MEMORIA ANUAL 2012 URCDP

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

MEMORIA ANUAL 2012 URCDP

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

Consejo Ejecutivo URCDP

Prólogo

La presente Memoria, correspondiente al año 2012, permite apreciar la labor cumplida en el período por la Unidad Reguladora y de Control de Datos Personales en el desarrollo de los cometidos que establece la normativa vigente, la cual coloca a la protección de datos personales –como no puede ser de otra manera– en la base humanista que sustenta el régimen jurídico nacional.

Con este fundamento siempre presente, el camino de la consolidación institucional de la Unidad que se indicara en el Prólogo de la Memoria 2011, prosiguió mediante la expedición de múltiples dictámenes de asistencia y asesoramiento, la realización de actividades de capacitación a fin de contribuir a un mayor conocimiento de la protección de datos y de los medios que lo hacen efectivo –de modo presencial-, a través de cursos en línea, de la publicación de boletines y de guías educativas. Estas últimas han relacionado esa protección directamente con diversos valores sociales y sectores de actividad tales como los de Educación, Salud, Administración Pública y Telecomunicaciones.

En lo que atañe a la legislación vigente, la Unidad planteó una iniciativa que se consagró en el art. 43 de la Ley de Rendición de Cuentas 2011, Nº 18.996 de 7-XI-2012 y que refiere a la noción de fuentes públicas o accesibles al público.

A nivel internacional, en octubre de 2012 se realizó la 34ª Conferencia Internacional de Autoridades de Protección de Datos en Punta del Este. En la oportunidad se efectuó, asimismo, la reunión de la Red Iberoamericana de Protección de Datos y también se realizaron "eventos paralelos" organizados por sectores de la sociedad civil y de la academia.

Las sesiones abiertas de la Conferencia, organizadas por nuestra Unidad, comprendieron diversos paneles bajo el título "Privacidad y tecnología en equilibrio".

De esta manera, nuestro país fue sede de una reunión de la mayor relevancia, tanto del punto de vista de la temática considerada, en general de las actividades realizadas así como de las personalidades presentes, que provinieron de todos los continentes.

Por otro lado, con fecha 21 de agosto de 2012, la Unión Europea -a través de sus órganos competentes y de acuerdo con su Directiva 95/46/CE- consideró que nuestra República "garantiza un nivel adecuado de protección de los datos personales transferidos" desde esa Unión.

Esa medida implica un reconocimiento de la adecuación del sistema uruguayo de protección de datos a los mejores estándares internacionales. En este sentido, además de la proyección que tiene en cuanto a la transferencia de datos desde y hacia Europa, la cual no exige –ahora – requerimientos específicos (modelos de cláusulas contractuales, reglas corporativas vinculantes, etc.) ha tenido una inmediata incidencia en el país al apreciarse un mayor número de consultas planteadas ante la Unidad.

Otra noticia relevante de 2012 fue la emisión de la Ley Nº 19.030, aprobada por ambas Cámaras legislativas en el decurso del año y promulgada por el Poder Ejecutivo el 27 de diciembre. Este acto legislativo habilita la adhesión del Uruguay al 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 y su Protocolo Adicional.

Este Convenio es un instrumento internacional abierto a países que no integran el Consejo de Europa lo que lo configura como un cuerpo normativo que tiende a una homogeneización de carácter global en la materia.

En otro aspecto cabe anotar que en el marco de la Reunión Ministerial y de las Autoridades de Gobierno Electrónico de América Latina y el Caribe se entregaron premios a la excelencia; Uruguay obtuvo dos de las tres menciones, una por el Portal de Datos Abiertos de Gobierno y la otra, por el sitio de Protección de Datos Personales.

Finalmente se señala que, la permanente movilidad de la tecnología en la comunicación e información impone acentuar la atención de los valores en juego que se relacionan con la protección de datos y, con ello, remarcar la aplicación de los principios en que ella se sustenta en tanto a través de su adecuada aplicación por todos los operadores, incluida esta Unidad, se entiende posible asegurar esa protección.

Felipe Rotondo Tornaría

01

Uruguay garantiza un nivel adecuado de protección

1. Uruguay garantiza un nivel adecuado de protección

Luego del Dictamen 6/2010 del Grupo de Trabajo de Protección de Datos del Artículo 29 (G29), la citada Decisión termina por rubricar favorablemente un proceso de examen iniciado tres años atrás, habilitándonos a ingresar en el reducido elenco de Estados, fuera del ámbito europeo, que disponen de tal reconocimiento.

Es preciso señalar que la Directiva sobre protección de datos de 1995 se aplica al Espacio Económico Europeo (EEE), lo que incluye todos los países de la UE además de Islandia, Liechtenstein y Noruega. Y desde su dictado se ha considerado necesario adoptar precauciones especiales al transmitir datos personales a países no pertenecientes al EEE, puesto que sin tales precauciones, los elevados niveles de seguridad establecidos por la Directiva de la UE se deteriorarían rápidamente, dada la facilidad con que los datos pueden transmitirse a través de las redes internacionales.

A eso apunta la declaración, a reconocer que Uruguay cumple los estándares requeridos. Hasta ahora, la Comisión había reconocido a Andorra, Argentina, Australia, Canadá (para destinatarios regidos por la ley federal canadiense y sin perjuicio de las competencias propias de sus provincias y territorios), Suiza, Israel; las Islas Feroe, Guernsey, Man, Jersey; Estados Unidos (a través de los principios de "Safe Harbour" para la protección de la vida privada y las correspondientes preguntas frecuentes (FAQs) publicadas por el Departamento de Comercio en el año 2000) como lugares seguros que ofrecen una protección adecuada. Y muy recientemente, el 19 de diciembre de 2012, lo hace también con Nueva Zelanda.

¿Qué debe entenderse por "protección adecuada"? El Grupo de Trabajo del artículo 29 ha publicado ciertas orientaciones al respecto, fundamentalmente en el work paper Nº 12 (WP 12) donde se concluyen dos elementos básicos: el contenido de las normas aplicables, y los medios para asegurar su aplicación eficaz.

Respecto de lo primero -se concreta en el reconocimiento de un conjunto de principios esenciales -limitación de objetivos, proporcionalidad y calidad de los datos, transparencia informativa, seguridad-, una serie de derechos especiales en favor de los titulares de los datos -acceso, rectificación y oposición-, la restricción autoimpuesta en materia de transferencias sucesivas a terceros países que no garanticen una protección adecuada, y algunas pautas adicionales para ciertos tipos de datos o tratamientos -datos sensibles, mercadotecnia directa, decisiones automatizadas-.

Respecto de lo segundo, si la característica nuclear de la adecuación la da la exigencia de una supervisión externa a través de una forma de autoridad. Se complementó la necesidad de perseguir ciertos objetivos fundamentales, reconducibles a tres aspectos: 1º) Asegurar un nivel satisfactorio de cumplimiento de las normas, sabiendo que ningún sistema por mejor que sea puede garantizar el cien por ciento de cumplimiento, pero también que habrá algunos sistemas mejores que otros, y que la efectividad es verificable de modo objetivo y en todo momento. 2º) Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos, sin costes excesivos y a través de mecanismos institucionales que permitan investigar las denuncias de forma independiente. 3º) Ofrecer vías de recurso adecuadas a quienes resulten perjudicados por la inobservancia de las normas, a través de instancias que incluyan la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones.

El régimen constitucional, legal y reglamentario uruguayo, así como las competencias y actividades que viene desarrollando el Órgano de Control, han sido evaluados positivamente a tales efectos por la Comisión Europea. En el plano práctico, este reconocimiento significa que, dentro de la jurisdicción y leyes del país, ninguna entidad pública o privada que realice "tratamientos de datos personales" (con el sentido laxo de la expresión reconocido por los Estándares Internacionales de Madrid de 2009) provenientes de países europeos u otros reconocidos, lo tendrá prohibido de principio, ni tampoco deberá pasar por el proceso de autorización previa y casuista que necesitaría si no se contase con el reconocimiento global recibido en términos de país.

