre los Derechos del Niño" (CRC/GC/2003/4), Apdo. 7. Disponible *on line*: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CRC%2fGC%2f2003%2f4&Lang=en.

[23] CRIN, "Submission to the High-level Working Group on Health & Human Rights of Women, Children & Adolescents", noviembre 2016. Disponible *on line*: https://www.crin.org/sites/default/files/crin_wg_health_submission_11_16.pdf.

confidenciales, sin necesidad del consentimiento de su padres o su custodio legal cuando los profesionales que examinen el caso determinen que ello redunda en el interés superior del niño. Los Estados deben aclarar los procedimientos legislativos para la designación de los cuidadores adecuados que se encarguen de los niños sin padres o representantes legales y puedan dar su consentimiento en representación del niño o ayudarle a dar su consentimiento en función de la edad y la madurez del niño. Los Estados deben estudiar la posibilidad de permitir que los niños accedan a someterse a determinados tratamientos e intervenciones médicos sin el permiso de un progenitor, cuidador o tutor, como la prueba del VIH y servicios de salud sexual y reproductiva, con inclusión de educación y orientación en materia de salud sexual, métodos anticonceptivos y aborto en condiciones de seguridad"[24].

Por último, en relación con los sujetos que manejan la información de los menores, el personal médico y sanitario y demás trabajadores del centro médico, el Comité de los Derechos del Niño ha exigido la confidencialidad de los mismos y ha señalado expresamente que "Los trabajadores de la salud tienen obligación de asegurar la confidencialidad de la información médica relativa a las adolescentes, teniendo en cuenta principios básicos de la Convención. Esa información sólo puede divulgarse con consentimiento del adolescente o sujeta a los mismos requisitos que se aplican en el caso de la confidencialidad de los adultos. Los adolescentes a quienes se considere suficientemente maduros para recibir asesoramiento fuera de la presencia de los padres o de otras personas, tienen derecho a la intimidad y pueden solicitar servicios confidenciales, e incluso tratamiento confidencial"[25]. Más aún, cuando hablamos de enfermedades como el virus VIH/SIDA, el Comité de los Derechos del Niño ha hecho especial hincapié en la confidencialidad de los médicos y asistentes sanitarios, así como el derecho a respetar la vida privada de los menores, incluso sin poner dicha información del menor en conocimiento de sus padres, aunque de nuevo se remite a los Estados el nivel de confidencialidad a establecer: "Los Estados Partes deben proteger la confidencialidad de los resultados de las pruebas de detección del VIH, en cumplimiento de la obligación de proteger el derecho a la vida privada del niño (art. 16), tanto en el marco de la atención sanitaria como en el sistema público de salud, y velar por que no se revelen sin su consentimiento, a terceras partes, incluidos los padres, información sobre su estado serológico con respecto al VIH"[26].

---

[24] Observación General nº 15, del Comité de los Derechos del Niño, de 17 de abril de 2013, sobre "El derecho del niño al disfrute del más alto nivel posible de salud (artículo 24)" (CRC/C/GC/15), Apdo. 31. Disponible on line: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CRC%2fC%2fGC%2f15&Lang=en. En esta misma línea, vid., Observación General nº 4, del Comité de los Derechos del Niño.

[25] Observación General 4º, del Comité de los Derechos del Niño.

[26] Observación General nº 3, del Comité de los Derechos del Niño, de 17 de marzo de 2003 (CRC/GC/2003/3), sobre "El VIH/SIDA y los derechos del niño". Disponible *on line*: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CRC%2fGC%2f2003%2f3&Lang=en.

d) En los medios de comunicación

Problemática de la información sobre menores en los medios

La CDN reconoce, en relación con los medios de comunicación, que éstos deberán permitir el acceso a la información y material que los niños requieran para su bienestar social, espiritual y moral, y salud física y mental (art. 17). En este ámbito, el problema en relación con el tratamiento de datos personales de los menores no vendrá tanto por la información que los medios de comunicación difundan y faciliten a los menores, sino a la inversa, por la información que sobre los menores los mismos medios difundan.

La cuestión que entra en juego entonces es la existencia de un conflicto entre el derecho del menor a controlar sus datos personales y las libertades de expresión e información ejercidas por los medios de comunicación, teniendo como telón de fondo la protección del menor como un sujeto vulnerable. Así, por ejemplo, en el Informe del Relator Especial de las Naciones Unidas, sobre la *Promoción y protección del derecho a la libertad de opinión y de expresión*, reconociendo a los menores como sujetos vulnerables, añade que las libertades informativas pueden y deben ser limitadas si la finalidad es evitar un grave daño para los derechos humanos de otros (tal y como recoge el art. 20 PIDCP)[27].

Imágenes de menores en los medios: caso JR38 y doctrina del Comité de Derechos del Niño

En relación con el uso de imágenes de menores por parte de los medios de comunicación se han pronunciado los organismos internacionales al hilo de la sentencia de la Corte Suprema del Reino Unido, caso *JR38 for Judicial Review (Northern Ireland)*, de 1 de julio de 2015 (UKSC 42), donde la Corte consideró que la toma de fotografías de un menor de 14 años durante una manifestación y su publicación en un periódico local para su identificación era una injerencia en su vida privada, aunque en el caso en cuestión no se lesionaba su vida privada, pues la publicación estaba justificada. A pesar de la ponderación correspondiente donde se hizo primar la finalidad legítima perseguida, lo destacable del caso es el análisis que los Jueces realizaron de la "expectativa razonable de privacidad" del menor y de su grado de madurez para entender lo que constituía una actividad pública y una privada. Al respecto el Comité de los Derechos del Niño añadió que dada la exigencia de cumplir con la protección del interés superior del menor (art. 3.1 CDN) dichas cuestiones debían ponerse en el contexto específico del caso analizado, y recordó que en cuanto a la publicación de la información de los menores en procesos judiciales deberían seguirse las llamadas Reglas de Beijing (sobre administración de justicia a menores)[28], con el fin de velar por la privacidad del menor en todas las partes del proceso, lo que conllevaría necesariamente analizar si la publicación de su imagen lesionaba o no su vida privada.

Por último sobre quién consiente a la publicación en los medios de comunicación los datos personales del menor, nos remitimos nue-

---

[27] Informe, de 20 de abril de 2010. Disponible *on line:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/130/52/PDF/G1013052.pdf?OpenElement.

[28] Las Reglas de Beijing fueron aprobadas por la Asamblea General de Naciones Unidas (A/RES/40/33), de 29 de noviembre de 1985. Disponibles *on line*: http://www.un.org/documents/ga/res/40/a40r033.htm.

vamente a la regla general sobre el consentimiento, su interés especial digno de protección y su grado de madurez.

e) Como partes de una relación contractual

Remisión al Derecho interno en materia contractual

A nivel internacional, en materia contractual, además de la previsión contenida en la CDN respecto del "sometimiento" del menor a la protección que les otorga la familia y el Estado (art. 5), habrá que tener en cuenta, tal y como establece el Comité de Derechos Humanos, que "los Estados deben indicar en sus informes la edad en que el niño alcanza la mayoría de edad en los asuntos civiles y asume la responsabilidad penal"[29].

Así las cosas, a pesar de la regla general de la falta de capacidad de los menores para concluir contratos, se plantea si esto afecta a los tratamientos de datos personales de los mismos que vayan implícitos en los contratos en los que puedan ser parte. En este sentido, se debe seguir las Directrices de la OCDE para el tratamiento de la información personal del menor necesaria para el contrato. Al no haber previsión alguna respecto de los menores, se seguirá la regla de su representación y del interés superior del menor en cuanto al tema de la prestación del consentimiento para el tratamiento de sus datos personales, dejando la cuestión de la validez del contrato a lo dispuesto por cada legislación nacional.

d) Como partes de un proceso judicial o administrativo

Reglas de la CDN y de Beijing sobre menores y justicia

La CDN reconoce el derechos de los niños a ser escuchados en todo proceso judicial o administrativo que les afecte (art. 12. 2). De la misma forma, se les garantiza el derecho, en caso de estar privados de libertad, a mantener el contacto con su familia por medio de correspondencia o visitas (art. 37.c). Nada se dice sobre la vigilancia de la correspondencia, entendiendo que tal cuestión cae bajo el ámbito de protección de la vida privada del menor (o por analogía a lo dispuesto en la Observación General nº 16 del Comité de Derechos Humanos, ya citada). En relación con este contacto familiar, si bien la CDN no detalla mucho más, la Asamblea General de las Naciones Unidas aprobó una Resolución estableciendo las *Reglas Mínimas de las Naciones Unidas para la administración de justicia a Menores* (conocida como *Reglas de Beijing*), donde se señaló que cada vez que un menor fuera detenido, la detención debería ser notificada inmediatamente a sus padres o tutores (art. 10.1), sin contar con el consentimiento del menor. En el caso de que el contacto ponga en peligro la integridad del menor, habrá que estar aquí al interés superior del mismo.

Por otro lado, con la finalidad de su reinserción y de proteger sus derechos, la misma CDN recoge que "se respetará plenamente su vida privada en todas las fases del procedimiento" (art. 40.2.vii), en conexión con el art. 16). Esta previsión se corresponde igualmente

[29] Observación General nº 17, del Comité de Derechos Humanos, Apdo. 4.

con los principios de confidencialidad establecidos, con carácter general, en las Directrices de la OCDE sobre protección de datos.

Excepciones a la publicidad de los procesos cuando involucran a menores

En este ámbito, asimismo, el artículo 14.1 PIDCP contiene un límite muy importante cuando se trata de la publicidad de los procesos judiciales, pues reconoce una excepción a la publicidad de las sentencias en materia penal cuando así lo exija el interés del menor. En función de dicho interés también habría que entender que esta regla debería hacerse extensiva a todos los procedimientos, judiciales del ámbito penal o civil o incluso administrativos, en los que interviniera un menor.

Esto es relevante si tenemos en cuenta que la divulgación de los datos personales de los menores involucrados, especialmente, en casos penales, pueden llegar a marcarles de por vida. Con referencia al Comité de los Derechos del Niño, el Tribunal Constitucional de Sudáfrica, en el caso *J. contra el National Director of Public Prosecutions y otros*, de 6 de mayo de 2014, recordó que en función de lo dispuesto por la CDN, los Estados deberían recordar que "no se publicará información que pueda conducir a la identificación de un delincuente infantil debido a su efecto de estigmatización en su capacidad para tener acceso a la educación, al trabajo, a la vivienda o para estar a salvo"[30].

Por este motivo, el Comité de los Derechos del Niño, en su Observación General nº 10 sobre *Los Derechos de los Niños en la Justicia*, dispone que "las autoridades públicas deben ser muy reacias a emitir comunicados de prensa sobre los delitos presuntamente cometidos por niños y limitar esos comunicados a casos muy excepcionales. Deben adoptar medidas para que los niños no puedan ser identificados por medio de esos comunicados de prensa", a lo que añade, además, que "los periodistas que vulneren el derecho a la vida privada de un niño que tenga conflictos con la justicia deberán ser sancionados con medidas disciplinarias y, cuando sea necesario (por ejemplo en caso de reincidencia), con sanciones penales".

Deber de confidencialidad de terceros

Por último, en relación con los sujetos que intervengan en el procedimiento y tengan conocimiento de los datos de los menores, con el fin de garantizar su privacidad, se exige que "todos los profesionales que intervengan en la ejecución de las medidas decididas por el tribunal u otra autoridad competente mantengan confidencial, en todos sus contactos externos, toda la información que pueda permitir identificar al niño". Se exige la confidencialidad no sólo de todos los profesionales a la hora de tratar la información, sino en relación con el acceso y tratamiento de los citados Registros de Antecedentes, recomendándose que sólo "podrán ser consultados por terceros, excepto por las personas que participen directamente en la investigación y resolución del caso". Y así, siguiendo con las citadas *Reglas de Beijing* (números 21.1 y 21.1), se mantiene que los datos de los menores "no se utilizarán en procesos de adultos relativos a casos subsiguientes en

[30] Con referencia a la Observación General nº 10, del Comité de los Derechos del Niño, sobre los *Derechos de los Niños en la Justicia*, de 25 de abril de 2007 (CRC/C/GC/10), Apdos. 12 y 43.5. Disponible *on line*: http://www2.ohchr.org/english/bodies/crc/docs/CRC.C.GC.10_sp.pdf.

los que esté implicado el mismo delincuente, o como base para dictar sentencia en esos procesos futuros"[31].

En relación con este tema destaca el caso *R. contra R.C.*, de la Suprema Corte de Canadá, de 28 de octubre de 2005 (3 S.C.R. 99, 2005 SCC 61), donde al hilo de analizar el caso de un menor de 13 años condenado por agredir y lesionar a su madre, se decidió incluirle en una base de datos como si de un adulto se tratara y sin tener en cuenta el hecho concreto ni su vulnerabilidad y falta de madurez. En este caso, la CRIN entendió que si uno de los objetivos esenciales de la justicia en los casos de los menores es la rehabilitación, el objetivo debería ser proponer servicios a la sociedad u otras medidas más que garantizarse la privacidad del menor por encima de la protección del interés público.

Los menores en los Registros de Antecedentes Penales

Más allá del tratamiento de los datos personales de los menores que puedan realizar las propias instituciones públicas o los medios de comunicación de los procesos judiciales, el Comité de los Derechos del Niño también se ha pronunciado sobre el tratamiento de los datos de los menores y su inclusión en los Registros de Antecedentes Penales o Delictivos. Sobre esta cuestión el Comité ha recordado a los Estados parte que "adopten normas que permitan la supresión automática en los registros de antecedentes penales del nombre de los niños delincuentes cuando éstos cumplan 18 años, o, en un número limitado de ciertos delitos graves, que permitan la supresión del nombre del niño, a petición de éste, si es necesario en determinadas condiciones (por ejemplo, que no haya cometido un delito en los dos años posteriores a la última condena)"[32].

Sobre este tema se pronunció la CRIN, al hilo de la Sentencia del TEDH de 4 de diciembre de 2008, asunto *S. y Marper contra Reino Unido*, y consideró que el derecho de los niños a la privacidad implica que los Gobiernos no deben retener su ADN, huellas dactilares u otra información de identificación a menos que hayan sido condenados por un delito grave e incluso hasta que alcancen la mayoría de edad.

1.4. Datos de los menores en Internet

Informe del Relator Especial sobre libertad de expresión

El ejercicio del derecho a la vida privada cobra una nueva dimensión con la aparición de Internet, y en el caso de los menores de edad se hace más evidente, en tanto que éstos conciben su vida vinculada al desarrollo tecnológico. Por este motivo, es esencial que Internet se perciba no sólo como un peligro para los menores de edad, sino que se les eduque para un uso adecuado del mismo en función de sus capacidades. En el Informe del Relator Especial de Naciones Unidas sobre la *Promoción y protección del derecho a la libertad de opinión y de expresión*, se ha enfatizado en el hecho de que "las medidas de protección deben tratar de reconocer la evolución de las facultades del niño,

[31] Observación General nº 10, del Comité de los Derechos del Niño, Apdos. 64 y 66.

[32] Observación General nº 10, del Comité de los Derechos del Niño, Apdo. 67.

en lugar de utilizar medidas de absoluto bloqueo o censura que afectan negativamente a los niños y adultos por igual"[33].

Directrices de la OCDE

Es evidente que la información suministrada y manejada por las redes y sistemas de información debe cumplir con unos mínimos de seguridad, y así lo ha puesto de manifiesto nuevamente la OCDE con sus "Directrices para la Seguridad de Sistemas y Redes de Información: Hacia una Cultura de Seguridad"[34]. En este caso, aunque sin mención expresa a los menores, se indica la responsabilidad de los Estados por aunar medidas que refuercen la seguridad de los sistemas y redes de información a la vez que son respetuosos con los valores propios de una sociedad democrática, entre los que destaca el respeto por la privacidad.

Más allá de las medidas de seguridad a implementar para un adecuado tratamiento de los datos personales, con referencia expresa a la actuación de los menores en la Red, debemos citar aquí los principios aprobados por la OCDE sobre la *Protección de los menores on line* (2011)[35], que evidencian no sólo la necesidad de políticas públicas adecuadas, sino la necesidad de una cooperación internacional que sea consciente de los problemas que para la privacidad y la seguridad de los menores tienen los fenómenos de las redes sociales como *Facebook*, o las aplicaciones como *Whatsapp* o *Instagram*, la creación de *Blogs*, los juegos *on line*, o un mal uso de los teléfonos móviles, y otros dispositivos electrónicos.

Frente a estos peligros, son los padres y los poderes públicos los que se enfrentan a la tarea de proteger a los menores, como recogen los instrumentos jurídicos internacionales. Pero la cuestión no es sencilla, especialmente cuando mucha, por no decir la mayoría, de la información personal es suministrada por parte de los propios menores de forma voluntaria, ya sea a través de correos electrónicos, mensajes instantáneos o videos. La presión social de sentirse admitidos o ser populares serán los motivos que provocarán que la regla general de comportamiento de los menores de edad sea publicar y compartir su información personal[36].

En relación con el uso de las redes sociales *on line*, la regla general en el plano internacional sería la aplicación de las Directrices de la OCDE y los *Principios de la Protección de los Menores on line* que acabamos de citar. Las Directrices deben aplicarse a todo tratamiento de datos personales, independientemente de que el tratamiento se produzca dentro o fuera de la Red. Pero la cuestión en este ámbito es que la participación de los menores en las redes sociales y su consen-

---

[33] Informe presentado el 21 de agosto de 2014 (A/69/335). Disponible *on line*: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/512/75/PDF/N1451275.pdf?OpenElement.

[34] Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad, de 25 de julio de 2002. Disponibles *on line*: http://www.oecd.org/sti/ieconomy/34912912.pdf.

[35] "The Protection of Children Online", OCDE, 2 de mayo de 2011 (http://dx.doi.org/10.1787/5kgcjf71pl28-en).

[36] Centro de Investigaciones de UNICEF-Innocenti, *Child Safety Online: Global Challenges and Strategies*, mayo de 2012, p. 28. Disponible *on line*: https://www.unicef-irc.org/publications/658/.

timiento a formar parte de las mismas y compartir información personal se podrá hacer sin consentimiento paterno una vez superada la edad exigida para formar parte de ellas. Los usuarios de las redes sociales, como "consumidores" de las mismas, se adhieren a sus condiciones de uso. Por lo tanto, esta cuestión dependerá de cada uno de los Estados, por lo que la edad para consentir variará de unos Estados a otros, aunque en todos los casos sigan siendo menores de edad, escapando así al control parental.

Los peligros de la Red según el Comité de Derechos del Niño y UNICEF

Además de la cuestión de la participación de los menores en las redes sociales, otro tema que preocupa especialmente a los poderes públicos son los peligros implícitos de la Red. Incluso en el caso de que todos los sujetos responsables del tratamiento de datos de los menores cumplan estrictamente con la normativa sobre protección de datos, en Internet los menores de edad se van a enfrentar a una serie de peligros que se valen del presunto anonimato que brinda Internet y de la publicidad voluntaria que ellos mismos hacen de su información personal, especialmente de sus imágenes (algunas, por no decir bastantes, de ellas con contenido sexual). Por desgracia, Internet es empleada como un medio para acceder y difundir pornografía infantil, lo que está aumentando exponencialmente[37]. Sobre esta cuestión, la CDN exige la protección específica del niño contra todo tipo de explotación y abusos sexuales (art. 34). Desde UNICEF se insiste en concienciar a los menores de la responsabilidad de utilizar sus imágenes en la Red y potenciar una ciudadanía digital responsable, pero no debemos olvidar la responsabilidad de los adultos (progenitores, docentes, instituciones, empresas) por proporcionar un entorno *on line* seguro[38].

Problemas transfronterizos

Además, dada la ausencia de barreras del entorno on line, se hace necesario una eficaz colaboración e intercambio de información entre las fuerzas del orden encargadas de combatir estos delitos. En este sentido, las fuerzas policiales de algunos países en colaboración con la Interpol han creado una base de datos con el fin de identificar a los menores que aparecen en dichas imágenes, para ayudar a identificarles[39]. El tratamiento de estas imágenes, bajo la premisa de la prevención del delito y la protección del menor, no requerirá consentimiento personal ni de representantes. Se exceptuará de cumplir con muchos de los principios generales a la hora de tratar los datos personales. No obstante, deberán observarse estrictamente las medidas de seguridad de las bases de datos que se creen para prevenir los delitos contra los menores a través de la Red. El problema de la creación de bases de datos transfronterizas se va a producir porque, a falta de un estándar universal que garantice el derecho a la protección de datos, nos podremos encontrar con que no todos los Estados van a proteger la infor-

[37] Centro de Investigaciones de UNICEF-Innocenti, *Child Safety Online: Global Challenges and Strategies*, mayo de 2012.

[38] Centro de Investigaciones de UNICEF-Innocenti, *Child Safety Online: Global Challenges and Strategies*, mayo de 2012.

[39] En 2004, Interpol se hizo cargo de la gestión de dicha base de datos (*International Child Sexual Exploitation* (ICSE): https://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification. Base de datos (la I 24/7) (https://www.interpol.int/INTERPOL-expertise/Data-exchange/I-24-7).

mación de la misma manera. Por este motivo, se requieren protocolos y directrices muy estrictos, con aplicación universal, en relación con la gestión de estas bases de datos (quién puede acceder a ellas, cómo se comparten las imágenes, etc.) con el fin de proteger mejor la privacidad de un niño y garantizar al mismo tiempo su seguridad. Como ha puesto de relieve UNICEF se debe presionar al sector privado para que pongan en marcha las medidas necesarias para proteger los derechos de los menores, sin que se alegue una supuesta pérdida de competitividad o de libertad de empresa o la lesión de su libertad de expresión[40].

Necesidad de protección contra el *ciberbullying*

Otro de los peligros relacionados con Internet y el uso de la información de los menores en la misma, se encuentra en los casos de *ciberbullying*. Si bien el *bullying* se caracteriza por ser una violencia ejercida de forma reiterada en el centro escolar, en la actualidad el salir de las aulas no acaba con este comportamiento violento, sino que el mismo persiste a través de las redes sociales y aplicaciones *on line* y de los dispositivos móviles[41]. Se evidencia la necesaria regulación de la materia, y no sólo por el uso ilícito de los datos personales que se produce al tratarse información de menores de edad sin el correspondiente consentimiento y para unos fines ilícitos[42].

El caso Nickelodeon

Se plantea, por lo tanto, establecer mecanismos que limiten el acceso de los menores a la Red o que monitoricen su uso. En este sentido, en relación con el rastreo de información de menores por Internet y su uso, la CRIN comenta el caso *Nickelodeon Consumer Privacy Litigation*, de 27 de junio de 2016 (3rd U.S. Circuit Court of Appeals, No. 15-1441), en el que los demandantes eran dos menores de 13 años respecto de los que las compañías *Viacom* y *Google* habían rastrearon sus hábitos de navegación por Internet. En este caso, el Tribunal se basó en la "expectativa de privacidad" que tenían, no tanto los menores, sino sus padres, que bajo su responsabilidad permitieron que sus hijos accedieran a Internet, lo que en último término provocó la lesión de la vida privada de los menores.

Por último la publicación en Internet o a través de dispositivos móviles, por parte de los menores, de datos personales que no son propios sino de terceros, sin contar con el correspondiente consentimiento supone una infracción de lo dispuesto en las Directrices de la OCDE.

1.5. Ejercicio por los menores de su derecho a la protección de datos

Directrices de la OCDE

Las Directrices de la OCDE reconocen las tradicionales facultades del derecho a la protección de datos personales (el acceso, la rectificación

[40] Centro de Investigaciones de UNICEF-Innocenti, *Child Safety Online: Global Challenges and Strategies*, mayo de 2012.

[41] Al respecto, vid. *World Report on Violence Against Children*, de las Naciones Unidas (2006). Disponible *on line*: http://www.unicef.org/violencestudy/ y https://www.unicef.org/violencestudy/reports/SG_violencestudy_sp.pdf.

[42] Un estudio de la ONG ECPAT Internationational recoge los delitos en su Informe *Violence against Children in Cyberspace* (2005). Disponible *on line* en: http://www.childcentre.info/projects/internet/dbaFile12243.pdf.

y la cancelación) a todo sujeto titular del derecho como parte del Principio de participación individual (art. 13), con la peculiaridad (no indicada expresamente, pero derivada de la falta de capacidad de obrar de los mismos) de que si son ejercidas por menores de edad, las mismas se ejercerán por sus representantes.

Límites a los derechos; el caso Hosking

En relación con el ejercicio de estos derechos, a este nivel, la cuestión se va a plantear no tanto por el ejercicio por parte de los menores, en tanto que los ejercerán en la mayoría de las ocasiones a través de sus representes legales, sino en relación con los límites con los que se van a encontrar. Por ello, un conflicto tradicional, como ha quedado dicho, lo van a plantear las libertades informativas. La regla general en caso de conflicto será identificar el interés superior del niño con la presunción de su permanencia dentro de la familia y, por tanto, vinculado a la patria potestad de sus padres o tutores.

En este sentido, podemos citar aquí el caso *Hosking and Hosking contra Runting and Pacific Magazines NZ Ltd*, de la Corte de Apelación de Nueva Zelanda, de 25 de marzo de 2004 ((2004) 7 HRNZ 301), donde la Corte, haciendo suya la interpretación de la CRIN sobre el derecho a la vida privada garantizado por la CDN, considera que la petición de un personaje público de que no fueran fotografiadas las imágenes de sus hijos hasta que éstos no tuvieran 18 años, no lesionaba la privacidad de los menores y que sus imágenes podrían ser publicadas porque la información no había sido obtenida de un lugar donde existiera una expectativa razonable de privacidad (como podría ser el domicilio familiar) y porque la publicidad de la información no resultaba excesivamente ofensiva para la persona.

Problemática de la cancelación y borrado de imágenes y otros datos

Por otro lado en relación con el ejercicio de cancelación o borrado de datos de menores, como pueden ser las imágenes de los mismos, la cuestión sigue siendo que al estar protegidos por el entorno familiar, esta decisión la tomarán los padres o tutores salvo que prime el interés superior del menor, o que por lo dispuesto en la normativa nacional, no se requiera el consentimiento del menor. El problema lo encontramos por la dificultad técnica que ello comporta. Por este motivo, como se ha puesto de manifiesto por UNICEF, la publicación de dichas imágenes, o incluso la amenaza de publicar imágenes sin consentimiento de su titular debe considerarse una infracción y una injerencia en la vida privada de los menores[43].

En este sentido, en el marco de revisión de las Directrices de la OCDE de 1980 que se produjo en el 2013, se indicó que el problema de las Redes sociales y de los perfiles creados en las mismas es la dificultad no tanto para acceder y borrar la información "colgada" personalmente, sino para acceder y borrar la información que sobre uno mismo publican terceras personas, con la dificultad añadida de su rápida diseminación e indexación por parte de buscadores *on line*.

Las Directrices OCDE de 1980 no contienen expresamente un principio relativo a la conservación de la información, por lo que se considera conveniente recoger dicha previsión teniendo en cuenta que en la actualidad es más fácil conservar la información que borrar-

[43] Centro de Investigaciones de UNICEF-Innocenti, *Child Safety Online: Global Challenges and Strategies*, mayo de 2012, p. 14.

la, con los efectos que ello provoca, especialmente en el caso de los menores de edad y en su futuro desarrollo personal y profesional.

En relación con el borrado, recordamos aquí, como ha hecho la CRIN, el caso *J. contra el National Director of Public Prosecutions* y otros, del Tribunal Constitucional de Sudáfrica, de 6 de mayo de 2014, que analizó el supuesto de un joven de 14 años de edad que había sido acusado de violar a otros menores y fue condenado por ello, procediendo, conforme a la normativa nacional, a incluírsele en un Registro Nacional de Delincuentes Sexuales. Aquí, como en los casos que hemos analizado, como regla general en este terreno, y como sostuvo el Tribunal competente, se debe proceder a su no inclusión o a su borrado por ser contraria dicha actuación al interés superior del menor.

Derecho a la información de los menores

Reconocido como un derecho para los titulares de los datos y como una obligación por parte de los responsables del tratamiento de los mismos, debemos mencionar aquí el principio o derecho a la información sobre el tratamiento de datos personales. Las Directrices de la OCDE de 1980 recogen la exigencia de ofrecer una información transparente sobre los tratamientos de datos que se produzcan (art. 12 sobre el Principio de transparencia), hablándose del titular de los datos, independiente de que fuera mayor o menor de edad. No obstante, esta recomendación recogida también en la mencionada Resolución Madrid sobre los Estándares Internacionales de Privacidad donde se habla de una información accesible y sencilla sobre el tratamiento de datos producido, se recoge, además, expresamente que esta obligación deberá cumplirse especialmente cuando los destinatarios sean menores de edad (Apdo. 10.5).

2. ÁMBITO LATINOAMERICANO

2.1. Marco normativo

Los derechos del niño y sus garantías en la OEA

La Organización de los Estados Americanos (OEA), como organismo regional intergubernamental, tiene entre sus objetivos, promover y proteger los derechos humanos en la región. La OEA tiene como principales instrumentos jurídicos la Carta de la OEA[44], y la Convención Americana sobre Derechos Humanos o Pacto de San José (CADH)[45], y su Protocolo Adicional (Protocolo de San Salvador)[46]. El Sistema Interamericano de Derechos Humanos reconoce la ya ci-

[44] La Carta de la OEA, adoptada en la Conferencia de Bogotá, de 30 de abril de 1948. Disponible *on line*: http://www.oas.org/es/sla/ddi/docs/tratados_multilaterales_interamericanos_A-41_carta_OEA.pdf.

[45] La Convención Americana sobre Derechos Humanos fue suscrita en la Conferencia especializada Interamericana sobre Derechos Humanos (B-32), en San José, Costa Rica, del 7 al 22 de noviembre de 1969. Disponible on line: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf.

[46] Protocolo adicional a la Convención Americana sobre Derechos Humanos en materia de derechos económicos, sociales y culturales, "Protocolo de San Salvador", adoptado en San Salvador, el 17 de noviembre de 1988. Disponible *on line*: http://www.oas.org/juridico/spanish/Tratados/a-52.html.

tada Convención de los Derechos del Niño (CDN) con el fin de proteger los derechos de niños y adolescentes en el ámbito latinoamericano y tiene como marco legislativo de referencia la citada CADH. La CADH garantiza los derechos del niño expresamente en su artículo 19, reconociendo la obligación de protección por parte de "su familia, de la sociedad y del Estado"; y además garantiza la honra y dignidad de "todas las personas" (art. 11), reconociéndoles un respeto por su vida privada. Se entienden comprendidos en su ámbito subjetivo a los menores de edad.

De la misma forma que a nivel internacional, en relación con la protección de los derechos reconocidos en la CADH, tanto dicha norma como la Carta de la OEA prevén unos mecanismos de garantía de los derechos por ellas garantizados entre los que se encuentra la Comisión Interamericana de Derechos Humanos (CIDH, art. 53 Carta de la OEA) y la Corte Interamericana de Derechos Humanos (Corte IDH, art. 33 b) CADH). En el caso concreto de los derechos del niño, homólogo al Comité de los Derechos del Niño de las Naciones Unidas, en el seno de la CIDH se creó, en 1998, la Relatoría sobre los Derechos de la Niñez con el fin de garantizar los derechos de niños y adolescentes en América latina[47]. De la misma forma, como organismo especializado de la OEA para los temas de la niñez se constituyó el Instituto Interamericano de los Derechos del Niño, la Niña y Adolescentes (IIN)[48]. Los derechos de los niños se harán valer a través de los pronunciamientos de los citados organismos teniendo presente, como señaló la Corte IDH, que los mismos son un grupo vulnerable[49].

Colaboración de Save the Children

Asimismo, junto al papel de los poderes públicos en este terreno, debemos destacar la importante labor que en el Sistema Interamericano han tenido las ONGs como Save the Children, que viene trabajando desde hace años en América Latina y ha elaborado y colaborado en la publicación de diferentes Guías y Estudios con el fin garantizar los derechos de los niños. Así, por ejemplo, destaca la colaboración con la Organización Internacional del Trabajo (OIT) con el fin de investigar sobre el trabajo infantil, o bien la publicación del Manual "Construyendo los derechos del niño en las Américas"[50].

Doctrina de la Corte IDH y remisión al Derecho interno

Como ocurría a nivel internacional, no existe una norma expresa que regule el tratamiento de los datos personales de los menores. No obstante, la Corte IDH ha sostenido que los niños poseen los mismos

[47] La Relatoría se creó en el 100º período ordinario de sesiones de la CIDH, celebrado en Washington D.C. del 24 de septiembre al 13 de octubre de 1998. Para más información sobre la Relatoría, vid. su web: http://www.oas.org/es/cidh/infancia/.

[48] Más información sobre el mismo se puede encontrar en su web: http://iin.oea.org/.

[49] Opinión Consultiva OC-17/02, de la Corte IDH, de 28 de agosto de 2002, sobre la "Condición jurídica y Derechos humanos del niño", a raíz del primer caso presentado ante la Corte donde los niños eran las víctimas de la violación de derechos (vid. caso "Niños de la calle (Villagrán Morales y otros) contra Guatemala", de 11 de septiembre de 1997).

[50] https://www.crin.org/en/library/organisations/save-children-sweden-regional-programme-latin-america-and-caribbean. En general, sobre la situación de los niños en Latinoamérica y el Caribe, vid. https://www.savethechildren.net/sites/default/files/libraries/Annual%20Report%202014_LAC.pdf.

derechos que les corresponden a todos los seres humanos, aunque tengan derechos especiales por su condición y deban ser protegidos por la familia, la sociedad y el Estado, teniendo siempre en cuenta el interés superior del menor[51]. Así las cosas, aunque existen unas Directrices de armonización para el tratamiento de datos personales en la región, no hay tampoco un instrumento normativo vinculante que regule la materia, y deberán ser los distintos Estados los que se encarguen de su desarrollo y, en su caso, de establecer las precisiones que consideren oportunas sobre el tratamiento de datos de los menores.

El habeas data en Latinoamérica

En la región latinoamericana, con carácter general, podemos afirmar que el desarrollo del derecho a la protección de datos personales no se produjo hasta bien entrada la década de los ochenta y de la mano de la figura conocida como "habeas data", que comienza a cobrar difusión a partir de los años noventa y que se desarrolla teniendo como referentes las Directrices de la OCDE y, especialmente, la normativa comunitaria en la materia, esto es, las Directivas comunitarias existentes. Por lo tanto, la referencia que estas normas concretas realizan sobre tratamiento de datos en general y en el caso de menores (lo que brilla por su ausencia) habrá que entenderlas aplicables al sistema interamericano. La mayor parte de los Estados iberoamericanos reconocen el derecho a la protección de datos personales de forma directa en el texto constitucional o por interpretación jurisprudencial. Incluso en alguno de estos Estados se ha reconocido de forma expresa en sus normas y en sus Constituciones, la titularidad del derecho por parte de los menores de edad. De hecho, en líneas generales podemos decir que la jurisprudencia interamericana ha venido garantizando el derecho a la protección de datos personales como parte del derecho a la honra y dignidad, o vida privada que se garantiza por el art. 11 CADH. La Corte IDH ha señalado que entre los ámbitos protegidos por el art. 11 CADH, se encuentra el secreto de todos los datos que se produzcan en el ámbito privado del sujeto. De esta forma, por ejemplo, la Corte está prohibiendo toda divulgación o publicación de información personal si no cuenta con el consentimiento de su titular por lesionar, en caso contrario, su vida privada (Por ejemplo, Sentencia de la Corte IDH, *Caso Fontevecchia y D'Amico contra Argentina*, de 29 de noviembre de 2011 (Fondo, Reparaciones y Costas), Apdo. 48).

La Declaración de Santa Cruz de la Sierra de 2003

Los Estados latinoamericanos han avanzado en el desarrollo y regulación del tratamiento de los datos personales y han dado un paso más desde la conocida como "Declaración de Santa Cruz de la Sierra", Declaración de la XIII Cumbre Iberoamericana de Santa Cruz de la Sierra (Bolivia), emitida por los Jefes de Estado y de Gobierno de veintiún países iberoamericanos, de noviembre de 2003. En su Apartado 45 se reconoció la importancia del derecho a la protección de datos como un derecho fundamental[52]. Se respaldaba así el trabajo

[51] Opinión Consultiva OC-17/02, de la Corte IDH, Apdos. 53-55 y 63-65.

[52] Apdo. 45 "*Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad*". Disponible *on line*: http://www.oei.es/historico/xiiicumbredec.htm.

llevado a cabo por la Red Iberoamericana de Protección de Datos, cuya labor es esencial en este terreno[53].

Las Directrices de armonización de 2007

En este ámbito regional, en el marco de los Encuentros promovidos por la Red, en el año 2007 (concretamente en el V Encuentro de la Red Iberoamericana de Protección de Datos, celebrado en Lisboa los días 8 y 9 de noviembre)[54], se aprobaron unas *Directrices para la armonización de la protección de datos en la Comunidad iberoamericana (Directrices de armonización)*[55]. Dicho Documento es realmente relevante, pues en él se recogen las directrices que se consideran necesarias para elaborar una adecuada y correcta norma que garantice el derecho a la protección de datos personales. Entre las mismas se citan como principios básicos que deberían constar en una norma sobre protección de datos personales, entre otros principios, los principios de calidad y proporcionalidad de los datos (entre los que se incluye la exigencia del consentimiento del titular de los datos para su tratamiento), el principio de transparencia o los derechos de acceso, rectificación, supresión y bloqueo de los datos. Asimismo, en el ámbito de aplicación de las normas que se elaboren, las citadas Directrices consideran conveniente que se apliquen a todo tratamiento de datos de las personas físicas, que serán los titulares de los datos o "interesados" como los denominan las Directrices, sin hacer distinción para el caso de que sean menores de edad o sin hacer mención alguna a la posibilidad de que el ejercicio del derecho a la protección de datos en esos supuestos se lleve a cabo por un representante.

El Memorándum de Montevideo de 2009

Junto a estos criterios generales sobre el tratamiento de datos personales, en la región latinoamericana, en relación con el tratamiento de datos personales en Internet, destaca el conocido "Memorándum de Montevideo", Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, presentado en julio de 2009[56]. En el citado Memorándum, dirigido a los países de América Latina y el Caribe, se recogen una serie de principios que deberían regir e inspirar las ventajas que ofrecen las tecnologías de la información e Internet y evitar los riegos que las mismas generan, especialmente para los sujetos más vulnerables, como son los menores y adolescentes.

Necesidad de instrumentos vinculantes

Debemos concluir señalando, como hicimos en relación con el marco jurídico internacional, que la ausencia de una regulación a nivel regional lationoamericano de un instrumento jurídico vinculante en materia de protección de datos personales resta eficacia a la regula-

[53] La Red fue creada en el II Encuentro Iberoamericano de Protección de Datos celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003. Al respecto, vid. la Declaración de La Antigua (http://www.redipd.es/documentacion/common/declaracion_2003_II_encuentro_es.pdf). Y sobre la Red, su web: http://www.redipd.org/index-ides-idphp.php.

[54] Disponible en: http://www.redipd.es/documentacion/common/declaracion_2007_V_encuentro_es.pdf.

[55] El texto de las Directrices, disponible *on line*: http://www.redipd.es/actividades/encuentros/V/common/9_nov/Directrices_de_armonizacion.pdf.

[56] El citado Memorándum tiene su origen en las Recomendaciones adoptadas en el *Seminario Derechos, Adolescentes y Redes Sociales en Internet*, que tuvo lugar en el seno del Instituto de Investigación para la Justicia, los días 27 y 28 de julio de 2009. Disponible *on line*: http://www.iijusticia.org/docs/MemoMVD_Es.pdf.

ción sectorial o nacional existente y, en el caso de los datos de menores, les deja en una situación de indefensión. Se deberían garantizar unos mínimos niveles de protección y unas buenas prácticas a la hora de tratar datos personales con especial atención cuando dichos tratamientos afectan a los datos personales de menores de edad. A falta de un documento concreto específico relativo al tratamiento de datos personales de los menores, sería conveniente la aprobación de un instrumento jurídico general en la materia el que se deberían incluir especiales referencias a los menores de edad como sujetos especialmente protegidos con el fin de garantizar su privacidad y su desarrollo personal.

2.2. El consentimiento del menor para el tratamiento de sus datos personales

Necesidad de representación hasta la madurez del menor

El artículo 16 del Protocolo adicional a la CADH añade a los derechos del niño (garantizados por el art. 19 de dicha norma) que los niños crecerán al amparo de sus padres. Por lo tanto, como hemos visto a nivel internacional, serán los padres o tutores los que presten el consentimiento por los menores a la hora de tratar sus datos personales.

En el caso del consentimiento para tratar datos personales, y en concreto en relación con Internet y las redes sociales, el Memorándum de Montevideo indica que no se debería permitir "la recopilación, tratamiento, difusión, publicación o transmisión a terceros de datos personales, sin el consentimiento explícito de la persona concernida" (Pto. 19). Debemos entender la referencia hecha a los padres o representantes. No obstante, el propio Memorándum diferencia entre adolescentes y jóvenes a la hora de prestar el consentimiento en relación con estos temas y la indexación de sus perfiles por buscadores como Google, pues indica que sólo se deberían indexar perfiles de usuarios (entre los que se incluye a adolescentes) cuando éstos lo hubieran solicitado y que, en ningún caso, deberían indexar los perfiles de los niños (Pto. 25). Así pues, el consentimiento de los menores no será tenido en cuenta, pero sí el de los adolescentes, que en estos casos, parecen no requerir del consentimiento paterno. Parece que habrá que estar nuevamente al grado de madurez del menor y a la edad establecida por cada uno de los Estados.

El desarrollo progresivo según la Corte IDH

Así las cosas, la regla general, será como ha venido manifestando la Corte IDH, que los derechos del menor se ejercerán según el desarrollo progresivo del mismo, por lo que "en su primera infancia" actuará "por conducto de sus familiares" (así lo ha manifestado, entre otras, en el caso *Gelman contra Uruguay*, de 24 de febrero de 2011, Fondo y Reparaciones, Apdo. 129; o en el asunto *Atalafa Riffo y Niñas contra Chile*, de 24 de febrero de 2012, Fondo, Reparaciones y Costas, Apdos. 68 y 199). Así lo manifestó también de forma clara la CIDH, aunque fuera del tema del tratamiento de sus datos personales o las redes sociales. Aquí la Comisión manifestó que la menor, de 13 años, "no tenía la capacidad legal para consentir" y que la voluntad

de la menor era "totalmente dependiente de la decisión tomada por la madre" (Informe nº 38/96 de la CIDH, caso nº 10.506, *X. e Y. contra Argentina*, de 15 de octubre de 1996 (Apdos. 101-103).

2.3. Ámbitos problemáticos

a) En las relaciones familiares

Conflictos intrafamiliares y decisión de los padres

La CADH, reiterando lo dispuesto por la CDN, reconoce en su Protocolo Adicional que "la familia es el elemento natural y fundamental de la sociedad" y que, como tal, debe ser protegida por el Estado. Asimismo, se indica que "todo niño" tiene derecho a ser protegido por su familia. Con estas premisas, teniendo como referente las citadas *Directrices de armonización para un adecuado tratamiento de datos personales*, los menores podrán ser titulares de sus datos personales y tendrán derecho a su vida privada, pero en el entorno familiar, o dependientes de las decisiones tomadas por sus padres o tutores. Si bien se deberá hacer primar el interés superior del menor en caso de conflicto, serán los padres los que decidan sobre el tratamiento de los datos personales de sus hijos.

Doctrina de la Corte Suprema de Colombia

Así, por ejemplo, la Sala de Casación Penal de la Corte Suprema de Colombia, en su Sentencia de 29 de julio de 2015 (Nº de providencia SP 9792-2015), analizó la denuncia presentada contra unos padres que accedieron a la cuenta de correo electrónico de su hija menor de 12 años con el fin de comprobar que mantenía relaciones con un hombre de 18 años, al que denunciaron por abusar de ella mental y psicológicamente. El denunciado alegó que la prueba de los mails no podía ser utilizada porque los padres habían lesionado la vida privada de su hija. En este caso, la Corte colombiana se planteó si la vigilancia de la actividad en línea de los niños por sus padres, en casos de sospecha de abusos contra los mismos, suponía una violación de su derecho a la privacidad. La Corte concluyó que los padres están "constitucional y legalmente autorizados para ayudar, guiar y controlar las comunicaciones de sus hijos menores de edad con el propósito de proteger y garantizar los derechos fundamentales de los niños y adolescentes". La Corte fundamentó su decisión apoyándose en la CDN, pero sin embargo dejó indicado que si los padres hubieran accedido a la información de su hija sin buscar su protección, habrían actuado de forma ilegal. Es decir, la Corte consideró que el deber de los padres de proteger a sus hijos no permite una violación de sus derechos. Sobre este caso se pronunció la CRIN, confirmando la necesidad de proteger la vida privada de los menores y la necesidad de respetar las obligaciones de los padres a la hora de guiar a sus hijos en el ejercicio de sus derechos de acuerdo con la capacidad de los mismos (arts. 16 y 5 CDN).

Derecho al registro desde el nacimiento

En relación con estas obligaciones paternas de velar por el correcto desarrollo del menor, en relación con el tratamiento de la información del menor, debemos destacar aquí que (igual que hiciera el art. 7 CDN), la OEA y el IIN se han referido a la obligación de inscribir a

los niños en el registro civil nada más nacer (antes del tercer mes de vida), teniendo el derecho, además, a un nombre y a conocer a sus padres y ser cuidados por ellos[57]. Es relevante la correcta inscripción del nombre del menor en tanto que del mismo se deriva la adquisición, no sólo de unos derechos y la correspondiente nacionalidad, sino la propia identidad del menor (garantizada por los arts. 8 y 30 CDN). Así, la Corte IDH, al hilo de pronunciarse en un caso de desaparición de menores señaló que "muchos de los niños y niñas desaparecidos eran registrados bajo información falsa o sus datos alterados, como ocurrió en el caso de Gregoria Herminia, aspecto que irradia sus efectos en dos sentidos: por un lado, para el niño o niña apropiada, a quien se le imposibilita buscar a su familia y conocer su identidad biológica y, por el otro, a su familia de origen, a quienes se les obstaculiza el ejercicio de los recursos legales para restablecer la identidad bilógica, el vínculo familiar" (Caso *Contreras y otros contra El Salvador*, de 31 de agosto de 2011 (Fondo, Reparaciones y Costas), Apdo. 89). Se demuestra así la importancia de un adecuado y legítimo tratamiento de los datos de los menores desde el mismo momento de su nacimiento.

Datos en sustracción de menores

Pero cuestiones más conflictivas en el entorno familiar se van a producir cuando exista una ruptura del mismo, que puede venir motivada por la separación de los padres del menor, fallecimiento de uno de ellos o de ambos o por secuestro del menor por parte de uno de los progenitores o representantes. En este sentido, y en relación con el necesario tratamiento de la información del menor, los casos más graves serán aquéllos en los que se produce la sustracción del menor. Aquí es indispensable contar con un sistema que ayude a su localización. De ahí que el intercambio de información de los menores debe respetar las *Directrices de armonización* en relación con su seguridad y confidencialidad. Este intercambio de información en el ámbito latinoamericano se ha visto reforzado por la aprobación del "*Programa Interamericano de cooperación para prevenir y reparar casos de sustracción internacional de menores por uno de sus padres*"[58].

b) En el entorno escolar

Interés superior del niño y derechos de los padres en el entorno educativo

El Protocolo Adicional a la CADH garantiza el derecho a la educación de "toda persona" (art. 13.1), sin referencia expresa a los menores o al tratamiento de su información en el proceso de escolarización, pero indicando que serán los padres los que decidirán sobre la educación de sus hijos (art. 12.4 CADH). En este sentido, el tratamiento de datos de los menores en el entorno escolar estará supeditado a la voluntad de sus padres o tutores, que son los que le representan y

[57] Así se acordó en la Décima Cumbre de Jefes de Estado y de Gobierno de los Países Iberoamericanos, celebrada en Panamá los días 17 y 18 de noviembre de 2000, "Declaración de Panamá. Unidos por la Niñez y la Adolescencia, Base de la Justicia y la Equidad en el Nuevo Milenio", Pto. 9.a). Disponible on line: http://www.oei.es/historico/xcumbredec.htm.

[58] Aprobado por Resolución de la Asamblea General de la OEA (AG/RES. 2028), de 8 de junio de 2004 (XXXIV-O/04).

deciden por ellos en este terreno. Todo ello bajo la premisa del principio del interés superior del menor. En esta misma línea, en el Memorándum de Montevideo se recomienda que en caso de conflicto a la hora de tratar datos personales de los menores por parte de los centros educativos, se tenga en cuenta el interés superior del menor (Pto. 5).

***Soft law* sobre datos en el entorno escolar**

Si no existe conflicto alguno a la hora de tratar datos personales de los menores, los centros escolares, así como su personal y el resto de sujetos que intervengan en el proceso educativo del menor, deben cumplir con las Directrices de armonización ya citadas, en especial, en lo relativo a las medidas de seguridad y confidencialidad y a la publicación y cesión de información de los menores a terceros, para lo que se requerirá, por regla general, el consentimiento del menor o el paterno.

En este terreno, las recomendaciones del Memorándum de Montevideo en materia de tratamiento de datos personales lo que indican es la necesidad de que en el proceso educativo de los menores se haga especial hincapié y se inculque a los mismos el respeto a la vida privada y a la reputación tanto personal como de terceras personas, con el fin de que los menores de edad comprendan que la publicación de sus datos personales o los de terceros puede poner en peligro su vida privada y la de estos terceros y tener una repercusión en su posterior desarrollo personal y profesional (Pto. 3.2).

c) En el ámbito sanitario

Interés superior del niño en el ámbito sanitario

El artículo 10 Protocolo Adicional a la CADH reconoce el derecho a la salud de "toda persona", lo que incluye al menor. El menor, dentro del campo de protección de los padres o tutores se verá bajo la voluntad de estos últimos, lo que supone que sus datos médicos o de salud serán tratados bajo la voluntad de sus padres. No obstante, cuando el menor tenga que hacer valer sus derechos en este ámbito en relación con su información médica o con los tratamientos médicos a los que prestará el consentimiento habrá que estar al principio del interés superior del mismo.

Doctrina de la Corte Constitucional colombiana y de la CIDH

Así, por ejemplo, interpretando la CADH y la CDN, la Corte Constitucional colombiana, en su sentencia de 12 de mayo de 1999 (SU 337/99) analiza la armonización de la vida privada del menor (que debía decidir sobre un determinado tratamiento médico) en el entorno familiar. En este caso, la Corte mantiene que "Los padres y tutores pueden tomar ciertas decisiones en relación con el tratamiento médico de los niños, incluso, a veces, contra la voluntad aparente de éstos. Sin embargo, ello no quiere decir que los padres puedan tomar, a nombre de su hijo, cualquier decisión médica relativa al menor, por cuanto el niño no es propiedad de nadie sino que él ya es una libertad y una autonomía en desarrollo, que tiene entonces protección constitucional". Así las cosas, en relación con el tratamiento de los datos de salud de los menores de edad, se deberá tener en cuenta el consentimiento informado del menor, que deberá ser teni-

do en cuenta, pero estará vinculado al paterno, tal y como ha confirmado la CIDH, en el ya citado Informe nº 38/96 de la CIDH, caso nº 10.506, *X. e Y. contra Argentina*, de 15 de octubre de 1996 (Apdos. 101-103).

d) En los medios de comunicación

Ponderación entre libertad de expresión y protección de datos

El Sistema Interamericano de Derechos Humanos otorga un papel esencial a los medios de comunicación como garantes de las libertades informativas y, por tanto, del principio democrático. No obstante, dichas libertades no son absolutas y uno de los límites con los que se va a enfrentar es el del derecho a la vida privada del menor y la necesidad de proteger sus datos personales[59].

Atendiendo a los derechos del menor, se debe realizar una ponderación de los intereses en juego. Aunque tanto la CIDH como la Corte IDH han destacado la relevancia de los medios de comunicación, también han destacado la necesidad de que los mismos actúen conforme a una conducta ética y responsable, tal y como señala (art. 6) la *Declaración de Principios sobre la Libertad de Expresión*, adoptada por la CIDH (2000)[60]. Asimismo, la CIDH ha tenido claro, por otro lado, que en la publicación de información relativa a procesos judiciales o administrativos, las leyes de privacidad no pueden restringir ni limitar con carácter general la información de interés público. Habrá que realizar una adecuada ponderación haciendo primar el interés superior del menor ante la posible colisión entre la vida privada de éste y la libertad de información de los medios[61]. En este sentido, el IIN ha indicado que a la hora de difundir información que afecte a menores de edad, especialmente cuando se publican noticas sobre casos de malos tratos o violencia, "es fundamental omitir su identidad o cualquier referencia a su entorno que permita la identificación (evitar difundir nombres de familiares, datos del barrio, entre otros)", debiendo tener en cuenta el citado interés del menor y consultado a sus padres sobre lo que se puede o no publicar[62].

Sobre el papel de los medios de comunicación utilizando datos personales o información de menores, UNICEF ha destacado que "la actividad periodística que afecte a la vida y el bienestar del niño siempre debería realizarse teniendo presente la situación vulnerable del niño. Los periodistas y las organizaciones de los medios de comunicación procurarán mantener las normas de conducta ética más elevadas

---

[59] Extraído del Informe sobre Libertad de expresión e Internet, de la CIDH, OEA, diciembre 2013, p. 26. Disponible *on line*: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf.

[60] Informe sobre *Violencia, Niñez y Crimen organizado*, de la CIDH, OEA, noviembre 2015, p. 234. Disponible *on line*: http://www.oas.org/es/cidh/informes/pdfs/violencianinez2016.pdf.

[61] Declaración de *Principios sobre Libertad de Expresión*, de la CIDH, octubre 2000, Pto. 10. Disponible *on line*: http://www.cidh.org/Basicos/Basicos13.htm.

[62] Guía "Medios de comunicación y niñez en perspectiva de derechos", elaborada por el IIN, 2012, pp. 16, 31-32 y 38-40. Disponible *on line*: http://iin.oea.org/pdf-iin/publicaciones/medios/guia_esp.pdf.

a la hora de informar sobre aspectos que atañan a los niños"[63]. Así lo ha reiterado la Corte IDH en el asunto *Granier y otros (Radio Caracas televisión) contra Venezuela*, de 22 de junio de 2015.

Doctrina de la CIDH

A este respecto la CIDH ha añadido que cuando en una noticia hay implicados menores, la misma debe ofrecerse en un lenguaje que no les estigmatice. Esto es especialmente relevante en una sociedad como la actual donde la mayoría de noticias aparecen ya en Internet y donde es difícil borrar la información una vez publicada en la Red. Por este motivo, desde la CIDH se solicita que los Estados protejan la identidad de las víctimas y testigos de casos de violencia, especialmente cuando hay implicados menores en el asunto[64].

Por último, en el caso concreto de que la información se difunda a través de Internet, la CIDH ha considerado que a la hora de la correspondiente ponderación de los derechos en juego se deberán tener en cuenta, además, las peculiaridades de Internet y su potencial efecto de difusión, y cómo no, cómo el mismo puede afectar en mayor medida a los menores de edad[65].

e) Como partes de una relación contractual

Responsabilidad de los padres en contratos suscritos por sus hijos

Tomando como referente la CDN, ya hemos visto cómo el Sistema Interamericano recoge en la CADH el hecho de que los menores están bajo la protección de la familia. Por este motivo, los menores, como parte de una relación contractual, verán tratados sus datos personales bajo la responsabilidad directa de sus padres o tutores, atendiendo en todo caso a lo dispuesto por la normativa civil de cada Estado.

Derecho de daños

Por otro lado, en relación concreta con los daños causados a sus datos personales como partes de una relación contractual, el Memorándum de Montevideo, en las Recomendaciones efectuadas a los Estados sobre la aplicación de las leyes, indica que "se debe fortalecer el uso de la responsabilidad civil extracontractual objetiva como mecanismo regulatorio para garantizar los derechos fundamentales en las aplicaciones en la Sociedad de la Información y Conocimiento, Internet y redes sociales digitales". Se parte de la idea de que en estos casos las sanciones judiciales por los daños derivados deberían ofrecer una respuesta inmediata, eficiente y capaz de desincentivar los "diseños peligrosos" que atenten contra la privacidad del menor. Se mantiene en el Memorándum que este tipo de responsabilidad civil se fundamenta en el interés superior del niño (Pto. 10.1).

---

[63] Informe de UNICEF sobre "Los derechos del niño y la práctica del periodismo: una perspectiva basada en los derechos", Dublin Institute of Technology, 2007. Disponible *on line*: https://www.unicef.org/mexico/spanish/manual_para_periodistas_ninez_y_medios.pdf.

[64] Informe sobre *Violencia, Niñez y Crimen organizado*, de la CIDH, OEA, noviembre 2015, p. 236.

[65] Declaración Conjunta sobre *Libertad de expresión en Internet* del Relator Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión y la Relatora Especial para la libertad de expresión de la CIDH, de 20 de enero de 2012 (Disponible *on line* en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=888&lID=2).

f) Como partes de un proceso judicial

Deber de anonimización en el Memorándum de Montevideo

Respecto de los datos de los menores tratados en los procesos judiciales, el principal problema en el que se va a centrar el sistema interamericano va a ser en la publicación o publicidad de los datos de los mismos. En este sentido, el Memorándum de Montevideo señala que si bien las decisiones judiciales deberán tener difusión, se deberán utilizar "técnicas de anonimización que garanticen la protección de datos personales". Reiteramos aquí lo indicado para los medios de comunicación y la ponderación de los intereses en juego.

Reglas de Heredia

En esta misma línea, en este terreno destacan las conocidas como *Reglas de Heredia*, que son unas Recomendaciones destinadas a hacer compatible la necesaria transparencia de los pronunciamientos judiciales y el respeto al tratamiento de los datos personales contenidos en los mismos, especialmente cuando la publicidad de las sentencias se va a producir en Internet[66]. En las citadas Reglas, concretamente en su Regla 5 se establece la prevalencia de "los derechos de privacidad e intimidad, cuando se traten datos personales que se refieran a niños, niñas, adolescentes (menores) o incapaces".

Límites a la publicidad procesal en Colombia

En relación con los procesos penales y su publicidad, teniendo como fundamento jurídico la CADH y la CDN, destaca la petición formulada por la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio (SIC) de Colombia en cuya Decisión, de 23 de enero de 2014, se ordenó a la Relatoría de la Sala Penal de la Corte Suprema de Justicia que se abstuviera de publicar en Internet una sentencia que permitía identificar a una menor de edad que había sido víctima de abusos sexuales. En este caso se reiteró la especial protección de los denominados datos sensibles, especialmente cuando podía afectar a los menores de edad. De hecho, en la mayoría de casos que se sustancian ante la Corte Constitucional colombiana contra menores, se realiza una anotación preventiva indicando, con carácter general, que "Como medida para proteger la intimidad de los menores de edad y reiterando decisiones similares adoptadas por la Corte Constitucional, la Sala ha decidido suprimir de esta providencia y de toda futura publicación relacionada con esta acción, el nombre real del joven a cuyo favor se interpuso la presente acción, así como de sus familiares y el de la institución educativa (Sentencia T365/14, de 11 de junio de 2014).

Doctrina de la Corte IDH sobre publicidad de sentencias y antecedentes penales

Sobre la justicia juvenil también ha tenido ocasión de pronunciarse sobre diferentes aspectos la Corte IDH. En relación concreta con la publicidad y el respeto a la vida privada de los menores implicados, la Corte ha señalado que el principio de publicidad del proceso (garantizado por el art. 8.5 CADH) puede verse limitado en los casos en los que intervengan menores, en tanto que dicho límite atiende "al interés superior del niño, en la medida en que lo preservan de apreciaciones, juicios o estigmatizaciones que pueden gravitar sobre su

[66] Las citadas Reglas tienen su origen en las Recomendaciones adoptadas en el *Seminario sobre Internet y el Sistema Judicial*, que tuvo lugar en el seno del Instituto de Investigaciones para la Justicia, los días 8 y 9 de julio de 2003. Disponible *on line*: http://www.iijusticia.org/heredia/Reglas_de_Heredia.htm.

vida futura" (Opinión Consultiva OC-17/02, de la Corte IDH, de 28 de agosto de 2002, sobre la *Condición Jurídica y los Derechos humanos del niño*, Apdo. 134).

Por otro lado, en relación con la inscripción y conservación de datos personales de menores en Registros de Antecedentes Penales o Delictivos, la Corte IDH se ha pronunciado manifestando que "los registros de menores delincuentes serán de carácter estrictamente confidencial y no podrán ser consultados por terceros, excepto por las personas que participen directamente en la investigación y resolución del caso" (Caso *Instituto de Reeducación del Menor contra Paraguay*, de 2 de septiembre de 2004 (Excepciones preliminares, Fondo, Reparaciones y Costas), Apdo. 211). Se deben cumplir, por lo tanto, los criterios generales indicados en las Directrices de armonización en lo relacionado con la seguridad y confidencialidad de los datos personales y con el requisito del consentimiento para su comunicación o publicación.

2.4. Datos de los menores en Internet

Recomendaciones del Memorándum de Montevideo sobre datos de menores en Internet

Como ya ha quedado dicho, en el sistema interamericano existe un instrumento específico que regula el tratamiento de datos personales de los menores en Internet: el *Memorándum de Montevideo*. Este instrumento, aunque no es vinculante, recoge las recomendaciones sobre el tratamiento de datos de los menores en Internet, con la peculiaridad de que no sólo busca la protección del menor en el entorno on line, sino que tiene como fundamento la protección del menor basándose en la CDN y en la garantía del principio del interés superior del menor.

En este terreno, ya ha quedado también señalado la necesidad del "consentimiento explícito de la persona concernida" para el tratamiento de sus datos personales (Pto. 19). Más allá de esta previsión general, el propio Memorándum indica a los proveedores de servicios de acceso a Internet, aplicaciones móviles o redes sociales, en el caso concreto de que los usuarios sean menores de edad, que si bien no contemplan una prohibición de tratamiento –lo cual se recomienda–, deberían pensar incluir, con la adecuada información, mecanismos de control parentales de acuerdo a la legislación de cada país (Pto. 19). Reiteramos aquí lo ya indicado para el caso de la indexación de perfiles de usuarios de redes sociales analizado por el Memorándum de Montevideo (Pto. 25), la necesidad de sus consentimiento y la diferencia entre menores y adolescentes, teniéndose en cuenta, por lo tanto, el grado de madurez del menor.

Los principios recogidos en el Memorándum han sido tomados como un referente por algunos Estados latinoamericanos como ha sido, por ejemplo, el caso de México o de Colombia. En este último país, su Corte Constitucional, al hilo de analizar un caso de una menor de 4 años cuyas imágenes aparecían en *Facebook*, indica que los peligros de las redes sociales no implican que "los menores no puedan acceder a la Sociedad del Conocimiento y la Tecnología, pero para

ello se deben atender las recomendaciones del Memorándum de Montevideo, en lo referente a que tal acceso debe ser paulatino, acompañado de las personas encargadas de su cuidado y acorde a la madurez y desarrollo sicológico que presenten" (Sentencia T-260/12, de 29 de marzo de 2012). Asimismo, también hace referencia a la CDN y al interés superior del menor que debe prevalecer en todo caso (art. 3.1).

Sobre los peligros de la Red para los más jóvenes, el propio Memorándum de Montevideo establece las pautas para evitar que las imágenes de menores puedan ser utilizadas con fines ilícitos como el acoso o la pornografía infantil (Pto. 3.3). La preocupación por evitar el uso de imágenes de menores sin su consentimiento ni el de sus padres con fines ilícitos es una preocupación constante en el sector iberoamericano que, como este problema, va en aumento. Esto ha llevado a los Estados latinoamericanos a comprometerse a erradicar todo tipo de violencia que afecte a los niños, y entre ellas, la distribución de pornografía infantil[67]. Se protegen así las imágenes de los menores frente al uso ilícito de las mismas. Con el fin de combatir los citados usos ilícitos y crear sistemas de intercambio de información seguros y que las bases de datos utilizadas, así como las aplicaciones cumplan con los estándares de privacidad exigidos por las *Directrices de armonización*, se insta a los Estados a crear estrategias comunes. Desde la Conferencia Iberoamericana de Ministras, Ministros y Altos Responsables de la Niñez y la Adolescencia se acordó en esta línea "Establecer estrategias conjuntas para el desarrollo de tecnología adecuada que permita identificar los sitios de distribución, consumo y difusión de pornografía que utiliza a personas menores de edad a fin de facilitar su filtración, la investigación y la identificación de los responsables"[68].

Por último, sobre las medidas de seguridad a seguir para el tratamiento de datos personales el Memorándum de Montevideo las considera necesarias en relación con las redes sociales y con la información contenida en las mismas. Indica, expresamente, que con el fin de que las bases de datos que se creen sean seguras y se garantice la privacidad de los usuarios, "los terceros que desarrollan las diferentes aplicaciones que el servicio ofrece (juegos, cuestionarios, anuncios, entre otros)" sólo podrán acceder a los datos personales de los usuarios cuando éstos sean necesarios y pertinentes para el funcionamiento de dichas aplicaciones. Se dispone que "La red social tiene que asegurar que los terceros que desarrollan aplicaciones en sus plataformas úni-

---

[67] VI Conferencia Iberoamericana de Ministras, Ministros y Altos Responsables de la Niñez y la Adolescencia, "Declaración de San José", de 18 y 19 de Octubre, 2004, "Por la Protección Integral de la Niñez y la Adolescencia ante la Violencia, la Trata, el Tráfico y la Explotación en Cualquiera de sus Manifestaciones". Disponible *on line*: http://white.lim.ilo.org/ipec//documentos/declaracion_san_jose_vi_iberoamericana_infancia_octubre_2004.pdf. Sobre este tema, vid., también, el trabajo elaborado por el IIN sobre "Explotacion Sexual Comercial de Niños, Niñas y Adolescentes e Internet", febrero 2011. Disponible *on line*: http://iin.oea.org/pdf-iin/Explotacion-sexual-comercial-version-digital.pdf.

[68] VI Conferencia Iberoamericana de Ministras, Ministros y Altos Responsables de la Niñez y la Adolescencia, Compromiso nº 9.

camente podrán acceder a los datos personales de los usuarios con el consentimiento expreso de estos. La red social digital debe asegurarse que los terceros desarrolladores soliciten únicamente la información indispensable, pertinente y no excesiva para el uso de dicha aplicación" (Pto. 26).

2.5. Ejercicio por los menores de su derecho a la protección de datos

***Soft law* latinoamericano sobre ejercicio por los menores de sus derechos**

Las *Directrices de armonización* reconocen y aconsejan la garantía de las facultades del derecho a la protección de datos (acceder, rectificar, cancelar y oponerse al tratamiento de los datos personales) por parte de su titular (Pto. 5), refiriéndose, además, no sólo a las Directrices de la OCDE de 1980, sino también la normativa comunitaria. Se plantea aquí nuevamente la cuestión del ejercicio de estas facultades por parte del menor, siendo la regla general, a falta de un criterio específico en este nivel, la del consentimiento o ejercicio paterno.

El Memorándum de Montevideo en las Recomendaciones dirigidas a los Estados indica expresamente (aunque enfocado al tratamiento de datos personales en Internet) que "los Estados deben legislar el derecho que tienen las niñas, niños y adolescentes directamente o por medio de sus representantes legales, a solicitar el acceso a la información que sobre sí mismos se encuentra en bases de datos tanto públicas como privadas, a la rectificación o cancelación de dicha información cuando resulte procedente, así como a la oposición a su uso para cualquier fin" (Pto. 8). Asimismo, en relación con los derechos de acceso, rectificación y cancelación, el Memorándum de Montevideo señala que "Toda red social digital, sistema de comunicación o base de datos debería contar con formas de acceso a la información, rectificación y eliminación de datos personales, para usuarios o no usuarios, tomando en consideración las limitantes de la ley" (Pto. 24). Por este motivo, el Principio 3 de la *Declaración de Principios sobre Libertad de Expresión* adoptada por la CIDH establece que "[t]oda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla".

En lo relativo al derecho de acceso a la información personal, recordamos aquí que en la región latinoamericana este derecho se ha plasmado en el conocido como "*habeas data*", reconocido y desarrollado en la mayoría de los Estados de la región. En este contexto, la Asamblea General de la OEA ha resaltado "la creciente importancia de la privacidad y la protección de datos personales"[69].

[69] Resolución de la Asamblea General de la OEA, sobre el *Acceso a la información pública y protección de datos personales* (AG/RES. 2811 (XLIII-O/13)), de 6 de junio de 2013. Con carácter previo, vid. el documento elaborado por la Comisión de Asuntos Jurídicos y Políticos de la OEA sobre "Principios y Recomendaciones Preliminares sobre la Protección de Datos", de 17 de octubre de 2011 (OEA/Ser.G CP/CAJP-2921/10 rev.1 corr. 1).

Respecto a la obligación de informar y el derecho a ser informado por parte de quien trata los datos personales, el Memorándum de Montevideo señala con mención expresa de los menores de edad y las páginas web (lo que puede hacerse extensivo a cualquier otro tipo de tratamiento de datos personales que tenga por destinatarios a los menores de edad), que "las reglas sobre privacidad de las páginas web, servicios, aplicaciones, entre otros, deberían ser explícitas, sencillas y claras, explicadas en un lenguaje adecuado para niñas, niños y adolescentes" (Pto. 21).

3. ÁMBITO EUROPEO

3.1. Marco normativo

Normas específicas en Europa sobre datos de menores; el SEPD

En relación con el tratamiento de datos personales a nivel europeo, a diferencia de lo que ocurre a nivel internacional y en el sistema interamericano, nos encontramos no sólo con normas vinculantes que reconocen y regulan de forma expresa el derecho fundamental a la protección de datos personales y el tratamiento de dichos datos, sino que, en las mismas, existen referencias expresas al tratamiento de datos de los menores de edad. Por contrapartida, aunque en Europa también se van a proteger los derechos de los menores de edad y existen varios organismos encargados de su defensa, no existe un organismo específico como tal encargado de la protección de los niños, aunque sí que existe para la garantía y control del derecho a la protección de datos: las conocidas Autoridades de Control o Autoridades de Protección de Datos, que en el caso de Europa se centra en la figura del Supervisor Europeo de Protección de Datos (SEPD)[70].

Convenios, Resoluciones y Recomendaciones del Consejo de Europa

A nivel regional europeo, el Consejo de Europa, además del Convenio Europeo de Derechos Humanos (1950, CEDH)[71], que garantiza los derechos en él recogidos a "toda persona" que se encuentre bajo la jurisdicción de un Estado miembro (y que reconoce en su artículo 8 el derecho a la protección de datos personales como un ámbito garantizado por el derecho a la vida privada)[72], nos encontramos, además, una norma específica que regula el tratamiento de los datos personales: el Convenio nº 108, de 1981[73], y su Protocolo adicional

[70] Sobre el SEPD, su web: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS?lang=es.

[71] Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, aprobado en Roma, el 4 de noviembre de 1950. Disponible *on line*: http://www.echr.coe.int/Documents/Convention_SPA.pdf.

[72] Será a partir del caso *Leander*, de 26 de marzo de 1987, cuando el TEDH afirme ya expresamente y con toda claridad que existe un derecho a la protección de datos personales como parte del derecho a la vida privada reconocido por el artículo 8 del CEDH. Y en el mismo sentido, también relevante, la STEDH *M.S. contra Suecia*, de 27 de agosto de 1997.

[73] Convenio nº 108, del Consejo de Europa, de 28 de enero de 1981, para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Disponible *on line*: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.

(1981)[74]. En este marco regional no podemos olvidar que antes de la aprobación del citado Convenio nº 108, en el Consejo de Europa con el fin de garantizar la vida privada frente a los peligros derivados del tratamiento de los datos personales se aprobaron la Resolución (73) 22, de 26 de septiembre de 1973, sobre la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado[75]; y la Resolución (74) 29, de 20 de septiembre de 1974, sobre la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público[76]. Estas Resoluciones son los primeros textos europeos en los que se recogen los principios básicos de todo tratamiento de datos personales y, a pesar del margen de actuación concedido a los Estados, imponen pautas estrictas de conducta en materia de protección de datos personales, pero no se recoge referencia alguna para el caso de que los datos personales pertenecieran a menores de edad.

No obstante, la propuesta de modernización del Convenio 108 recoge una referencia expresa al tratamiento de datos de los menores, indicándose que las Autoridades de Protección de Datos deberán prestar especial atención al tratamiento de datos de los menores y de los grupos vulnerables, aunque se pierde la oportunidad de introducirlo expresamente como sujeto titular de los datos personales[77].

Como complemento de esta normativa general en materia de tratamiento de datos personales, el Comité de Ministros del Consejo de Europa ha elaborado numerosas Recomendaciones para normalizar la protección de datos personales en sectores que requieren una regulación específica, tales como el sector médico, el estadístico, el de investigación científica, el de *marketing* o el de Seguridad Social, pero ninguna específica dirigida al tratamiento de datos de los menores de edad[78]. Asimismo, debemos señalar que, salvo contadas excepciones, ninguna de dichas Recomendaciones contiene referencia expresa a los casos en los que los datos tratados pertenezcan a menores de edad.