El país recibe, de este modo, un voto de confianza, bien ganado a partir de los méritos realizados desde la promulgación de la Ley Nº 18.331. Con el resguardo de que no se trata de un cheque en blanco sino todo lo contrario, según bien lo establece la propia Decisión en varios tramos, de los cuales citaremos solamente el Artículo 4º: "La Comisión supervisará el funcionamiento de la presente Decisión e informará al Comité creado por el artículo 31 de la Directiva 95/46/CE de cualquier hecho pertinente y, en particular, de cualquier elemento que pueda afectar la apreciación del artículo 1 de la presente Decisión de que la República Oriental del Uruguay garantiza un nivel adecuado de protección de datos personales a los fines del artículo 25 de la Directiva 95/46/CE, así como de cualquier elemento que demuestre que la presente Decisión se está aplicando de forma discriminatoria".

Se espera el buen recibimiento de esta Decisión europea por parte de los agentes sociales y económicos. La competencia regional por la deslocalización del mercado de servicios es apreciable en sectores como los call-centers, la informática, las finanzas y algunos segmentos de las industrias de medicamentos. El reconocimiento recibido puede facilitar el incremento de los negocios de índole internacional cuya operativa consiste o adiciona tratamientos de datos personales.

DECISIÓN DE EJECUCIÓN DE LA COMISIÓN
de 21 de agosto de 2012 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales.

(2012/484/UE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Vista la 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 (1), y, en particular, su artículo 25, apartado 6,

Previa consulta al Supervisor Europeo de Protección de Datos,

Considerando lo siguiente:

(1) De conformidad con la Directiva 95/46/CE, los Estados miembros solo permitirán la transferencia de datos personales a un tercer país si éste garantiza un nivel de protección adecuado y se cumplen en él, con anterioridad a la transferencia, las disposiciones legales que los Estados miembros aprueben en aplicación de otros preceptos de dicha Directiva.

(2) La Comisión puede dictaminar que un tercer país garantiza un nivel de protección adecuado. En tal caso, pueden transferirse datos personales desde los Estados miembros sin que sea necesaria ninguna garantía adicional.

(3) De conformidad con la Directiva 95/46/CE, el nivel de protección de los datos debe evaluarse atendiendo a todas las circunstancias que concurran en la transferencia o conjunto de transferencias de datos y estudiando con especial atención una serie de elementos pertinentes para la transferencia, enumerados en el artículo 25 de dicha Directiva.

(4) Ante los diferentes enfoques sobre la protección de datos adoptados en los terceros países, tanto la evaluación de la adecuación como la ejecución de las decisiones en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE, deben hacerse sin que originen, en igualdad de condiciones, una discriminación arbitraria o injustificada contra terceros países o entre ellos, ni constituyan una restricción comercial encubierta contraria a los actuales compromisos internacionales de la Unión Europea.

(5) La Constitución de la República Oriental del Uruguay, adoptada en 1967, no reconoce expresamente el derecho a la vida privada y la protección de datos personales. Ahora bien, el catálogo de derechos fundamentales no es una lista cerrada, ya que el artículo 72 de la Constitución establece que la enumeración de derechos, obligaciones y garantías que se recoge en la misma no excluye otros que son inherentes a la naturaleza humana o que derivan del sistema republicano de gobierno. El artículo 1° de la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008, establece expresamente que «El derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República». El artículo 332 de la Constitución establece que los preceptos de la Constitución que reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas, no dejarán de aplicarse por falta de la reglamentación respectiva; sino que ésta será suplida, recurriendo a los fundamentos de leyes análogas, a los principios generales de derecho y a las doctrinas generalmente admitidas.

(6) Las normas jurídicas de protección de datos personales en la República Oriental del Uruguay se basan en gran medida en las normas establecidas en la Directiva 95/46/CE y figuran en la Ley N° 18.331 de Protección de Datos Personales y de Acción de Habeas Data), de 11 de agosto de 2008. Esta Ley se refiere tanto a las personas físicas como a las jurídicas.

(7) La Ley se complementa con el Decreto N° 414/009, de 31 de agosto de 2009, adoptado para clarificar varios aspectos de la Ley y establecer la normativa detallada sobre la organización, las facultades y el funcionamiento de la autoridad de control de protección de datos. El preámbulo del Decreto establece que es conveniente adaptar el sistema jurídico nacional en esta materia al régimen jurídico comparable más ampliamente aceptado, fundamentalmente el establecido por los países europeos a través de la Directiva 95/46/CE.

(8) Algunas disposiciones sobre protección de datos figuran también en una serie de leyes especiales de creación y regulación de bases de datos, a saber, leyes de regulación de determinados registros públicos (escrituras públicas, propiedad industrial y marcas registradas, actos personales, bienes inmuebles, información crediticia o minera). La Ley N° 18.331 se aplica subsidiariamente a las materias que no están reguladas en estos instrumentos jurídicos específicos, con arreglo al artículo 332 de la Constitución.

(9) Las normas jurídicas de protección de datos aplicables en la República Oriental del Uruguay cumplen todos los principios básicos necesarios para ofrecer un nivel adecuado de protección a las personas físicas, y también prevén excepciones y limitaciones para proteger intereses públicos importantes. Estas normas jurídicas de protección de datos y excepciones se basan en los principios establecidos en la Directiva 95/46/CE.

(10) La aplicación de las normas jurídicas de protección de datos está garantizada por recursos judiciales y administrativos y, en particular, por la acción Habeas Data, que permite al interesado emprender una acción judicial contra el responsable del tratamiento de datos para ejercitar su derecho de acceso, rectificación y supresión, así como por el control independiente que realiza la autoridad de control, la Unidad Reguladora y de Control de Datos Personales (URCDP), que tiene facultades de investigación, intervención y sanción, en consonancia con el artículo 28 de la Directiva 95/46/CE, y actúa con absoluta independencia. Además, cualquier parte interesada puede interponer un recurso para solicitar una indemnización por daños y perjuicios causados por un tratamiento ilegal de los datos personales.

(11) Las autoridades de protección de datos de Uruguay han ofrecido explicaciones y garantías sobre cómo debe interpretarse el Derecho uruguayo, así como garantías de que la normativa de protección de datos uruguaya se aplica de conformidad con esa interpretación. Han explicado, en particular, que con arreglo al artículo 332 de la Constitución, la Ley N° 18.331 se aplica de forma subsidiaria a materias no reguladas por leyes especiales que crean y regulan determinadas bases de datos. También han aclarado que, en lo que respecta a las listas de los datos mencionados en el artículo 9, letra C), de la Ley Nº 18.331, cuyo tratamiento no requiere el previo consentimiento del interesado, la Ley también se aplica, en particular los principios de proporcionalidad y finalidad y los derechos de los interesados, y que tales listas están sujetas al control de la autoridad de protección de datos. En lo que respecta al principio de transparencia, las autoridades uruguayas de protección de datos han informado de que la obligación de suministrar la información necesaria al interesado se aplica en todos los casos. En relación con el derecho de acceso, la autoridad de protección de datos ha aclarado que es suficiente que el interesado demuestre su identidad al presentar una solicitud. Las autoridades uruguayas de protección de datos han aclarado que las excepciones al principio de las transferencias internacionales establecido en el artículo 23, apartado 1, de la Ley N° 18.331, deben interpretarse en el sentido de que su aplicación no se extenderá más allá de lo previsto en el artículo 26, apartado 1, de la Directiva 95/46/CE.

(12) La presente Decisión tiene en cuenta y se basa en estas explicaciones y garantías.

(13) La República Oriental del Uruguay es también parte de la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica), de 22 de noviembre de 1969, en vigor desde el 18 de julio de 1978 (1). El artículo 11 de esta Convención reconoce el derecho a la vida privada, y el artículo 30 establece que las restricciones permitidas, de acuerdo con la Convención, al goce y ejercicio de los derechos y libertades reconocidos en la misma, no pueden ser aplicadas sino conforme a leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas. Además, la República Oriental del Uruguay ha reconocido la jurisdicción de la Corte Interamericana de Derechos Humanos. Por otra parte, en la 1.118ª reunión de los delegados de los Ministros del Consejo de Europa, celebrada el 6 de julio de 2011, los delegados invitaron a la República Oriental de Uruguay a adherirse al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (ETS 108) y su Protocolo adicional (ETS n o 118), previo dictamen favorable del Comité consultivo competente.