Más allá de estas Recomendaciones, en el seno del Consejo de Europa se han aprobado dos Convenios que, al hilo de ir destinados a proteger a los menores, han tocado de forma tangencial la cuestión relativa al tratamiento de sus datos personales en el marco de la regu-

---

Vid., también, su Memoria Explicativa: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434.

[74] Protocolo Adicional al Convenio nº 108, en relación con las autoridades de contol y el flujo transfronterizo de datos personales, de 8 de noviembre de 2001. Entrada en vigor el 1 de julio de 2004. Disponible *on line* en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680080626.

[75] Resolución 73 (22). Disponible *on line* en: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=589402&SecMode=1&DocId=646994&Usage=2.

[76] Resolución 74 (29). Disponible *on line* en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=-09000016804d1c51.

[77] Sobre la citada propuesta de reforma consolidada (septiembre, 2016), vid: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a616c, art. 12bis.2.e).

[78] Para más información sobre dichos instrumentos legales, vid. http://www.coe.int/en/web/data-protection/legal-instruments.

lación que ofrecen. Nos referimos al *Convenio para la Protección de los Niños frente a la Explotación y los Abusos Sexuales* (2007), conocido como "*Convenio de Lanzarote*"[79], y al *Convenio sobre Ciberdelincuencia* (2001), también denominado *Convenio sobre el Cibercrimen*[80]. El Convenio de Lanzarote destaca porque recoge por primera vez el delito de acoso sexual a través de la Red o *cibergrooming* (art. 23). Asimismo, con el fin de proteger y combatir la explotación y el abuso sexual de los niños se establece un sistema de recogida de datos, manifestándose en todo caso el "*debido respeto a las exigencias de protección de los datos de carácter personal*" (art. 10.2. b). El Convenio sobre el Cibercrimen se centra en la prevención de actos delictivos contra la integridad, confidencialidad y disponibilidad de sistemas y redes de información, prestando especial atención a las formas de delincuencia informática cuando las mismas tienen por objeto la pornografía infantil (art. 9).

La CDF de la Unión Europea

Centrándonos ya en el terreno comunitario, la Unión Europea reconoce en su Carta de Derechos Fundamentales (CDFUE)[81], los derechos del niño, indicándose expresamente que en cualquier actividad que estén involucrados menores, tanto poderes públicos como sector privado deberán tener en cuenta que "el interés superior del niño constituirá una consideración primordial" (art. 24). Asimismo, la CDFUE reconoce de forma expresa un derecho fundamental a la protección de datos personales (art. 8), siendo su titular "toda persona", por lo que debemos entender incluidos a los menores como titulares del citado derecho. La CDFUE, a diferencia de otras Declaraciones de derechos fundamentales, reconoce de forma diferenciada y como derechos autónomos, el derecho a la protección de datos personales y el derecho a la vida privada (art. 7), garantizado igualmente a "toda persona". Asimismo, en Europa, tomando como referente la CDN, con las peculiaridades que la niñez tiene en Europa, en el año 1992 el Parlamento Europeo aprobó la Carta Europea de los Derechos del Niño, que reproduce básicamente los derechos reconocidos a nivel internacional a los menores y adolescentes[82].

La Directiva 95/46/CE

Al margen de estas normas, la norma jurídica por excelencia que va a regular el tratamiento de datos personales a nivel comunitario es la conocida Directiva 95/46/CE sobre Protección de Datos[83]. A pesar

---

[79] Convenio de Lanzarote, de 25 de octubre de 2007. Texto disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680084822.

[80] Convenio sobre Ciberdelincuencia, de 23 de noviembre de 2001. Texto disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c.

[81] Carta de Derechos Fundamentales de la Unión Europea (2016/C 202/02). Disponible *on line*: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12016P/TXT&from=ES.

[82] Resolución del Parlamento Europeo A3-0172/92, de 8 de julio de 1992, sobre una *Carta Europea de los Derechos del Niño* (DOCE C 241, de 21 de septiembre de 1992).

[83] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible *on line*: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML.

de ello, la Directiva no recoge una mención expresa del tratamiento de datos de los menores de edad, sino que se refiere directamente a cualquier persona física, entendiéndose incluidos, por lo tanto, a los menores de edad. El resto de Directivas aprobadas en este terreno no son una excepción. Se encargan de regular el tratamiento de datos personales en diferentes sectores, como puede ser el de las comunicaciones electrónicas, pero no se refieren de forma expresa a los menores de edad[84]. Lo mismo sucede con el Reglamento 45/2001 sobre Protección de Datos Personales por parte de las instituciones y órganos comunitarios, que dio origen al ya mencionado Supervisor Europeo de Protección de Datos (SEPD). No obstante, como sucedía en el Consejo de Europa, de forma tangencial a la hora de proteger a los menores frente al abuso y la pornografía infantil, se ha regulado por primera vez a nivel comunitario, mediante una Directiva, el delito de *grooming*, protegiéndose así los datos de los menores, sus imágenes, de fines ilícitos[85].

Grupos de Trabajo en la Unión Europea

Además de los instrumentos de garantía de los derechos humanos y fundamentales reconocidos en el CEDH o en la CDFUE, y de las específicas Autoridades administrativas en materia de protección de datos, existen en la Unión Europea dos grupos de trabajo que van a ser un referente en la materia a la hora de interpretar y configurar el derecho a la protección de datos personales. Nos referimos al denominado "Grupo de Berlín" (*International Working Group on Data Protection in Telecommunications*, IWGDPT)[86] y al Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE, conocido como "G29"[87]. En ambos casos se han enfrentado al tema del tratamiento de datos de los menores de una forma directa a través de diferentes trabajos.

Últimas reformas normativas en la UE: Directiva 2016/680 y Reglamento 2016/679

Por último, a nivel comunitario, debemos señalar que a pesar del esfuerzo por parte de las instituciones comunitarias en reconocer derechos fundamentales y en proteger la vida privada y garantizar el poder de disposición sobre los datos personales, el avance de las nuevas tecnologías ha provocado la obsolescencia de la normativa vigente y, con ella, la aprobación de una nueva regulación comunitaria del tratamiento de datos personales. Fruto de un largo proceso de reforma normativa en este terreno se aprobaron la Directiva (UE) 2016/680, relativa al tratamiento de datos personales con fines de

---

[84] Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Disponible *on line*: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF.

[85] Directiva 2011/92/UE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo. Disponible *on line* en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32011L0093&from=EN.

[86] Más sobre el Grupo de Berlin: https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt.

[87] Sobre el G29, vid.: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

prevención e investigación de sanciones penales[88]; y el Reglamento (UE) 2016/679, conocido como "Reglamento General de Protección de Datos" (RGPD)[89]. Será este último el que sustituya a la actual Directiva 95/46/CE a partir de mayo de 2018. A pesar de que el RGPD todavía no es aplicable, es una norma aprobada y que está en vigor por lo que resulta relevante para analizar la visión de futuro que ofrece a los problemas actuales, sobre todo porque en el mismo sí que se recoge una mención expresa al tratamiento de datos personales de los menores de edad.

Normas sobre menores en el Reglamento General de Protección de Datos

Aunque el RGPD menciona a los menores por la preocupación de que se vean afectados por fines de mercadotecnia o de elaboración de perfiles de personalidad o de usuario, entendemos que muchas de sus previsiones generales se podrán hacer extensivas a los menores de edad en tanto que el RGPD considera que "los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales" (Considerando 38). Con el fin de conseguir dicha protección específica para los menores, el Reglamento comunitario aconseja, por un lado, la elaboración de Códigos de conducta, entre otras causas, para especificar la aplicación de la normativa comunitaria cuando ésta tiene como destinatarios a los menores, especialmente cuando lo que se quiera aclarar y desarrollar sean cuestiones relativas a la "información proporcionada a los niños y la protección de éstos" y la "manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño" (Art. 40.2. g) RGPD).

Por otro lado, el RGPD prohíbe (por las consecuencias negativas que para el futuro desarrollo del menor y su dignidad pueda tener) la utilización de los datos personales de los menores para la elaboración de sus perfiles con el fin de tomar decisiones sobre el mismo o de predecir "sus preferencias personales, comportamientos y actitudes" (Considerandos 24, 30 y 71 y art. 22 RGPD). Esta prohibición de elaborar perfiles será recogida también por la citada Directiva (UE) 216/680 en relación con fines de prevención de delitos y su investigación (Considerando 51).

---

[88] Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Disponible *on line* en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0680&from=EN.

[89] Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). Disponible *on line* en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

3.2. El consentimiento del menor para el tratamiento de sus datos personales

El consentimiento en la normativa de la UE

A pesar de que el consentimiento a nivel europeo no se menciona de forma expresa en el Convenio nº 108 del Consejo de Europa (cuestión subsanada en su proceso de reforma), su necesidad para el tratamiento de los datos personales se extrae del requisito de legitimidad del mismo. Así lo recogen expresamente a nivel comunitario tanto la Directiva 95/46/CE como el RGPD. En todo caso, deberá ser prestado por sus titulares, o como indica el citado Convenio, por los "sujetos concernidos" (art. 2 a); o por el "interesado" (art. 2 a) y h), como dice la normativa comunitaria. Estas definiciones debemos hacerlas extensivas al caso de los menores de edad.

Una novedad que incluye el Reglamento comunitario, con carácter general, para todos los tratamientos de datos personales (por lo que lo hacemos extensivo para el caso de los menores de edad), es el hecho de que ya no se admite un consentimiento tácito para el tratamiento de los datos, esto es, el consentimiento para que se traten nuestros datos personales deberá ser un consentimiento expreso "que debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen" (Considerando 32 y Art. 11 RGPD).

El consentimiento en el G29

Sobre el requisito del consentimiento de los menores, el G29 concluye que siendo conscientes de que "las condiciones de validez de su consentimiento difieren de un Estado miembro a otro", dado que o bien se requiere el consentimiento del menor y su representante, o sólo se requiere el del menor si ha alcanzado cierta madurez, se evidencia la necesidad de un procedimiento que armonice la verificación de la edad y la madurez del menor. El problema en este punto es, por lo tanto, que no hay una edad de madurez para consentir al tratamiento de datos personales que se encuentre reflejada por ninguna norma (y la misma puede variar de un Estado a otro); y, por otro lado, que no existe ningún mecanismo de comprobación de la edad del menor. La cuestión es, además, como el propio G29 observó, que es un tema que entra dentro del ámbito de la regulación de Derecho civil de cada uno de los Estados[90].

Verificación de la edad en el RGPD

Debemos señalar aquí que el tema de la verificación de la edad no es una cuestión baladí, especialmente en determinadas situaciones, como en el caso de la inmigración irregular o en casos de trata de menores y abusos sexuales. La nueva normativa europea en protección de datos personales, esto es, el RGPD, refiriéndose de forma expresa al consentimiento de los menores en los casos que se traten sus datos personales requerirá que en caso de duda sobre la edad del titular de los datos tratados, se compruebe que el sujeto cumple con el requisito de la mayoría de edad exigido correspondientemente. La

[90] Dictamen 15/2011, del G29, sobre la definición del consentimiento, adoptado el 13 de julio de 2011 (WP 187) (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_es.pdf), Apdo. III.A.4.

comprobación la deberá realizar el sujeto que trate los datos personales y deberá realizar todos los "esfuerzos razonables para conseguir un consentimiento verificable, teniendo en cuenta la tecnología disponible" (art. 8.2 RGPD).

Madurez e interés superior del niño

La cuestión se complica si, además, tenemos en cuenta que no podemos olvidar el derecho del niño al desarrollo personal reconocido por Tratados Internacionales y Europeos, lo que hace necesario tener en cuenta su grado de madurez. Por lo tanto, en relación con el requisito del consentimiento a la hora de tratar sus datos personales, serán las legislaciones nacionales las que decidan si el menor tiene el grado de madurez necesario para consentir que se traten sus datos personales y no requiere el consentimiento paterno. Así las cosas, el G29 también ha dejado señalado que "cuando el tratamiento de los datos de un niño haya requerido el consentimiento de su representante legal, al alcanzar la mayoría de edad el niño podrá retirar su consentimiento. Pero si desea que continúe el tratamiento de sus datos, parece que el interesado deberá dar su consentimiento expreso siempre que se le requiera"[91].

En cualquier caso, en este terreno debe primar, como en todo lo relacionado con los derechos de los menores de edad, el principio del interés superior del niño, incluso en aquellos casos en los que se exima legalmente del requisito del consentimiento. Así por ejemplo, con expresa referencia a los menores, el Reglamento comunitario indica que el sujeto que trate datos personales lo podrá hacer sin consentimiento del titular de los datos si es necesario para satisfacer un interés legítimo, salvo que se lesionen derechos fundamentales de dichos titulares, especialmente menores (art. 6.1 f) RGPD).

Se busca proteger al menor ante todo. Y así, aunque no podemos olvidar el tema de la representación legal del mismo, si se llegara a demostrar (y el menor, por su grado de madurez, pudiera demostrar) que el consentimiento prestado en su nombre por los sujetos que le representan le causa un perjuicio, se considera que en estos supuestos los menores "deberían tener derecho a ser oídos por las autoridades competentes, incluidas las autoridades de protección de datos"[92]. Por este motivo, el RGPD comunitario añade que "el consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños" (Considerando 38 RGPD). El problema en esta materia es que habrá que estar a lo que dispongan los diferentes ordenamientos jurídicos nacionales sobre la edad a la que se adquiere ese grado de madurez, cuestión (reiteramos) no recogida en ninguna de las normas de referencia en materia de protección de datos, estando sujeta, además, a la legislación civil correspondiente.

Pronunciamientos del Grupo de Berlín y del SEPD

En relación con la cuestión del consentimiento cuando el mismo es prestado por los menores en Internet destaca el trabajo del Grupo

[91] Dictamen 2/2009, del G29, sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas), emitido el 11 de febrero de 2009 (WP 160). Disponible *on line*: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp160_es.pdf.

[92] Dictamen 2/2009, del G29.

de Berlín sobre "La privacidad de los menores en Internet: el papel del consentimiento parental". A diferencia de lo dispuesto por la CDN respecto de la consideración de menor al sujeto que tenga menos de 18 años, el Grupo de Berlín considera que es menor el sujeto por debajo de la edad de 16 años. En este Documento el Grupo de Berlín, entre otras cuestiones, viene a concluir que el consentimiento de los padres sólo debe plantearse cuando sea necesario proteger el interés superior del menor, recomendando que el mismo se solicite cuando se vaya a producir la recogida de datos personales del menor, se revelen sus datos a terceros o con otros fines distintos de para los que fueron recogidos (como podría ser el caso del marketing), o bien cuando los datos se vayan a publicar en Internet[93].

Sobre el tratamiento de datos personales de menores en Internet también se pronunció el SEPD[94], entendiendo que la protección de datos de los menores era una cuestión ligada a su seguridad y que esto debería venir vinculado a los sistemas de bloqueo o control parental, avisando de los peligros que para el ejercicio de los derechos de los menores se podrían producir. En este punto, "el SEPD recuerda que en principio no deben ser los proveedores de servicios quienes efectúen dicho control, y ciertamente no de una forma sistemática", a lo que añade que si bien se deben utilizar con prudencia dichas tecnologías de bloqueo, se debe respetar la intimidad de los usuarios, aunque añade, por otro lado, que "los filtros serían inicializados por los padres y podrían desactivarse, de forma que el adulto conserva el pleno control del efecto de filtrado".

Problemática del *sexting*

Para finalizar debemos señalar que la aparición (y en aumento) del fenómeno conocido como *sexting*, esto es, el intercambio a través de móviles y otros dispositivos electrónicos de imágenes o vídeos de contenido sexual, donde son los propios menores los que, por regla general, de forma voluntaria comparten dicha información personal, vuelve a plantear la cuestión del consentimiento del menor y del control parental, así como la necesidad de una legislación que regule el tema de manera global. La cuestión es que esta práctica está experimentando un constante aumento y que, al margen de cuando se pueda considerar un delito o una falta (por realizarse sin el correspondiente consentimiento del titular de los datos y en función del grado de connotación sexual de la imagen o vídeo), este tipo de actividades puede generar en otras más graves como el *ciberbullying*, el *ciberacoso sexual* o la llamada *sextorsión*, sin perder de vista las consecuencias que para el desarrollo personal del menor puede tener la existencia de una imagen cuyo borrado puede ser difícil (por no decir imposible) de

[93] Documento de trabajo, adoptado en el 31º Encuentro del Grupo, celebrado en Auckland (Nueva Zelanda", el 26 y 27 de marzo de 2002. Disponible *on line* en: https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group.

[94] Dictamen del SEPD, de 23 de junio de 2008, sobre la propuesta de Decisión del Parlamento Europeo y del Consejo por la que se establece un programa comunitario plurianual sobre la protección de la infancia en el uso de Internet y de otras tecnologías de la comunicación. Disponible *on line*: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:002:0002:0006:Es:PDF.

Bases de Datos inscritas en el Registro Nacional

conseguir. El mencionado Convenio de Lanzarote del Consejo de Europa indica que los Estados deberán adoptar las medidas legislativas correspondientes para tipificar como delito la conducta intencionada de producir pornografía infantil (art. 20.1 a). No es una cuestión sencilla y serán los Estados los que tengan la última palabra.

En conclusión, la falta de armonización a nivel europeo y el margen dejado a los diferentes Estados genera inseguridad jurídica. Sería conveniente establecer un límite de edad y de "madurez", así como los criterios y el procedimiento para determinarla con el fin de legitimar el consentimiento prestado exclusivamente por el menor para el tratamiento de sus datos personales.

3.3. Ámbitos problemáticos

a) En las relaciones familiares

Doctrina del TEDH y pronunciamientos del G29

En los instrumentos europeos sobre los derechos del niño, como la Carta Europea de los Derechos del Niño, se reproducen básicamente las previsiones de la CDN en relación con los orígenes del niño y su derecho a conocer su información personal sobre este tema, pero se deja un amplio margen de actuación a los Estados. El TEDH ha tenido ocasión de pronunciarse en diversas ocasiones sobre este tema, y ha venido manteniendo la necesidad de hacer primar el interés superior del menor a conocer la información relativa a su nacimiento y sus orígenes con el fin de procurarle un adecuado desarrollo personal (asunto *Mikulic contra Croacia*, de 7 de febrero de 2002). Así lo ha mantenido incluso en asuntos en los que la madre había solicitado expresamente permanecer en el anonimato (Citamos aquí por ser los más relevantes, los asuntos Odièvre contra Francia, de 13 de febrero de 2003; y Godelli contra Italia, de 25 de septiembre de 2012.). Se produce un conflicto de derechos donde el TEDH hace primar el interés superior del menor.

Por otro lado, en relación con la obligación de inscribir en el registro el nacimiento de los niños, en íntima conexión con su derecho a una vida privada y desarrollo personal y a obtener una identidad, el TEDH ha dado un giro en sus pronunciamientos y lo ha reflejado en el asunto *Paradiso y Campanelli contra Italia*. En este caso, el TEDH aunque inicialmente (en su Sentencia de 27 de enero de 2015) concluyó el derecho del menor, concebido por gestación subrogada, a ser inscrito, en atención al interés superior del mismo y a no privársele de una identidad, en Gran Sala (Sentencia de 24 de enero de 2017) el TEDH se pronunció negando la inscripción del menor y dejando caer el tema en el margen de apreciación que tienen los Estados para regular las relaciones paterno-filiales.

Otra cuestión relacionada con el tratamiento de los datos personales del menor por parte de la familia surge a la hora de valorar el grado o nivel de las medidas de control parental que los padres pueden ejercer sobre los datos personales de los menores. Una de las medidas que se ha planteado ha sido el uso de dispositivos de geolo-

calización aplicados a los menores. Aquí el G29 considera que si bien se requiere el consentimiento parental para este tipo de aplicaciones o dispositivos, "hay que evitar en todo caso que, por motivos de seguridad, los niños sean sometidos a una vigilancia excesiva que limite su autonomía. En este contexto, hay que alcanzar un equilibrio entre la protección de la intimidad y la vida privada de los niños y su seguridad"[95].

También dentro del entorno familiar se plantea la grabación de imágenes de los menores y la necesidad o no de su consentimiento. En el TEDH se discutió el caso de una menor de 14 años que había sido grabada por su padrastro estando ella desnuda. En este caso el TEDH consideró que el permiso existente en la legislación sueca de grabar a un sujeto sin necesidad de su consentimiento y la ausencia de un mecanismo de protección contra el caso de ser grabado, máxime cuando podían darse responsabilidades civiles o criminales, lesionaba la vida privada de la demandante, especialmente cuando ésta era una menor y había sido grabada en su domicilio y en su entorno familiar bajo una expectativa de privacidad (STEDH de 12 de noviembre de 2013, asunto *Söderman contra Suecia*). Se deriva, por tanto, la conclusión de que al margen de cuestiones delictivas, la toma de fotografías de un menor en el entorno familiar cae dentro de su "expectativa de privacidad" y de la voluntad paterna. De ahí que haya que extremar el cuidado con la publicación y difusión de las mismas, teniendo en cuenta la voluntad del menor en conexión con su grado de madurez.

Por otro lado, a nivel europeo, también resulta interesante la cuestión de los menores extranjeros no acompañados que viajan a otros países de manera ilegal o que son objeto de tráfico y explotación sexual o de pornografía infantil, planteándose el problema de la determinación de su edad. No obstante, se les aplicarán los principios generales en la materia ya que el RGPD, que no hace distinción entre si los "interesados" o titulares de los datos están en una situación legal o jurídica en Europa.

b) En el terreno escolar

Directrices del G29 sobre datos y colegios

En este terreno destaca el trabajo elaborado por el G29 sobre *La protección de datos personales de los niños (Directrices generales y el caso especial de los colegios)*[96]. En este ámbito son los profesores y los miembros del centro docente los responsables del tratamiento de datos de los menores y, aquí, como señala el G29, debe regir el principio del interés superior del menor. Dicho principio deberá regir para valorar la situación del menor y los tratamientos de datos que se realicen,

[95] Dictamen 13/2011, del G29, sobre los servicios de geolocalización en los dispositivos móviles inteligentes, adoptado el 16 de mayo de 2011 (WP 185) (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_es.pdf), con referencia expresa al Dictamen 2/2009 del G29. Con carácter previo al Dictamen 13/2011, el G29 se pronunció en su Dictamen 5/2005, sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido, adoptado el 25 de noviembre de 2005 (WP 115).

[96] Dictamen 2/2009, del G29.

especialmente en el caso del intercambio o comunicación de los mismos. En este sentido, el G29 considera que hay que extremar el cuidado y, en atención al principio de finalidad del tratamiento, habría que tener en cuenta el principio de proporcionalidad. Esto es, se podrán tratar datos personales de menores en función de que la finalidad perseguida sea legítima y proporcionada como, por ejemplo, el caso de la instalación de cámaras en centro docentes con motivos de seguridad. Para el caso de los circuitos cerrados de televisión deberemos tener en cuenta que "hay que evitar en todo caso que, por motivos de seguridad, los niños sean sometidos a una vigilancia excesiva que limite su autonomía. En este contexto, hay que alcanzar un equilibrio entre la protección de la intimidad y la vida privada de los niños y su seguridad"[97].

Así las cosas, a la hora de recoger información de los menores para elaborar sus expedientes escolares y para la necesaria gestión de su vida en el centro, como puede ser también en el caso de los comedores escolares o de la participación en determinados cursos o actividades, habrá que tener en cuenta que el tratamiento de la información del menor deberá regirse por el citado principio del interés superior del menor y en función de la finalidad para la que los datos son utilizados, sin que su utilización pueda provocar una situación de discriminación del menor. Esto es, información sobre el menor como pueden ser sus creencias religiosas o los ingresos económicos de sus padres se deberán utilizar con la estricta finalidad de la gestión administrativa del centro y del desarrollo de sus actividades en el mismo, y en ningún caso con otra finalidad, máxime si ésta atenta contra la dignidad del menor.

Los mismos principios deben regir a la hora de comunicar datos o acceder a los datos que el centro escolar tenga sobre el menor. El acceso a la información del menor se podrá hacer por el mismo o por sus representantes legales –lo que consiste en el ejercicio de sus derecho de acceso–, pero en ciertas ocasiones será necesario que terceros sujetos accedan a dicha información si la finalidad es legítima, no es incompatible con la finalidad para la que fueron recogidos, y se busca proteger al menor. Este es el caso, por ejemplo, de los procedimientos disciplinarios, un tratamiento médico en el centro o, una adaptación o educación especial por cuestiones de salud. Esto es, en relación con la comunicación de la información titularidad de los menores, habrá que estar a los principios citados anteriormente, especialmente para el caso de las publicaciones en Internet, o por cualquier otro medio, de sus imágenes. En este caso concreto, cumpliendo estrictamente con los principios generales en materia de protección de datos, teniendo en cuenta la proporcionalidad y la finalidad del tratamiento, la regla general será que "en el caso de fotografías colectivas de, por ejemplo, acontecimientos escolares, y de conformidad con la legislación nacional, las escuelas no estarán obligadas a obtener el consentimiento escrito de las padres cuando las fotografías no permitan identificar fácilmente a los alumnos. No obstante, en tales casos las escuelas deberán informar a los niños, los padres y los repre-

[97] Dictamen 2/2009, del G29.

sentantes escolares, de que se va a tomar la fotografía y para qué fines se utilizará"[98].

Obligaciones de sensibilización en el RGPD

Por último, el RGPD impone a la Autoridad de control correspondiente llevar a cabo campañas de sensibilización sobre el tratamiento de datos personales, que deberán ser objeto de especial atención cuando vayan dirigidas a los niños (Art. 57.1 b) RGPD). Se insiste en la educación del menor en el respeto a su privacidad y a la de terceros, jugando la escuela un importante papel.

c) En el ámbito sanitario

Protección de datos médicos según el Consejo de Europa

En relación con los datos médicos y la necesidad del consentimiento expreso de su titular para su tratamiento, en el caso de los menores, la Carta Europea de los Derechos del Niño dispone que para los tratamientos médicos se requerirá el consentimiento de los padres. No obstante, cuando el menor alcance la mayoría de edad, será necesario que los responsables de los tratamientos, como pueden ser los centros médicos, requieran el consentimiento expreso del sujeto que ha dejado de ser menor de edad (Pto. 8.30). La idea sobre la que se sustenta esta disposición es que si el menor no tiene capacidad para decidir sobre un determinado tratamiento o acto médico, como puede ser una intervención, tampoco lo tendrá para que se traten los datos médicos derivados de dicha actuación.

Las normas que regulan el tratamiento de datos a nivel europeo se refieren a los datos médicos como datos sensibles o especialmente protegidos. El artículo 6 Convenio nº 108, hablando de las categorías particulares de datos se refiere tanto a los datos sanitarios como a los datos de condenas penales, aunque sin referencia expresa a cuando sus titulares sean menores de edad, y remitiendo a las legislaciones nacionales para que regulen su tratamiento. No obstante, en relación con los datos de salud, en el marco del Consejo de Europa se aprobó la Recomendación R (97) 5, de 13 de febrero de 1997, sobre la protección de los datos médicos y aquí sí que se refirió a los menores, concretamente equiparando los no nacidos a los menores. La Recomendación indicaba que en el caso de los niños no nacidos, la referencia a sus datos personales debería entenderse y deberían protegerse de la misma forma que se protegen los datos de los menores de edad, a menos que la legislación nacional dispusiera otra cosa, actuando el titular de las responsabilidades parentales como legalmente facultado respecto de los datos personales señalados (Pto. 4.5)[99].

Datos médicos en la Directiva 95/46 y en el G29

A nivel comunitario, la Directiva 95/46/CE recoge el tratamiento de los datos de salud en su art. 8, calificándolos como una "categoría especial" de datos personales que requerirán en todo caso el consentimiento expreso de su titular para poder ser tratados. Debemos entender pues que el tratamiento de los datos de salud de los menores de-

[98] Dictamen 2/2009, del G29.

[99] Vid. Recomendación en la dirección *on line*: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=-09000016804f0ed0.

berá contar con el consentimiento expreso de sus representantes o tutores legales. Aunque aquí, tal y como se hiciera por el Consejo de Europa, se remite a lo que disponga la legislación de cada Estado.

Prevención para una protección más eficaz

En este terreno, como con carácter general para todo tratamiento de datos personales, se debe cumplir con el principio de calidad de los datos, no debiendo utilizarse más datos de los necesarios para el tratamiento legítimo perseguido. Y del mismo modo se deberán extremar las medidas de seguridad de la información. Por ello, en un caso muy concreto del uso de datos biométrico, el G29 hizo referencia al hecho de que "deberá limitarse la recogida y el tratamiento de sus impresiones dactilares, y los límites de edad se adaptarán a los límites de edad vigentes en otras grandes bases de datos biométricos (como Eurodac)". Aquí, además, el G29 se refirió a una edad mínima para la recogida de huellas dactilares de los menores (nunca por debajo de 6 años y a partir de 14 años si la recogida de los datos se hacía a efectos identificativos)[100].

Como vemos, en todos los casos se hace una remisión a la legislación nacional, por lo que debemos entender que se deja en manos de cada Estado la edad en la que el menor podrá consentir por sí solo el tratamiento de sus datos médicos, cuestión que vendrá de la mano de su grado de madurez. En cualquier caso, en este ámbito también va a primar el principio del interés superior del menor. Por ello, se podrán ceder datos médicos de menores, por los propios centros médicos o por centros docentes o cualquier otra institución que se haga cargo del menor (incluso en aquéllos casos en los que exista un conflicto con los padres o representantes legales de los menores) si la finalidad es proteger al menor física o psicológicamente[101]. Así, por ejemplo, como medida de seguridad y garantía adicional que debe regir en todo tratamiento de datos personales, en el Convenio de Lanzarote se recoge la confidencialidad que debe rodear el proceso y a los sujetos que intervienen cuando se detecte un presunto abuso sexual durante una exploración médica (art. 12).

Doctrina del TEDH

En conexión con esta cuestión de quién puede acceder o a quién se le pueden comunicar datos relacionados con la salud de los menores, el TEDH también se ha pronunciado a la hora de ponderar entre el derecho de acceso por parte del titular de los datos a la información relativa a cuando era menor de edad y el deber de confidencialidad de los centros que tratan dicha información. En el asunto *Gaskin contra el Reino Unido*, de 7 de julio de 1989, el TEDH concluyó que debía primar la necesidad del sujeto de conocer sobre los hechos ocurridos

[100] Dictamen 3/2007, del G29, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica la Instrucción consular común dirigida a las misiones diplomáticas y oficinas consulares de carrera en relación con la introducción de datos biométricos, y se incluyen disposiciones sobre la organización de la recepción y la tramitación de las solicitudes de visado (COM (2006) 269 final), adoptado el 1 de marzo de 2007 (WP134). Disponible *on line*: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp134_es.pdf. Y en la misma línea, vid. el Dictamen 3/2012, del G29, sobre la evolución de las tecnologías biométricas, adoptado el 27 de abril de 2012 (WP 193). Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_es.pdf.

[101] Dictamen 2/2009, del G29.

durante su infancia sin que ello supusiera una lesión de la confidencialidad que debían mantener, en todo caso, los expedientes médicos o sociales.

d) En los medios de comunicación

Ponderación con la libertad de expresión en el Derecho de la UE

Uno de los principales conflictos con los que se encuentra el tratamiento de datos de los menores por los medios de comunicación es el hecho de que el derecho a la protección de datos del menor se haga valer frente a otros derechos fundamentales como son las libertades de expresión e información. La cuestión en este ámbito es el conflicto entre derechos y ver cuál debe prevalecer.

La Directiva 95/46/CE se refiere, concretamente, en su Considerando nº 17 y en su artículo 9 al tratamiento de datos personales con fines periodísticos. La regla general es que los principios que rigen el tratamiento de los datos relativos al sonido y a la imagen, especialmente en el sector audiovisual, se aplicarán de forma restringida, debiendo conciliarse ambos derechos. Estas previsiones generales se hacen extensivas a los menores de edad, aunque la Carta Europea de Derechos del Niño recoge la exigencia de que todo niño sea protegido "contra la utilización de su imagen de forma lesiva para su dignidad". Se deberá tener en cuenta, por lo tanto, el interés superior del menor (art. 24 CDFUE).

Por último, y de forma un tanto peculiar, sobre la información publicada o difundida por los medios de comunicación, con carácter general, aplicable por lo tanto a los datos de los menores, el Reglamento comunitario si bien indica que existe un derecho a la supresión de dicha información (el llamado derecho al olvido), máxime cuando la información se refiere a menores de edad, posteriormente se afirma que las limitaciones del derecho a la protección de datos no tendrán lugar cuando el tratamiento sea necesario para ejercer la libertad de expresión e información (Art. 17.3 a) RGPD). Se hace necesaria la estricta observación del caso concreto y del interés del menor afectado.

e) Como partes de una relación contractual

Remisión al Derecho interno

En este ámbito debemos diferenciar bien lo que es el consentimiento prestado por el menor para que traten sus datos personales y, otra muy diferente, el consentimiento de los mismos para obligarse contractualmente, lo que se debe ver sujeto a la normativa civil de cada Estado. Con esta idea se ha manifestado el RGPD al señalar expresamente en relación con el consentimiento prestado por los menores de edad, que al margen de la edad establecida para el tratamiento de datos de los menores y de que éstos puedan prestar su consentimiento, ello "no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño" (art. 8.3).

La Resolución 393/96 del Parlamento Europeo

En este mismo sentido, en la Resolución 393/96 del Parlamento Europeo sobre *Medidas de protección de los menores*, se hacía referencia al hecho de que la edad de los menores para adquirir la capacidad de obrar dependería de lo que establecieran a nivel interno los Estados miembros y, conforme disponen la mayoría de los mismos al grado de madurez y capacidad de "discernimiento" del menor. Por ello, en algunos Estados se han adoptado previsiones para anular los actos jurídicos que, realizados sin el consentimiento paterno, pueden perjudicar a los menores[102]. La regla general es que si legalmente los menores no tienen la edad para contraer obligaciones contractuales y prestan su consentimiento sin el consentimiento de sus representantes, los contratos celebrados no serán válidos. De lo que se podría derivar que el consentimiento para prestar sus datos personales tampoco lo sería. Pero esta es una cuestión controvertida[103].

Dictámenes del G29 y novedades del RGPD

El G29 ha elaborado diversos documentos donde, en este entorno del sector privado, al hilo de analizar cuestiones relativas al tratamiento de datos en el terreno de la publicidad y del marketing, se ha planteado el supuesto en el que dichos datos pertenecen a menores. Se analiza el tratamiento de datos de los menores desde su consideración como consumidores y partes de una relación contractual, en "los casos de datos facilitados por éstos para participar en un juego, en una actividad publicitaria similar o conseguir un premio". El G29 ha mantenido que es necesario el requisito del consentimiento paterno para solicitar datos sensibles de los menores, so pena de considerar el tratamiento de los datos ilegal, de la misma forma que si se tratan datos de los menores sobre su salud o vida sexual o situación financiera de los mismos o de terceros, como sus padres o amigos[104]. Del mismo modo, como consumidores y/o potenciales consumidores se analiza la legitimidad del tratamiento de sus datos de comportamiento. En este caso, el G29 considera que si bien la regla general es que "el consentimiento de los niños deben darlo sus padres u otros representantes legales", en este caso, teniendo en cuenta su vulnerabilidad,

---

[102] Resolución A4-0393/1996, del Parlamento Europeo, de 12 de diciembre de 1996, sobre Medidas de Protección de Menores en la Unión Europea (DOCE C 20, de 20 de enero de 1997).

[103] Así por ejemplo, lo ha mantenido la Agencia Española de Protección de Datos (AEPD): Informe jurídico de la AEPD 466/2004. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2004-0466_Comunicaci-oo-n-a-los-padres-de-las-calificaciones-de-sus-hijos-menores-de-edad..pdf. Pero en contra se han pronunciado los Tribunales españoles que han considerado que la incapacidad para contratar no debe suponer una incapacidad para consentir el tratamiento de los datos personales (Así, por ejemplo, las Sentencias de la Audiencia Nacional de 14 de enero de 2009 (JUR 2009, 59625), y de 10 de febrero de 2010 (JUE 2010, 82779)).

[104] Sobre esta cuestión, vid. los Dictamen 3/2003, del G29, relativo al *Código de conducta europeo de la FEDMA sobre la utilización de datos personales en la comercialización directa*, adoptado el 13 de junio de 2003 (WP77) (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp77_es.pdf); y el Dictamen 4/2010, del G29, relativo al «Código de conducta europeo de la FEDMA sobre la utilización de datos personales en la comercialización directa», adoptado el 13 de julio de 2010 (WP 174) (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_es.pdf), Secc. 6.

los proveedores de redes de publicidad no deberían utilizar publicidad a medida para los niños ni enviársela o influir en ellos de ninguna manera. Se marca la edad de 12 años para empezar a utilizar sus datos y dirigirles publicidad personalizada[105]. No obstante habrá que revisar dicha previsión en tanto que el RGPD, que comenzará a aplicarse en mayo de 2008, prohíbe la mercadotecnia y los perfiles comportamentales, y señala de forma expresa para los menores de edad (aunque sólo se centra en el supuesto de los servicios de la sociedad de la información) que en el caso de ofertas directas a menores, de partida se considerará lícito el consentimiento del niño cuando tenga como mínimo 16 años y, para el caso de que tenga menos de 16 años, el consentimiento lo deberá dar el titular de la patria potestad o tutela del menor, o bien autorizarlo. En este caso se marca la edad de los 16 años, pero la normativa comunitaria indica igualmente que "los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años" (art. 8 RGPD). Entendemos, como ya ha quedado dicho, que las previsiones contenidas en el Reglamento comunitario no se limitan a los servicios de la sociedad de la información y que las condiciones del consentimiento previstas en la citada norma deben hacerse extensivas al consentimiento del menor ante cualquier tratamiento de datos personales del mismo.

f) Como partes de un proceso judicial

Doctrina del TEDH sobre publicidad procesal y menores

Recordamos aquí la exigencia de la CDN de proteger la privacidad del menor en todas las partes del proceso (derivado de sus arts. 16 y 40). Con esta misma idea de garantizar la privacidad del menor en todas las fases del proceso se pronunció, haciendo referencia expresa a dicha norma internacional, el TEDH en el asunto *T. y V. contra el Reino Unido*, de 16 de diciembre de 1999, conocido caso en el que dos menores ingleses de 10 años secuestraron y asesinaron a otro menor de 2 años y fueron sometidos a un proceso público a pesar de haber solicitado ocultar su identidad. El TEDH concluyó que se había producido una lesión del derecho a un juicio justo de los menores (art. 6.1 CEDH) basándose en el argumento de que a la hora de tratar a un menor acusado de un delito se deberían tener en cuenta "sobre todo su edad, su grado de madurez y su capacidad intelectual y emocional, y que se adopten las medidas que favorezcan su aptitud para entender el proceso y participar en él. Por lo que se refiere a un niño de corta edad acusado de un delito grave que atrae enormemente el interés de los medios de comunicación y de la opinión pública, esto puede implicar la necesidad de realizar la vista a puerta cerrada, de modo que disminuyan en lo posible los senti-

[105] Dictamen 2/2010, del G29, sobre publicidad comportamental en línea, adoptado el 22 de junio de 2010 (WP 171) (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp171_es.pdf), Pto. 4.1.4; y Dictamen 16/2011, del G29, sobre la recomendación de mejores prácticas de EASA/IAB sobre publicidad comportamental en línea, adoptado el 8 de diciembre de 2011 (GT 188) (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_es.pdf), Apdo. II.3.A)).

mientos de intimidación e inhibición del niño o, si fuera conveniente, proceder a una selección de los asistentes y establecer criterios de información sensatos".

Con la intención de reinsertar al menor y proteger su desarrollo personal, teniendo como telón de fondo la CDN, se pronunció el TEDH sobre el tema de los Registros de Antecedentes Penales. En el ya citado asunto *S. y Marper, contra el Reino Unido*, de 4 de diciembre de 2008, el TEDH concluyó que la inclusión en una base de datos de información relativa a huellas dactilares, muestras biológicos y ADN en el caso de dos menores, después de haber sido absueltos o habérseles retirado los cargos, lesionaba la vida privada de los mismos. El TEDH consideró que si bien la finalidad de retener dicha información era legítima, en el presente caso, dado la vulnerabilidad de los sujetos, se estaba lesionando su vida privada. El Tribunal añadió, además, que la retención de los datos de las personas no condenadas puede ser especialmente perjudicial en el caso de menores, dada su situación especial y la importancia de su desarrollo e integración en la sociedad, tal y como exige el artículo 40 CDN. Sobre este tema volvió a pronunciarse el TEDH en el caso *B.B. contra Francia*, de 17 de diciembre de 2009 (en el que los demandantes eran tres menores de 15 años acusados de violación cuyos datos fueron incluidos en un Registro de Delincuentes Sexuales) consideró que la inclusión de los menores, en atención a la gravedad del delito y al hecho de que la conservación de la información era por un periodo de 30 años, la finalidad perseguida era la prevención del delito y existía un deber de confidencialidad para los sujetos que manejaban y accedían al citado Registro, no suponía una lesión de su vida privada. Serán pues los Tribunales los que determinen, en atención al caso concreto, la necesidad o no de conservar los datos de los menores en estos casos.

3.4. Datos de los menores en Internet

Guía del Consejo de Europa sobre derechos de los usuarios de Internet

En los últimos años la regulación a nivel europeo sobre el acceso a Internet y el uso de la Red está provocando un gran volumen de normas, sentencias y ríos de tinta, especialmente, cuando tienen por objeto a los menores de edad. La protección de datos personales de los menores en Internet es una cuestión que ha preocupado a nivel europeo de manera constante a todas las instituciones y organismos públicos comunitarios. La connatural falta general de madurez de los menores y los intereses del mercado por manejar información de "potenciales" y fácilmente manipulables consumidores, junto con la ventaja que el "presunto" anonimato de la Red ofrece para cometer actos ilícitos, provoca que la utilización y difusión de datos personales de menores en este ámbito reciba una atención especial no sólo por parte de los directamente afectados, sino por parte de todos los sectores implicados, que buscan una finalidad legítima o ilegítima con el uso de dicha información. No podemos dejar de aprovechar las ventajas que los avances tecnológicos nos ofrecen, pero debemos hacerlo con precaución, máxime si hay menores implicados.

Así, por ejemplo, en relación con el acceso a Internet, desde el Consejo de Europa se elaboró una *Guía de los derechos humanos de los usuarios de Internet* señalando que es responsabilidad del Estado promover el acceso a la Red y que nadie podrá ser desconectado salvo que consienta expresamente a ello, exista una autorización judicial o se prevea por la normativa estatal propia de los contratos (so pena de lesionar sus libertades informativas). En el caso de los menores de edad se traduce, como se recoge expresamente en la citada Guía, en que su acceso a la Red puede verse limitado en el contexto del control parental y dependiendo de la edad del niño y de su grado de madurez (Apdo. 13)[106]. En este sentido, en la práctica europea, a pesar de las medidas legislativas existentes (dado que la eliminación de datos personales utilizados con una finalidad ilícita en Internet es una tarea complicada), la opción está siendo utilizar medidas preventivas como "listas de bloqueo y filtrado" y el citado control parental. La cuestión aquí es que la aplicación de estas medidas, con carácter general, sin analizar y ponderar las circunstancias en el caso concreto, puede suponer la lesión de otros derechos relacionados con las libertades informativas o con la vida privada del menor. No es infrecuente en países no democráticos el bloqueo de acceso a la Red bajo el pretexto de proteger a colectivos vulnerables como los menores o evitar la comisión de delitos como la incitación al odio. Ni es infrecuente en países democráticos, el exceso de celo paterno limitando el ejercicio de los derechos de sus hijos.

Doctrina del TEDH

Por estos motivos, reforzando y reafirmando los derechos de los menores en Internet, y lo dispuesto en la citada *Guía de los derechos humanos de los usuarios de Internet*, el TEDH ha afirmado que los Estados tienen las obligaciones positivas de proteger los derechos y libertades de los sujetos en Internet, especialmente la libertad de expresión, y máxime el deber de proteger a los niños y jóvenes (Al respecto, vid. *STEDH, caso K.U. contra Finlandia*, de 2 de diciembre de 2008).

Dictámenes del G29

Con el fin de regular la participación del menor en Internet o hacer uso de las aplicaciones destinadas a sus dispositivos electrónicos e informáticos, el G29, al elaborar los documentos sobre el tratamiento de datos personales en las redes sociales[107], y sobre las aplicaciones de los dispositivos inteligentes[108], analizó el supuesto en el que

[106] Recomendación CM/Rec (2014) 6, del Comité de Ministros, a los Estados Miembros sobre una *Guía de los derechos humanos de los usuarios de Internet*, adoptada el 16 de abril de 2014, Pto. 33. Disponible on line en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=-09000016804d5b31. Esta Recomendación tiene como antecedente la Recomendación R (99) 5, sobre protección de la privacidad en Internet, de 23 de febrero de 1999. Disponible on line: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f4429, que no hacía referencia alguna expresa a los menores.

[107] Dictamen 5/2009, adoptado el 12 de junio, sobre las redes sociales *on line* (WP 163) (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_es.pdf), Pto. 4.

[108] Dictamen 2/2013, del G29, sobre las aplicaciones de los dispositivos inteligentes, adoptado el 27 de febrero de 2013 (WP 202) (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_es.pdf).

los titulares de la información eran menores. En estos casos, concretamente en el caso de las redes sociales, el G29 concluyó que lo conveniente en este terreno sería llevar a cabo campañas de sensibilización entre los menores y, sobre todo, no pedirles datos sensibles a la hora de registrarse en la red social, así como no realizar campañas de comercialización a los mismos sin el consentimiento previo paterno, lo que además debería ir acompañado de programas informáticos que verificaran la edad del menor y de códigos de buenas prácticas entre los proveedores de tales servicios. Y en relación concreta con las aplicaciones, el G29 señala que las aplicaciones destinadas a los menores de edad deberían tener en cuenta el límite de edad fijado por las legislaciones nacionales y aplicar los principios propios de la normativa sobre protección de datos como el de calidad y finalidad, recomendándose a los proveedores de dichas aplicaciones que se abstengan de recoger a través de los menores, datos de terceros como pueden ser familiares o amigos.

Otros documentos relevantes sobre menores e Internet

Por otro lado, respecto de los contenidos, desde el Consejo de la Unión Europea, en las Conclusiones a la *Estrategia Europea para un mejor Internet para los niños* (2012), se hace especial hincapié en los contenidos de Internet y en su producción por parte de menores, así como en la necesidad de potenciar una configuración de la privacidad de las redes sociales por defecto[109]. En esta línea, la citada *Guía de los derechos humanos de los usuarios de Internet*, dirigiéndose expresamente a los menores y adolescentes recuerda que los menores y adolescentes requieren de una protección especial cuando utilizan Internet, y que, entre otras cosas, tienen derecho a recibir información en un lenguaje apropiado para su edad en atención a preservar su privacidad. Se indica, asimismo, que tienen un derecho de acceso a la información que han creado, así como el derecho a eliminarla cuando lo deseen. Esta idea tiene como objeto evitar posibles delitos que tengan como destinatarios a los menores por la información que hayan publicado en Internet. Por ello, desde el Consejo de Europa se aprobó una Resolución en la que se establecía que con el fin de combatir la pornografía infantil se deberían tener en cuenta las previsiones establecidas en el llamado Convenio de Lanzarote (Pto. 5)[110].

En este punto, no podemos olvidar el pronunciamiento de las Autoridades expertas en esta materia, las Autoridades de Control, y así, debemos citar aquí la *Resolución sobre Protección de la Privacidad en las Redes Sociales* aprobada en la XXX Conferencia Internacional

---

[109] Conclusiones del Consejo de la Unión Europea sobre la *Estrategia para un mejor Internet para los niños*, aprobada en Bruselas el 27 de noviembre de 2012. Disponible *on line*: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/educ/133824.pdf.

[110] Resolución 1843 (2011), de la Asamblea parlamentaria del Consejo de Europa, sobre la *Protección de la vida privada en Internet y los medios on line*. Disponible *on line*: http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xODAzOSZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE4MDM5.

de Autoridades de Protección de Datos y Privacidad (2008)[111]. La Resolución aconseja, entre otros aspectos, y de forma expresa para el caso de los menores que a la hora de publicar información en las redes sociales se evite "revelar sus domicilios o números de teléfono".

Asimismo, respecto de la seguridad de los menores en Internet, la *Guía de los derechos humanos de los usuarios de Internet* indica que el bienestar moral y físico del menor es esencial para garantizarle también el derecho a su vida privada (Pto. 92). Así lo ha reconocido también el TEDH en el mencionado caso *K.U. contra Finlandia*, de 2 de diciembre de 2008, donde el TEDH analizó el caso de un robo de identidad por Internet y concluyó que las legislaciones nacionales deben prever un mecanismo que garantice la confidencialidad de los servidores de Internet a la vez que aseguran la persecución de delitos, especialmente cuando la víctima es un sujeto vulnerable como un menor de edad.

Estos son sólo algunos ejemplos de la preocupación de las instituciones comunitarias por la materia, pero son relevantes, por ejemplo, el Dictamen del Comité de las Regiones sobre la *Protección de la infancia en el uso de Internet (2009-2013)*, de 2008, animando a legisladores, responsables políticos, industria y usuarios, con especial atención a padres, tutores y educadores, a educar en un uso inteligente y crítico de Internet[112]; o los *Principios de la Unión Europea para Redes Sociales más seguras* elaborados por la Comisión Europea, que suponen un acuerdo de autorregulación entre las redes sociales europeas más importantes con el fin de proteger la seguridad de los menores en la Red[113]. Entre las medidas propuestas se recogen la existencia de un "botón de denuncia de abusos", que los perfiles de menores de 18 años no sean ni indexables ni accesibles y que estén predeterminados como "privados", que la forma en la que acceder a la opciones de privacidad sea accesible, y que los menores de edad no utilicen sus servicios si son menores de 13 años.

3.5. Ejercicio por los menores de su derecho a la protección de datos

Catálogo de los derechos de los menores

Tanto el artículo 8 Convenio nº 108, como la Directiva 95/46/CE y, también, el el RGPD, recogen las facultades propias del sujeto concernido o titular de los datos como "garantías complementarias" o "derechos", refiriéndose al acceso, rectificación, cancelación, oposición e, incluso, olvido. Se entienden propias también de los menores

[111] Resolución aprobada el 17 de octubre de 2008 en Estrasburgo. Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/08-10-17_Strasbourg_social_network_ES.pdf.

[112] Dictamen del Comité Europeo de las Regiones sobre "Protección de la Infancia en el uso de Internet (2009-2013)", adoptado el 9 de octubre de 2008. Disponible *on line* en: http://cor.europa.eu/es/activities/opinions/pages/opinion-factsheet.aspx?OpinionNumber=CDR%20174/2008.

[113] Sobre dicho Informe, vid. *on line*: http://europa.eu/rapid/press-release_IP-09-232_es.htm?locale=en.

de edad. En la citada *Guía de los derechos humanos de los usuarios de Internet*, se hacía referencia a los derechos de acceso a la información creada por los menores y adolescentes cuando utilizan la Red, así como a su borrado y a recibir información en un lenguaje apropiado para su edad.

Información

El derecho a ser informado, requisito indispensable para poder prestar el necesario consentimiento legitimador del tratamiento de datos, cobra cierta especialidad en el caso de los menores y así es constante la exigencia de que la información que se les facilite debe utilizar un lenguaje "sencillo, conciso y didáctico de fácil comprensión"[114]. Como mantiene el RGPD "un lenguaje claro y sencillo que sea fácil de entender" (Considerando 58 y art. 12.1). En este mismo sentido se pronuncia la Directiva (UE) 2016/680, relativa al tratamiento de información con fines de prevención de delitos y su investigación, que exige además que la información sea "accesible" (Considerandos 39 y 50).

Acceso

Sobre el derecho de acceso, nuevamente debemos tener en cuenta que estos derechos serán ejercidos, por regla general, por los representantes de los menores y que los responsables darán cuenta a los mismos. No obstante, teniendo en cuenta el interés del menor y el principio de proporcionalidad, en determinadas circunstancias en las que el menor ha dado algunos datos personales sin consentimiento ni conocimiento por parte de sus padres y, posteriormente, solicita tener acceso a los mismos, podrá hacerlo de forma unilateral, aunque la cuestión está en saber si los representantes podrían acceder igualmente. Como ha señalado el G29, este puede ser el caso en que un menor haya facilitado datos a un médico o a servicios sociales y haya informado sobre cuestiones de salud o sobre su vida sexual, consumo de drogas o intentos de suicidio, sin que consienta a comunicárselo a sus padres o tutores. En estos casos, en los que el menor podría oponerse a dar dicha información a sus representantes legales habrá que ponderar los intereses en juego bajo el principio del interés superior del menor y respetando no sólo su derecho a la protección de datos, sino el resto de derechos del mismo, como el derecho a la intimidad. En los casos mencionados, para realizar la valoración oportuna podría ser conveniente tener en cuenta la opinión del médico o persona que ha tratado al menor. En todo caso, "el criterio de acceso no sólo será la edad del niño sino también si los datos fueron proporcionados por los padres o por el niño, lo cual es un indicador del grado de madurez y autonomía de éste"[115].

Cancelación

Respecto del derecho de cancelación o borrado de la información, en el caso de Internet, la *Guía de los derechos humanos de los usuarios*

[114] Dictamen 2/2009, del G29. Sobre esta cuestión también se pronunció el G29 en su Dictamen 10/2004 sobre una mayor armonización de las disposiciones relativas a la información, adoptada el 25 de noviembre de 2004 (WP 100) (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp100_es.pdf); así como en su Recomendación sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea, aprobada el 17 de mayo de 2001 (WP 43) (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp43_es.pdf).

[115] Dictamen 2/2009, del G29.

de Internet recuerda que para garantizar correctamente este derecho es necesario entender que el contenido que los niños y jóvenes crean en Internet y el uso que hacen de esa información, así como el uso de Internet o de los contenidos que otros han creado en relación con ellos (por ejemplo, imágenes, videos, texto u otro contenido) o las huellas de este contenido (registros, registros y procesamiento) puede durar o estar permanentemente accesible, vulnerando así su desarrollo personal. Como dejó señalado el G29, "Al estar los niños en proceso de desarrollo, los datos sobre ellos cambian y rápidamente pueden quedar anticuados y dejar de ser pertinentes para los fines originarios de recogida. Cuando esto suceda, se dejará de conservar los datos"[116].

Derecho al olvido

En relación con el tema del borrado o periodo de conservación de los datos, en íntima conexión con el llamado "derecho al olvido", el mismo cobra especial relevancia en el caso de los menores de edad. Recordamos aquí que el derecho al olvido fue reconocido por el Tribunal de Justicia de la Unión Europea (TJUE) en su Sentencia sobre el conocido como "Caso Costeja" o "Caso Google contra AEPD"[117]. Sobre el derecho al olvido, reconocido ya expresamente en el RGPD (aunque bajo la denominación de "derecho de supresión", art. 17), se realiza una mención expresa a los menores, para el caso de que se hubiera dado el consentimiento cuando se era un niño y no se era consciente de las repercusiones de sus actos "y más tarde quiere suprimir tales datos personales, especialmente en internet". En estos casos se indica la posibilidad de borrar, olvidar, la información salvo que el tratamiento de la información sea necesario"para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, 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, o para la formulación, el ejercicio o la defensa de reclamación" (Considerando 65 y art. 17 RGPD). Con el fin de poner en práctica este derecho cuando se ejerza por menores, el G29 ha señalado que la Autoridad de Control que se encargue de tutelar este derecho deberá tener en cuenta el principio del interés superior del menor[118].

Representación e invisibilización

En líneas generales podemos concluir que a nivel europeo el ejercicio del derecho a la protección de datos personales por parte de los menores de edad, salvo puntuales excepciones, no tiene un reconoci-

---

[116] Dictamen 2/2009, del G29.

[117] STJUE, de 13 de mayo de 2014, asunto Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González (C-131/12). Disponible *on line*: http://curia.europa.eu/juris/document/document.jsf?-docid=152065&doclang=ES.

[118] Directrices, del G29, sobre la implementación de la Sentencia del Tribunal de Justicia de la Unión Europea sobre "Google Spain e Inc. contra la Agencia Españolad de Protección de Datos (AEPD) y Mario Costeja González" C131-12, adoptadas el 26 de noviembre de 2014 (WP225). Disponible *on line*: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

miento expreso y va a ser ejercitado por sus representantes cayendo, por lo tanto, en las reglas de representación que disponga cada Estado. La ausencia de una edad mínima para el ejercicio del citado derecho invisibiliza a los menores de edad como titulares de un derecho que les ayudará a desarrollarse personalmente.

II. PANORAMA NACIONAL

1. ANDORRA

1.1. Normativa

Silencio legal y determinación de la Agencia: minoría de edad hasta los 14 años

En el ordenamiento jurídico del Principado de Andorra no se dispone actualmente de un Código Civil. Las referencias legislativas que encontramos son la Ley Cualificada de la Jurisdicción de Menores, de modificación parcial del Código Penal y de la Ley Cualificada de la Justicia, de 22 de abril de 1999, y la Ley Cualificada de Adopción y otras formas de Protección del Menor Desamparado, de 21 de marzo de 1996. Ni la vigente Ley de protección de datos ni su Reglamento de desarrollo incluyen una redacción concreta relativa al tratamiento de los datos personales de los menores, por lo que se plantea la duda respecto a la franja de edad a partir de la cual se consideraba que el menor disponía de capacidad suficiente para ejercer sus derechos, con plena capacidad, a la información, consentimiento, acceso, rectificación, oposición y supresión en materia de tratamiento de sus datos personales. La respuesta era: o bien se tenía en cuenta como límite la edad de 18 años o bien se atendía a la normativa europea y andorrana, donde se considera el menor penalmente responsable a partir de los 14 años. Teniendo en cuenta estas normas, la Agencia ha establecido esta última como la franja de edad mínima para considerar que un menor de edad tiene la capacidad suficiente para la comprensión de los derechos y deberes regulados en la normativa de protección de datos. Además, sería ilógico no adaptarse a la necesidades de la sociedad, donde presenciamos un incremento exponencial del uso de la nuevas tecnologías, de Internet, y también de la apuesta de la sociedad andorrana y del sistema educativo andorrano por el uso de las nuevas tecnologías en el sistema educativo a partir de la educación secundaria. Todo esto nos da aún más motivos para tener en cuenta los criterios arriba mencionados para establecer como menores de edad aquellos jóvenes comprendidos entre los 14 y los 18 años.

Es cierto que la falta de regulación clara y específica al respecto puede llevar a múltiples interpretaciones, pero una vez sentadas las bases, éstas se han tenido en cuenta como por ejemplo en el anteproyecto de Ley de la historia clínica compartida y derechos de los pacientes, actualmente en trámite parlamentario, donde se prevén una disposiciones muy concretas respecto al tratamiento de los datos de salud de los menores. Estos mismos criterios se han tenido en cuenta en la tramitación de varias reclamaciones admitidas por la Agencia en aplicación de la Ley andorrana de protección de datos en los que,

después de la tramitación del procedimiento administrativo, se han aplicado las sanciones previstas en la Ley.

Problema de la falta de colaboración de empresas en el extranjero

Pese a la opción señalada, no se pueden negar las dificultades para llegar a conclusiones finales en los expedientes tramitados. Las particularidades de Andorra, que es un Estado pequeño, y "país tercero" para la Unión Europea, no facilitan la tramitación de los mismos. En algunos casos no solamente no hemos recibido ninguna información de los operadores de ciertas redes sociales a los que se las ha requerido, sino que ciertas Autoridades europeas responden con evasivas o simplemente no responden a las solicitudes de colaboración enviadas por la Agencia andorrana, dificultando aún más si cabe poder ejercer con absoluta normalidad las funciones de control y sanción atribuidas por la Ley. Hemos de tener en cuenta que cuando se trata de redes sociales, sus domicilios comerciales se encuentran fuera del territorio andorrano y por ello nos hemos de dirigir a los domicilios sociales que constan en las cláusulas de privacidad y legales de las mismas, requiriendo en alguna ocasión la colaboración de las Autoridades nacionales donde se encuentran domiciliadas dichas redes sociales. En resumen se tendrá que llegar una colaboración, clara, transparente y de confianza mutua, respetando los estándares de protección de datos de cada país, a fin de conseguir una acción eficaz por parte de las Autoridades de control.

1.2. El consentimiento del menor para el tratamiento de sus datos personales

Necesidad de consentimiento de padres o tutores hasta los 14 años

De acuerdo con la legislación andorrana, los datos relativos a un menor de edad pueden ser tratados con el consentimiento de sus padres, tutores o representantes legales. En caso de menores de 14 años o incapaces se exigirá, en todo caso, el consentimiento de sus padres o tutores legales para tratar sus datos personales. Este consentimiento será igual al exigido en otros casos a los afectados por el tratamiento, con la diferencia de que quién deberá otorgarlo será el representante legal del menor. Para que el consentimiento sea válido debe ser libre, inequívoco, específico e informado.

Obligaciones de los responsables de los ficheros

Será el responsable del fichero quien deberá garantizar que el consentimiento obtenido es válido y, por ello, deberá asegurarse de que la persona que presta el mismo es quién está capacitada para ello. Lo normal es que el responsable del fichero exija el pasaporte u otra forma de identificación personal a dicha persona.

Además, al solicitar el consentimiento el responsable del fichero deberá informar de forma clara y concisa de una serie de aspectos como: a) la existencia un fichero de datos de carácter personal, de la finalidad para la que se recogen éstos y de los receptores de la información; b) el carácter forzoso o voluntario de su respuesta a las preguntas que les sean propuestas; c) los efectos de la recogida de los datos o de la negativa a facilitarlos; d) la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición; e) el nombre y dirección del responsable del tratamiento o, en su caso, de su representante.

En cuanto a la demostración de dicho consentimiento, el artículo 7 del Reglamento señala que es el responsable del fichero quien deberá probar la existencia del mismo mediante cualquier medio admisible, y en supuestos de menores de edad, se establecerán mayores exigencias atribuyendo al responsable del fichero procedimientos para garantizar que se ha comprobado válidamente la edad del menor y la legitimidad del consentimiento otorgado por los padres o tutores legales. No existe en la norma un procedimiento determinado dejando libertad al responsable para que establezca el que considere adecuado.

Límites del tratamiento de datos de menores

De otro lado, el tratamiento de datos de menores no podrá ser indiscriminado sino que deberá limitarse en dos aspectos. En primer lugar, no pueden solicitarse datos que permitan la obtención de información relativa a otros miembros de la familia del menor o características de los mismos (p. ej., profesión o situación económica) sin el debido consentimiento del titular. En segundo lugar, sólo podrán solicitarse los datos de identidad y dirección de los padres o tutores con la finalidad de obtener el consentimiento necesario.

Podemos concluir, por tanto, que los datos personales de menores de 14 años sólo pueden ser recogidos y tratados con el consentimiento expreso de sus progenitores o tutores legales y que para obtener ese consentimiento es necesario informarles previa y claramente sobre las finalidades de ese tratamiento y la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición así como la dirección del responsable del fichero

1.3. Ámbitos problemáticos: publicidad dirigida a menores

Necesidad de protección de menores en la publicidad

Los niños y jóvenes son los futuros consumidores y sus conductas dirigen las campañas de marketing de muchas empresas, sea porque suponen su principal *target* comercial o porque serán sus futuros consumidores. Pues bien, en esta materia debemos establecer una consideración especial a los menores, que todavía no están formados ni tienen criterio suficiente para decidir sobre ciertas cuestiones. La ley de protección de datos reconoce que la persona interesada o afectada tiene facultad y capacidad para controlar estos datos personales y decidir sobre ellos. Por ello, cuando hablamos de menores, la protección ha de ser máxima y las empresas han de conocer la normativa.

Obligaciones de las empresas

Tal y como hemos visto en el apartado anterior, necesitamos del consentimiento expreso de los responsables legales de los menores para el tratamiento de sus datos y deberemos adaptar la información dada a los mismos a su lenguaje y conocimientos. Resulta así fácil entender lo importante que resulta que una empresa respete el marco legal y se presente de una manera clara y transparente frente a los niños y los padres, para generar confianza y seguridad y no sólo en supuestos de empresas dirigidas expresamente a menores sino que también deberán ser más precavidas aquellas que tengan en cuenta que los menores puedan ser sus potenciales clientes, como pueden ser empresas tecnológicas cuyas campañas se dirigen al público adulto sin tener en consideración que una de las actividades favoritas de los menores de hoy día tiene que

ver con todo lo relacionado con Internet y sus aplicaciones. Por todo esto, las empresas deberán seguir una doble estrategia: ser atractivas y adaptadas a los menores (p. ej., utilización de la página web como herramienta publicitaria y de ocio mediante uso de juegos o aplicaciones) y sean percibidas como seguras por parte de los progenitores.

1.4. Datos de menores en Internet

Riesgos del tratamiento de datos de menores en Internet

Normalmente, los menores desconocen los riesgos que puede suponer la publicación de fotografías u otros datos en Internet ya que valores como la privacidad o la propia imagen no son percibidos como necesarios. Al mismo tiempo, los adultos responsables buscan conocer a qué contenidos han accedido sus hijos y qué datos están siendo ofrecidos de forma imprudente por parte de los mismos. Sabemos además que los niños son especialmente vulnerables en la red: reciben ofertas de foros, páginas web, chats, que son muy atractivas para ellos y no son capaces de discernir qué es publicidad y qué son hechos. Los principales riesgos a los que se exponen los menores residen en la posibilidad de comunicarse con individuos malintencionados, la revelación de información personal por parte de ellos mismos o terceros, el acceso a contenidos inapropiados para su edad y la contratación de servicios por error o desconocimiento.

Prevención y formación

Por todo esto, consideramos necesaria una doble estrategia de prevención y formación de menores: por un lado, los padres o responsables legales deben acompañar a los menores durante sus primeras experiencias navegando por la red para ayudarles a diferenciar qué contenidos son potencialmente peligrosos, asegurarse que no accedan a contenidos perniciosos y educarles sobre el intercambio responsable de fotografías o datos personales con amigos o desconocidos. Por ello, la Agencia organiza periódicamente campañas de sensibilización e información, como "Navega Segur" (dirigida exclusivamente a menores de edad) o "Dades Ni Piu: Que no se't escapin", en las que de forma atractiva, visual y sencilla se informa sobre los peligros de la red y del derecho de protección de datos.

1.5. Ejercicio por los menores de su derecho a la protección de datos

Centros educativos: colaboración de la Agencia con el Ministerio de Educación

Uno de los principales campos donde los menores pueden ejercer su derecho a la protección de datos es en el ámbito escolar. Cada vez es más habitual que centros educativos dispongan de perfiles en las redes sociales que se usan para establecer una comunicación fluida con los padres y que estos puedan participar del día a día de sus hijos en la escuela a través de la publicación de fotografías o documentos[1]. En

[1] El sistema educativo andorrano está haciendo una progresión en la introducción de las nuevas tecnologías en las escuelas a partir de segunda enseñanza: a partir de los 11 años es obligatorio que todos los niños dispongan de un dispositivo *tablet*, que es el canal de comunicación y progreso educativo del alumno.

este ámbito se ha establecido una estrecha colaboración entre la Agencia y el Ministerio encargado de la educación, estableciéndose sinergias muy positivas entre ambas instituciones que facilitan el respeto al derecho fundamental a la protección de los datos de los menores en todos los ámbitos: en el ordenamiento administrativo (publicación de los ficheros en el Boletín Oficial del Principado de Andorra) y en el legal (redacción de la clausulas informativas, obtención el consentimiento del padre-tutor o representante legal para la utilización de los datos del menor, incluyendo la obtención de fotografías en actividades, escolares y extraescolares), a lo que se añade un asesoramiento continuo en la utilización de programas informáticos que se instalan, o se pretenden instalar, informando de los posibles riesgos que algunas plataformas de conocidas multinacionales ponen a la disposición de las escuelas sin cargos y que en realidad no resultan tan gratuitas. Esta sinergia también nos ha llevado a analizar la implementación de un módulo de protección de datos en las escuelas, que actualmente se encuentra en la fase de proyecto, pero que ha tenido una buena acogida por las autoridades competentes en la materia.

Datos en actividades extraescolares

Fuera de los centros educativos encontramos el caso de actividades extraescolares que, ya sea por desconocimiento o por creencia que no son ellos los responsables de los datos, captan fotografías de menores y usan las mismas para fines publicitarios o de difusión de sus actividades. Estos casos también deben protegerse con la normativa de Protección de Datos, esto es, deben realizarse siempre con el conocimiento y el consentimiento expreso de los padres o representantes legales y del menor, si este fuera mayor de 14 años.

1.6. Herramientas y recursos de la autoridad en materia de menores

Actividades de difusión realizadas por la Agencia

Desde la APDA consideramos vital un acercamiento entre nuestra institución y los menores ya que en última instancia son estos el grupo social que más se relaciona usando medios telemáticos, ignorando muchas veces las consecuencias o los rastros que su presencia en Internet o redes sociales pueden tener en su privacidad. Por este motivo, además de charlas y campañas de concienciación, desde la APDA se pone a disposición un portal web de protección de datos destinado a menores[2], sus progenitores y educadores para entender qué bienes protege la protección de datos y los riesgos que inconscientemente afrontamos. Además encontramos todo tipo de contenido útil en la web como enlaces de interés, noticias relacionadas con la protección de datos, cambios legislativos relevantes o publicaciones realizadas por la propia agencia. Igualmente, la Agencia sigue interesada en captar aún más la atención de estos menores y por este motivo estamos trabajando en la incorporación de un apartado en el portal joven en la que colgaremos guías detalladas (a modo de "WikiHow") en las que detallaremos los pasos a seguir para múltiples comportamientos on-line, como por ejemplo, como darse de baja de redes sociales de forma segura.

[2] http://portaljove.apda.ad/

2. ARGENTINA

2.1. Normativa

La Convención de Derechos del Niño y la Ley 26.061

En Argentina los tratados internacionales tienen jerarquía constitucional y deben entenderse complementarios de los derechos y garantías reconocidos por la Constitución. En la materia que nos ocupa, merece mención especial la Convención sobre los Derechos del Niño (en especial, sus arts. 5, 13, 16 y 17), ya mencionada (I, 1). Esta Convención, aprobada mediante la Ley Nº 23.849, que diera luego lugar a la Ley 26.061, implicó un férreo impulso al afianzamiento de los derechos de los niños, no obstante lo cual se encuentra pendiente el desarrollo de una normativa específica para las actividades de tratamiento de datos personales de los niños, niñas y adolescentes.

En la Ley 26.061, de Protección Integral de los Derechos de Niños, Niñas y Adolescentes, destacamos sus artículos 2 (aplicación obligatoria de la Convención), 3 (interés superior), 19 (derecho a la libertad), 22 (derecho a la dignidad), 24 (derecho a opinar y a ser oído) y 29 (principio de efectividad). Interesa transcribir el artículo 22, según el cual "Las niñas, niños y adolescentes tienen derecho a ser respetados en su dignidad, reputación y propia imagen. Se prohíbe exponer, difundir o divulgar datos, informaciones o imágenes que permitan identificar, directa o indirectamente a los sujetos de esta ley, a través de cualquier medio de comunicación o publicación en contra de su voluntad y la de sus padres, representantes legales o responsables, cuando se lesionen su dignidad o la reputación de las niñas, niños y adolescentes o que constituyan injerencias arbitrarias o ilegales en su vida privada o intimidad familiar".

Minoría de edad hasta los 18 años

Según el Código Civil y Comercial de la Nación, "Menor de edad es la persona que no ha cumplido dieciocho años. Este Código denomina adolescente a la persona menor de edad que cumplió trece años" (art. 25). Por su parte, según el artículo 26, "La persona menor de edad ejerce sus derechos a través de sus representantes legales. No obstante, la que cuenta con edad y grado de madurez suficiente puede ejercer por sí los actos que le son permitidos por el ordenamiento jurídico. En situaciones de conflicto de intereses con sus representantes legales, puede intervenir con asistencia letrada. La persona menor de edad tiene derecho a ser oída en todo proceso judicial que le concierne así como a participar en las decisiones sobre su persona".

Propuesta de reforma legal de la DNPDP

La Dirección Nacional de Protección de Datos Personales (DNPDP) impulsó entre mayo y diciembre de 2016 un proceso de discusión abierta sobre la necesidad de una reforma a la Ley 25.326 mediante la presentación de un borrador de proyecto. Este proceso fue convocado dentro del Programa "Justicia 2020", del Ministerio de Justicia y Derechos Humanos de la Nación, en una plataforma a fin de recibir comentarios y aportes de la ciudadanía y principales actores implicados. En lo que respecta a menores se propuso un régimen específico para el consentimiento en el artículo 18 relativo al tratamiento de datos de menores.