(14) Por consiguiente, debe considerarse que la República Oriental del Uruguay ofrece un nivel de protección adecuado de los datos personales según lo dispuesto en la Directiva 95/46/CE.

(15) La presente Decisión debe referirse a la adecuación de la protección prevista en la República Oriental del Uruguay a los requisitos del artículo 25, apartado 1, de la Directiva 95/46/CE. No debe afectar a otras condiciones o restricciones de aplicación de otras disposiciones de la Directiva relativas al tratamiento de datos personales en los Estados miembros.

(16) Aunque se haya comprobado que el nivel de protección es adecuado, en aras de la transparencia y para proteger la capacidad de las autoridades pertinentes de los Estados miembros de garantizar la protección de

las personas en lo que respecta al tratamiento de datos personales, resulta necesario especificar las circunstancias excepcionales que pudieran justificar la suspensión de flujos específicos de información.

(17) La Comisión debe hacer un seguimiento del funcionamiento de la Decisión e informar de todo hecho pertinente al Comité creado con arreglo al artículo 31 de la Directiva 95/46/CE. Dicho seguimiento debe abarcar, entre otras cosas, el régimen que la República Oriental del Uruguay aplica a las transferencias en el marco de los tratados internacionales.

(18) El Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29 de la Directiva 95/46/CE, ha emitido un dictamen favorable sobre el nivel de protección de datos personales, que ha sido tenido en cuenta al preparar la presente Decisión.

(19) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité creado en virtud del artículo 31, apartado 1, de la Directiva 95/46/CE.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

1. A los fines del artículo 25, apartado 2, de la Directiva 95/46/CE, se considera que la República Oriental del Uruguay garantiza un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea.

2. La autoridad de control competente de la República Oriental del Uruguay para la aplicación de las normas jurídicas de protección de datos en la República Oriental del Uruguay figura en el anexo de la presente Decisión.

Artículo 2

1. Sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las normas nacionales adoptadas de conformidad con preceptos diferentes a los previstos en el artículo 25 de la Directiva 95/46/CE, las autoridades competentes de los Estados miembros podrán ejercer su facultad de suspender los flujos de datos hacia un receptor de la República Oriental del Uruguay, a fin de proteger a las personas contra el tratamiento de sus datos personales, en los casos en que:

a) la autoridad uruguaya competente compruebe que el receptor ha vulnerado las normas de protección aplicables, o

b) existan grandes probabilidades de que se estén vulnerando las normas de protección, existan razones para creer que la autoridad uruguaya competente no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión, se considere que la continuación de la transferencia podría crear un riesgo inminente de grave perjuicio a los afectados y las autoridades competentes del Estado miembro hayan hecho esfuerzos razonables en estas circunstancias para notificárselo a la entidad responsable del tratamiento en la República Oriental del Uruguay y proporcionarle la oportunidad de recurrir.

2. La suspensión cesará en cuanto esté garantizado el cumplimiento de las normas de protección y ello se haya notificado a las autoridades competentes de los Estados miembros interesados.

Artículo 3

1. Los Estados miembros informarán inmediatamente a la Comisión de la adopción de las medidas basadas en el artículo 2.

2. Los Estados miembros y la Comisión se informarán recíprocamente de aquellos casos en que la actuación de los organismos responsables del cumplimiento de las normas de protección en la República Oriental del Uruguay no garantice dicho cumplimiento.

3. Si la información recogida con arreglo al artículo 2 y a los apartados 1 y 2 del presente artículo demuestra que alguno de los organismos responsables del cumplimiento de las normas de protección en la República Oriental del Uruguay no está ejerciendo su función eficazmente, la Comisión lo notificará a la autoridad competente de la República Oriental del Uruguay y, si procede, presentará un proyecto de medidas con arreglo al procedimiento previsto en el artículo 31, apartado 2, de la Directiva 95/46/CE, a fin de anular o suspender la presente Decisión o limitar su ámbito de aplicación.

Artículo 4

La Comisión supervisará el funcionamiento de la presente Decisión e informará al Comité creado por el artículo 31 de la Directiva 95/46/CE de cualquier hecho pertinente y, en particular, de cualquier elemento que pueda afectar a la apreciación del artículo 1 de la presente Decisión de que la República Oriental del Uruguay garantiza un nivel adecuado de protección de datos personales a los fines del artículo 25 de la Directiva 95/46/CE, así como de cualquier elemento que demuestre que la presente Decisión se está aplicando de forma discriminatoria.

Artículo 5

Los Estados miembros adoptarán todas las medidas necesarias para cumplir la presente Decisión en el plazo de 3 meses a partir de su fecha de notificación.

Artículo 6

Los destinatarios de la presente Decisión serán los Estados miembros.

Hecho en Bruselas, el 21 de agosto de 2012.

Por la Comisión

Viviane REDING

Vicepresidenta

ANEXO

Autoridad de control competente mencionada en el artículo 1, apartado 2, de la presente Decisión:

Unidad Reguladora y de Control de Datos Personales (URCDP),

Andes 1365, Piso 8

Teléfono: +598 2901 2929 Int. 1352

11.100 Montevideo

URUGUAY

Correo electrónico: http://www.datospersonales.gub.uy/sitio/contactenos.aspx.

Reclamaciones en línea:

http://www.datospersonales.gub.uy/sitio/denuncia.aspx.

Sitio web: http://www.datospersonales.gub.uy/sitio/index.aspx.

02

Mención especial para la Unidad Reguladora y de Control de Datos Personales

2. Mención Especial para la Unidad Reguladora y de Control de Datos Personales

En el marco de la Reunión Ministerial y de Autoridades de Gobierno Electrónico de América Latina y el Caribe, realizada en Costa Rica el 26 y 27 de noviembre, las 29 delegaciones congregadas en Costa Rica votaron a los ganadores de los premios a la excelencia en Gobierno Electrónico, excelGOB, convocados en el marco de la Red Gealc (Red de Gobierno Electrónico de América Latina y el Caribe). Uruguay fue distinguido con dos de tres menciones: una de ellas fue para el sitio web de la Unidad Reguladora y de Control de Datos Personales (URCDP), http://www.datospersonales.gub.uy

03

Principales temas analizados en 2012

3. Principales temas analizados en 2012

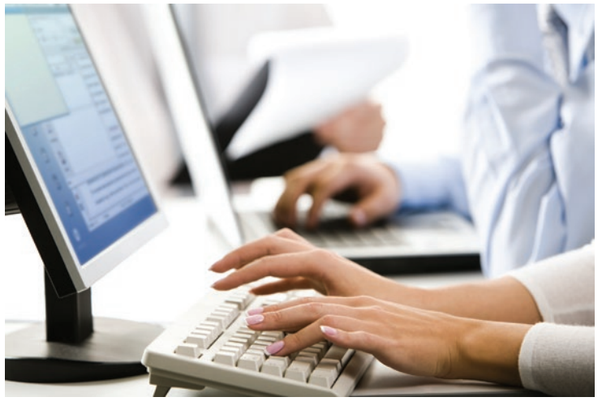
En virtud de los cometidos asignados por la Ley No 18.331 referidos al asesoramiento y asistencia a las personas, organismos y empresas, el Consejo Ejecutivo de la URCDP ha emitido diferentes resoluciones y dictámenes en temas de interés relacionados con la protección de datos.

A continuación, se realiza un detalle de los pronunciamientos relacionados con la actividad desarrollada en el año 2012.

a. Apostasía

A raíz de la conformación de un grupo llamado "Apostasía Colectiva en Uruguay", se consulta respecto a si resulta procedente la aplicación de las disposiciones de la Ley Nº 18.331.

En el Dictamen N° 1, de 15 de marzo, se establece que apostatar, según el diccionario de la Real Academia Española significa: "Negar la fe de Jesucristo recibida en el bautismo". Mediante "el bautismo se asienta el acto de celebración de uno de los sacramentos que otorga la Iglesia Católica, no constituyendo, por ende, un dato que pueda tildarse de inexacto total o parcialmente, erróneo o falso, para apostatar, o, como exige la normativa de protección de datos, para proceder a su rectificación, actualización o eliminación. (artículos 10, 11 y 13 del Decreto Nº 414/009 y artículo 15 de la LPDP)".