2.2. El consentimiento del menor para el tratamiento de sus datos personales

Regla de consentimiento del representante del menor, salvo autorización legal expresa

La Ley 25.326 no contiene ninguna referencia expresa sobre el consentimiento del menor para el tratamiento de sus datos personales, por lo que esta materia se rige básicamente por los principios de la Convención de los Derechos del Niño[3] y sobre todo por el Código Civil y Comercial de la Nación (CC). Al respecto debe tenerse presente el principio general establecido por el artículo 26 CC, según el cual el menor (en la medida que cuente con edad y grado de madurez suficiente) puede ejercer por sí los actos que le son permitidos por el ordenamiento jurídico, es decir, el menor sólo puede realizar aquellos actos expresamente autorizados por la ley. En tal sentido, el menor podrá ejercer por sí aquellos actos previstos por normativa específica (p. ej., arts. 64, 66, 117, 684, 1323 o 1922 a), mientras que los restantes actos requerirán de la conformidad sus representantes, salvo autorización judicial.

En los contratos de escasa cuantía cabe consentimiento del menor

Resulta relevante a los fines del presente análisis señalar algunas de las implicancias prácticas que se derivan del artículo 684 CC, que dispone que "los contratos de escasa cuantía de la vida cotidiana celebrados por el hijo, se presumen realizados con la conformidad de los progenitores". En tales casos, cuando se produzca la contratación de servicios relativos a la vida cotidiana (como lo podría ser el alta en un sitio educativo en Internet relativo a la actividad escolar del menor) que sean adecuados a su edad y grado de madurez, cabría presumir que cuenta con la autorización paterna, y en tal caso, el consentimiento para el tratamiento de sus datos personales será válido siempre y cuando se cumpla con los requisitos de licitud de la Ley 25.326 (p. ej. los datos que sean necesarios y no excedan el objeto del contrato). A dicha circunstancia se suman los contratos de menores emancipados (art. 27 del CC) y de aquellos menores mayores de 16 años que estén autorizados por sus padres para ejercer trabajo. En tales casos, se entiende que el menor de edad podrá figurar en ficheros de morosos si incurre en deudas con terceros.

---

[3] Recordemos que según el art. 2 de la Ley 26.061 la Convención es de aplicación obligatoria en las condiciones de su vigencia y que los derechos y las garantías de los sujetos de esta ley son de orden público, irrenunciables, interdependientes, indivisibles e intransigibles. Asimismo, el artículo 13 de la Convención sobre los Derechos del Niño dispone que el niño tendrá derecho a la libertad de expresión, que incluye la libertad de buscar, recibir y difundir informaciones e ideas de todo tipo, sin consideración de fronteras, ya sea oralmente, por escrito o impresas, en forma artística o por cualquier otro medio elegido por el niño; y que el ejercicio de tal derecho podrá estar sujeto a ciertas restricciones, que serán únicamente las que la ley prevea y sean necesarias: a) Para el respeto de los derechos o la reputación de los demás; o b) Para la protección de la seguridad nacional o el orden público o para proteger la salud o la moral públicas. Por otro lado, como límites a dichos derechos la misma Convención dispone en su art. 5 que "los Estados Partes respetarán las responsabilidades, los derechos y los deberes de los padres… según establezca la costumbre local, de los tutores u otras personas encargadas legalmente del niño de impartirle, en consonancia con la evolución de sus facultades, dirección y orientación apropiadas para que el niño ejerza los derechos reconocidos en la presente Convención".

Conveniencia de normativa específica

No obstante, como puede desprenderse de lo hasta aquí expuesto, sería aconsejable una regulación específica para la tutela de los datos personales de los menores, junto con el diseño e implementación de tareas de concientización y capacitación que los prepare para tutelar su información personal en su vida cotidiana.

2.3. Ámbitos problemáticos

a) Publicidad dirigida a menores

Ausencia de normativa especial y aplicación de la Ley 25.326

No se ha regulado por ley en forma específica la publicidad dirigida a menores, si bien en algunas normativas locales, como en la ciudad de Buenos Aires, se han dispuesto algunas limitaciones sobre la promoción de alcohol y tabaco entre los menores. Resulta entonces aplicable a la publicidad dirigida a menores el artículo 27 de la Ley 25.326, que regula la actividad en conjunto con lo dispuesto por el Código Civil y Comercial[4].

[4] Cabe también hacer referencia a otras normas de autorregulación de Cámaras del sector publicitario (CONARP) relativa a menores (disponible en http://www.conarp.org.ar/): "Código de ética y autorregulación publicitaria... Artículo 33º.- Toda publicidad deberá tener especial cuidado de la credulidad de los niños y la falta de experiencia de las personas jóvenes.- En consecuencia deberá: 1. Cuidar el contenido de los mensajes que se incluyan en los programas dirigidos a ellos, los precedan o sigan y los que se inserten en publicaciones destinadas a los mismos. 2. Evitar la presentación visual de prácticas o situaciones peligrosas, de manera que puedan inducir a los niños y adolescentes a emularlas a riesgo de su seguridad. 3. Evitar mostrar al alcance y uso de niños, objetos que por sí entrañan peligros, como armas, elementos cortantes, medicamentos, substancias tóxicas, cáusticas o inflamables. 4. Evitar mostrar a niños pequeños accionando artefactos eléctricos o a gas, o encendiendo fuego, sin la guía de los mayores. 5. Evitar mostrar a niños manejando vehículos de adultos, ni protagonizando acciones que impliquen riesgo a peligros, ni contraviniendo normas de seguridad. 6. Evitar mostrar a niños cometiendo actos ilegales o que contravengan ordenanzas o reglamentaciones. Artículo 34º.- La publicidad dirigida a los niños o adolescentes: 1. Debe evitar inducirlos a realizar actos que resulten física, mental o moralmente perjudicial a los mismos. 2. No se debe aprovechar de la natural credibilidad infantil ni de la inexperiencia de los jóvenes, ni deformar el sentido de lealtad de los mismos. 3. No debe mostrárselos en lugares inadecuados, ni en situaciones de riesgo o peligro para su edad, ni contener declaraciones o presentaciones visuales que puedan llevarlos a ellas. 4. No debe ofrecerse productos que no sean apropiados para ellos. Artículo 35º.- Ningún mensaje de productos para niños o adolescentes debe: 1. Socavar sus valores sociales, sugiriendo que su uso o tenencia le dará una ventaja física, social o psicológica sobre otros niños o jóvenes. 2. Socavar la autoridad, responsabilidad, juicio o criterio de los padres y educadores. La comunicación comercial que invite a los menores a contactarse con el vendedor debe advertir que es necesario contar con el permiso previo de sus padres o adulto responsable, además de informar sobre el costo de la comunicación, si corresponde. La información personal sobre menores sólo puede ser obtenida por terceros si la entrega de la misma es autorizada previamente por sus padres, observando las leyes de privacidad vigentes. Por otra parte, los padres o tutores deben participar y supervisar las actividades de los menores, en especial a lo referente a comunicaciones interactivas. 3. Contener frases mandatarias o compulsivas que insten al menor a obtener el producto por cualquier medio. Artículo 36º.- Ningún mensaje dirigido a los menores de edad debe crear ansiedad ni sugerir que sus padres o familiares no cumplen con sus deberes si no la satisfacen. Artículo 37º.- Ningún mensaje de productos para niños debe insinuar que si un niño no lo compra, signifique para él una minimización y sea

Autorregulación de la DNPDN

La DNPDP, mediante la Disposición 4/2004, de Homologación del Código de Ética de la Asociación de Marketing Directo e Interactivo de Argentina, aprobó la siguiente autorregulación:

> Definiciones. Niños: cualquier persona menor de 13 años […]. 12.5.- Disposiciones Específicas para Niños. 12.5.1.- Al recolectar datos sobre niños, el Responsable deberá siempre realizar todo esfuerzo razonable a fin de garantizar que el niño y su Representante Legal estén informados acerca de las finalidades del Tratamiento de los datos. El aviso de la información deberá ser destacado, de fácil acceso y comprensible para los niños, en particular, cuando se utilicen materiales comerciales dirigidos a ellos. 12.5.2.- En los casos en que la ley aplicable de protección de datos requiriera el consentimiento del Titular para su Tratamiento, los Responsables deberán obtener del Representante Legal, el consentimiento previo e informado. 12.5.3.- Los Responsables deberán constatar razonablemente que la persona que ejerce los derechos del niño sea su Representante Legal. 12.5.4.- El Responsable concederá al Representante Legal los mismos derechos que los descriptos en el punto 12.1 de este Libro. Los Responsables no ahorrarán ningún esfuerzo razonable para verificar que la persona que pretende ejercer los derechos del niño sea su Representante Legal. 12.5.5.- Los Responsables no condicionarán la participación de un niño en un juego, el ofrecimiento de un premio o cualquier otra actividad que involucre un beneficio promocional, a que el niño revele más Datos Personales que aquellos que sean estrictamente necesarios en función de la finalidad de la campaña, la que deberá estar adecuada a los principios generales de este Código.

b) Menores responsables penalmente y víctimas de delitos

Prohibición general de difusión de sucesos con menores

Además del ya mencionado artículo 22 de la Ley 26.061, el artículo 1 de la Ley 20.056 prohíbe "en todo el territorio de la República la difusión o publicidad por cualquier medio de sucesos referentes a menores de dieciocho (18) años de edad incursos en hechos que la ley califica como delitos o contravención o que sean víctimas de ellos, o que se encuentren en estado de abandono o en peligro moral o material, o cuando por esa difusión o publicidad fuera escuchado o exhibido el menor o se hagan públicos sus antecedentes personales o familiares de manera que pueda ser identificado".

Limitación a la difusión de sentencias con datos de menores

En cuanto a la difusión de las sentencias, cabe recordar el artículo 14.1 PIDCP, según el cual "toda sentencia en materia penal o contenciosa será pública, excepto en los casos en que el interés de menores de edad exija lo contrario, o en las actuaciones referentes a pleitos matrimoniales o a la tutela de menores". Según el artículo 164.2 del

---

mirado con menos respeto o sea objeto de burlas u otras formas de ridiculización. Artículo 38º.- La publicidad de juguetes debe cumplir con ciertos requisitos para evitar el desencanto de los niños. a) Si se indica el precio debe especificarse lo que brinda en razón del mismo. b) El tamaño del juguete debe ser indicado de alguna manera suficientemente ilustrativa. c) Cuando un mensaje muestra los resultados que un niño puede obtener mediante sus habilidades manuales, los mismos deben ser razonablemente alcanzables para la mayoría de los niños que integren el segmento de edad correspondiente. Además, deberá brindar toda la información acerca de posibles compras adicionales, como accesorios o elementos individuales dentro de una colección o serie, necesarias para obtener el resultado final que se muestra o describe".

Código Procesal Civil y Comercial de la Nación (Ley 17.454), "Las sentencias de cualquier instancia podrán ser dadas a publicidad salvo que, por la naturaleza del juicio, razones de decoro aconsejaren su reserva, en cuyo caso así lo declarará. Si afectare la intimidad de las partes o de terceros, los nombres de éstos serán eliminados de las copias para la publicidad".

Por su parte, la Ley 26.856 (desarrollada por las Acordadas 15/2013 y 24/2013) dispone la publicidad de las sentencias una vez notificadas las partes, al igual que un listado de la totalidad de las causas en trámite. Según el artículo 3, "Las publicaciones precedentemente dispuestas se realizarán a través de un diario judicial en formato digital que será accesible al público, en forma gratuita, por medio de la página de internet de la Corte Suprema de Justicia de la Nación, resguardando el derecho a la intimidad, a la dignidad y al honor de las personas, y en especial los derechos de los trabajadores y los derechos de los niños, niñas y adolescentes". La Acordada de la Corte Suprema de Justicia de la Nación de 17 de diciembre de 1952 (reglamento para la Justicia Nacional, ADLA, XIII-A) incluye como excepciones a la revisión de expedientes los "que contengan actuaciones administrativas que tengan carácter reservado" así como los "referentes a cuestiones de derecho de familia (divorcio, filiación, nulidad de matrimonio, pérdidas de la patria potestad, tenencia de hijos, insania, etc.), así como aquellos cuya reserva se orden especialmente" (art. 64).

Doctrina de la DNPDP: disociación y anomización de los datos judiciales sobre menores

La Dirección Nacional de Protección de Datos Personales sancionó la Disposición 12/2010, relativa a los datos personales destinados a difusión pública (juicios, jurisprudencia y similares) en la que se resguarda específicamente los datos de menores. Según el artículo 1, "Cuando se efectúen tratamientos de datos personales destinados a difusión pública que contengan datos sensibles en los términos de la Ley Nº 25.326 o referente a menores, incapaces, asuntos de familia y cualquier otra categoría de datos protegida por ley, deberá observarse la aplicación de procedimientos eficaces de disociación y/o de todo procedimiento riguroso de protección a fin de evitar la identificación del titular del dato, en defensa de sus derechos de intimidad o cualquier otro que se encuentre en juego".

En el Dictamen 21/08, la DNPDP, recordando su Dictamen 269/06, el fallo "Kook Weskott" de la Corte Suprema de Justicia, el artículo 14.1 PIDCP y las "Reglas de Heredia" (documento de consenso entre los Poderes Judiciales de América Latina sobre la difusión de información judicial en Internet), según las cuales "prevalecen los derechos de privacidad e intimidad cuando se traten datos personales que se refieran a niños, niñas, adolescentes (menores) o incapaces; o asuntos familiares; […] o cuando se trate de datos sensibles o de publicación restringida según cada legislación nacional aplicable o hayan sido así considerados en la jurisprudencia emanada de los órganos encargados de la tutela jurisdiccional de los derechos fundamentales" (Regla 5), opinó que la información que involucre a menores "deberá ser anonimizada, esto es pasible de la aplicación de procedimientos de disociación que impidan relacionarla con personas determinadas o determinables".

c) Datos médicos

Doctrina de la DNPDP: necesidad de consentimiento de representantes en datos médicos de menores

En su Dictamen 6/04, la DNPDP ha opinado, con sustento en el Código Civil entonces vigente, que "la inmadurez de los menores los priva de voluntad propia, por carecer de discernimiento (art. 921 CC), cualidad que junto con la intención y la libertad (art. 897 CC), constituyen elementos esenciales para el otorgamiento válido de los actos. Al respecto, el ordenamiento jurídico argentino ha previsto un sistema de representación (arts. 56 y 57.2 CC) en cabeza de sus padres, quienes la detentarán a través de la patria potestad (art. 264 CC) o bien de terceros a través del régimen de la tutela (art. 377 CC), en caso de ausencia de los primeros. De lo expresado se desprende que, jurídicamente, los menores de edad se encuentran incapacitados para disponer de su persona, cuerpo y salud, por lo que carecen de aptitud legal para prestar su consentimiento respecto de todo acto terapéutico o de diagnóstico que modifique su statu quo. Por ello, desde la simple consulta médica hasta la más compleja práctica, pasando por todos los estudios o análisis, deben ser autorizados por los representantes del menor".

En su Dictamen 243/06, la DNPDP sostuvo que "como se trata de un estudio a realizarse con pacientes desde los 6 años de edad, se ha previsto la firma del Formulario de Asentimiento para Niños, en el que se expresan en forma sencilla y adecuada al entendimiento de un menor, los aspectos analizados precedentemente. Sobre el particular, cabe destacar que [hasta la mayoría de edad] deberá contarse con la firma de la respectiva autorización de los representantes legales del menor (padres o tutores, según el caso), sin perjuicio de que los interesados suscriban un formulario de asentimiento. Previsiones como esta coinciden con lo establecido en la Declaración de Helsinki de la Asociación Médica Mundial cuando establece que en el caso de incapacidad legal, el consentimiento informado debe obtenerse del tutor legal de conformidad con la legislación nacional, y que asimismo cuando el menor de edad está de hecho capacitado para otorgar su consentimiento, debe obtenerse además del consentimiento de su representante, el asentimiento del menor".

d) Diseño de aplicaciones

La Disposición 18/2015 de la DNPDP

La Disposición 18/2015 de la DNPDP, denominada "Guía de buenas prácticas en privacidad para el desarrollo de aplicaciones", señala: "Uso de aplicaciones por niños. Si tu aplicación puede ser usada por niños o adolescentes, deberás procurar un cuidado especial. Se trata de un grupo que hace un uso intensivo de la tecnología, que la saben manejar, pero que por su edad pueden carecer de la reflexión crítica necesaria para identificar los peligros que el mal uso de su información personal puede aparejar. Son una población vulnerable, y por lo tanto, será necesario que incorpores salvaguardas especiales para resguardarlos. - Limita al máximo el tipo y la cantidad de información que sobre ellos recolectas. - Contempla estrictas medidas de seguridad

sobre la información que necesariamente debas recabar. - Evita compartir información personal de menores con terceros. - Bríndales información adecuada a su nivel de comprensión sobre el uso responsable de sus datos y alerta sobre los peligros que se relacionan a una mala utilización. - Siempre que corresponda, obtén el consentimiento de sus padres. Establece mecanismos de resguardos para mantenerlos informados acerca de los usos que se hacen de la información personal de los menores".

e) Otros ámbitos

Promociones, concursos y videovigilancia

La normativa argentina no prohíbe la realización de promociones y concursos dirigidos a menores, pero tampoco las exceptúa del consentimiento de sus representantes legales, por lo cual sólo serán lícitas si cuentan con dicho consentimiento.

No existe normativa específica sobre videovigilancia de menores, por lo que esta materia se rige por las disposiciones generales aplicables al caso (Ley 25.326 y Disposiciones DNPDP 10/2015 y 20/2015).

2.4. Datos de menores en Internet

Propuesta normativa de la DNPDP

No existe una normativa específica que tutele el tratamiento de datos personales de menores en Internet, por lo que esta materia se rige por la normativa nacional arriba expuesta y en consecuencia por la necesidad del consentimiento parental o del tutor para los menores de 18 años como principio general.

A fin de cubrir dicha falencia y mejor incorporar la Convención sobre los Derechos del Niño, la DNPDP diseñó un proyecto de reforma de la Ley 25.326, que prevé una regulación específica para los datos de menores. Nuestra propuesta es la siguiente:

> ARTÍCULO 18. — (Tratamiento de datos de menores). 1. En el tratamiento de datos concernientes a un niño, niña o adolescente, se deberá privilegiar la protección del interés superior de éstos, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral. 2. Se considerará válido el consentimiento de un niño, niña o adolescente cuando se aplique al tratamiento de datos vinculados a la utilización de servicios de la sociedad de la información específicamente diseñados y aptos para ellos. En estos casos, el consentimiento se considerará lícito cuando el niño, niña o adolescente tenga como mínimo trece (13) años. Si el niño es menor de trece (13) años, tal tratamiento únicamente se considerará lícito si el consentimiento lo otorgó el titular de la responsabilidad parental o tutela sobre el niño, y solo en la medida en que se dio o autorizó. 3. El responsable del tratamiento deberá realizar esfuerzos razonables para verificar en tales casos que el consentimiento fue otorgado por el titular de la responsabilidad parental o tutela sobre el niño, niña o adolescente, teniendo en cuenta sus posibilidades para hacerlo.

Asimismo, a los fines de tutelar los derechos del menor que puedan verse afectados a través de Internet, la DNPDP posee como antecedente de interés las facultades que esgrimió como Órgano de Control (a fin de ordenar a un buscador el bloqueo o supresión de información de menores) en el caso del Dictamen 3/11, al que nos remitimos. Se tuvo en cuenta para emitir dicho dictamen que determinar la aplicación de protección de datos personales a Internet requiere deslindar el ejercicio de la libertad de expresión de la actividad que implica el tratamiento de datos personales. La Ley 25.326 en principio no resulta aplicable a la libertad de expresión, pues implicaría una censura previa, prohibida por nuestra Constitución Nacional. Como todo derecho humano, la libertad de expresión no puede ser limitada en su ejercicio a través de un órgano administrativo o norma de rango reglamentaria, sino que requiere de sentencia fundada en ley. Por tales motivos, afectar o limitar los contenidos de los sitios en Internet, en la medida que impliquen el ejercicio de la libertad de expresión, en principio no será objeto de la protección de los datos personales, y por lo tanto requerirá de intervención judicial para su limitación, salvo que la actividad o contenido del sitio en Internet pueda calificarse como tratamiento de datos personales. En tal sentido, al ser el buscador en Internet un medio técnico de tratamiento de datos personales, los resultados que brinde (luego del procesamiento de los datos personales incorporados por el usuario), o sea los datos personales que difunda, resultarán alcanzados y tutelados por la Ley 25.326 cuando resulten perjudiciales a los derechos de sus titulares.

El Dictamen 3/11 de la DNPDP sobre buscadores

Por su parte, en el Dictamen 3/11, la DNPDP resolvió que "los buscadores realizan un tratamiento de datos que les permite relacionar los datos contenidos en una página en Internet con el dato de la búsqueda introducida por el usuario, utilizando como intermediario un índice pre elaborado por el mismo buscador. Al respecto, cabe resaltar que la incorporación del nombre del denunciante o su hija en el buscador de Google Inc. permite acceder a información personal que resulta claramente lesiva de su intimidad (tutelada en el art. 1071 bis. y el art. 1º Ley Nº 25.326), con el agravante de referirse también a una menor (cuyos derechos son particularmente protegidos por la Constitución nacional en los Tratados Internacionales referidos a los derechos del niño), y que asimismo, por su pérdida de vigencia (año 2008 sin posterior actualización), antes que informar, el resultado estigmatiza, operando más como un banco de datos de información histórica que como divulgador de noticias. Por tales motivos, y considerando que el art. 1º de la Ley Nº 25.326 define como su objeto la protección integral de los datos personales que sean objeto de tratamiento por distintos medios técnicos, la DNPDP de Protección de Datos Personales entiende que en atención al resultado que brinda en el presente caso el buscador […], dicho tratamiento de datos resulta alcanzado por el art. 1º de la Ley Nº 25.326 […]. Pero tal solicitud y a fin de preservar también los derechos de su hija Valentina, tema que hace al espíritu de su pretensión, va de suyo que debe ir acompañada de la supresión de la información correspondiente a la menor, cuestión que corresponde que la DNPDP asuma de oficio. Ello, teniendo

en cuenta que nuestro país ha ratificado y otorgado jerarquía constitucional, conforme a lo dispuesto en el artículo 75, inciso 22, de la Constitución Nacional, a la Convención de los Derechos del Niño, la que les reconoce, entre otros, el derecho a la privacidad. Este derecho es un aspecto esencial en cuanto a que ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, domicilio, correspondencia, ni ataques a su honra o reputación. "Estos derechos y libertades son imprescindibles para el desempeño de los menores, que deben disfrutar de los derechos humanos con los mismos alcances que los adultos", encontrándose los Estados Partes "obligados a adoptar todas las medidas legislativas, administrativas, sociales y educativas apropiadas para proteger a los niños contra todo abuso físico, mental, descuido, trato negligente, malos tratos,…". En consecuencia, entiende la DNPDP que resulta procedente, aplicar la Ley Nº 25.326 al tratamiento que realiza el buscador … y requerirle la supresión o bloqueo de cualquier resultado relativo a los enlaces (links) denunciados en estas actuaciones, en cuanto responda a una búsqueda bajo el nombre del titular del dato "xxx", "xxxzz" o "zzzz", o "yyyyyy" o "yyyzzzz", al afectar el honor e intimidad de sus titulares con motivo de dicho tratamiento en los términos del art. 1º de la Ley Nº 25.326 y 43 de la Constitución Nacional".

2.5. Ejercicio por los menores de su derecho a la protección de datos

Normativa relevante del Código Civil

No se prevé en nuestra normativa de protección de datos personales y acción de habeas data una reglamentación específica para el ejercicio de los derechos de los menores, por lo que esta materia se rige por las disposiciones generales, de entre las cuales destacamos los siguientes preceptos del Código Civil y Comercial de la Nación:

> Artículo 26.- La persona menor de edad tiene derecho a ser oída en todo proceso judicial que le concierne así como a participar en las decisiones sobre su persona.
>
> Artículo 30.- Persona menor de edad con título profesional habilitante. La persona menor de edad que ha obtenido título habilitante para el ejercicio de una profesión puede ejercerla por cuenta propia sin necesidad de previa autorización. Tiene la administración y disposición de los bienes que adquiere con el producto de su profesión y puede estar en juicio civil o penal por cuestiones vinculadas a ella.
>
> Artículo 677.- Representación. Los progenitores pueden estar en juicio por su hijo como actores o demandados. Se presume que el hijo adolescente cuenta con suficiente autonomía para intervenir en un proceso conjuntamente con los progenitores, o de manera autónoma con asistencia letrada.
>
> Artículo 679.- Juicio contra los progenitores. El hijo menor de edad puede reclamar a sus progenitores por sus propios intereses sin previa autorización judicial, si cuenta con la edad y grado de madurez suficiente y asistencia letrada.
>
> Artículo 683.- Presunción de autorización para hijo mayor de dieciséis años. Se presume que el hijo mayor de dieciséis años que ejerce

algún empleo, profesión o industria, está autorizado por sus progenitores para todos los actos y contratos concernientes al empleo, profesión o industria. En todo caso debe cumplirse con las disposiciones de este Código y con la normativa especial referida al trabajo infantil. Los derechos y obligaciones que nacen de estos actos recaen únicamente sobre los bienes cuya administración está a cargo del propio hijo.

Artículo 684.- Contratos de escasa cuantía. Los contratos de escasa cuantía de la vida cotidiana celebrados por el hijo, se presumen realizados con la conformidad de los progenitores.

2.6. Herramientas y recursos de la autoridad en materia de menores

El Programa "Con Vos en la Web"

La DNPDP impulsó en el año 2012 el Programa "Con Vos en la Web"[5], creado en el ámbito de las actividades de capacitación, promoción y difusión de la DNPDP (Resolución MJDH 1990/12). Este Programa busca crear un espacio propicio para generar la comunicación, la difusión, la información, el asesoramiento y la participación de los diferentes grupos interesados dentro de la comunidad en temas vinculados con la protección de los datos personales de niñas, niños y adolescentes ante las nuevas tecnologías de la información y la comunicación. En ese sentido, su misión es contribuir a promover la importancia de la protección de sus datos personales como mecanismo de protección de su honor, intimidad y privacidad. Desde este programa se busca dar a conocer a un grupo de usuarios específico cuáles son las ventajas y desventajas en materia de seguridad y privacidad que presentan las nuevas tecnologías. Para alcanzar los objetivos de este programa la DNPDP desarrolla materiales de concientización y promoción de los derechos tanto para jóvenes como para adultos. Algunos de estos materiales se han realizado en colaboración con EDUC.AR, otros con UNICEF, y otros han sido de creación propia. Finalmente, cabe destacar que "Con Vos en la Web", en el marco de las actividades de capacitación genera espacios de educación a través de cursos tales como el de "Protección de Datos Personales en Internet" o el de "Adultos y Chicos en la web", que han sido implementados para docentes y padres a través de las plataformas virtuales de EDUC.AR y del CAMPUS VIRTUAL PDP. También se desarrollan charlas o cursos presenciales en todo el territorio nacional.

Durante 2016 el programa "Con Vos en la Web" continuó su actividad y se abocó a renovar sus contenidos y generar nuevos espacios de comunicación:

- Reestructuración de contenidos y adaptación de la imagen del sitio "Con Vos en la Web" al nuevo manual de estilo 2016/2017 con las nuevas premisas para la comunicación en general.
- Reestructuración de capacitaciones. Las capacitaciones presenciales se realizaron a nivel masivo para una mayor llegada del mensaje. La DNPDP ofreció charlas y diversos talleres en PLANIED (Plan Nacional Integral de Educación Digital), iniciativa del Ministerio de Educación y Deportes de la Nación dirigido a la comunidad educativa. A su vez participó del Encuentro

[5] http://www.convosenlaweb.gob.ar/

Educar, en la ciudad de Guaymallén, Mendoza, del Primer Encuentro de "Innovación Pedagógica en Educación Digital", con el fin de abordar aspectos relativos a la inclusión y el uso seguro de las TIC en las aulas, en la Universidad Nacional de Córdoba en el marco de la segunda edición de "Internet Recorre" (IR) donde se dictaron diversos talleres y brindo una jornada de capacitación sobre "Protección de Datos Personales" en la delegación de La Plata. El alcance de estas capacitaciones superaron los 600 asistentes. Asimismo, se realizó un gran número de capacitaciones virtuales con la intención de formar nuevos formadores.

- Formador de Formadores: tiene como objetivo capacitar a docentes para que enseñen a los alumnos cómo proteger sus datos personales, ya sea dentro del ámbito tecnológico como en lo social. El eje central fue capacitar a docentes de manera virtual y en algún caso presencial, para brindarles materiales para poder trabajar en clase. La idea que subyace a este proyecto es generar un efecto contagio y que la capacitación no se limite a las cuatro paredes del aula sino que los docentes y alumnos puedan replicar los conocimientos por fuera, a otros compañeros y a los padres.
- En el transcurso de 2016 se incrementaron los suscriptores del canal de YouTube como los seguidores y las visitas de Google+; también se amplió la cantidad de seguidores en Twitter e Instagram, lo que manifiesta un marcado interés en torno al programa.

Los materiales del programa disponibles durante 2016 fueron los siguientes:

- 1 Video animado "Zamba te da consejos sobre los riesgos a la hora de hablar con desconocidos".
- 1 Video animado "Zamba te da consejos sobre Discriminación Web".
- 1 Video Discriminación Web: si a nadie le gusta, el Ciberbullying desaparece.
- 1 Video Padres en la Web: acompañamos a los chicos en el mundo digital.
- 7 videotutoriales: Configuración rápida de la privacidad en Facebook; Cómo crear listas en Facebook; Cómo denunciar un perfil en Facebook; Cómo configurar la privacidad en Whatsapp para Android; cómo configurar Facebook para Android; Cómo configurar la privacidad de Instagram para Android; Configuración de la privacidad en los mails de Gmail y Google Plus.
- Boletín de Con Vos en la Web para docentes.
- Documento en PDF con recomendaciones para subir fotografías a las Redes Sociales.
- Infografía para padres.
- Infografía para docentes.
- Modificaciones para navegación más actualizada en sitio web.
- Actualización de Guía de Grooming, en conjunto con Unicef.

– Actualización de la Guía de Cyberbullying.
– Guía de Reputación Web.
– Guía sobre Sexting.
– Guía de amenazas en Internet.
– Guía sobre uso seguro de WI-FI.
– Guía para el cuidado de los datos personales de l@s chic@s - Escuelas 2.0.
– La Ley 25.326 para chicos en su versión para niñ@s.
– Consejos para proteger tus Datos Personales.

3. CHILE

Los datos de menores como datos sensibles

Si bien en la definición de datos sensibles contenida en la Ley N° 19.628, sobre Protección de la Vida Privada, no se mencionan expresamente los datos relativos a los menores de edad, para efectos de determinar la normativa que les resulta aplicable y que rigen su tratamiento, éstos constituyen datos sensibles. El tratamiento de los datos concernientes a un menor de edad debe realizarse en consonancia con el principio del interés superior del niño, exigiendo niveles más estrictos de seguridad, como ocurre con los datos sensibles.

La divulgación de estos últimos datos se rige por lo dispuesto en el artículo 10 de la Ley N° 19.628, según el cual el tratamiento de los datos sensibles no está permitido, salvo que una ley lo autorice, exista consentimiento expreso del titular, o se trate de datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

El interés superior del niño

Por su parte, conviene recordar el principio del interés superior del niño establecido en el artículo 3.1 CDN (I, 1). Con fundamento en él, el Consejo para la Transparencia estableció que los datos personales de los menores merecen protección frente a las falencias de la legislación en la materia, especialmente teniendo en consideración que uno de los principios es el del "interés superior del niño".

Reglas de consentimiento del Código Civil

La titularidad de los datos de los menores de edad pertenece a éstos, los que son, sin embargo, incapaces. Por lo tanto, el consentimiento debe prestarlo por quien o quienes ostenten su representación legal. Al respecto, deben tenerse en consideración las siguientes normas del Código Civil:

a) El artículo 224 dispone que "Toca de consuno a los padres, o al padre o madre sobreviviente, el cuidado personal de sus hijos".
b) El artículo 225 señala que "Si los padres viven separados podrán determinar de común acuerdo que el cuidado personal de los hijos corresponde al padre, a la madre o a ambos en forma compartida". El inciso 2° dispone que "El cuidado personal compartido es un régimen de vida que procura estimular la corresponsabilidad de ambos padres que viven separados, en la crianza y educación de los hijos comunes". A falta del acuerdo del inciso 1°, los hijos continuarán bajo el cuidado personal del padre o madre con quien estén conviviendo. El

inciso 4° de la norma agrega que "cuando las circunstancias lo requieran y el interés superior del hijo lo haga conveniente, el juez podrá atribuir el cuidado personal del hijo al otro de los padres, o radicarlo en uno solo de ellos, si por acuerdo existiere alguna otra forma de ejercicio compartido".

c) El artículo 224 indica que "La patria potestad será ejercida por el padre o la madre o ambos conjuntamente, según convengan en acuerdo […]. A falta de acuerdo, toca al padre y a la madre en conjunto el ejercicio de la patria potestad". Por su parte, el artículo 245 señala que "Si los padres viven separados, la patria potestad será ejercida por aquel que tenga a su cargo el cuidado personal del hijo, o por ambos, de conformidad al artículo 225 / Sin embargo, por acuerdo de los padres, o resolución judicial fundada en el interés del hijo, podrá atribuirse la patria potestad al otro padre o radicarla en uno de ellos si la ejercieren conjuntamente. Además, basándose en igual interés, los padres podrán ejercerla en forma conjunta".
d) Por su parte, el artículo 43 establece que "Son representantes legales de una persona, el padre o la madre, el adoptante y su tutor o curador". De este modo, y dado que se permite una patria potestad compartida, ambos padres pueden representar legalmente al hijo no emancipado.

Doctrina del Consejo para la Transparencia sobre datos médicos de menores

En base a las citadas normas legales, el Consejo para la Transparencia ha resuelto que "Si no es posible determinar o no se ha acreditado por el solicitante que detenta la calidad de representante legal del menor respecto del cual efectúa su requerimiento, conforme la jurisprudencia de este Consejo habrá de determinar el tipo de información que se requiere. En efecto, a partir de lo resuelto en las decisiones de amparos Roles C230-15 y C390-15, en el caso de requerirse la ficha clínica del menor por uno de los padres, deberá acreditarse por estos últimos, que detenta la representación legal conforme lo exige el artículo 13 de la Ley N° 20.584, que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención de salud. Sin embargo, tal exigencia no es necesaria que concurra cuando se requiere otro tipo de antecedentes o información por parte de los padres en relación a sus hijos. Se arribó a dicha conclusión considerando que en el primer caso fue el propio legislador quien estableció una vía excepcional para otorgar el acceso a la información relativa a las fichas clínicas, lo que no acontece respecto a otro tipo de información o antecedentes que se pida"[6].

De esta forma, tratándose de antecedentes de menores de edad, distintos a una ficha clínica, el Consejo ha resuelto que no podrá impedirse a los padres que puedan acceder a dicha información. Lo anterior, ya que son precisamente los padres quienes detentan la patria potestad del menor y, consecuentemente, su representación legal. Lo anterior, también, en base a lo señalado por la Convención Internacional de Derechos del niño, niña y adolescente.

[6] Así se señaló por este Consejo, en Oficio N° 179, de 12 de enero de 2016, por el cual se evacuó un pronunciamiento requerido por la División Jurídica del Ministerio de Educación.

Acceso a los datos de los menores a progenitores, incluso sin patria potestad

En la decisión de amparo Rol C1196-11, el Consejo resolvió que ambos padres tienen el deber de crianza, el que va más allá del cuidado personal y que no sólo corresponde a quien tenga la patria potestad, el cual supone un conocimiento de las condiciones en que se encuentra el menor, de manera que le presten un apoyo adecuado en su proceso de desarrollo. En razón de ello y por aplicación del principio del interés superior del niño, estos últimos pueden desarrollarse en mayor medida si ambos padres están al tanto de su situación, pues así podrán cooperar de mejor manera para que obtengan su mayor realización espiritual y material posible. En definitiva, y conforme concluyó este Consejo en el oficio citado más arriba, procede la entrega de información relativa a menores de edad "a aquel de los padres que incluso no ha acreditado detentar el cuidado personal a que obliga la legislación civil, en tanto se entiende que en su calidad de padre y responsable de la crianza y educación de sus hijos puede acceder a dicha información".

Por otra parte, a propósito de la discusión en el Congreso Nacional de un proyecto de ley de Sistema de Garantía de los Derechos de la Niñez, este Consejo sugirió, en una minuta enviada a la Comisión de Familia de la Cámara de Diputados, que se establezca expresamente que los datos personales de los menores de edad son datos sensibles y que, por lo tanto, éstos deben ser especialmente protegidos.

4. COLOMBIA

4.1. Normativa

Derechos de los niños en la Constitución y en el Código de Infancia y Adolescencia

El artículo 44 de la Constitución Política de Colombia, que relaciona los derechos fundamentales de los niños, establece que "la familia, la sociedad y el estado tienen la obligación de asistir y proteger al niño para garantizar su desarrollo armónico e integral y el ejercicio pleno de sus derechos". Esta norma, además, preceptúa que los derechos de los niños prevalecen sobre los derechos de los demás.

De otra parte, el artículo 33 del Código de Infancia y Adolescencia (Ley 1.098/ 2006) señala que "Los niños, las niñas y los adolescentes tienen derecho a la intimidad personal, mediante la protección contra toda injerencia arbitraria o ilegal en su vida privada, la de su familia, domicilio y correspondencia. Así mismo, serán protegidos contra toda conducta, acción o circunstancia que afecte su dignidad". Por tanto, es claro que en Colombia los niños, niñas y adolescentes son sujetos de especial protección y, por tanto, las entidades del Estado, la familia, las instituciones educativas y la sociedad, en general, deben intervenir en la protección de sus derechos y en el crecimiento y realización personal de cada uno de ellos.

Ya en el tema específico de la protección de datos personales, el artículo 7 de la Ley 1.581/2012, conocida como el Régimen General de Protección de Datos Personales, señala que en el tratamiento de la información de los niños, niñas y adolescentes se debe asegurar el respeto a sus derechos prevalentes y prohíbe el tratamiento de los

Prohibición general de tratamiento de datos de menores en la ley y excepciones según la Corte Constitucional

datos personales de los menores de edad, salvo aquellos que sean de naturaleza pública. Además, señala que es tarea del Estado y de las entidades educativas capacitar a los tutores o representantes legales de los menores sobre los riesgos a los que se enfrentan estos respecto del tratamiento indebido de sus datos personales y proveer de conocimiento acerca del uso responsable y seguro que deben hacer los niños, niñas y adolescentes de sus datos personales y de su derecho a la privacidad. Como se observa, el texto legal incluye una prohibición del tratamiento de los datos personales de los menores a excepción de la información que se considera pública; sin embargo, tal prohibición no es absoluta; así lo expresó la Corte Constitucional colombiana en la sentencia C-748 de 2011, de análisis de exequibilidad de la Ley 1581/2012:

> Esta sala observa que la interpretación del inciso segundo, no debe entenderse en el sentido de que existe una prohibición casi absoluta del tratamiento de los datos de los menores de 18 años, exceptuando los de naturaleza pública, pues ello daría lugar a la negación de otros derechos superiores de esta población como el de la seguridad social en salud, interpretación ésta que no se encuentra conforme con la Constitución. De lo que se trata entonces, es de reconocer y asegurar la plena vigencia de todos los derechos fundamentales de esta población, incluido el habeas data. […]. En definitiva, el inciso segundo del artículo objeto de estudio es exequible, si se interpreta que los datos de los niños, las niñas y adolescentes pueden ser objeto de tratamiento siempre y cuando no se ponga en riesgo la prevalencia de sus derechos fundamentales e inequívocamente responda a la realización del principio de su interés superior, cuya aplicación específica devendrá del análisis de cada caso en particular.

En ese sentido, el Decreto 1.074/2015[7] incluye los requisitos especiales para el tratamiento de datos personales de niños, niñas y adolescentes como son: que el tratamiento responda y respete el interés superior de los niños, niñas y adolescentes y que se asegure el respeto de sus derechos fundamentales.

Obligaciones de distintos sujetos en el tratamiento de datos de menores

El mencionado Decreto indica también que si se cumplen los anteriores requisitos, el representante legal del menor otorgará la autorización para el tratamiento de su información previo ejercicio de su derecho a ser escuchado y que la opinión del menor será valorada teniendo en cuenta su madurez, autonomía y capacidad para entender el asunto. Señala también este Decreto que todos los Responsables y Encargados del tratamiento de información de menores de edad deben velar por el uso adecuado de esos datos y que la familia y la sociedad deben velar porque estos sujetos cumplan las obligaciones y principios establecidos en la Ley 1.581/2012. Ahora bien, el artículo 7 de esta última incluye también una obligación para el Gobierno Nacional de reglamentar la materia en lo atinente a la capacitación tanto a padres, tutores, representantes legales, como educadores y personal administrativo de las instituciones educativas en materia de

[7] Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo y recopila el Decreto 1377 de 2013 por medio del cual se reglamenta parcialmente la Ley 1581 de 2012.

protección de datos personales de los menores de edad y sobre los riesgos a los que se ven expuestos los menores por la difusión no controlada de su información personal; razón por la cual la Superintendencia de Industria y Comercio elaboró un proyecto de decreto reglamentario para presentarlo al Gobierno Nacional con el fin de garantizar que toda la comunidad educativa y los padres de familia tomen conciencia sobre la necesidad de proteger la información de los menores de edad contra accesos no autorizados y usos abusivos que pongan en riesgo la vida e integridad de los niños, niñas y adolescentes.

4.2. El consentimiento del menor para el tratamiento de sus datos personales

Necesaria autorización de los representantes del menor en el tratamiento de sus datos

Como se mencionó anteriormente, la legislación en Colombia considera los datos de los menores de edad como una categoría especial de datos personales y prohíbe su tratamiento, a excepción de la información pública. Sin embargo, la jurisprudencia señaló que tal prohibición no puede ser absoluta pues de esa manera se podrían afectar otros derechos de los menores como la educación, la salud o incluso la vida. Es por esa razón que el Gobierno Nacional reglamentó lo relacionado con el tratamiento de información personal de los menores y señaló específicamente que será posible tratar sus datos personales siempre respetando sus derechos y cuando dicho tratamiento tenga por finalidad la protección de los menores o el ejercicio de sus derechos prevalentes e indicó taxativamente que son los padres, representantes legales o tutores quienes autorizarán tal tratamiento. Además, especificó que se tendrá en cuenta la opinión del menor, siempre valorando previamente su madurez, autonomía y capacidad para entender el asunto.

4.3. Ámbitos problemáticos

Sin normativa sobre menores morosos

La normativa en Colombia regula el tratamiento de datos personales de menores en general y existen ámbitos en los que no hay disposiciones particulares, como es el de los reportes negativos de información respecto de moras en las que incurren los menores de edad que tienen capacidad para celebrar contratos, pues la Ley 1.266/2008, que reglamenta la materia, no incluyó nada al respecto ni señaló particularidades especiales para esos casos, de tal manera que, en principio, se aplican las disposiciones generales, sin ninguna consideración o excepción específica.

Proyecto de ley sobre publicidad dirigida a menores

En materia de publicidad dirigida a menores, el 1 de marzo de 2017 en Colombia se radicó, por iniciativa parlamentaria, un proyecto de ley que tiene por objeto "regular la publicidad dirigida a niños, niñas y adolescentes suministrada a través de medios de comunicación masivos digitales o análogos y de campañas de mercadeo directo, incluidas todas las actividades de promoción, publicidad, patrocinio,

distribución y venta" e incluye un listado de conductas que serían reprochables y sancionables en materia de publicidad dirigida a los menores. En especial, el artículo 4 de este proyecto de ley prohíbe, entre otros aspectos:

> e) La recopilación, uso y/o divulgación de los datos personales de menores de edad sin la autorización expresa de sus padres quienes deberán manifestar estar enterados del uso que se dará a la información recabada. No se podrá condicionar la participación de un niño en una actividad lúdica o recreativa a la entrega de un premio o a la entrega de información personal que no sea razonablemente necesaria para participar de esas actividades. En cualquier caso, la autorización por parte de los padres o representantes legales del menor deberá darse de manera separada para cada uso específico y en formatos que faciliten su lectura explicando el fin por el cual se recogerá, usará o revelará la información personal de los menores. La autorización deberá ser clara, detallada, escrita y completa. Todo uso o transmisión a terceros de la información de los menores que no sea autorizada previamente por los padres o representantes legales queda terminantemente prohibida.
>
> f) El uso de cualquier herramienta de geolocalización, recolección de datos o patrones de tráfico web con el fin de dirigir publicidad a niños, niñas y adolescentes. Los proveedores de servicios de internet deberán bloquear los sitios web que realicen estas prácticas.

Guía de la SIC sobre videovigilancia de menores

En relación con los datos recolectados por sistemas de video vigilancia, la SIC publicó el año pasado una guía orientada a los Responsables y Encargados del Tratamiento que capturan información personal en dichos sistemas. En particular, se precisa que para recolectar imágenes de niños, niñas y adolescentes se debe: a) contar con la autorización de los padres o representantes legales y la aquiescencia de los menores, teniendo en cuenta su madurez, autonomía y capacidad para entender el asunto; b) informar a los padres o representantes acerca de la finalidad y uso al cual serán sometidos los datos de los menores y los derechos que les asisten; c) limitar la recolección y demás actividades de tratamiento de acuerdo a lo que resulte proporcional y adecuado en consideración a la finalidad informada; d) garantizar la seguridad y reserva de los datos de los menores; y e) restringir el acceso y circulación de acuerdo con lo establecido en la ley. Se señala también en esa guía que el padre y/o representante legal del menor solo podrá acceder a las imágenes de este y en caso de que se pretenda permitir el acceso o circular imágenes de clases y/o actividades donde aparezcan otros niños, se deberá solicitar la autorización de los padres o representantes de todos ellos.

4.4. Datos de menores en Internet

Considerando el rápido avance de la tecnología y la aparición de nuevas herramientas de conectividad como aplicaciones, juegos y redes sociales en general, la difusión de los datos personales de los menores de edad se hace cada vez más preocupante.

La estrategia "En TIC confío"

En Colombia se hacen esfuerzos conjuntos para proteger a los menores de edad en las redes sociales y, de contera, su información personal. Un ejemplo exitoso ha sido el programa "En TIC confío", una "estrategia de promoción de uso responsable de internet y de las nuevas tecnologías del Ministerio de las Tecnologías de la Información y las Comunicaciones que ayuda a la sociedad a desenvolverse e interactuar responsablemente con las TIC, al tiempo que promueve la cero tolerancia con la pornografía infantil y la convivencia digital"[8]. Dentro de esa estrategia se han desarrollado programas como "Teprotejo" que, en convenio con RedPapaz, una corporación sin ánimo de lucro que aboga por la protección de los derechos de los niños, niñas y adolescentes en Colombia, promueve entre los menores el uso sano, seguro y constructivo de las tecnologías de la información y facilita a la comunidad la presentación en línea de denuncias de conductas relacionadas con los delitos de pornografía infantil, explotación sexual comercial, intimidación escolar, ciberacoso, contenidos inapropiados (violencia, consumo de drogas, sexualidad irresponsable, etc.), venta de alcohol y drogas a menores y maltrato, trabajo y abuso infantil.

4.5. Ejercicio por los menores de su derecho a la protección de datos

Obligaciones de los defensores y comisarios de familia

En relación con el ejercicio de derechos, la ya citada Ley 1.098/2006 señala que corresponde a los defensores de familia y comisarios de familia promover la realización y restablecimiento de los derechos de los menores reconocidos en tratados internacionales, en la Constitución Política y en dicho Código. Añade que, tanto los representantes legales del menor como los mismos menores de edad, pueden solicitar ante el defensor o comisario de familia la protección de sus derechos consagrados en la Carta Política y en el Código de Policía.

Derecho de petición

Adicionalmente, el artículo 13 de la Ley 1.755/2015 señala que todas las personas tienen derecho a presentar peticiones respetuosas ante las autoridades y a obtener una solución completa y de fondo, añadiendo que el ejercicio de ese derecho de petición es gratuito y que no será necesario presentarlo mediante la representación de un abogado o de una persona mayor cuando se trata de menores de edad en relación a las entidades dedicadas a su protección o formación. Así, en Colombia está garantizado el derecho de acceso de los menores a las actuaciones administrativas mediante el ejercicio del derecho de petición y la promoción de actuaciones en pro de sus derechos prevalentes y especiales.

4.6. Herramientas y recursos de la autoridad en materia de menores

Convenios para divulgación

La Superintendencia de Industria y Comercio suscribió un convenio con la corporación "RedPapaz" con el fin de crear espacios de colaboración y ayuda mutua para la divulgación de los programas,

[8] http://www.enticconfio.gov.co/

acciones y eventos que se realicen de manera conjunta o separada en pro de los derechos de los niños, niñas y adolescentes y participa en la mesa de TIC e infancia, organizada por esa corporación junto con el Ministerio de Tecnologías de la Información, el Instituto Colombiano de Bienestar Familiar, las Direcciones de Infancia y Adolescencia de la Policía Nacional, la Unidad de delitos tecnológicos de la DIJIN, la Empresa de Telecomunicaciones de Bogotá y otras empresas privadas, para promover el uso seguro, responsable y constructivo de las Tecnologías de la Información y las Comunicaciones (TIC) en los niños, niñas y adolescentes.

Herramientas digitales de información y denuncia

Desde la página de la Superintendencia, www.sic.gov.co, es posible acceder al link de la estrategia "En TIC confío"[9] donde los ciudadanos pueden conocer los diferentes programas, opiniones e información importante para mejorar en el uso de las tecnologías de la información y donde es posible ingresar al programa "Teprotejo"[10] para denunciar aquellas conductas que afectan a los menores de edad.

Adicionalmente, la SIC adelantó una estrategia de protección de datos personales de niños, niñas y adolescentes y para tal efecto realizó la publicación en redes sociales de la entidad (Facebook – YouTube) de dos videos[11] dirigido a los menores en los que se concientiza sobre la importancia de proteger sus datos personales. Adicionalmente se publicaron imágenes en redes sociales (Facebook – Twitter) enviando mensajes sobre los peligros que pueden correr los menores al exponer su información en Internet.

5. ESPAÑA

5.1. Normativa; consentimiento del menor para el tratamiento de sus datos personales

Aplicación a los menores de la normativa general

Como cuestión previa, se debe señalar que los principios, derechos y garantías de la normativa de protección de datos (LOPD y su reglamento de desarrollo, RLOPD)[12] se aplican íntegramente a los trata-

[9] http://www.sic.gov.co/proteccion-de-datos-personales

[10] http://www.teprotejo.org/index.php/es/

[11] https://www.youtube.com/watch?v=cKK0V0JIvfA.
https://www.youtube.com/watch?v=hy_dmT2oGzU

[12] La normativa más importante sobre protección de datos es la siguiente. *Sobre protección de datos en general*: Constitución (art. 18.4); Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (de aplicación hasta el 24 de mayo de 2018); Reglamento de la Ley Orgánica 15/1999, aprobado por Real Decreto 1270/2007 (de aplicación hasta el 24 de mayo de 2018); Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos (de aplicación hasta el 24 de mayo de 2018); Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, aplicable a partir del 25 de mayo de 2018). *Algunas leyes relevantes sobre sectores concretos*: Ley 41/2002, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; Ley Orgánica 1/1996, de Protección Jurídica del Menor; Ley Orgánica 2/2006, de Educación

mientos de datos personales de menores de edad, por lo que los mecanismos para su protección serían los mismos que para los adultos, si bien el RLOPD incluye ciertas garantías que, dada su vulnerabilidad, están dirigidas a reforzar sus derechos.

El artículo 13 del Reglamento

Es en el RLOPD donde se establece, en su artículo 13 que a continuación se transcribe, la única disposición específica sobre menores, que básicamente tiene que ver con la edad para prestar el consentimiento, si bien también trata de cómo se ha de facilitar la información y de los modos para acreditar la edad o el consentimiento paterno:

> Artículo 13. Consentimiento para el tratamiento de datos de menores de edad
>
> 1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.
>
> 2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos.
>
> No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.
>
> 3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.
>
> 4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Incidencia del Derecho de la Unión Europea

Por su parte, como ya se vio (I, 3), el Reglamento General de Protección de Datos (Reglamento europeo) establece en su artículo 8 una edad mínima de 16 años que los Estados miembros pueden rebajar hasta los 13 años[13]. El Reglamento europeo dedica al tratamiento de datos de los menores su considerando 38 y el artículo 8, aunque también se encuentran referencias en otros artículos[14]. La fijación de

[13] En Estados Unidos, de donde proceden muchos de los servicios que los menores utilizan en Internet, como redes sociales o mensajería instantánea, la edad para prestar el consentimiento en internet es de 13 años, conforme a la Ley de la Privacidad Infantil en Internet *(Children´s Online Privacy Protection Act*, COPPA). Debido a ello, las redes sociales como Facebook, tuvieron que adaptar sus productos para el control de la edad de los que se bajaban la aplicación.

[14] "Considerando 38. Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o

la edad mínima en 14 años proporciona seguridad jurídica y precisa para el ámbito de la protección de datos el principio de madurez que establece el Código Civil.

Problemas de verificación de la edad y del consentimiento

No existen instrumentos eficaces de verificación de la edad real de los menores cuando prestan el consentimiento. El Real Decreto 869/2013, que modifica la normativa sobre el Documento Nacional de Identidad, establece que este, cualquiera que sea la edad del titular, tiene activada la identificación digital y puede ser utilizada. En la práctica, salvo Tuenti en su momento, no es utilizado como instrumento para acreditar la edad por las redes sociales y demás servicios dirigidos a menores en internet.

En cuanto al procedimiento para comprobar de modo efectivo la autenticidad del consentimiento paterno, cabe indicar que el artículo 8 del Reglamento Europeo establece que el responsable del tratamiento hará esfuerzos razonables para verificar que el consentimiento fue dado por los padres teniendo en cuenta la tecnología disponible. Es interesante la regulación de la COPPA norteamericana.

Otro problema es el otorgamiento del consentimiento en el caso de progenitores separados, cuando ambos ostentan la patria potestad sobre sus hijos y no están de acuerdo, así como el acceso a la información, sanitaria y escolar, en esta situación. En el primer caso el conflic-

---

tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños."

"Artículo 8. Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información. 1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años. 2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible. 3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño."

"Artículo 6. Licitud del tratamiento. 1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; […] f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

"Artículo 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios."

to ha de ser planteado ante la jurisdicción correspondiente y, en el segundo ambos progenitores tendrán acceso a la información sobre sus hijos menores de edad siempre que sea en el ejercicio de la patria potestad en beneficio del menor.

5.2. Datos de menores en Internet

Denuncias recibidas en la AEPD sobre datos de menores en Internet

Entre las denuncias que en relación al tratmiento de datos de menores de edad se han presentado a la Agencia cabe citar:

a) Apertura de una cuenta a nombre de un menor en una institución financiera realizada por una guardería, sin el consentimiento de los padres o tutores.
b) Recogida de datos por una página Web que ofrecía participar en la cabalgata de Reyes a menores de 7 a 12 años, sin que se ofreciera la información a la que hace referencia el artículo 5 LOPD ni existiera ninguna opción para solicitar la autorización de los padres o tutores.
c) En un portal de Internet orientado a favorecer el contacto personal entre usuarios, fundamentalmente adolescentes o jóvenes, tratamiento de datos de menores sin consentimiento paterno, entre ellos su dirección electrónica, asociada a una imagen fotográfica y, en algunos casos, al nombre del usuario. Las medidas adoptadas para verificar que los usuarios eran mayores de 14 años no se demostraron eficaces. El sitio web requería una especial diligencia y cuidado para evitar que los datos personales fueran susceptibles de ser utilizados para que usuarios malintencionados pudieran entrar en contacto con personas vulnerables. Tampoco se ofrecía la información que requiere la LOPD.
d) Publicación en un perfil de Facebook de fotografías y datos de profesores en los que se vertían insultos y alusiones de contenido sexual, por parte de una menor de 11 años. Se apercibió al titular de la línea desde la que se creó y actualizó el perfil en Facebook con los datos de los profesores sin el consentimiento de éstos.
e) Publicación en el perfil personal de Facebook, accesible libremente para cualquier usuario de dicha red social, de un vídeo en el que aparecen varios escolares menores de edad que estaban de visita en el zoológico de Madrid y que resultan identificables, sin consentimiento de sus padres o tutores (la denuncia fue presentada por el director del colegio).
f) Campaña de promoción de una entidad que ofrecía regalos y en cuyas bases se establecía que podían participar menores de edad, para lo que se habilitaría una opción para obtener el consentimiento de los padres o tutores accesible a través de la página Web o mediante la descarga de un formulario en el que se requieren los datos personales y su reenvío a la entidad, sin facilitar la información que establece la LOPD ni solicitar el consentimiento de los padres.

g) Publicación de imágenes de alumnos menores de edad en la web de centros educativos y redes sociales sin el consentimiento de los padres.

5.3. Ejercicio por los menores de su derecho a la protección de datos

Regla de necesidad de consentimiento del representante hasta los 14 años

Dado que el consentimiento para el tratamiento de los datos se puede otorgar a partir de los 14 años, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela, los derechos de acceso, rectificación, cancelación y oposición, que son personalísimos, serán ejercitados en el caso de los menores de 14 por sus padres o tutores. Si superan esa edad se pueden ejercitar por ellos mismos o por sus representantes legales.

5.4. Herramientas y recursos de la Agencia Española de Protección de Datos en materia de menores

La protección de los menores, eje prioritario del Plan Estratégico de la AEPD 2015-2019

La Agencia Española de Protección de Datos, en su Plan Estratégico 2015 – 2019, ha establecido la prevención y la concienciación como una de sus líneas de actuación prioritaria para reforzar el derecho a la privacidad y protección de datos de los menores, colectivo que por su vulnerabilidad exige una especial sensibilidad y atención por parte de los poderes públicos. Conforme a este Plan Estratégico, la Agencia despliega esta especial atención a los menores a través de medidas y acciones dirigidas fundamentalmente a fomentar su educación y concienciación sobre el valor de la privacidad, la importancia de la información personal y el uso responsable en Internet, impulsando la colaboración con los distintos actores, públicos y privados, implicados en la protección de los menores con la finalidad de dotar de mayor efectividad a las actuaciones desplegadas.

Para el cumplimiento de este objetivo, las actuaciones que en ejecución del Plan Estratégico se han llevado a cabo han sido las siguientes:

Ampliación y actualización del portal "Tú decides en Internet"

a) Reforma integral del portal específico de la agencia dirigido a los menores, al tratamiento de sus datos y a su privacidad www.tudecideseninternet.es, donde se accede a los materiales y recursos educativos destinados a los menores, los padres y los profesores, así como a información, resoluciones y enlaces de interés. Se mantiene actualizado.

Promoción de la comunicación entre docentes, padres y menores

b) Canal de comunicación con centros educativos, docentes, padres y menores, específico de la Agencia, para potenciar la comunicación entre estos colectivos sobre las cuestiones que afecten al tratamiento de datos de y por menores. A las tres vías de acceso de las que inicialmente dispuso (línea telefónica, de WhatsApp y buzón de correo electrónico) se le han añadido las consultas que a este respecto se reciben a través de la sede electrónica de la Agencia para su atención especializada. Se busca facilitar la comunicación con estos colectivos con el

objetivo de contribuir a resolver las dudas y las cuestiones que les puedan surgir, sirviendo de medida preventiva en la medida que se planteen con carácter previo a su resolución, y para eso es imprescindible establecer vías de comunicación que la favorezcan, sobre todo en colectivos como los menores que son usuarios intensivos de distintos servicios de internet, en particular de las redes sociales, en las que encuentran el cauce natural para expresarse y comunicarse.

Convenio Marco con el Ministerio de Educación; incorporación en los planes de estudio

c) Convenio marco de colaboración con el Ministerio de Educación, Cultura y Deporte, suscrito en octubre de 2015, cuyo objeto es la realización de proyectos y acciones de carácter educativo para la formación y sensibilización de los menores de edad en materia de privacidad y protección de datos en el uso de las TIC, entre otros medios, mediante la elaboración y difusión de materiales y recursos, la formación de profesores y padres, la elaboración de guías para los centros educativos, la convocatoria de premios o la colaboración en acciones formativas.

La colaboración con el Ministerio de Educación está igualmente relacionada con la demanda de inclusión de la educación digital en los itinerarios curriculares, petición que se ve reforzada por las resoluciones de la Conferencia Internacional de Autoridades de Protección de Datos, la última celebrada recientemente en Marrakech, en la que, con carácter prioritario, se aboga por incluirla en los planes y programas de estudio con contenidos que fomenten la creación de una cultura de protección de datos y privacidad, a la vez que se hace un llamamiento para formar a los educadores y se establece un marco internacional de competencias para su enseñanza. En esta dirección, en España se ha adoptado una estructura curricular que incorpora estos contenidos, en el marco de las competencias digitales, que se vienen desarrollando por las distintas administraciones educativas, y para lo que los contenidos, materiales y recursos de la web www.tudecideseninternet.es están a disposición de las administraciones educativas.

Materiales y recursos

d) Materiales y recursos para profesores, padres y alumnos (guías, fichas prácticas). Con la intención de impulsar la formación y concienciación de los más de ocho millones de alumnos escolarizados, la Agencia, durante 2016 y continuando con la línea de colaboración iniciada con la firma del convenio con el Ministerio de Educación, Cultura y Deporte, ha desarrollado y puesto a disposición de la comunidad educativa y demás agentes interesados nuevos materiales y recursos. Se han publicado dos guías dirigidas a los menores de entre 10 y 14 años, franja de edad que se ha considerado clave para su formación digital, con un lenguaje ajustado a su grado de madurez.

La Agencia, consciente de que para una adecuada educación digital de los menores es imprescindible contar con el apoyo de sus padres y profesores, ha dotado a cada guía con una versión dirigida a ellos con el objetivo de servir de ayudar

en la tarea educativa y de fomentar hábitos responsables entre los jóvenes en materia de privacidad y protección de datos. En ella se ofrecen algunas de las claves necesarias para que profesores y padres puedan contribuir a ayudar al menor a desarrollar su identidad digital.

La primera de las guías "No te enredes en internet", para los menores, y "Guíales en internet", para los adultos, incluyen contenidos que van desde explicar a los menores qué son los datos personales y qué información podría obtener un desconocido si se los facilitan, a las consecuencias de publicar o reenviar fotos y vídeos de uno mismo o de terceros sin plantearse las consecuencias. Incluyen también consejos y recomendaciones en temas como el reenvío automático de mensajes, la utilización segura de contraseñas, el comportamiento en grupos de mensajería instantánea, qué hacer para eliminar fotos o vídeos en los que aparece el menor o cómo reaccionar ante el acoso.

La segunda de las guías publicadas "Sé legal en internet", dirigida a los propios menores, y "Enséñales a ser legales en internet", destinada a los padres y profesores, también busca sensibilizar acerca de las graves consecuencias de determinadas conductas realizadas en internet. En las guías didácticas se explica de forma detallada y con ejemplos prácticos cómo una utilización inadecuada de la información personal puede ser no sólo una infracción de la normativa de protección de datos, sino que puede llegar a ser constitutiva de un delito que, en ocasiones, se comete por simple desconocimiento.

La Agencia considera imprescindible que los jóvenes posean información, adaptada a su grado de madurez, acerca de las consecuencias que determinadas conductas online pueden acarrear para ellos mismos, sus familiares y otras personas, ya sea por desconocimiento o una falsa sensación de impunidad o anonimato. Se busca de que los menores reflexionen acerca de cómo se sentirían si, por ejemplo, se difundiera un vídeo en el que aparecen cambiándose de ropa, se comentaran detalles de su enfermedad en una red social, o recibieran amenazas para obligarles a facilitar los datos bancarios de sus familiares. Se explica qué es el ciberbullying, el ciberbaiting, el grooming y el sexting, figuras que incluyen conductas delictivas, y ofrece consejos para evitar ser su objetivo o convertirse en partícipe de las mismas, destacando el mensaje de que no permitan que nadie les acose, que no participen en el acoso a otras personas, ni consientan que se acose a terceros. La versión dirigida a familiares, profesores y personas próximas al menor sirve de complemento a la de los menores y contiene orientaciones y pautas útiles en su labor de educación y formación.

El objetivo es que estas guías se utilicen, tanto en las aulas como en casa, para propiciar un ambiente de concienciación que contribuya a fomentar un uso de internet seguro y respetuoso con los demás y a evitar que los menores puedan come-

ter un delito o que su propia conducta, y sin ser conscientes de ello, favorezca su comisión por terceros. La finalidad es prevenir que los menores se vean involucrados en situaciones de riesgo que en el mundo online, debido al efecto multiplicador de la Red, producen un daño difícil de reparar.

Campañas en televisión y vídeos educativos

e) Campañas en televisión y vídeos educativos. Con el objetivo de llegar al mayor número posible de menores, para lo que la televisión sigue siendo el medio más potente, se ha colaborado con Clan, el canal infantil y juvenil de TVE, para la realización de una campaña de educación digital en el uso responsable de internet y las redes sociales entre los más jóvenes, a través de vídeos protagonizados por los personajes de la serie de ficción "Big Band Clan", que promueven la privacidad como un valor imprescindible a la hora de usar las tecnologías de la información y la comunicación. Los vídeos se emitieron durante todo el verano de 2016 y están accesibles en www.tudecideseninternet.es y en la web de Clan.

En colaboración con el Instituto Nacional de Ciberseguridad (INCIBE) se ha elaborado una guía de privacidad y seguridad en internet, donde mediante 18 fichas independientes entre sí se abordan otras tantas situaciones de riesgo en el uso cotidiano de la Red ofreciendo soluciones concretas para cada caso, junto con vídeos tutoriales sobre cómo configurar la privacidad en Facebook, Twitter, Google +, YouTube, Instagram, Snapchat y WhatsApp.

Igualmente, durante 2016, se ha finalizado la elaboración de una serie de cuatro vídeos educativos con los que se trata de concienciar a los más jóvenes para que utilicen de manera responsable las tecnologías y puedan obtener el mayor provecho de las oportunidades que ofrecen con seguridad. Esta serie de vídeos, que tendrá en las escuelas y las familias el cauce ideal para llegar a los menores, ya está finalizada y serán objeto de presentación próximamente. Es un material con el que se pretende dotar a los profesores y a los padres para facilitarles su labor educativa y atraer la atención de los menores, en el que se tratan cuestiones como:

– La información personal, ¿qué es?, ¿por qué es valiosa?, la importancia de la privacidad online y offline, la identidad digital, cómo borrar información si te arrepientes.
– El uso saludable de internet, el buen uso de redes sociales y la configuración de los perfiles.
– La seguridad en internet.
– Las situaciones de riesgo: ciberbullying, ciberbyting, gromming, sexting.

Talleres y jornadas

f) Talleres y jornadas. Con ocasión de la celebración del Día Europeo de la Protección de Datos, el 28 de enero de 2016, se celebró en la sede de la Agencia una jornada sobre "Menores, privacidad y conductas delictivas" que contó con la presencia de miembros de la comunidad educativa, del Ministerio de Educación Cultura y Deporte, del de Justicia, la Fiscalía, la

Secretaría de Estado de Seguridad y de la Fundación ANAR, y en la que se presentaron las guías "Sé legal en internet" y "Enséñales a ser legales en internet".

Asimismo, la Agencia, con el objetivo de concienciar y formar a las familias y de que dispongan de recursos para educar a sus hijos en el mundo digital, ha organizado un taller para familias que ha sido objeto de grabación y que se está editando para, a través de la web www.tudecideseninternet.es, ponerlo a disposición de las familias y del resto de la comunidad educativa y demás interesados.

Colaboración con otras instituciones

g) Colaboración con las Administraciones educativas. Con base en el convenio suscrito con el Ministerio de Educación, Cultura y Deporte, pues resulta esencial para llegar a los menores.

Se mantienen contactos periódicos con las Administraciones educativas a través de la Comisión General de Educación, en cuyo seno se les ha presentado un marco de conocimientos y habilidades en materia de privacidad y seguridad en el ámbito de las tecnologías de la información y la comunicación, partiendo del adoptado por la Conferencia Internacional de Autoridades de Protección de Datos en su reunión de Marrakech (2016), y se ha participado en jornadas organizadas por las Inspecciones de las Administraciones educativas.

h) Colaboración con la Fiscalía, las Fuerzas y Cuerpos de Seguridad, Ministerio de Justicia y el Instituto Nacional de Ciberseguridad (INCIBE), que son actores clave en la seguridad de los menores en internet y que han colaborado en la elaboración de los contenidos de los materiales publicados.

La colaboración con las Fuerzas y Cuerpos de Seguridad, a través de la Secretaría de Estado de Seguridad, se ha extendido a la participación en diferentes encuentros y a formar a formadores en el marco del Plan Director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos.

Premios y concursos

i) Premios y concursos. La 20ª edición de los Premios de Protección de Datos Personales convocados por la Agencia Española de Protección de Datos incluyó por primera vez un premio a las buenas prácticas educativas en privacidad y protección de datos para un uso seguro de internet, con dos modalidades: una orientada a los centros educativos y otra a personas o entidades que hayan destacado por difundir el uso seguro de internet entre los menores. Este nuevo galardón, encuadrado en las actuaciones previstas en el Plan Estratégico, tiene por objeto premiar la adopción de buenas prácticas que promuevan el conocimiento del derecho fundamental a la protección de datos entre los alumnos de Educación Primaria, Secundaria, Bachillerato y Formación Profesional, y que contribuyan a concienciar a los alumnos sobre el valor de la privacidad y el uso responsable de la información personal que comparten en internet, tanto propia como de terceros. La primera modalidad premia las buenas prácticas llevadas a cabo por centros educativos públicos, concertados y privados y está dotado con

material escolar por valor de 3.000 euros. La segunda modalidad reconoce el compromiso de personas, instituciones, organizaciones y asociaciones, públicas y privadas, que se hayan distinguido de manera destacada en el impulso y la difusión entre los menores de edad del uso seguro de internet, relacionado fundamentalmente con la información personal y con el valor de la privacidad. Este galardón es honorífico y consiste en un trofeo así como, en su caso, la difusión de las iniciativas y proyectos premiados.

Asimismo, la Agencia ha colaborado, junto con el Instituto Nacional de Seguridad (INCIBE), la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN) y la Confederación Española de Asociaciones de padres y Madres de Alumnos, (CEAPA), en el concurso organizado por la Organización de Consumidores y Usuarios (OCU) y Google en el marco de la campaña "Vive un Internet Seguro", lanzado en enero de 2017.

Otras acciones

j) La Agencia Española de Protección de Datos es parte del Grupo de Trabajo de Educación Digital, puesto en marcha para alcanzar los objetivos de la Resolución sobre educación digital para todos, adoptada por la Conferencia Internacional de Autoridades de Protección de Datos en su reunión de Varsovia de 2013.

5.5. Herramientas y recursos de la Autoridad Catalana de Protección de Datos en materia de menores

El Programa de educación digital "Menores, Internet y Tecnologías"

Bajo el nombre "Menores, Internet y Tecnologías: Crecer y convivir en un mundo digital", la APDCAT diseñó en 2014 un programa de educación digital en respuesta al uso cada vez más habitual y precoz de las nuevas tecnologías por parte de los menores en casa, en la escuela o en sus actividades extraescolares.

Según el Informe de la Sociedad de la Información en España 2016, el 62,2 % de los menores de edades comprendidas entre los diez y los quince años dispone de teléfono móvil, el 91,3% ha utilizado el ordenador y el 94,3% ha accedido a Internet en los últimos tres meses. El futuro pasa por un mundo digital, una sociedad digital, y por tanto, la tecnología no será un simple instrumento, sino que irá orientada a formar parte de nuestra realidad. No podemos presuponer que los menores actúan bajo nuestros mismos parámetros, los niños, como siempre ha sido, son niños, y su crecimiento personal y social, se produce hoy, también, en un mundo digital. Su forma de aprender, compartir, relacionarse y expresarse se llevará a cabo por medios digitales, por lo que la APDCAT ha querido acercarse a los menores, a su entorno, a las escuelas, para conocer de primera mano cuáles son sus preocupaciones y cuáles son sus expectativas y compartirlas y debatirlas con sus familias y la comunidad educativa. El objetivo es concienciar a los menores y su entorno sobre la gestión responsable de los datos personales cuando utilizan las tecnologías.

El programa ha sido diseñado en base a tres grandes ejes:

– Visión positiva del uso de internet y de las tecnologías: el punto de partida es considerar que la experiencia digital es constructiva y que favorece el desarrollo positivo del menor en todos los aspectos que forman parte de su personalidad, presente y futura, y en su actitud ante el uso de las tecnologías, que ahora, y ya para siempre, formarán parte de muchas de sus vivencias.
– Proceso reflexivo: queremos conocer qué opinan los menores, cuáles son sus intereses y preocupaciones en relación con el uso de las tecnologías y de internet, partiendo de la base de que para definir unos hábitos digitales saludables conviene escuchar a los menores, creando y compartiendo con ellos orientaciones y consejos y por supuesto guiándolos en todo este proceso de reflexión.
– Acción continuada: si hablamos de sociedad digital, el espacio en el que hay que interactuar no se acaba en el aula, hay que dotar de continuidad las acciones y sumar los resultados ya alcanzados con otras iniciativas de objetivos similares; queremos ir a las aulas, pero también queremos explicar a los adultos que forman parte del entorno de los menores qué hemos hecho en el aula para que puedan reforzar las orientaciones y consejos que se les ha dado.