Se concluye finalmente "que los datos contenidos en los libros de bautismo no configuran en sentido estricto, la categoría de bases de datos, sino simplemente un conglomerado de datos que implica dificultad de búsqueda, acceso e identificación, atento a que no se encuentran organizados o estructurados ni alfabéticamente ni por fecha de nacimiento, sino por fecha de celebración del bautismo (artículo 4º, literal A de la LPDP)".

b. Gestión de datos de salud

- A través del Dictamen N° 7, de 10 de mayo, se brinda respuesta al Banco de Previsión Social (BPS) acerca de si se debe considerar suficiente la solicitud de turno o cita a efectos de recabar el consentimiento del usuario, para acceder a la historia clínica, o si es necesario algún paso adicional en el encuentro clínico.

En dicho Dictamen se considera que los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar datos personales relativos a la salud física o mental de los pacientes respetando los principios del secreto profesional, la normativa específica y lo establecido en la Ley. En este caso "se entiende que se recaba el consentimiento del titular cuando se realiza la llamada telefónica ya que la persona solicita determinado servicio, por lo que se está ante una manifestación de voluntad, libre, inequívoca e informada. Por tanto, a la hora de pedir la cita o turno se autoriza el acceso a los datos necesarios para realizar el tratamiento y no es necesario ningún otro requisito".

- Por otra parte, la Dirección de Epidemiología del Ministerio de Salud Pública consulta respecto al tratamiento y comunicación de los datos contenidos en las bases de datos relativas a la mortalidad, natalidad, información perinatal y enfermedades de notificación obligatoria, de las cuales es responsable.

Mediante Dictamen N° 23, de 4 de octubre, se determina que son bases que contienen datos sensibles por lo cual la Ley exige que para el tratamiento y comunicación de los mismos, se cuente con el consentimiento expreso y escrito del titular, admitiéndose sólo las excepciones previstas en la norma.

c. Monitoreo del correo electrónico de trabajadores

Mediante Dictamen N° 9, de 24 de mayo, se evacua la consulta formulada por un integrante del Comité de Seguridad de la Información de la Agencia Nacional de Vivienda, respecto a la pertenencia y uso del correo electrónico entregado a los usuarios, así como a la regulación de la privacidad de la información contenida en los mismos.

Se considera que la jurisprudencia laboral es clara al entender que es una herramienta y un recurso propio del empleador, entregado en tal carácter para que cumpla con las tareas asignadas, por lo cual se poseen ciertas potestades de control y de supervisión, que habilitan a adoptar las medidas necesarias y proporcionales, tendientes a salvaguardar la seguridad del sistema y el desarrollo adecuado de las actividades laborales.

Respecto a la regulación de la privacidad de la información contenida en los mismos, en el Documento "Repertorio de recomendaciones prácticas de la OIT" (Ginebra, 1996), sobre la protección de la vida privada de los trabajadores, se señala que el tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuánime y lícita y limitarse exclusivamente a asuntos directamente pertinentes para la relación laboral.

Se considera que el correo electrónico institucional de un funcionario, muchas veces puede contener información que ataña a su privacidad, incluso datos sensibles que requieren una protección especial, por ello para ejercer el control, es necesario informar expresamente y por anticipado de manera expresa, precisa e inequívoca acerca del mecanismo que se utilizará, la finalidad que tiene y el alcance del mismo, ya sea mediante una circular o reglamento de circulación interna, salvo razones imperiosas que justifiquen continuar con la vigilancia encubierta cuando ésta proceda (art. 13 de la Ley N° 18.331).

Finalmente se establece que, tanto la Administración Pública como las empresas, tienen derecho a controlar, pero limitándose en lo posible a los datos sobre tráfico más que al contenido en sí de las comunicaciones, salvo que ello sea necesario.

d. Cesión de datos del Registro de Estado Civil

Mediante Dictamen N° 17, de 16 de agosto, se brinda respuesta a la consulta formulada por el Ministerio de Educación y Cultura, Dirección General de Registro de Estado Civil, en relación con las solicitudes de datos que se reciben por parte de organismos públicos y privados, respecto a la información contenida en sus bases de datos.

En el mismo se establece que las bases de datos de la Dirección General de Registro de Estado Civil se regulan por el Decreto-Ley N° 1.430 de 12 de febrero de 1879, por ello, respecto a la aplicación de la Ley N° 18.331 debe tenerse presente lo dispuesto por su artículo 3° literal C), en cuanto a su ámbito objetivo de aplicación, donde se excluye a las bases creadas y reguladas por leyes especiales, situación que encuadra en la consulta formulada.

Sin perjuicio de ello, corresponde considerar que la Ley N° 18.331 configura el régimen general en materia de protección de datos personales, como derecho inherente a la persona humana comprendido en el artículo 72 de la Constitución de la República y esto obliga a que, al resolver sobre la entrega de la información a los posibles solicitantes, la consultante debe ajustar sus decisiones a los principios fundamentales en materia de protección de datos personales.

En definitiva, la información contenida en estas bases no puede ser comunicada en forma excesiva o

indiscriminada pues ello podría violentar los derechos, además en cada caso procede atender la pertinencia de la respectiva solicitud y la finalidad para la cual se requieren los datos.

e. Envío de publicidad y tarjetas de créditos no solicitadas

Al resolver sobre las denuncias presentadas contra instituciones comerciales que envían tarjetas de créditos sin que se hayan entregado los datos para esa finalidad, la URCDP expresa que la institución bancaria involucrada "parte de un análisis jurídico erróneo respecto del alcance del art. 9° de la Ley, al decir que los datos que no requieren previo consentimiento informado, o que figuran en la Central de Riesgos o en el Clearing de Informes, son "datos públicos, transmisibles libremente y que se encuentran fuera del ámbito de protección de la Ley".

Agrega que, tal como lo indican los artículos 13 y 17 de la Ley, los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados para el cumplimiento de fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular, así como se deberá informar en forma expresa, precisa e inequívoca la finalidad y quiénes pueden ser sus destinatarios.

Finalmente considera que el Dictamen del Grupo de Trabajo del art. 29 de la UE (junio 2010), favorable a Uruguay, se establece que aunque no sea necesario obtener el permiso de la persona afectada, el responsable sólo puede tratar los datos cuando el tratamiento esté incluido en el ámbito de los objetivos explícitos y legítimos identificados, así como la obligación de informar al interesado se aplica en todos los casos. También en el Dictamen del Consejo de la URCDP Nº 26/010, de 17 de diciembre de 2010 se establece que el encargado de tratamiento tiene la obligación de cumplir principalmente con los deberes de confidencialidad, seguridad de la información, finalidad de los datos tratados y no cesión a terceros, considerando además que el tratamiento de datos personales obtenidos de listados y de Internet, debe respetar los principios de protección de datos, fundamentalmente el principio de finalidad.

f. Creación de bases con datos sensibles

El Instituto Nacional de las Mujeres (INMUJERES) - Departamento de las Mujeres Afrodescendientes, del Ministerio de Desarrollo Social (MIDES), consulta acerca de la formación e inscripción de una base de datos territorial de profesionales y/o técnicos de origen afrodescendiente.

La URCDP se expresa en el Dictamen N° 14, de 28 de junio, señalando que por regla, los datos de origen racial o étnico, -datos sensibles-, sólo pueden ser objeto de recolección y tratamiento con consentimiento expreso y escrito del titular o cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo (art. 18).

Indica que la especial tutela adjudicada a estos datos, tiene por objeto evitar la discriminación, no obstante también existe obligación de los Estados de actuar mediante políticas públicas adecuadas para favorecer el desarrollo de grupos y sectores de la sociedad que no tienen objetivamente las mismas posibilidades, propendiendo a la consolidación de una política social redistributiva de carácter progresivo, tal como se expresa en el Decreto N° 286/006, de 22 de agosto de 2006. Debido a esto, determinadas entidades públicas, de acuerdo con sus fines y cometidos, podrán mantener registro de este tipo de datos personales pues la finalidad es la justificación y fundamento para las políticas públicas que se adoptan, evaluar los avances que se han producido y su influencia en el colectivo afrodescendiente.