El Proyecto constaba, en su primera edición, de las siguientes etapas establecidas de acuerdo con los ejes señalados: taller, sesión con los alumnos, reunión con las familias y Congreso. Los profesores organizan un taller preparatorio de la sesión que los voluntarios irán a hacer a las aulas siguiendo las instrucciones facilitadas por la APDCAT. A continuación se lleva a cabo por parte de los voluntarios de la APDCAT la sesión con los estudiantes. La sesión con las familias tenía lugar el mismo día si la escuela lo solicitaba. El objetivo principal de esta iniciativa de la APDCAT, en la que intervienen anualmente unos 3.000 alumnos de toda Cataluña, es concienciar a los menores y su entorno sobre la gestión responsable de los datos personales cuando utilizan las tecnologías e Internet. Por ello, las sesiones finalizan con 5 consejos básicos de comportamiento con el fin de que puedan llevar a cabo un uso saludable de las redes sociales: 1) En internet, hay que evitar el contacto con desconocidos; 2) Debemos vigilar qué información personal publicamos en las redes sociales (donde vivimos, donde estudiamos, nuestras planes de fin de semana, etc.); 3) Debemos pensar dos veces qué fotografías y vídeos publicamos. Una vez publicado se pierde el control sobre esta información; 4) Tengamos cuidado de la información personal de los que nos rodean como si fuera nuestra; 5) Ante una situación de conflicto o que te genera angustia, hay que buscar orientación y apoyo.

En 2015 se llevó a cabo el Congreso que contó con la participación de expertos y de una representación de los menores participantes en el proyecto. El acto fue dirigido por Jordi Gil, presentador de los informativos infantiles "InfoK" de Televisión de Cataluña, convirtiendo el congreso en noticia destacada en el InfoK de ese día, dando

un importante eco mediático al mismo dada la elevada audiencia del programa entre la población infantil en Cataluña.

La APDCAT, en el marco de su colaboración con las autoridades homólogas a nivel europeo, presentó esta iniciativa en la 37ª Conferencia Internacional de Protección de Datos en Ámsterdam. Esta presentación permitió compartir los aprendizajes en torno a la experiencia catalana y valorar su viabilidad y continuidad a nivel europeo.

Acciones internacionales

La APDCAT es miembro del *Working Group on Digital Education*, donde fue invitada a participar por su experiencia en programas de formación en privacidad y protección de datos en el campo de la enseñanza. Durante este año 2016, la APDCAT ha seguido participando en este grupo de trabajo internacional de protección de datos en el entorno educativo, ha colaborado activamente en la elaboración de un kit tutorial, *Training the trainers,* para la formación del profesorado en materia de protección de datos y privacidad. Asimismo, coorganizó y participó con la CNIL y el Gioda, en la conferencia final del proyecto europeo ARCADES en Barcelona, el 4 de marzo de 2016. Este proyecto tenía como objetivo, introducir la privacidad y la protección de datos en las escuelas de la Unión Europea. En el informe de actividad del ejercicio 2015-2016 del *Working Group on Digital Education* se puso de relieve la participación de la APDCAT en diversas actividades como la organización de la conferencia ARCADES y la contribución destacada a las conclusiones del grupo.

La APDCAT aportó también sus observaciones y comentarios a la propuesta de acuerdo para establecer un marco de competencias de enseñanza en materia de privacidad, que se presentó en la 38ª Conferencia Internacional de Autoridades de Protección de Datos, celebrada del 16 al 18 de octubre de 2016 en Marrakech. La Resolución, que se aprobó el 18 de octubre de 2016 en el marco de la 38ª Conferencia Internacional, adopta un marco de competencias a nivel internacional sobre Educación de Privacidad, para promover la integración de módulos de enseñanza en materia de protección de datos y privacidad en los programas de formación del profesorado y programas escolares. En este momento la APDCAT continúa su participación en este grupo de trabajo internacional para definir el programa de trabajo y las próximas acciones en materia de educación digital, tal como se acordó en la sesión cerrada de la 38ª Conferencia Internacional de Autoridades de Protección de datos.

6. MÉXICO

6.1. Normativa

Los derechos del niño y el interés superior de la niñez en la legislación y jurisprudencia mexicanas

El artículo 4 de la Constitución Política de los Estados Unidos Mexicanos señala que "En todas las decisiones y actuaciones del Estado se velará y cumplirá con el principio del interés superior de la niñez, garantizando de manera plena sus derechos. Los niños y las niñas tienen derecho a la satisfacción de sus necesidades de alimentación, salud, educación y sano esparcimiento para su desarrollo integral. Este principio deberá guiar el diseño, ejecución, seguimiento y evaluación de las políticas públicas dirigidas a la niñez. Los ascendientes, tutores y custodios tienen la obligación de preservar y exigir el cumplimiento de estos derechos y principios".

En concordancia con lo anterior, la Ley General de los Derechos de las Niñas, Niños y Adolescentes (LGDNNA) señala que el interés superior de la niñez es un principio rector[15]. En ese sentido, la Suprema Corte de Justicia de la Nación, a través de la Tesis de Jurisprudencia 25/2012 (9 a)[16], ha recordado la doctrina de la Corte Interamericana de Derechos Humanos en cuya virtud "la expresión interés superior del niño […] implica que el desarrollo de éste y el ejercicio pleno de sus derechos deben ser considerados como criterios rectores para la elaboración de normas y la aplicación de éstas en todos los órdenes relativos a la vida del niño". De lo anteriormente expuesto, es posible destacar que el interés superior del menor implica la elaboración de normas y la aplicación de las mismas en todos los órdenes relativos a la vida de los menores, de tal forma que se garantice plenamente el ejercicio de sus derechos.

La Suprema Corte de Justicia de la Nación ha determinado que las instancias y organizaciones públicas o privadas tienen la obligación de observar el interés superior del menor en su actuar, de tal suerte que garanticen la prevalencia de su interés y beneficio, a la vez que sirve como base de referencia cuando varios intereses entran en convergencia[17]. No obstante, el Máximo Tribunal ha acotado que en el ámbito jurisdiccional se ponderarán diversos intereses respecto a una cuestión debatida en torno a los menores, como en el caso de interpretar una norma que pueda afectar directamente uno de sus derechos[18].

Protección de datos de menores en la legislación y jurisprudencia mexicanas

Por lo que respecta a la divulgación de los datos personales de un menor de edad, incluyendo su imagen, el artículo 76 LGDNNA se-

[15] Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGDNNA_041214.pdf. Consultada el 14/03/2017.

[16] Amparo Directo en Revisión 2076/2012. 19 de septiembre de 2012. Cinco votos. Ponente: Guillermo I. Ortiz Mayagoitia. Secretario: Alejandro García Núñez. Disponible en http://sjf.scjn.gob.mx/SJFSist/paginas/DetalleGeneralV2.aspx?id=159897&Clase=DetalleTesisBL

[17] Acción de inconstitucionalidad 2/2010, resuelta por el Pleno de la Suprema Corte de Justicia de la Nación. Consultable en http://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralScroll.aspx?id=22553&Clase=DetalleTesisEjecutorias.

[18] Amparo en revisión 48/2015, resuelto por la Segunda Sala de la Suprema Corte de Justicia de la Nación. Consultable en http://207.249.17.176/segundasala/asuntos%20lista%20oficial/AD-48-2015.pdf.

ñala que las "niñas, niños y adolescentes tienen derecho a la intimidad personal y familiar, y a la protección de sus datos personales. Niñas, niños y adolescentes no podrán ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia; tampoco de divulgaciones o difusiones ilícitas de información o datos personales, incluyendo aquélla que tenga carácter informativo a la opinión pública o de noticia que permita identificarlos y que atenten contra su honra, imagen o reputación". De ello es posible concluir que, por regla general, los datos personales de las niñas, niños y adolescentes no podrán ser objeto de divulgación, incluyendo aquélla que tenga carácter informativo a la opinión pública o de noticia que permita identificarlos y que atenten contra su honra, imagen o reputación.

La Suprema Corte de Justicia de la Nación[19] ha privilegiado la protección de los derechos de la personalidad del menor frente al interés público en la divulgación de su información o imágenes, tal y como a continuación se muestra:

> En la actualidad es factible que un menor de edad pueda ostentar el carácter de figura pública al verse involucrado en un asunto que guarde relevancia pública. Sin embargo, a pesar de que exista un genuino interés público en la divulgación de información o imágenes de dicho menor, el estándar para poder utilizarlas deberá de ser mucho más estricto ya que se tendrá que otorgar una particular preferencia a la protección de los derechos de la personalidad del menor. No obstante lo anterior, la afectación de los derechos de la personalidad se realiza en el momento de la publicación de la información, por lo que la cuestión a determinar para que exista la debida protección legal reforzada es si la persona afectada era menor de edad al momento de la difusión, puesto que en caso contrario no estarán en juego los intereses de ningún menor.

6.2. El consentimiento del menor para el tratamiento de sus datos personales

Regla general de necesidad de consentimiento

Según el artículo 7 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22. Cuando no se actualicen algunas de las causales de excepción previstas en este precepto, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma libre (sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular), específica (referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento) e informada (que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales).

[19] Amparo directo, radicado bajo el número de expediente 3/2011 relacionado con el amparo directo 4/2011, radicado bajo la ponencia del Ministro Arturo Zaldívar.

Consentimiento de menores (remisión)

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil, a las que después nos referiremos. Adelantemos que las personas facultadas para otorgar el consentimiento para el tratamiento de los datos personales de un menor de edad son aquellas que sobre él ejerzan su patria potestad, o bien, ostenten la representación de dicho menor por ministerio de ley o determinación judicial.

Materias no conciliables

De otro lado, el artículo 107 de la Ley, relativo a la conciliación entre las partes, señala que "Queda exceptuado de la etapa de conciliación, cuando el titular sea menor de edad y se haya vulnerado alguno de los derechos contemplados en la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, vinculados con la Ley y el Reglamento, salvo que cuente con representación legal debidamente acreditada".

Contratos realizados por menores

En México son hábiles para contratar todas las personas no exceptuadas en el Código Civil (art. 1798 CC) y entre estas se encuentran los menores de edad, sin que esta incapacidad signifique que no puedan ejercer sus derechos o contraer obligaciones por medio de representantes (arts. 23, 24 y 450 CC). Asimismo, el menor emancipado mediante el matrimonio puede administrar sus bienes, pero para la enajenación, gravamen o hipoteca de bienes raíces necesita de autorización judicial y de un tutor para el caso de negocios judiciales.

Omisión del menor en la regulación sobre ficheros de morosos y contratación laboral

Por lo que se refiere a los "ficheros de morosos", en México no se contempla dicha figura, para referir a las listas de datos con personas y empresas que no cumplieron con sus obligaciones de pago[20]. Se cuenta con el llamado Buró de Crédito, que se rige por las "Reglas generales a las que deberán sujetarse las operaciones y actividades de las sociedades de información crediticia y sus usuarios", y ninguna distinción hacen al tratamiento de los datos cuando se trata de menores de edad.

Según reporta el Instituto Nacional de Estadística y Geografía (INEGI), "En el 2013, en México había 2,5 millones de niños, niñas y adolescentes de 5 a 17 años que realizan alguna actividad económica, y de los cuales el 67% son hombres y el 33% son mujeres"[21], cifras que hacen referencia a la contratación laboral de los menores, indicando que uno de los principales factores por los cuales los menores realizaron algún trabajo económico fueron "porque en sus hogares necesitaban de sus ingresos para poder subsistir, para poder pagar su escuela o para sus propios gastos y poder tener un oficio".

Lo que nos lleva a precisar que la edad límite para que sea consentida la contratación de menores es de 15 años con las limitaciones que establece la ley: así lo prevén los artículos 3, 31 y 123-A-III constitucionales, y los artículos 173 a 180, el 988 y 995 de la Ley Federal del Trabajo. Disposiciones que después de una exhaustiva revisión establecen diversas prevenciones para proteger los derechos del menor

[20] Consultado en http://www.burodecredito.com.mx/glosario.html, el 22/02/2016.

[21] Consultado en http://cuentame.inegi.org.mx/poblacion/ninos.aspx?tema=P, el 22/.02/2016.

pero sin mencionar específicamente nada relativo a la privacidad de sus datos personales.

6.3. Ámbitos problemáticos

a) Medios de comunicación, publicidad e imagen de los menores

Limitaciones a la difusión de datos sobre menores en los medios

Los artículos 77, 78 y 80 de la Ley General de Derechos de Niñas Niños y Adolescentes[22], limitan la divulgación de datos personales de menores en el contexto de medios de comunicación. De esta normativa se desprende:

a) Se considerará violación a la intimidad de niñas, niños o adolescentes cualquier manejo directo de su imagen[23] o datos personales que permitan su identificación en los medios de comunicación, así como medios impresos, o en medios electrónicos, que menoscabe su honra o reputación, sea contrario a sus derechos o que los ponga en riesgo, conforme al principio de interés superior de la niñez.
b) Cualquier medio de comunicación que difunda entrevistas a niñas, niños y adolescentes deberá recabar el consentimiento por escrito o cualquier otro medio, de quienes ejerzan la patria potestad o tutela, así como la opinión de la niña, niño o adolescente.

[22] Artículo 77. Se considerará violación a la intimidad de niñas, niños o adolescentes cualquier manejo directo de su imagen, nombre, datos personales o referencias que permitan su identificación en los medios de comunicación que cuenten con concesión para prestar el servicio de radiodifusión y telecomunicaciones, así como medios impresos, o en medios electrónicos de los que tenga control el concesionario o medio impreso del que se trate, que menoscabe su honra o reputación, sea contrario a sus derechos o que los ponga en riesgo, conforme al principio de interés superior de la niñez.

Artículo 78. Cualquier medio de comunicación que difunda entrevistas a niñas, niños y adolescentes, procederá como sigue: I. Deberá recabar el consentimiento por escrito o cualquier otro medio, de quienes ejerzan la patria potestad o tutela, así como la opinión de la niña, niño o adolescente, respectivamente, conforme a lo señalado en el artículo anterior y a lo previsto en el párrafo segundo del artículo 76 de la presente Ley, y […] No se requerirá el consentimiento de quienes ejerzan la patria potestad o tutela de niñas, niños o adolescentes, cuando la entrevista tenga por objeto que éstos expresen libremente, en el ejercicio de su derecho a la libertad de expresión, su opinión respecto de los asuntos que les afecten directamente, siempre que ello no implique una afectación a sus derechos, en especial a su honra y reputación.

Artículo 80. Los medios de comunicación deberán asegurarse que las imágenes, voz o datos a difundir, no pongan en peligro, de forma individual o colectiva, la vida, integridad, dignidad o vulneren el ejercicio de derechos de niñas, niños y adolescentes, aun cuando se modifiquen, se difuminen o no se especifiquen sus identidades, y evitarán la difusión de imágenes o noticias que propicien o sean tendentes a su discriminación, criminalización o estigmatización, en contravención a las disposiciones aplicables.

[23] Sobre el derecho a la imagen en general, téngase en cuenta también La Ley Federal del Derecho de Autor, y en especial sus arts. 85 a 85, donde se destaca el valor del consentimiento del titular de la imagen: Ley Federal de Derechos de Autor en http://mexico.justia.com/federales/leyes/ley-federal-del-derecho-de-autor/titulo-iv/capitulo-ii/.

c) Los medios de comunicación deberán asegurarse que las imágenes, voz o datos a difundir, no pongan en peligro, de forma individual o colectiva, la vida, integridad, dignidad o vulneren el ejercicio de derechos de niñas, niños y adolescentes, aun cuando se modifiquen, se difuminen o no se especifiquen sus identidades.
d) Se deberá evitar la difusión de imágenes o noticias que propicien o sean tendentes a la discriminación, criminalización o estigmatización de los menores.

Obligaciones de protección

Asimismo, los artículos 66 a 68 LGDNNA mandatan a las autoridades federales, de las entidades federativas, municipales y de las demarcaciones territoriales del Distrito Federal, a que en el ámbito de sus respectivas competencias actúen y protejan a los menores contra los riesgos derivados del acceso a los medios de comunicación y a los sistemas de información, absteniéndose de difundir o transmitir información, imágenes o audios que afecten o impidan objetivamente el desarrollo o que hagan apología del delito. Este mismo criterio lo retoma la Ley Federal de Telecomunicaciones y Radiodifusión, que contiene otras restricciones que pretenden proteger el derecho a la información de las audiencias, como las previstas en los artículos 238, 245 y 256, relativos a la publicidad engañosa o que conlleve a discriminación.

b) Datos de menores tutelados

Aplicación de la normativa general a los menores tutelados

El fenómeno de acompañamiento, por parte de organizaciones sociales de carácter público o privado, de los menores hasta que adquieren autonomía suficiente para valerse por sí solos, independientemente de si únicamente se les proporciona un lecho u otras prestaciones como casa, alimentos, estudios o trabajo, es considerado por el Estado mexicano como asistencia pública, en principio a cargo del Sistema Nacional para el Desarrollo Integral de la Familia (DIF). Sus tareas, como las de cualquier otro organismo (llámese "casa hogar", "albergue", "hospicio") dirigido a la infancia, están reguladas por la Ley General de Prestación de Servicios para la Atención, Cuidado y Desarrollo Integral Infantil, cuyo artículo 11 mandata la observancia de una serie de derechos de los menores[24], sin que entre ellos se contemple la privacidad[25]. Resultan así aplicables las disposiciones ya

[24] Véase el texto completo del artículo 11 referido en el Anexo 1.

[25] No hay normativa específica sobre la protección de la privacidad de los menores en condición de "pobreza", pese a la magnitud de este problema en México. El concepto de exclusión social, tal como se conoce en la Comisión Europea (http://epp.eurostats.ec.europa.eu/tgm/table.do?, consultada el 21/02/2017), no existe en México, donde se habla más bien de pobreza, como categoría que abarca las situaciones existenciales más extremas. Según UNICEF, en México el 44,2% de la población vive en pobreza, 33,7% (36 millones de mexicanos) en pobreza moderada y 10,5% (11,2 millones) en pobreza extrema y los niños, niñas y adolescentes se ven afectados de manera desproporcionada por la pobreza y la privación de sus derechos básicos: el 51,3% de ellos vive en pobreza (un 44,2% de la población mexicana total: https://www.unicef.org/mexico/spanish/17046_17487.htm, consultada el 21/02/2017. Asimismo, en el estudio "Pobreza y derechos sociales de niños, niñas y adolescentes en México" se asevera: "En el caso de la población infantil y adolescente, la asociación

mencionadas de la LGDNNA, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y de la Ley General de Protección de Datos Personales en Posesión de Sujetos Regulados, que establecen un nivel superior de protección para los datos personales sensibles.

c) Promociones y concursos dirigidos a menores

Normas sobre datos de menores en juegos y responsabilidad parental

En México los juegos y sorteos de azar son regulados por la Ley Federal de Juegos y Sorteos y su Reglamento, sin que exista ordenamiento que regule los jurados calificadores de concursos donde, sin que intervenga el azar, la premiación se determine por haberse demostrado alguna capacidad o por la valoración de los miembros de un jurado. En ese contexto, la legislación existente no establece ninguna disposición para proteger la privacidad o los datos personales de los participantes en los mismos (en ocasiones, inclusive obliga la publicación de los nombres de los ganadores), independientemente de que sean adultos o menores, pero sí establece en su Reglamento diversas disposiciones prohibiendo la participación de estos últimos. Nos referimos a los artículos 5 (prohibición de acceso o permanencia a menores)[26], 9 IV (Obligación de advertir que está prohibida la participación de menores)[27] y 142 XVII (Premios a los menores a través de padres o tutores)[28].

De otro lado, el artículo 44 LGDNNA añade que "Corresponde a quienes ejerzan la patria potestad, tutela o guarda y custodia de niñas, niños y adolescentes, la obligación de proporcionar las condiciones de vida suficientes para su sano desarrollo". No obstante lo anterior, dado que en la mayor parte de los casos estos concursos, juegos o sorteos están organizados por particulares a quienes en su caso se les

---

entre pobreza e incumplimiento de derechos es particularmente grave, pues la falta de recursos en los hogares pobres suele estar asociada con situaciones de riesgo específicas para esta población, tales como la desnutrición, el abandono escolar o la falta de acceso a servicios médicos. Estas circunstancias pueden afectar las oportunidades de niñas, niños y adolescentes para desarrollarse en el futuro, pues los efectos de la pobreza son difíciles de remontar e incluso llegan a ser irreversibles. Aunque las carencias descritas no son exclusivas de la población infantil y adolescente, es altamente probable que éstas no sólo les acompañen a lo largo de su vida, sino que sean un factor determinante para perpetuar la transmisión intergeneracional de la pobreza": https://www.unicef.org/mexico/spanish/MX_Pobreza_derechos.pdf, consultada el 21/02/2017.

[26] "Se prohíbe el acceso o permanencia […] a las personas que: I. Sean menores de edad, excepto cuando en compañía de un adulto ingresen a espectáculos en vivo. En ningún caso los menores de edad podrán participar en el cruce de apuestas".

[27] "La publicidad (y propaganda de los juegos con apuestas y sorteos) deberá incluir mensajes que indiquen que los juegos con apuestas están prohibidos para menores de edad".

[28] Son facultades y obligaciones de los inspectores: […] XVII. Evitar la entrega de premios a *menores de edad*, debiendo hacerlo únicamente a sus padres o tutores, previa comprobación de su personalidad mediante los documentos idóneos con los que acrediten esa calidad, así como a través de las identificaciones respectivas. En los casos en que se requiera facturación o escrituración, ésta deberá hacerse a nombre del menor".

entrega una concesión, se observa que generalmente se solicita la intervención de quienes ejercen la patria potestad, atendiendo a lo dispuesto por la LGDNNA, y que cuando se les hace publicidad en los medios, su realización va acompañada de un "Aviso de Privacidad", lo que pone en evidencia la penetración de esta práctica en el ámbito publicitario.

6.4. Datos de menores en Internet

Implicación proactiva del INAI

Evitar las consecuencias de un mal cuidado de los datos personales por parte de sus titulares o de los jurídicamente responsables de su protección, depende del establecimiento de hábitos de autocuidado por parte de sus titulares y de quienes los tratan, costumbres que implican autodominio y criterio[29], comportamientos que por estar fuera del alcance de los menores que navegan en internet y hacen uso de las redes sociales, hacen necesario el desarrollo de políticas públicas que en ocasiones se apoyan en ordenamientos jurídicos que idealmente se espera que cubran todas las situaciones que hipotéticamente podrían considerarse amenazas para los titulares. Los organismos de la sociedad civil y el INAI, más allá de conformarse con el establecimiento de la normatividad en materia de protección de datos y de atenerse a la tipificación vigente de delitos e ilícitos informáticos, periódicamente realizan, de manera proactiva, diversas actividades para ponderar lo más ampliamente posible las medidas que se deben tomar para proteger y educar a los menores en el empleo de las tecnologías.

Reformas en el Código Penal

Así, el pasado mes de diciembre de 2016 se aprobó en la Cámara de Diputados el dictamen que reforma al Código Penal Federal, para tipificar el ciberacoso y acoso sexual, y sancionar la difusión de fotos o videos sexuales sin autorización del afectado[30], que representa la conclusión de una lucha por darles a los menores la protección necesaria en tiempos de internet pues aun cuando ya estaban tipificados los delitos de corrupción de menores (art. 201), pornografía de menores (art. 202), turismo sexual en contra de menores (art. 203 y 203 bis), lenocinio de menores (art. 204), y pederastia (art. 209), no encuadraban conductas realizadas con o a través de las tecnologías desprotegiéndolos contra esos y otros peligros tales como la pornografía infantil, sexting, ciberbullying, secuestros, trata de personas[31], entre otros.

---

[29] Como lo es el pedir más información antes de entregar más datos, o acostumbrarse a pensar antes de escribir y no escribir lo que se piensa, o simplemente, limitar el tiempo de exposición en las redes sociales.

[30] Véase http://www5.diputados.gob.mx/index.php/esl/Comunicacion/Agencia-de-Noticias/2016/12-Diciembre/14/5363-Reforman-diputados-Codigo-Penal-Federal-para-tipificar-el-ciberacoso-y-acoso-sexual-y-sancionar-la-difusion-de-fotos-o-videos-sexuales-sin-autorizacion-del-afectado.

[31] Entendida como el comercio ilegal de personas con propósitos de esclavitud reproductiva, explotación sexual, trabajos forzados, extracción de órganos, o cualquier forma moderna de esclavitud.

6.5. Ejercicio por los menores de su derecho a la protección de datos

Reglas generales sobre la patria potestad

Como quedó apuntado, la legislación de protección de datos personales, para el ejercicio de los derechos ARCO de menores de edad, remite a las reglas de representación dispuestas en el Código Civil Federal. En ese sentido, de conformidad con el artículo 412 del Código Civil Federal, los menores de edad no emancipados se encuentran bajo el estado jurídico de la patria potestad, mientras exista alguno de los ascendientes que deban ejercerla conforme a la ley[32].

Según lo sustentado por el Poder Judicial de la Federación[33], la patria potestad es un estado jurídico que constituye el conjunto de prerrogativas y obligaciones legalmente reconocidas, en principio, al padre y a la madre, parcialmente a los ascendientes, respecto a los hijos menores considerados tanto en sus personas, como en sus patrimonios. Por ende, la patria potestad no sólo constituye un conjunto de prerrogativas a favor de los padres, como la de exigir obediencia y respeto del menor no emancipado y llevar su representación legal, administrar los bienes del menor, sino que es también una obligación en el sentido verdadero del término, a cargo de los padres y a favor de los hijos, respecto de la educación, principalmente, y conservación, asistencia, protección y alimentación, además de obligaciones de naturaleza ético-espiritual, como la dirección, los cuidados y la rectitud de la conducta, de importancia determinante para la subsistencia y desarrollo de los hijos. Ahora bien, el Pleno de la Suprema Corte de Justicia de la Nación ha acotado que la representación legal de los menores corresponde a los que sobre ellos ejercen la patria potestad[34].

Ejercicio por menores de los derechos ARCO

Según el artículo 49 de la Ley, para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO) será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante. El ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

En el ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación. Como se ha señalado, no existen disposiciones expresas en el ámbito federal que regulen el ejer-

---

[32] Véase Código Civil Federal en https://www.oas.org/dil/esp/Art%C3%ADculos%20411%20a%20424%20del%20C%C3%B3digo%20Civil%20Federal%20Mexico.pdf Consulado el 14/03/2017

[33] Razonamiento plasmado en la tesis aislada, Registro: 186501, Novena Época, publicada en el Semanario Judicial de la Federación y su Gaceta, en el Tomo XVI, cuyo rubro es: "PATRIA POTESTAD. LA SUPLENCIA DE LA DEFICIENCIA DE LA QUEJA OPERA A FAVOR DE LOS MENORES, AUNQUE NO SEAN PARTE MATERIAL EN EL JUICIO DE AMPARO. Consultable en http://ius.scjn.gob.mx/SJFSist/Documentos/Tesis/186/186501.pdf.

[34] Al respecto la Tesis Aislada, Registro: 286449, Quinta Época, publicada en el Semanario Judicial de la Federación en el Tomo XI, indica que: "MENORES. Su representación legal toca a los que sobre ellos ejercen la patria potestad". Consultable en http://ius.scjn.gob.mx/sjfsist/Documentos/Tesis/286/286449.pdf.

cicio de derechos ARCO para menores de edad de manera directa. Así, se deberá estar a las reglas de representación y patria potestad previstas por el Código Civil Federal. Bajo ese contexto, de conformidad con el artículo 23 del Código Civil Federal35, la minoría de edad implica una restricción a la personalidad jurídica, y por ello, el ejercicio de los derechos de un menor únicamente podrá ser realizado por medio de un representante.

Reglas sobre el ejercicio de la patria potestad

En concordancia con lo anterior, la minoría de edad, entre otras situaciones jurídicas, implica limitante al ejercicio directo de los derechos por parte de los menores, por ello, y de conformidad con lo establecido en los artículos 412, 413, 414, 424, 425 y 426 del Código Civil Federal, serán los padres quienes ejerzan la patria potestad de sus hijos menores de edad. A su vez, la patria potestad será ejercida sobre la persona menor de edad y los bienes de ésta, conforme a lo siguiente:

> Artículo 412. Los hijos menores de edad no emancipados están bajo la patria potestad mientras exista alguno de los ascendientes que deban ejercerla conforme a la ley.
>
> Artículo 413. La patria potestad se ejerce sobre la persona y los bienes de los hijos. Su ejercicio queda sujeto en cuanto a la guarda y educación de los menores, a las modalidades que le impriman las resoluciones que se dicten, de acuerdo con la Ley sobre Previsión Social de la Delincuencia Infantil en el Distrito Federal.
>
> Artículo 414. La patria potestad sobre los hijos se ejerce por los padres. Cuando por cualquier circunstancia deje de ejercerla alguno de ellos, corresponderá su ejercicio al otro. A falta de ambos padres o por cualquier otra circunstancia prevista en este ordenamiento, ejercerán la patria potestad sobre los menores, los ascendientes en segundo grado en el orden que determine el juez de lo familiar, tomando en cuenta las circunstancias del caso.
>
> Artículo 425. Los que ejercen la patria potestad son legítimos representantes de los que están bajo de ella, y tienen la administración legal de los bienes que les pertenecen, conforme a las prescripciones de este Código.
>
> Artículo 426. Cuando la patria potestad se ejerza a la vez por el padre y por la madre, o por el abuelo y la abuela, o por los adoptantes, el administrador de los bienes será nombrado por mutuo acuerdo; pero el designado consultará en todos los negocios a su consorte y requerirá su consentimiento expreso para los actos más importantes de la administración.

Doctrina de la Suprema Corte de Justicia

En ese sentido, en el orden jurídico mexicano, a nivel federal, no existen disposiciones que reconozcan la posibilidad de que los menores ejerzan directamente algún derecho en relación con sus datos personales. Sirve de sustento a lo anteriormente expuesto, lo establecido por la Suprema Corte de Justicia de la Nación en la tesis jurisprudencial 1a./J. 42/2015 (10 a)[36], respecto de la patria potestad:

---

[35] "La minoría de edad, el estado de interdicción y demás incapacidades establecidas por la ley, son restricciones a la personalidad jurídica que no deben menoscabar la dignidad de la persona ni atentar contra la integridad de la familia; pero los incapaces pueden ejercitar sus derechos o contraer obligaciones por medio de sus representantes".

[36] Disponible en: http://200.38.163.178/sjfsist/Documentos/Tesis/2002/2002848.pdf y consultado por última vez el 14/03/2017.

> PATRIA POTESTAD. SU CONFIGURACIÓN COMO UNA INSTITUCIÓN ESTABLECIDA EN BENEFICIO DE LOS HIJOS. La configuración actual de las relaciones paterno-filiales ha sido fruto de una importante evolución jurídica. Con la inclusión en nuestra Constitución del interés superior del menor, los órganos judiciales deben abandonar la vieja concepción de la patria potestad como poder omnímodo del padre sobre los hijos.
>
> Hoy en día, la patria potestad no se configura como un derecho del padre, sino como una función que se le encomienda a los padres en beneficio de los hijos y que está dirigida a la protección, educación y formación integral de estos últimos, cuyo interés es siempre prevalente en la relación paterno-filial, acentuándose asimismo la vigilancia de los poderes públicos en el ejercicio de dicha institución en consideración prioritaria del interés del menor.
>
> Es por ello que abordar en nuestros días el estudio jurídico de las relaciones paterno-filiales y en particular de la patria potestad, requiere que los órganos jurisdiccionales partan de dos ideas fundamentales, como son la protección del hijo menor y su plena subjetividad jurídica.
>
> En efecto, por un lado, el menor de edad está necesitado de especial protección habida cuenta el estado de desarrollo y formación en el que se encuentra inmerso durante esta etapa vital. La protección integral del menor constituye un mandato constitucional que se impone a los padres y a los poderes públicos.

Conforme a lo anterior, no existe duda de que el menor de edad es titular de derechos. Sin embargo, su incapacidad legal le impide el ejercicio de los mismos de manera directa, recayendo este ejercicio sobre quienes ostentan su patria potestad, o bien, la representación de dicho menor por ministerio de ley o determinación judicial, siempre entendiendo el interés superior del menor como principio rector de su actuación.

6.6. Herramientas y recursos de la autoridad en materia de menores

El portal "Niñ@s INAI"

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, cuenta con un micrositio denominado "Niñ@s INAI", este se encuentra en su portal, accesible con el enlace http://ifaininos.ifai.org.mx/, en donde a través de posters, videos, audios y consejos, se da a conocer a la población infantil y a los padres de familia la importancia de que la información personal en la nuevas tecnologías de la información, este debidamente protegida. Los menores son alertados sobre las prácticas que pueden poner en riesgo su seguridad y la privacidad de sus datos personales, esto a través de juegos, videos, audios, en los cuales se les da a conocer el correcto uso de internet y de las redes sociales, y el provecho que se puede obtener de los mismos.

El Concurso para el Pleno "Niños y Niñas"

Actualmente el INAI está desarrollando el Concurso para ser Comisionado y Comisionada Infantil y formar parte del Pleno Niños y Niñas, el cual tiene como objetivo promover la importancia de la privacidad y protección de datos personales entre los menores de edad, como parte de la campaña de educación cívica para el ejercicio

del derecho de protección de datos personales. Podrán participar menores de edad de 10 a 12 años cumplidos a la fecha de emisión de la convocatoria, de nacionalidad mexicana, que acrediten estar cursando el ciclo escolar vigente en escuelas públicas o privadas. La participación será a través de un video, de 3 a 5 minutos, en el que expongan sus argumentos e ideas con relación a algún tema vinculado con la privacidad y protección de datos personales de los menores de edad. Se elegirán a 7 ganadores, los cuales acudirán a la Ciudad de México a realizar una sesión del Pleno Niñas y Niños, fungiendo como Comisionados Infantiles. En dicha sesión, analizarán un caso práctico que involucre un tema de datos personales de menores de edad. Los ganadores serán premiados con un viaje a la Ciudad de México con todos los gastos pagados y una tableta electrónica.

Proyecto con "Plaza sésamo"

Asimismo, está en desarrollo un proyecto con la asociación civil Plaza Sésamo, para promover el uso seguro y responsable de las Tecnologías de la Información, entre los menores de edad. Los trabajos se recibirán del 13 de marzo al 14 de julio de 2017, para cada categoría se otorgarán premios para el primer, segundo y tercer lugar, consistentes en computadoras, tableta inteligente, material didáctico y diploma. Además para los tres primeros lugares de cada categoría se incluye un viaje con todos los gastos pagados (en compañía del tutor o de un familiar adulto con autorización expresa del tutor), a la sede de la ceremonia de premiación en caso de no radicar en la ciudad donde se lleve a cabo dicho evento.

Concurso de cuentos

Para este año también contaremos con el Primer Concurso Nacional de Cuento Juvenil con el tema "Ciberconvivencia responsable" el cual tiene como objetivo estimular la creatividad y la expresión escrita entre jóvenes estudiantes de educación secundaria y medio superior (preparatoria o equivalente), así como promover el uso responsable de la información personal en las redes sociales. Los trabajos se recibirán del 28 de marzo al 22 de septiembre de 2017, se contará con dos categorías, habrá un primero, segundo y tercer lugar en cada una de ellas, y corresponderá a aquellos escritos que hayan sido mejor evaluados. Los premios serán, diploma, computadora personal, tableta inteligente y material literario¸ Para los tres primeros lugares de cada categoría se incluye un viaje con todos los gastos pagados (en compañía del tutor o de un familiar adulto con autorización expresa del tutor, en caso de ser menores de edad), a la sede de la ceremonia de premiación en caso de no radicar en la ciudad donde se lleve a cabo dicho evento.

Las "Fiestas de la Verdad"

Otra actividad importante son las Fiestas de la Verdad que tienen como objetivo primordial ampliar el conocimiento y ejercicio de los derechos de acceso a la información y de protección de datos personales entre la población y sectores específicos. En estas fiestas el sector infantil resulta de especial relevancia pues la mayoría de las actividades están dirigidas para ellos, como es el caso del Memorama, la Lotería, Serpientes y escaleras, Gol por la transparencia, Tiro con ARCO y muchas otras actividades más. Para este año tenemos programada la realización de 3 Fiestas de la Verdad en tres distintas entidades del país, las cuales se realizan en colaboración con los Órganos Garantes locales y con las autoridades administrativas de la entidad. Es impor-

tante mencionar que debido a la relevancia que tiene el sector infantil en estas ferias en el mes de abril de cada año se realiza una de ellas con el fin de conmemorar el día del niño.

Publicación de cuentos infantiles

Otra actividad de suma relevancia y que está dirigida a nuestros niñas y niños son las publicaciones de cuentos infantiles, en el año 2015 se presentó el titulado "Ina y el Cuervo" que aborda el tema de la importancias en el manejo responsable de los datos personales y para el presente año esta próxima la emisión del cuento "Como ir Ganando Cinco a Cero" que aborda la relevancia en nuestros vida cotidiana de contar con información oportuna y fidedigna (Transparencia y Acceso a la Información Pública) que contribuya a una mejor toma de daciones.

7. PERÚ

7.1. Normativa

Reconocimiento general de los derechos del niño

El artículo 4 de la Constitución Política del Perú de 1993 establece una protección especial al niño de la siguiente manera: "La comunidad y el Estado protegen especialmente al niño, al adolescente, a la madre y al anciano en situación de abandono. También protegen a la familia y promueven el matrimonio. Reconocen a estos últimos como institutos naturales y fundamentales de la sociedad". En esta línea, el artículo IX del Código de los Niños y Adolescentes (Ley 27.337/2000) señala que "En toda medida concerniente al niño y al adolescente que adopte el Estado a través de los poderes Ejecutivo, Legislativo, Judicial, del Ministerio Público, los Gobiernos Regionales, Gobiernos Locales y sus demás instituciones, así como en la acción de la sociedad, se considerará el Principio de Interés Superior del Niño y del Adolescente y el respeto a sus derechos".

Obligaciones de sujetos públicos

Por otro lado, la Autoridad Nacional de Protección de Datos Personales tiene entre sus funciones promover y fortalecer una cultura de protección de los datos personales de los niños y de los adolescentes, coordinar la inclusión de información sobre la importancia de la vida privada y de la protección de datos personales en los planes de estudios de todos los niveles educativos y fomentar, asimismo, la capacitación de los docentes en estos temas (art. 33.6 y 7 LPDP). Asimismo, el Reglamento de la LPDP enfatiza en la obligación de los titulares de bancos de datos personales, especialmente de las entidades públicas, de colaborar con el fomento del conocimiento del derecho a la protección de datos personales de los niños, niñas y adolescentes, así como de la necesidad de que su tratamiento se realice con especial responsabilidad y seguridad.

7.2. El consentimiento del menor para el tratamiento de sus datos personales

Respecto de las manifestaciones de voluntad del menor, el artículo 43 del Código Civil establece como regla la incapacidad absoluta del

Reglas generales de capacidad del Código Civil

menor de 16 años, y por ende la nulidad de sus manifestaciones de voluntad, salvo para los actos determinados por la ley. En esa línea, el artículo 44 señala que en el caso de mayores de 14, cesa la incapacidad a partir del nacimiento del hijo, para reconocer a sus hijos, demandar gastos de embarazo y parto y para demandar y ser parte en los procesos de tenencia y alimentos a favor de sus hijos y en los procesos de filiación extramatrimonial de sus hijos. El mismo precepto califica como relativamente incapaces a los mayores de 16 y menores de 18, estableciendo para este grupo el cese de la incapacidad con el matrimonio o la obtención de un título profesional.

Reglas especiales del Reglamento de la LPDP

Respecto al consentimiento para el tratamiento de datos personales de menores, el artículo 27 del Reglamento de la LPDP establece que "Para el tratamiento de los datos personales de un menor de edad, se requerirá el consentimiento de los titulares de la patria potestad o tutores, según corresponda". En el caso de mayores de 14 y menores de 18, el artículo 28 del Reglamento señala que pueden dar su consentimiento, siempre que la información haya sido expresada en un lenguaje sencillo, compresible por ellos, salvo que la ley exija para su otorgamiento la asistencia de los titulares de la patria potestad o tutela. Asimismo, el artículo 29 de la LPDP señala que no pueden recabarse de un menor datos sobre los demás miembros de su grupo familiar, salvo aquellos datos de identidad y dirección de los padres o de los tutores con la finalidad de obtener el consentimiento a que se refiere el artículo 27.

7.3. Datos de menores en Internet

Problemas abordados por la Autoridad

En el Perú uno de los ámbitos más problemáticos respecto al tratamiento de datos de menores es la falta de consentimiento para la publicación de imágenes de los menores en páginas web, especialmente en los centros de educación. Al respecto, la Autoridad Nacional de Protección de Datos Personales ha fiscalizado a 22 centros educativos desde el año 2014, de los cuales, a la fecha se ha abierto procedimiento sancionador a ocho y se ha sancionado a seis por no tener el consentimiento de los titulares de la patria potestad para publicar las imágenes en los portales web de las mencionadas instituciones. Dichos portales web muestran imágenes de los estudiantes en diversas actividades en el colegio, así como en algunos casos se indica el grado y salón de clase.

Otro ámbito problemático que se ha encontrado es que algunas empresas realizan concursos dirigidos a menores en los que solicitan datos de menores de 14 años vía web, sin solicitar el consentimiento de los padres.

El mayor problema es la falta de cultura de protección de datos en los menores de edad, quienes cuelgan fotos e información sobre ellos y sobre sus familiares en las redes sociales sin tener en cuenta las medidas de seguridad y de privacidad que deben usar.

7.4. Herramientas y recursos de la Autoridad en materia de menores

Charlas a docentes y estudiantes

En cumplimiento del precitado artículo 33 LPDP, la Autoridad ha realizado desde 2014 ocho charlas dirigidas a docentes a nivel nacional, capacitando a 301 docentes sobre el derecho a la protección de datos personales. Asimismo, ha realizado 29 charlas a nivel nacional dirigidas a menores, difundiendo el derecho a la protección de datos a 4.333 estudiantes. Durante las charlas se entrega a los estudiantes material con mensajes informativos, tales como mochilas, reglas, cartucheras, stickers o lapiceros, que permiten que el menor recuerde el tema de la charla, es decir, que debe proteger su información. Asimismo, la Autoridad ha informado a centros educativos de la ciudad de Lima sobre sus obligaciones respecto a la protección de datos de menores.

Vídeos y cartillas informativas

Por otro lado, la APDP cuenta con un video informativo dirigido a menores, que tiene como objetivo explicar los riesgos de publicar en internet, especialmente en las redes sociales, sin el cuidado necesario. Además cuenta con una cartilla informativa, la que también se encuentra publicada en el siguiente link. https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-menores.pdf

8. URUGUAY

8.1. Normativa

La protección de datos como derecho humano fundamental en Uruguay

La Ley 18.331/2008 establece en su artículo 1 que el derecho a la protección de la información personal de todas la personas (incluidos los menores de edad) es un derecho humano fundamental en los términos del artículo 72 de la Constitución de la República.

Normas relevantes del Código de la Niñez y Adolescencia

El reconocimiento expreso de los derechos de niños y adolescentes se encuentra actualmente en la Ley 17.823/2004, que instituyó el Código de la Niñez y la Adolescencia. Este Código establece que los niños y adolescentes son titulares de los derechos, deberes y garantías inherentes a su calidad de personas humanas (art. 2). El artículo 4 del Código establece que para su interpretación deberán considerarse las disposiciones y principios generales de la Constitución de la República, la Convención sobre Derechos del Niño (donde destaca el principio del interés superior del niño y adolescente), así como las leyes nacionales e instrumentos internacionales que obligan al país. Asimismo, en el artículo 9 se indica que son derechos esenciales, entre otros, la dignidad, la integridad y la imagen de los niños, que puede entenderse como referencia implícita a la protección de datos personales de los menores.

En lo que refiere específicamente a la protección de los datos personales, el artículo 11 del Código precitado señala que "Todo niño y adolescente tiene derecho a que se respete la privacidad de su vida. Tiene derecho a que no se utilice su imagen en forma lesiva, ni se publique ninguna información que lo perjudique y pueda dar lugar a

la individualización de su persona". El énfasis en la privacidad de los menores también se refleja cuando el Código establece la orientación de la atención de niños y adolescentes hacia la creación de sistemas de indicadores de desarrollo, respetando en todos los casos el derecho a la privacidad y el secreto profesional (art. 22 g).

Finalmente, cabe señalar que el artículo 221 del Código, dentro de las obligaciones del Instituto del Niño y Adolescente del Uruguay establece la obligación de garantizar el uso reservado y confidencial de los datos de cada niño o adolescente, "en concordancia con su interés superior y en cumplimiento del derecho a la privacidad de su historia personal, como único propietario de la misma".

8.2. El consentimiento del menor para el tratamiento de sus datos personales

Normas generales sobre capacidad, consentimiento y representación

En el Uruguay, el Código precitado establece como edad de corte para distinguir niños de adolescentes, los 13 años cumplidos de edad. Asimismo, excluye del concepto de adolescentes a los efectos del Código a los mayores de 18 años.

Estas normas deben complementarse con las normas generales en materia de capacidad[37]. El Código Civil uruguayo (en la última reforma dada por la Ley 16.603/1994) regula con respecto a los menores de edad tres regímenes diferenciados: a) incapacidad absoluta de los menores impúberes (varones menores de 14 años y mujeres menores de 12 años), que sólo pueden actuar a través de un representante legal; b) incapacidad relativa de los menores púberes (varones mayores de 14 años y mujeres mayores de 12 años) sometidos a patria potestad, que pueden realizar determinados actos sin la intervención de su representante; c) menores casados que requieren de un representante para actos excepcionales previstos por la ley.

Solución propuesta: cabe el consentimiento autónomo de los mayores de 14 años pero debe atenderse a cada caso

Es decir, en los dos últimos casos la incapacidad es relativa, pues sus actos pueden tener valor en determinadas circunstancias y bajo ciertos requisitos determinados por las leyes. Por ello, en el primer grupo deberá de recabarse necesariamente el consentimiento de los representantes legales de los menores[38]. La duda puede plantearse en el caso de los menores púberes, en cuyo caso deberá de evaluarse si potencialmente puede resolver sobre la forma de tratamiento de sus datos, así como la forma de ejercicio de sus derechos. En este punto, deberán tenerse en cuenta los principios generales consagrados en el artículo 8 del Código de la Niñez y la Adolescencia, que expresamente establece el goce de los derechos inherentes a la persona humana de todo niño y adolescente y su ejercicio conforme la evolución de sus

[37] La doctrina uruguaya ha distinguido la capacidad de goce (aquella que poseen todos los individuos de la especie humana y que les permite ser titulares de derechos) de la capacidad de ejercicio (que habilita el ejercicio efectivo y personal de los derechos, y que en el caso de los menores debe contar en la mayoría de los casos con la asistencia de un representante).

[38] La representación de los menores de edad y según los casos deberá resolverse conforme los institutos de la patria potestad, la tutela, y en determinados casos la curatela (arts. 252 y ss., 313 y ss. y 458 y ss.).

facultades, en la forma establecida por la Constitución, tratados internacionales y leyes nacionales. Consagra además expresamente el derecho a ser oído y obtener respuestas cuando se tomen decisiones que afecten su vida. En este sentido y para estos menores, puede entenderse que dependiendo de cada situación y luego de un pormenorizado análisis de ésta, es viable considerar como válido el consentimiento del menor para el tratamiento de sus datos personales. Lo antedicho también resulta de aplicación para las consideraciones asociadas al uso de su propia imagen.

Requisitos generales del consentimiento

En todo caso, el consentimiento, aun en el caso de la representación, y también a falta de normas específicas en sede de protección de datos personales, deberá contener las características previstas en el artículo 9 de la Ley 18.331; en líneas generales, libre, previo, expreso, informado y documentado.

8.3. Ámbitos problemáticos

Publicidad dirigida a menores: normas generales

Con referencia a las promociones y a la publicidad, las normas generales en materia de protección de datos personales (art. 21 de la Ley 18.331) habilitan el tratamiento de datos personales obtenidos a través de fuentes accesibles al público, facilitados por los titulares u obtenidos con su consentimiento. Estas normas deben complementarse con las que regulan las relaciones de consumo (Ley 17.250/2000), que prohíben a los proveedores en general la publicidad engañosa, así como la obligación de divulgar y transmitir la publicidad de forma que sea posible identificarla como tal.

Menores tutelados y en riesgo social

En caso de menores tutelados y en riesgo social, se entiende pertinente considerar con mayor relevancia la necesidad de contar con el consentimiento de los representantes de los menores para el tratamiento de sus datos, así como el rol preponderante que debe de adoptar el Estado en el marco de las obligaciones conferidas por el Código de la Niñez y la Adolescencia ya mencionado.

Datos médicos

El artículo 11 bis (agregado por la Ley 18.426/2008) del Código de la Niñez y la Adolescencia estableció en materia de derecho a la salud: "Todo niño, niña o adolescente tiene derecho a la información y acceso a los servicios de salud, inclusive los referidos a la salud sexual y reproductiva, debiendo los profesionales actuantes respetar la confidencialidad de la consulta y ofrecerle las mejores formas de atención y tratamiento cuando corresponda". En este mismo ámbito, el Decreto 274/2010, reglamentario de la Ley 18.335/2008, establece en concreto que "Los adolescentes a quienes, de acuerdo al principio de autonomía progresiva, los profesionales de la salud consideren suficientemente maduros para recibir atención fuera de la presencia de los padres, tutores u otros responsables, tienen derecho a la intimidad y pueden solicitar servicios confidenciales e incluso tratamiento confidencial". De esta forma se reconoce expresamente el principio de autonomía progresiva respecto a los menores de edad.

Antecedentes penales

Por otra parte, el Código de la Niñez y la Adolescencia aclara que la información relativa a niños y adolescentes no podrá ser utilizada

como base de datos para su rastreo luego de alcanzada la mayoría de edad, debiendo además destruirse sus antecedentes cumplidos los 18 años, salvo excepciones impuestas por mandato judicial (art. 222).

8.4. Herramientas y recursos de la autoridad en materia de menores

El Plan CEIBAL de inclusión digital de los menores: Dictamen de la URCDP

En Uruguay se ha venido promoviendo la inclusión tecnológica y digital de los menores, a través de la iniciativa Plan CEIBAL, orientada por el Centro CEIBAL. La inclusión digital importa beneficios pero también retos, máxime desde la perspectiva de la protección de datos personales. En este marco, Centro CEIBAL consideró importante brindar determinadas herramientas para facilitar la labor de docentes, estudiantes y sus representantes a través de los servicios prestados por Google (especialmente las "Apps for Education"). Previo a hacerlas disponibles se solicitó expresamente la opinión de la URCDP, quien se expidió a través del Dictamen 12/2015, de 7 de julio de 2015, donde se señaló la importancia de brindar información clara, completa y en idioma español, y estableciendo en concreto que a los efectos consultados debía de obtenerse el consentimiento de los representantes del menor (padres, tutores o curadores, según los casos).

Acciones en la educación formal: Comisión de Trabajo y guías para formadores

La Unidad ha tratado además de hacer énfasis en la inclusión de la temática de la protección de datos en la educación formal, principalmente luego de considerar la importancia de que los menores tengan contacto en las etapas iniciales de su aprendizaje con los principios y conceptos de la protección de datos personales. A este respecto puede mencionarse la conformación de una Comisión de Trabajo multidisciplinaria, conjuntamente con las autoridades de la educación, que brega por la organización de un curso dirigido a los interesados y asociado a la protección de datos en la labor docente. Más en concreto, se colaboró fuertemente con el desarrollo de las guías de conocimiento para el desenvolvimiento del curso de Formación de Formadores de la Administración Nacional de Educación Pública.

El concurso "Tus Datos Valen"

De otro lado, se llevó adelante la 4ª edición del concurso correspondiente a la campaña "Tus Datos Valen", que año a año congrega a niños de 5º y 6º años de escuelas públicas y privadas de todo el país, quienes son convocados a participar a partir de una consigna determinada en el desarrollo de situaciones que impliquen la protección de los datos personales. Esta es una forma de llegar a un importante número de escolares con una temática nueva y diferente que es rápidamente comprendida y aprehendida por los niños que participan en la experiencia.

Guías y vídeos de la URCDP

En lo que refiere especialmente al tratamiento de datos personales en las redes sociales la Unidad ha realizado eventos dirigidos a esta problemática (vinculados a la identidad digital, a los menores y la educación), y buscado otras vías para acercarse a estos a través de la puesta a disposición de guías y videos que refieren específicamente a esta temática y que pueden consultarse en los sitios https://www.datospersonales.gub.uy/inicio/publicaciones/Guias+de+ayuda/ y https://www.youtube.com/channel/UCMqktFD3glI5gk9MiQS-MaA.

9. SÍNTESIS[39]

9.1. El consentimiento del menor para el tratamiento de sus datos personales

La ausencia de normativa clara y específica sobre el derecho a la protección de datos de los menores de edad es la tónica general. En todos los países se reconoce, expresa o tácitamente, el derecho a la intimidad de los menores al máximo nivel (constitucional o de tratado internacional) pero sin claridad sobre las condiciones de su ejercicio; resulta significativa la común referencia al ambiguo "interés superior del niño", sin mayor concreción. Por ejemplo, en Colombia existe una prohibición legal del tratamiento de datos de menores, que sin embargo ha sido muy matizada por la Corte Constitucional; de hecho, el reglamento de desarrollo admite dicho tratamiento, por cuanto lo somete a requisitos especiales. En México la situación es similar: prohibición de difusión de datos de menores pero solo si es "ilícita". Reglas tan generales provocan inseguridad jurídica, que ha intentado paliarse por la doctrina de diversas autoridades. Consciente de esta situación, la autoridad argentina ha propuesto una reforma legislativa en la materia, todavía en discusión.

Omisiones y ambigüedades legales sobre datos de menores

Como excepción, encontramos normativa específica en España y en Perú: en ambos países la normativa permite expresamente a los menores prestar por sí solos el consentimiento para el tratamiento de sus datos a partir de los 14 años, requiriéndose el de sus padres o tutores antes de esta edad.

Legislación específica en España y Perú

En síntesis, el tratamiento de los datos de los menores exige el consentimiento (el cual, como regla general, debe ser libre, inequívoco, específico e informado) de los padres o tutores hasta los 14 años en Andorra, España y Perú (en el primer y último caso, según la doctrina de la autoridad de protección de datos, pues la legislación no es clara). En Argentina, la ley admite el consentimiento de los menores con madurez suficiente (no se establece una edad concreta, pero cabría pensar también en los 14 años) pero solo para los "contratos de escasa cuantía de la vida cotidiana". En Chile y Colombia no hay claridad al respecto y la línea dominante parece ser la necesidad de consentimiento de padres o tutores hasta los 18 años. En Uruguay la legislación exige el consentimiento de los padres hasta los 18 años, salvo un análisis específico de las situaciones de niñas y niños en los casos de menores púberes.

Heterogeneidad en la fijación de la edad exigida para el consentimiento autónomo

En todo caso, el responsable del fichero debe garantizar la validez de este consentimiento, lo cual incluye la información pertinente. Por ejemplo, en Andorra y España la legislación establece expresamente que la prueba del consentimiento corresponde al responsable del fichero, estableciéndose mayores cautelas en el caso de los menores. También la normativa andorrana y española, a las que se suma la pe-

Requisitos, límites y problemas del consentimiento

[39] Esta Síntesis se basa exclusivamente en los datos suministrados por los funcionarios designados por las agencias para colaborar en este Informe. La referencia a normas de Derecho nacional o a actuaciones de las agencias es meramente ejemplificativa y no implica que no existan otras normas o actuaciones.

ruana, establecen límites en lo relativo al tratamiento de los datos de los familiares del menor.

La prestación del consentimiento provoca algunos problemas en todos los países, entre los cuales cabe destacar dos: la verificación de la edad y el otorgamiento del consentimiento de los padres cuando estos se encuentran separados. En Chile la autoridad ha destacado que incluso los padres privados de patria potestad tienen acceso a los datos de sus hijos.

9.2. Ámbitos problemáticos

Publicidad dirigida a menores

Sin citar normativa específica, la agencia andorrana destaca la necesidad de controlar la publicidad dirigida a menores, en especial en cuanto al otorgamiento efectivo de su consentimiento (directo o por medio de sus representantes) y a la información a suministrar por las empresas. Es interesante la autorregulación de esta materia producida en Argentina, en un caso homologada por la propia autoridad (Código de Ética de la Asociación de Marketing Directo e Interactivo). En Colombia se discute actualmente un proyecto de ley sobre la publicidad dirigida a menores, que incluye un precepto específico sobre sus datos personales.

Menores en conflicto con la ley penal y protegidos

La legislación argentina prohíbe la difusión de datos de menores "incursos en hechos que la ley califica como delitos o contravención o que sean víctimas de ellos, o que se encuentren en estado de abandono o en peligro moral o material". En lo que se refiere a la difusión de información judicial, dos importantes resoluciones de la autoridad han dictaminado la necesidad de disociar o anonimizar los datos de los menores, ponderando así adecuadamente el principio de publicidad de las actuaciones judiciales con los derechos de los menores. En México y con relación a los menores tutelados, se aplica la normativa general sobre privacidad en los organismos de protección.

Datos médicos

La autoridad argentina ha enfatizado la necesidad de consentimiento de los representantes legales de los menores en todo lo referente al tratamiento de sus datos médicos. Por su parte, la autoridad peruana ha insistido en la importancia de acreditar la representación en estos casos, no exigiéndose sin embargo cuando se trata de información de los padres en relación con sus hijos. La normativa uruguaya, por su parte, es más flexible, pues reconoce el "principio de autonomía progresiva", según el cual los menores pueden consentir y acceder a sus datos médicos según su grado de madurez.

Videovigilancia

La autoridad colombiana ha publicado una importante guía sobre los datos de menores recolectados mediante sistemas de videovigilancia, estableciendo requisitos especiales muy rigurosos, como la necesidad de autorización de sus padres o representantes, inclusive para el acceso o circulación de imágenes en clase o actividades extraescolares.

Medios de comunicación

La legislación mexicana establece una prohibición general de difusión de datos e imágenes de los menores en los medios de comunicación, si bien solo en los casos en que "se menoscabe su honra o re-

putación, sea contrario a sus derechos o que los ponga en riesgo" o se propicie o tienda "a la discriminación, criminalización o estigmatización de los menores". En todo caso, la difusión de entrevistas con menores requiere el consentimiento de sus padres o tutores. Complementariamente, la ley mexicana establece obligaciones públicas genéricas de protección en este ámbito.

9.3. Datos de menores en Internet

Problemática de los datos de los menores en Internet: ejemplos

La agencia andorrana resume bien la problemática de los datos de los menores en Internet: estos suelen desconocer los riesgos que puede suponer la publicación de fotografías u otros datos en Internet ya que valores como la privacidad o la propia imagen no son percibidos como necesarios. Al mismo tiempo, los adultos responsables buscan conocer a qué contenidos han accedido sus hijos y qué datos están siendo ofrecidos de forma imprudente por parte de los mismos. Sabemos además que los niños son especialmente vulnerables en la red: reciben ofertas de foros, páginas web, chats, que son muy atractivas para ellos y no son capaces de discernir qué es publicidad y qué son hechos. Los principales riesgos a los que se exponen los menores residen en la posibilidad de comunicarse con individuos malintencionados, la revelación de información personal por parte de ellos mismos o terceros, el acceso a contenidos inapropiados para su edad y la contratación de servicios por error o desconocimiento. Siguen algunos ejemplos de denuncia en este ámbito, extraídos de la práctica de la agencia española: recogida de datos de menores en una web que ofrecía participar en una cabalgata de Reyes, sin la información legalmente necesaria ni opción a solicitar la autorización de sus padres; difusión de imágenes de menores en web de contactos, accesibles a terceros y sin verificación eficaz de su edad; difusión en Facebook de vídeo con imágenes de menores en visita escolar sin consentimiento de sus padres; formulario para participar en la campaña publicitaria para la obtención de regalos a menores, también sin la información legalmente necesaria ni opción a solicitar la autorización de sus padres.

Reformas normativas recientes en México y propuesta de la autoridad argentina

En estas circunstancias, parece necesario, en primer lugar, un marco normativo especialmente dirigido a la protección de los datos de los menores en la red. La respuesta más contundente viene dada por la legislación penal. Interesa destacar a este respecto la reciente reforma del Código Penal mexicano, de diciembre de 2016, que tipifica el ciberacoso y castiga la difusión de fotos o vídeos sexuales sin autorización del afectado. En un plano más moderado, destaca la propuesta de reforma legislativa presentada por la agencia argentina, que exige el consentimiento paterno para los menores de 13 años y conmina al responsable del tratamiento a "realizar esfuerzos razonables para verificar que el consentimiento […] fue otorgado por el titular de la responsabilidad parental".

Órdenes y sanciones

En cuanto a las acciones concretas realizadas por las agencias en este ámbito, destacamos dos especialmente significativas: la orden al buscador Google, emitida por la autoridad argentina, de supresión o

bloqueo de los datos almacenados de las búsquedas realizadas por un denunciante y su hija, y los procedimientos sancionadores abiertos por la autoridad peruana por publicación de imágenes de menores, sin el necesario consentimiento de sus padres, en diversos sitios web de centros educativos.

Promoción de derechos por las autoridades

Más allá de las actuaciones administrativas encaminadas a la protección de derechos (órdenes y sanciones a las empresas), todas las autoridades iberoamericanas han realizado importantes esfuerzos de prevención, que resultan especialmente relevantes de cara a evitar que el daño se produzca. Como respuesta al problema de la falta de cultura de uso adecuado de la red, cabe mencionar las campañas informativas, dirigidas a los menores y a sus padres, alertando de los peligros de la red y recomendando su buen uso, como por ejemplo las realizadas en Andorra (campañas "Navega Segur" y "Dades Ni Piu: Que no se't escapin") o Colombia ("En TIC confío", en colaboración con el Ministerio, y "Teprotejo", en colaboración con una corporación sin ánimo de lucro). En el último apartado de este capítulo se hará mención a otras herramientas y recursos.

9.4. Ejercicio por los menores de su derecho a la protección de datos

Representación de menores e inseguridad jurídica

En el apartado 9.1 hicimos referencia a la regulación del consentimiento del menor para el tratamiento de sus datos y a la heterogeneidad existente en Iberoamérica en cuanto a las edades a partir de las cuales cabe dicho consentimiento autónomo, cuestión regulada normalmente en los códigos civiles, todo lo cual resulta aplicable también al ejercicio de sus derechos. Los problemas de inseguridad jurídica arriba relatados se reiteran en lo relativo al ejercicio por el menor de sus derechos. Como señala la autoridad mexicana, cuyas apreciaciones son trasladables a los demás países, la situación es la siguiente: no existe duda de que el menor de edad es titular de derechos. Sin embargo, su incapacidad legal le impide el ejercicio de los mismos de manera directa, recayendo dicho ejercicio sobre quienes ostentan su patria potestad o representación, siempre entendiendo el interés superior del menor como principio rector de su actuación.

Mecanismos de tutela en Colombia

En Colombia existen instituciones especialmente destinadas a promover y restablecer los derechos de los menores en general, que resultan aplicables al ejercicio de su derecho a la protección de datos, como los defensores y los comisarios de familia; en todo caso, como recuerda la autoridad colombiana, los menores pueden ejercer por sí mismos el derecho de petición ante cualquier vulneración de sus derechos, incluida la protección de su datos personales.

Protección en centros educativos en Andorra

De nuevo, las autoridades han desplegado esfuerzos para paliar las lagunas normativas y facilitar un correcto ejercicio del derecho a la protección de datos por este colectivo, mediante técnicas variadas. A título ejemplificativo cabe citar el trabajo de la autoridad andorrana, que se ha preocupado especialmente de garantizar el ejercicio del derecho en los centros educativos. Así, en colaboración en algún caso

con el Ministerio de Educación, ha contribuido a la publicación de ficheros, redacción de cláusulas informativas e implementación de un módulo de protección de datos en las escuelas, así como ha prestado asesoramiento continuo en la utilización de programas informáticos.

9.5. Herramientas y recursos de las autoridades en materia de menores

Sistematización de las herramientas y recursos en materia de menores

Seguramente el trabajo más relevante en el ámbito que analizamos, común denominador de todas las autoridades de protección de datos, ha consistido en la elaboración y difusión de herramientas para la sensibilización, capacitación, difusión y promoción del derecho a la protección de datos de los menores de edad. Estas actividades, realizadas en muchos casos en colaboración con otros organismos públicos y privados, pueden sistematizarse como sigue:

a) Charlas, cursos y campañas de capacitación o concienciación, en Andorra, Argentina, España o Perú. En España resulta de particular interés la colaboración, con enfoque primordial en la capacitación, con las instituciones encargadas de garantizar la seguridad pública, como las fiscalías, las fuerzas y cuerpos de seguridad, el Ministerio de Justicia o el Instituto Nacional de Ciberseguridad.
b) Portal web de información (con la posibilidad, en varios países, de presentar consultas e incluso denuncias por vía telemática) de los derechos de los menores, en Andorra, Argentina, Colombia, España o México.
c) Utilización de las redes sociales en Argentina o Colombia.
d) Campañas en televisión o vídeos educativos en Argentina, Colombia, España, Perú y Uruguay.
e) Guías informativas y fichas prácticas en Argentina, España, Perú y Uruguay.
f) Premios y concursos en España, México y Uruguay.

Hacia la inclusión de la educación digital en las escuelas

Interesa por último hacer especial referencia al convenio celebrado entre la autoridad española y el Ministerio de Educación de este país, por cuanto, en línea con las resoluciones de la Conferencia Internacional de Autoridades de Protección de Datos, ha logrado la inclusión de la educación digital en los planes de estudios. Entre otras, la autoridad uruguaya está trabajando de forma intensa para conseguir este mismo objetivo.

COLABORADORES

Mónica Arenas Ramiro es Profesora Contratada Doctora de la Universidad de Alcalá. Redactó el apartado I (Panorama internacional) de la Parte II.

María Adriana Báez Ricardez es Directora General de Prevención y Autorregulación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México. Coordinó los apartados sobre México de las Partes I y II.

Alejandra Celi Maldonado es Investigadora Principal del PRADPI, de la Universidad de Alcalá. Amplió el apartado V (Agencia Española de Protección de Datos) de la Parte I, redactó la versión preliminar del apartado VI (Autoridad Catalana de Protección de Datos), el apartado VII (Agencia Vasca de Protección de Datos) de la Parte I y editó todas las contribuciones de la Parte I y redactó la Síntesis de la Parte I.

Joan Crespo es Director de la Agencia Andorrana de Protección de Datos. Redactó los apartados sobre Andorra de las Partes I y II.

Guillermo Escobar Roca es Director del Departamento de Ciencias Jurídicas y del PRADPI, de la Universidad de Alcalá. Diseño la estructura y método del Informe, coordinó todas las contribuciones, editó la Parte II y redactó la Síntesis de la Parte II.

Diana Cristina Gil es Asesora de la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio de Colombia. Redactó los apartados sobre Colombia de las Partes I y II.

María Alejandra González Luna es Directora (e) de Supervisión y Control de la Dirección General de Protección de Datos Personales de Perú. Redactó los apartados sobre Perú de las Partes I y II.

Joana Marí Cardona es Responsable de Evaluación y Estudios Tecnológicos de la Autoridad Catalana de Protección de Datos. Redactó los apartados sobre Cataluña de las Partes I y II.

Laura Nahabetián Brunet es Gerente de la División de Derechos Ciudadanos - Ciudadanía Digital en la Unidad Reguladora y de Control de Datos Personales de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento de Uruguay. Junto con **Gonzalo Sosa** redactó los apartados sobre Uruguay de las Partes I y II.

Miguel Ángel Pérez Grande es Vocal Asesor en la Unidad de Apoyo de la Agencia Española de Protección de Datos. Colaboró con el Director del Informe en la coordinación y revisión de todas las contribuciones.

Loreto Pozo Marques es Analista de Relacionamiento y Comunicaciones del Consejo para la Transparencia de Chile. Redactó los apartados sobre Chile de las Partes I y II.

Julián Prieto Hegueta es Subdirector General de Registro General de Protección de Datos de la Agencia Española de Protección de Datos. Redactó el apartado sobre España de la Parte II.

Pablo Segura es Coordinador Técnico Legal de la Dirección Nacional de Protección de Datos Personales de Argentina. Redactó los apartados sobre Argentina de las Partes I y II.

Lidia Suárez Espino es Investigadora Colaboradora del PRADPI, de la Universidad de Alcalá. Redactó el primer borrador del apartado sobre España de la Parte I.

ENTIDADES ACREDITADAS DE LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

MIEMBROS

ANDORRA
Agencia Andorrana de Protección de Datos (APDA)
https://www.apda.ad

ARGENTINA
Dirección Nacional de Protección de Datos Personales (DNPDP)
http://www.jus.gob.ar/datos-personales.aspx

CHILE
Consejo para la Transparencia (CplT)
http://www.consejotransparencia.cl

COLOMBIA
Superintendencia de Industria y Comercio - Delegación de Protección de Datos Personales (SIC)
http://www.sic.gov.co/proteccion-de-datos-personales

COSTA RICA
Agencia de Protección de Datos de los Habitantes (PRODHAB)
http://www.prodhab.go.cr

ESPAÑA
Agencia Española de Protección de Datos (AEPD)
http://www.agpd.es

Autoridad Catalana de Protección de Datos (APDCAT)
http://apdcat.gencat.cat

Agencia Vasca de Protección de Datos (AVPD)
http://www.avpd.euskadi.eus

MÉXICO
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)
http://inicio.ifai.org.mx

Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFODF)
http://www.infodf.org.mx/

Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (INFOEM)
http://www.infoem.org.mx/

PERÚ
Dirección General de Protección de Datos (APDP)
https://www.minjus.gob.pe/proteccion-de-datos-personales

PORTUGAL
Comissão Nacional de Proteção de Dados (CNPD)
https://www.cnpd.pt/

URUGUAY
AGESIC. Unidad Reguladora y de Control de Datos Personales (URCDP)
http://www.agesic.gub.uy/

OBSERVADORES

ARGENTINA
Defensoría del Pueblo de la Ciudad de Buenos Aires

BRASIL
Ouvidoria Geral da Uniao. Ministerio de la Transparencia, Fiscalización y Controladoria-General de la Unión

CABO VERDE
Comissão Nacional de Protecçao de Dados (CNPD)

CHILE
Subsecretaría de Economía y Empresas de Menor Tamaño

ECUADOR
Función de Transparencia y Control Social (FTCS)

EL SALVADOR
Instituto de Acceso a la Información Pública (IAIP)

GUATEMALA
Procurador de los Derechos Humanos. Comisión de Acceso a la Información Pública (CAIP)

HONDURAS
Instituto de Acceso a la Información Pública (IAIP)

PARAGUAY
Secretaría de la Función Pública

REPÚBLICA DOMINICANA
Dirección General de Ética e Integridad Gubernamental (DIGEIG)

ORGANIZACIÓN DE ESTADOS AMERICANOS

Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP)

Supervisor Europeo de Protección de Datos (EDPS) de la Unión Europea

La Red Iberoamericana de Protección de Datos, creada en el Encuentro Iberoamericano de Protección de Datos de Antigua, Guatemala, en junio de 2003, es un foro integrador de los actores, públicos y privados, que desarrollan iniciativas y proyectos relacionados con la protección de datos personales en la región, con la finalidad de fomentar, mantener y fortalecer un estrecho y permanente intercambio de información, experiencias y conocimientos entre ellos, así como promover los desarrollos normativos necesarios para garantizar una regulación avanzada de este derecho, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común.

Con este I Informe de la Red, auspiciado por su Secretaría Permanente, la Agencia Española de Protección de Datos, y coordinado por el Programa Regional de Apoyo a las Defensorías del Pueblo de Iberoamérica, de la Universidad de Alcalá, se presentan dos investigaciones: la descripción, articulada conforme a un esquema común, de la actividad de las Autoridades de Protección de Datos en 2016, y el estudio de un tema monográfico, en esta primera ocasión la protección de datos de los menores de edad, que necesariamente ha de partir de la exposición del panorama internacional en la materia. Las dos partes del Informe se cierran con una síntesis, centrada en la comparación de normas y experiencias de los países que conforman la Red, con miras al conocimiento y difusión de elementos comunes y en su caso diferenciados, y en especial de las mejores prácticas de las Autoridades, a fin de preparar desarrollos futuros y, en la medida de lo posible, nuevos proyectos compartidos para avanzar en una mejor garantía del derecho a la protección de datos personales en los países de la región.

Universidad de Alcalá
PROGRAMA REGIONAL DE APOYO A LAS DEFENSORÍAS DEL PUEBLO DE IBEROAMÉRICA

RED IBEROAMERICANA DE PROTECCION DE DATOS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

ISBN 978-84-945692-4-1
9 788494 569241