El MIDES tiene los cometidos asignados en la Ley de creación N° 17.866, de 25 de marzo de 2005 y normas posteriores, por lo cual no sería exigible recabar el consentimiento informado de los titulares, en tanto estos sean efectiva o potencialmente beneficiarios de sus programas, aplicándose el inciso B) del artículo 9° de la Ley N° 18.331.

Se establece por último que la referida base de datos, deberá ser inscripta en el Registro de la URCDP dentro del plazo de 90 días contados desde su creación, así como contar con medidas de seguridad acordes.

g. Almacenamiento de datos en sistemas de compras on line o comercio electrónico

Se analizaron varias denuncias formuladas contra una empresa de comercio electrónico, por presunto almacenamiento de datos de tarjetas de créditos de quienes realizan compras on line. En el marco de esas denuncias, el cuerpo inspectivo de la URCDP realizó dos inspecciones a efectos de constatar fehacientemente si esos datos quedaban almacenados en alguna de las bases de datos que la empresa posee. También se procedió a estudiar técnicamente cómo funciona la operativa y cómo se realiza el tratamiento de los datos por parte del tercero que se encuentra ubicado en el exterior del país. A su vez, junto a los representantes legales de la empresa se analizaron las nuevas políticas de privacidad disponibles a partir de las denuncias, en el sitio web.

h. Mantenimiento de datos relativos a sanciones en la Web

Se estudian las denuncias presentadas contra un organismo público, por mantener en su página web, los datos personales de los profesionales que han sido suspendidos, vinculados a las decisiones de suspensión y rehabilitación en su ejercicio, función establecida a dicho organismo por mandato legal.

Se considera que el aspecto medular objeto de la denuncia y de la resolución adoptada, es el derecho que le asiste al denunciante a ejercer el control de sus datos personales, motivo por el cual se solicita al responsable de la base la actualización y supresión de los mismos cuando ya se ha verificado el fin de la sanción.

El derecho que el denunciante ha reclamado, específicamente por persistir en la Web determinada información que le causa un claro perjuicio a su imagen profesional, a su honor y dignidad, se relaciona con el actual desarrollo de la protección de datos personales. En este sentido, la URCDP considera muy especialmente un nuevo derecho denominado "Derecho al Olvido", cuya aplicación se impone cada vez a fuerza de los reclamos de las personas afectadas por la difusión de su información personal en forma indefinida en el tiempo y el espacio.

Tan importante es el desarrollo del mismo que la Unión Europea ya lo ha incorporado a su paquete de reformas al sistema de protección de datos.

Este derecho, -que es en realidad una aplicación del actual derecho a la cancelación, supresión u oposición-, enfatiza que los responsables del tratamiento están obligados a suprimir los datos de los interesados que así lo soliciten. Muchos afirman que esta obligación recae directamente sobre el responsable que primero publicó esos datos personales, aunque los mismos luego hayan sido recogidos o publicados en otros sitios de Internet, por lo cual será quien debe dirigirse a estos para pedir la cancelación.

i. Disociación de datos y aplicación de los principios de finalidad y proporcionalidad en resoluciones publicadas por organismos públicos

Se consulta por parte de la Asesoría Letrada de la Dirección General de Registro (DGR), sobre la publicación en la página web de las resoluciones administrativas derivadas de peticiones o de contenciosos administrativos, con la finalidad de dar a conocer la posición de esta Dirección en las diferentes materias.

Mediante Dictamen N° 18, de 30 de agosto, la URCDP entiende que la Dirección Nacional de Registros cuenta con una ley especial de creación y regulación, la Ley N° 16.871, de 28 de setiembre de 1997, por lo que entra dentro de la excepción planteada en al literal C) de la Ley N° 18.331. Respecto al consentimiento previo e informado que establecen los artículos 9° y 17, no sería necesario recabarlo si los datos provienen de fuentes públicas tales como registros públicos.

Por último, se recomienda tratar los datos personales de acuerdo con los principios generales aplicables en la materia, específicamente en lo relativo a la publicación en la página web efectuando a tales efectos un proceso de disociación.

También se ha evacuado una consulta respecto a cómo adecuar el contenido de las Resoluciones del Directorio de la Administración de las Obras Sanitarias del Estado (en adelante OSE), a lo establecido en la Ley N° 18.331 con la finalidad de ser publicadas en la Web de dicho organismo público.

Mediante Dictamen N° 26, de 1° de noviembre se señala que no hay soluciones uniformes y globales que puedan abarcar la universalidad de hipótesis que puedan plantearse en cada organismo público; sin embargo hay datos que deben ser resguardados pues se trata de datos personales que requieren previo consentimiento informado según se establece en la Ley N° 18.331 y en el artículo 10 Núm. II de la Ley N° 18.381.

Por otra parte, en aras de proteger la dignidad de aquellas personas sometidas a un sumario administrativo, el expediente podría ser clasificado como reservado de acuerdo con el art. 9° D) de la Ley N° 18.381, y dicha reserva debería durar hasta tanto se resuelva definitivamente sobre el asunto, brindándose luego acceso a la resolución que corresponda.

En cuanto a la publicación en la Web de las resoluciones, corresponde tener presente que de acuerdo con el art. 9° existen determinados datos personales que no requieren el previo consentimiento para ser tratados. A su vez, el literal b) del artículo 9° establece que no es necesario recabar el previo consentimiento informado cuando se está ante el "ejercicio de funciones propias de los Poderes del Estado", o la recolección de datos se efectúa "en virtud de una obligación legal", por lo cual en este caso es razonable interpretar que la Ley N° 18.381 de Acceso a la Información Pública contiene una obligación legal que tiene como objetivo garantizar la transparencia de la administración pública.

De todas maneras, corresponde analizar ante el caso concreto, si el contexto no revela directa o indirectamente otro tipo de información que podría afectar en forma desproporcionada la privacidad de una persona, por lo cual debería efectuarse la publicación con los datos disociados tal como se establece en el art. 17 Literal D) de la Ley N° 18.331.

j. Estudio de artículos y proyectos normativos que impactan en la protección de datos personales

Mediante Dictamen N° 27, de 15 de noviembre, la URCDP se pronuncia respecto al Proyecto de Ley presentado por los Señores Senadores Francisco Gallinal y Luis Alberto Lacalle (Carpeta 978/2012 de la Cámara de Senadores) para modificar la redacción del artículo 22 de la Ley Nº 18.331.

En el texto proyectado se proponen una serie de modificaciones al régimen de tratamiento de los datos personales comerciales y refieren a la obligación de notificar a los deudores inscriptos en registros privados abiertos a la consulta por parte de terceros, a un procedimiento de descargos del titular del dato, a la disminución de los plazos de registro de los morosos, a la prohibición de registrar datos comerciales positivos y un régimen a seguir para el registro de morosidades provenientes de deudas ante organismos estatales.

Se considera que el proyecto se adecua, en general, al criterio tuitivo de la normativa sobre protección de datos personales y por ende, se comparte la solución de notificar a los deudores personas físicas su registro, con requisitos de plazo y contenido al efecto. Sin embargo, presenta algunos puntos susceptibles de adecuación, a saber: extensión a las personas jurídicas del requisito de notificación registral y oportunidad de plantear descargos; remisión más genérica respecto del régimen sancionatorio del art. 2º (cita del art. 35 de la Ley Nº 18.331, sus modificativos y concordantes) y empleo de los términos "acreedor o registrador" en vez de "obligado" en el inciso 2 de ese artículo.

También se realiza el análisis del art. 291 del Proyecto de Ley de Rendición de Cuentas y Balance de Ejecución Presupuestal- Ejercicio 2011: "Incorpórase al artículo 2 de la Ley N° 18.812, de 23 de setiembre del 2011, el siguiente inciso a continuación del primero:

"Sin perjuicio de lo dispuesto en el inciso precedente, una vez transcurrido el plazo para que los datos permanezcan inscriptos en la Central de Riesgos Crediticios, el Banco Central del Uruguay podrá mantenerlos como datos estadísticos con el único fin de realizar estudios de riesgo de crédito para el desarrollo de sus funciones de regulación, adquiriendo tales datos, en este caso, carácter confidencial".

Por parte de la URCDP se resuelve solicitar al BCU que aporte información acerca de si los datos serán conservados más allá de los plazos legales establecidos en forma disociada de sus titulares, al amparo de lo previsto por el literal D) del artículo 17 de la misma norma y que a su vez aclare el alcance de la finalidad expresada en la frase: con el único fin de realizar estudios de riesgo de crédito para el desarrollo de sus funciones de regulación.

k. Intercambio de información entre organismos del Estado

Varios organismos consultan acerca de cómo implementar el intercambio de datos que deben realizar con otros organismos para cumplir con sus funciones o cometidos.

Entre los consultantes se encuentra el Banco de Previsión Social que hace referencia al Sistema Nacional de Certificación Laboral. Se informa que en el marco del Sistema Nacional Integrado de Salud (SNIS), en los contratos de gestión que firmó la Junta Nacional de Salud (JUNASA) con los efectores de la salud, obliga a estos, a que informen lo actuado –tras la solicitud del trabajador- al Instituto de Seguridad Social por medios electrónicos para que el trabajador pueda acceder al subsidio.

En este caso, el consentimiento es prestado por el trabajador en el formulario que se transmite por medios electrónicos mediante su suscripción, por lo que se entiende que se está dando cumplimiento a este requisito. En cuanto al interés legítimo del emisor, éste se verifica en que el trabajador desea acceder al subsidio por enfermedad. A su vez, el interés del destinatario radica en cumplir las funciones asignadas por Ley. Atento a ello, se considera que la comunicación de datos es legítima, y que cumple con todos los requisitos exigidos por la normativa vigente.

En tanto el subsidio por enfermedad, beneficio que abona BPS a los trabajadores activos, que por razones médicas se encuentran imposibilitados de trabajar de acuerdo con lo establecido en el Decreto Ley N° 14.407, de 22 de julio de 1975 y disposiciones concordantes, el Sistema Nacional de Certificación Laboral tiene como objetivo general aplicar un nuevo procedimiento de certificaciones médicas que permita consolidar la capacidad de gestión asociada al subsidio por enfermedad, rediseñando el modelo de atención en salud en el marco del Sistema Nacional Integrado de Salud, por ende en el caso concreto resulta aplicable el artículo 17 de la Ley que establece, por remisión al artículo 9° literal b) que no es necesario recabar el consentimiento cuando se trata de organismos en ejercicio de sus funciones. En este caso concreto, el BPS está ejerciendo una competencia propia asignada por Ley.

En tanto, se evacua la consulta sobre la celebración de un Convenio de intercambio de conocimientos y datos entre la Intendencia de Canelones (IC) y Obras Sanitarias del Estado (OSE). A través de este convenio la IC brindará la información relativa al nomenclátor (numeración y calles), además de aspectos catastrales y toda otra relevante concerniente a la georeferenciación de padrones del departamento; y OSE, por su parte, brindará la información de sus clientes: dirección, localidad, padrón, titular del contrato, tipo de documento (CI, Pasaporte, CC), número de documento, teléfono, email, relación con el servicio (propietario, inquilino, ocupante, etc.), dirección de envío, dirección de suministro.

Mediante Dictamen N° 4, de 26 de abril, se determina que la información a aportar por parte de la Intendencia de Canelones (IC) relativa a nombres de calles y números de padrones, en principio constituye información pública siempre que esté disociada de los titulares y por ende no presentaría objeciones desde el punto de vista de la protección de datos personales. En cuanto al término "toda otra información relevante relativa a la georeferenciación de padrones del departamento de Canelones", cabe tener presente que la Unidad ya se expidió en el Dictamen N° 6/2010 de 11 de febrero de 2010, respecto a que en las cédulas catastrales se encuentra el nombre de una persona relacionado con un determinado padrón, por lo que podría constituir un dato determinable de acuerdo con lo establecido en el artículo 4° de la LPDP, por lo cual deberá establecerse con claridad el alcance de este término en el convenio definitivo.

Respecto a la información a aportar por parte de OSE, el art. 9° C) de la Ley establece que no será necesario el previo consentimiento cuando los datos se encuentren en listados y se limiten a los que se indican en dicho artículo. Hay otros datos que en cambio sí requieren consentimiento como: número de Credencial Cívica, número de teléfonos fijos o celulares, correos electrónicos y tipo de relación con el servicio (propietario, inquilino, ocupante, etc.).

En definitiva, se considera que, tanto la IC como OSE, deberán solicitar el consentimiento de los titulares para comunicar los datos que requieren el previo consentimiento informado, así como para el caso de publicación o divulgación al público de dicha información, se deberá estar en consonancia con lo establecido en las Leyes N° 18.331 de Protección de Datos Personales y N° 18. 381 de Derecho de Acceso a la Información Pública (art. 10 Núm. II y fine).

Por otra parte, mediante el Dictamen N° 13, de 28 de junio, se evacúa la consulta formulada respecto al sistema de defunciones digital que actualmente está implantando el Ministerio de Salud Pública (MSP), que habilita a que los médicos certifiquen la defunción de una persona a partir del ingreso al sistema informático con su firma, al igual que lo hacen para el certificado de nacido vivo. Para ello, existe un Web service que provee información de las defunciones certificadas por el MSP, al que sólo accede el Registro Civil, sin embargo otros organismos o entidades también han planteado el interés de acceder al mismo.

El análisis se centra en los arts. 157 a 160 de la Ley N° 18.719, sobre intercambio de información entre Entidades Públicas, estatales o no, sobre todo en el art. 158 que establece que a los efectos del intercambio, una de las obligaciones consiste en recabar el consentimiento de acuerdo con lo previsto en la Ley Nº 18.331, cuando el objeto de intercambio refiere a información privada o de particulares que requiere el previo consentimiento informado. En tanto que en el art. 159 se establece que dichas entidades deberán ajustar su actuación a una serie de principios, entre ellos el de previo consentimiento informado, el de finalidad y los de confidencialidad y seguridad, los cuales a su vez, sirven de criterio interpretativo para resolver las cuestiones que puedan suscitarse.

Se considera que el aspecto central a considerar es la finalidad del intercambio, por eso debe analizarse el marco de poderes y competencias que han sido asignadas por ley a cada organismo, para determinar si es posible aplicar algunas de las excepciones establecidas en la Ley N° 18.331.

En el caso que se consulta, atento a los cometidos asignados al MSP en la Ley de su creación N° 9.202, de 12 de enero de 1934, y normas posteriores, así como al Registro Civil, por las Leyes N° 13.737 (art. 154) y N° 14.269, y demás normas existentes, no es exigible recabar el consentimiento informado de los titulares de los datos, pues resulta aplicable el inciso B) del artículo 9°. No obstante, en el caso de que dicha comunicación se realice a otras entidades, como por ejemplo al BROU, se deberá recabar el previo consentimiento ya que los cometidos específicos de esta entidad no habilitan a interoperar directamente con el MSP, sino que corresponde que los datos de las defunciones de sus clientes sean proporcionados directamente por el Registro de Estado Civil.

Respecto a la confidencialidad de la causa de muerte, la Unidad expresa que ésta se trata de un dato clínico reservado en virtud de lo dispuesto en la Ley N° 18.335 sobre Derechos de los Pacientes y Usuarios, así como en la Ley N° 18.331 de Protección de Datos Personales, y en este sentido la codificación de dicho dato clínico, es un mecanismo idóneo para garantizar la reserva y confidencialidad.

04

Avances en materia de protección de datos

4. Avances en materia de protección de datos

a. Uruguay, país adecuado

Con fecha 21 de agosto de 2012 por decisión de la Comisión Europea nuestro país adquirió el estatus de adecuado -como se mencionó en el punto 2 ut supra-, lo que constituye un hito y una ventaja competitiva para el país.

b. Aprobación del Convenio N° 108 del Consejo de Europa

En setiembre de 2011 el Poder Ejecutivo envió un proyecto de Ley al Parlamento con el objeto de ratificar el Convenio Nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo Adicional.

Así, el 13 de noviembre de 2012, dicho proyecto fue aprobado por el Senado, pasando luego a estudio de la Cámara de Representantes, quien el 12 de diciembre lo aprueba, incorporando al Derecho Positivo Nacional el Convenio y su Protocolo Adicional mediante la Ley Nº 19.030.

Hasta la fecha, Uruguay es el único país no miembro de la Unión Europea invitado a adherir al Convenio y su Protocolo Adicional.

c. Iniciativa nacional relacionada con la protección de datos

Durante el año 2012, corresponde mencionar a nivel nacional, la incorporación a la Ley Nº 18.331 del artículo 9° bis que establece lo qué se considera fuente pública o accesible al público. (Ley N° 18.996, de 21 noviembre de 2012, artículo 43).

d. Iniciativas internacionales relacionadas con la protección de datos

En 2012 Colombia, Nicaragua y Filipinas aprobaron leyes de protección de datos. De esta manera han pasado a integrar el grupo de países con legislación en la materia.

Colombia

En el año 2012, Colombia se unió a la nómina de países latinoamericanos que cuentan con legislación en materia de protección de datos personales.

El 17 de octubre de 2012, publicó la Ley Estatutaria N° 1.581 para la Protección de Datos Personales.

Esta cuenta con 30 artículos estructurados en 9 Títulos que refieren a: objeto, ámbito de aplicación y definiciones; principios rectores, categorías especiales de datos, derechos y condiciones de legalidad para el tratamiento de datos; procedimientos, deberes de los responsables del tratamiento y encargados del tratamiento de los mecanismos de vigilancia y sanción; transferencia de datos a terceros países, y otras disposiciones.

En su artículo 4° se detallan los principios rectores: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

El artículo 8° establece los derechos de los titulares y el 19 designa como autoridad a la Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales. Este organismo puede imponer sanciones tales como multas, suspensión y cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.

También se crea un Registro Nacional de Bases de Datos en la órbita de la Superintendencia de Industria y Comercio.

Nicaragua

El 21 de marzo de 2012 se aprueba la Ley Nº 787 de protección de datos personales en Nicaragua, siendo otro país más de la región que realiza sus avances en la materia.

Dicha ley cuenta con 9 Capítulos formados por 56 artículos, en los que se regulan definiciones generales y disposiciones transitorias, las obligaciones de los responsables de los ficheros, derechos de titular del dato; aparece el derecho al olvido informático, así como se define qué es un dato personal informático y la obligatoriedad de la inscripción de los ficheros; crea la Dirección de Protección de Datos Personales adscripta al Ministerio de Hacienda y Crédito Público, que contará con un Director designado por la máxima autoridad administrativa de dicho ministerio y que tiene por objeto el control, supervisión y protección del tratamiento de los datos personales contenidos en ficheros de datos de naturaleza pública y privada.

Esta Dirección tendrá personal calificado para realizar las inspecciones a los ficheros.

A su vez regula las infracciones, las que clasifica en leves y graves, así como las sanciones administrativas.

Filipinas

Fuera del plano de América, el 15 de agosto de 2012, Filipinas aprobó su Ley de Protección de Datos Personales N° 10.173. La misma obliga tanto a las personas públicas como a las privadas a garantizar la privacidad, seguridad e integridad de los datos personales.

La Ley busca cumplir los estándares internacionales, dado que se basa en la Directiva 95/46/CE.

El documento cuenta con 45 artículos ordenados en 9 Capítulos.

El Capítulo 2 crea la Comisión Nacional de la Privacidad como órgano encargado de supervisar el cumplimiento de la ley. Esta comisión estará compuesta de un Comisionado y dos Subdirectores: uno a cargo de sistemas de procesamiento de datos y otro a cargo de políticas y planeamiento.

Los principios de la protección de datos se establecen en el Capítulo 3 y los derechos de los titulares de datos en el capítulo 4.

Uruguay avanza en Protección de Datos Personales

Ley Nº 18331

Aprobación de la Ley Nº 18331 de Protección de Datos y Acción de Habeas Data.

11.8.2008

Consejo Ejecutivo URCDP

Asumieron los miembros del Consejo Ejecutivo de la URCDP.

24.4.2009

URUGUAY MIEMBRO
Conferencia Internacional

Uruguay fue aceptado como miembro de la Conferencia Internacional de PD.

2009

Proceso de Adecuación y RIPD

- El Grupo de Trabajo del Artículo 29 PD adoptó un dictamen favorable sobre el nivel de protección de datos en Uruguay en el proceso de Adecuación de la Unión Europea.
- Uruguay es miembro del Consejo Ejecutivo de la Red Iberoamericana de Protección de datos personales.

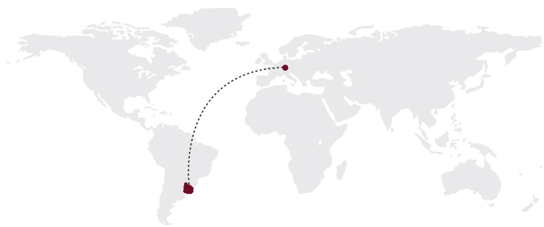
2010

URUGUAY ANFITRIÓN

Uruguay es seleccionado como país anfitrión de la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad

2011

Consejo de Europa invitó a Uruguay
Convenio Nro 108



- El Consejo de Europa invitó a Uruguay a ratificar el Convenio Nro 108 y su Protocolo Adicional.
- Uruguay es miembro del Comité Ejecutivo de la Conferencia Internacional

2012

URUGUAY ADECUADO
Declarado por la Unión Europea

Uruguay fue declarado país adecuado por la Unión Europea en materia de Protección de Datos Personales, de conformidad con la “Directiva 95/46/CE”.

Octubre
34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad

12 de Diciembre
Ley N° 19.030

Uruguay aprobó la adhesión al Convenio N° 108

05

Jurisprudencia

5. Jurisprudencia

Jurisprudencia internacional

Sentencia del Juzgado Federal Nº 2 de Santa Fe, Argentina Nº 61, de 19 de mayo de 2012.

En materia de protección de datos, resulta relevante reseñar la Sentencia N° 61[1] del Juzgado Federal N° 2 de Santa Fe, Argentina, de 19 de marzo de 2012.

En el presente caso, la actora interpone una acción de habeas data contra AFIP-DGI (Agencia Santa Fe).

Mediante la acción, la actora busca dar de baja la CUIT (clave única de identificación tributaria) a su nombre, con toda la información relacionada.

La demandada indica que el derecho de la actora se puede desdoblar en el derecho de acceso a los datos (que fueron aportados en instancia penal) y en los derechos de rectificación, actualización y/o supresión. De los segundos no se pudo dar cumplimiento atento a que no tenían conocimiento de la falsedad de las firmas que obraban en los documentos con anterioridad a la acción en trámite.

En el relato de hechos surge que la actora extravió su documento de identidad, el que fue usado por terceros para obtener una CUIT a su nombre en el rubro de "cultivo de cereales". La actora presenta una acción penal y una nota ante la demandada reclamando el derecho de acceso a sus datos. No obtiene respuesta de la demandada en el plazo legalmente establecido y la Sede no recibe el argumento de que toda la información había sido aportada en la instancia penal.

Asimismo indica que la acción de habeas data se aplica a la finalidad buscada por la actora, ya que busca evitar el uso abusivo de los datos personales.

Esta sentencia es relevante porque demuestra la importancia de los derechos del titular del dato en la esfera personal y económica.

Sentencia[2] del Tribunal Supremo, Sala de lo Contencioso Administrativo, Sección Sexta, España de 8 de febrero de 2012

Otra sentencia de interés es la dictada en fecha 8 de febrero de 2012, por el Tribunal Supremo, Sala de lo Contencioso Administrativo, Sección Sexta, España.

En esta sentencia se resuelve el recurso presentado por la Federación Comercio Electrónico y Marketing Directo contra varios artículos del decreto que reglamenta la Ley de protección de datos personales. Argumentan que dichos artículos contradicen la Directiva 95/46/CE del Consejo de Europa, al establecer nuevas restricciones y requisitos para el tratamiento de datos personales; explícitamente solicita el inequívoco consentimiento del afectado, salvo disposición contraria de la ley.

1 Sentencia extraída de la página web de la Dirección Nacional de Protección de Datos Personales. El texto completo de la sentencia se puede consultar en: http://www.jus.gob.ar/scripts/dnpdp-jurisprudencia/im_verpag.asp?ID=705

2 Sentencia extraída de la página web de la Agencia de Protección de Datos de la Comunidad de Madrid. El texto completo de la sentencia se puede consultar en: http://www.madrid.org/cs/Satellite?cid=1252308394502&language=es&pagename=PortalAPDCM%2FPage%2FPAPD_listado

Indica el Tribunal que la normativa comunitaria proclama el principio del consentimiento inequívoco, siempre que no concurran otras causas legítimas.

Según la Directiva si no media el consentimiento, se puedan tratar los datos cuando exista un interés legítimo del responsable o los destinatarios de los datos, siempre que no deba prevalecer el interés de los derechos del titular del dato. La normativa española adiciona al interés legítimo el hecho de que los datos deben figurar en fuentes accesibles al público. Estas fuentes son enumeradas taxativamente en la Ley.

Ellas son el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo, así como los diarios y boletines oficiales y los medios de comunicación.

Sostiene el Tribunal que la gravedad de la lesión de los derechos de la persona afectada por el tratamiento puede variar según los datos se encuentren o no en fuentes públicas.

La relevancia de esta sentencia está en que valora varios puntos de interés como el consentimiento del titular, la existencia de fuentes públicas y la adaptación de la normativa nacional a normativa comunitaria.

Jurisprudencia nacional

Es de interés la referencia a aquellas sentencias dictadas por los Tribunales Nacionales que se destacan por estar vinculadas a la aplicación de la normativa de protección de datos, por lo que se reseña lo tratado a lo largo de 2012.

Sentencia del Tribunal de lo Contencioso Administrativo N° 269, de 29 de mayo de 2012

La presente sentencia refiere a una acción de nulidad solicitada por una empresa dedicada a proporcionar información crediticia, respecto de la Resolución N° 28/009, de 31 de julio de 2009, dictada por la Unidad Reguladora y de Control de Datos Personales (URCDP) en que dispone la adecuación de las bases de datos de la empresa a las disposiciones de la Ley N° 18.331. La empresa sostiene que los datos incluidos son identificatorios de personas físicas y que refieran a su calidad de fallecidas, por lo tanto son datos públicos que no pueden estar sujetos a limitaciones temporales.

En la evacuación de vista la demandada indica que el acto que se pretende anular no es lesivo. Asimismo, como la finalidad de la empresa es brindar informe objetivos de carácter comercial, toda la operativa de la misma recae en el artículo 22 de la Ley N° 18.331. Los datos personales, se indica, deben calificarse y regularse según la finalidad para la que fueron recolectados y no por una caracterización abstracta descontextualizada del uso que van a tener esos datos.

El Tribunal, en forma unánime rechaza la demanda, confirmando la resolución de la URCDP. Establece que las distinciones que realiza la empresa actora sobre datos personales identificatorios y comerciales, positivos y negativos, referidos a personas vivas y a personas fallecidas, no resulta de recibo ya que la ley no realiza estas distinciones. Tampoco resultan de recibo las manifestaciones realizadas por la accionante en el sentido que los datos identificatorios son tratados con una finalidad diferente a la comercial.

Por estos argumentos es que se rechaza la acción interpuesta, confirmándose el acto recurrido.

Se destaca en la presente sentencia la importancia atribuida al principio de finalidad en el tratamiento de datos personales.

Sentencia del Tribunal de Apelaciones en lo Civil de 2° Turno N° 171, de 31 de julio de 2012

Esta sentencia revoca la primera instancia tramitada en el Juzgado Letrado de Primera Instancia en lo Civil de 9º Turno Nº 10, de 8 de marzo de 2012, basándose en la inaplicabilidad de las Leyes N° 18.331 y N° 18.381.

Sostiene el Tribunal que lo reclamado no refiere a datos personales tutelables por medio del "habeas data" de la Ley N° 18.331.

Nada excluye, indica el Tribunal, que puedan existir datos de carácter personal utilizados con fines de pago y otras operaciones realizadas por un organismo proveedor de medios de pago, pero el reclamo que realizó el actor no fue basado en la afectación de datos personales sino que fue realizado debido a la información que se le proporcionó a la actora del por qué tenía menos dinero disponible que el depositado. Esta debió demandar por incumplimiento utilizando la vía civil como correspondería.

En este caso el Tribunal realiza una interpretación que no condice con el concepto de dato personal de acuerdo al artículo 4 literal D) de la Ley.

Sentencia del Tribunal de Apelaciones en lo Civil de 6º Turno Nº 115, de 16 de mayo de 2012

Esta sentencia confirma la primera instancia donde se condena por daños y perjuicios a un banco por inclusión errónea en una base de datos crediticia.

El actor canceló una deuda mantenida con el banco por una tarjeta de crédito y erróneamente fue incluido con posterioridad en una base de datos de morosidad.

Al banco en cuestión no le constaba la cancelación de la deuda, y por la inclusión en la base de datos el actor pierde la posibilidad de obtener un préstamo. Finalmente, el actor presenta el documento que acredita el pago.

La presente sentencia es relevante porque toma en cuenta el daño moral que produce la inclusión errónea en una base de datos personales.

Sentencia del Juzgado Letrado de Primera Instancia en lo Civil de 9° Turno N° 10, de 8 de marzo de 2012

En esta sentencia la Sede resuelve acerca de una acción de Protección de Datos Personales fundada como Acceso a la Información Pública.

En la presente, la actora solicita información acerca de retenciones operadas en sus haberes de naturaleza salarial y que cobra a través de una caja de ahorro bancaria.

Haciendo uso del principio iura novit curiae, el sentenciante realiza la correspondiente subsunción en base a una normativa diferente de la invocada sin alterar la pretensión. Aún cuando no considera de injerencia a la Ley Nº 18.381 de Acceso a la Información Pública sí lo sería la Ley Nº 18.331, de Protección de Datos Personales y Acción de Habeas Data.

Asimismo, indica que no existen razones de forma ni de fondo que obsten el acceso a la investigación administrativa que pretende la actora, por lo que la negativa de la parte demandada a brindar ese acceso resulta ilegítima por contrariar las normas constitucionales y legales aplicables. Se otorga a la accionada un término de diez días para el cumplimiento del fallo.

El interés de esta sentencia radica en la correcta aplicación que realiza el Juez de la normativa en materia de protección de datos.

Sentencia del Juzgado Letrado de Primera Instancia en lo Penal de 4º Turno Nº 56, de 11 de junio de 2012

Esta sentencia resuelve sobre un pedido de derecho de respuesta a raíz de la utilización sin previo consentimiento y por parte de diferentes medios de comunicación de una imagen.

El accionante indica que su imagen fue difundida sin difuminarse, asociada a la noticia de un hurto en un edificio de apartamentos. Asimismo, se hacía referencia a que el portero del edificio (actor de esta causa) había permitido el ingreso de los delincuentes.

El actor indica que su imagen fue captada en un ámbito privado (su trabajo) y fue difundida sin su consentimiento, trayéndole problemas como por ejemplo su despido.

Varios de los medios, responden que no procede el derecho a respuesta, atento a que las imágenes no son agraviantes de por sí y fueron difundidas en el desarrollo de una noticia de innegable interés.

Asimismo indican que el derecho de respuesta se utiliza para la contestación de informaciones inexactas o agraviantes pero no es un instrumento de defensa del derecho a la imagen.

La Sede falla denegando el pedido, atento a que sostiene que de las publicaciones no surge ningún agravio para el actor, ni las imágenes publicadas constituyen información inexacta.

En esta sentencia se valora únicamente la Ley de Prensa N° Ley 16.099, de 4 de diciembre de 1989, pero en ningún momento de valora la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data.

06

Presentación de la Memoria 2011

6. Presentación de la Memoria 2011

El 2012 significó el cuarto año de funcionamiento de la Unidad, período en el que se cumplieron importantes hitos, entre ellos la declaración de Uruguay como país adecuado, la ratificación del Convenio N° 108 y su Protocolo Adicional, y la designación de Uruguay como país anfitrión de la 34ª Conferencia Internacional de Autoridades de Protección de Datos Personales y Privacidad.

El 4 de junio se presentó la Memoria Anual 2011 de la Unidad Reguladora y de Control de Datos Personales (URCDP). En esa oportunidad, además se realizó el lanzamiento oficial de la 34ª Conferencia Internacional de Autoridades de Protección de Datos Personales y Privacidad.

Este acto se llevó a cabo en el Edificio José Gervasio Artigas" (Anexo) del Palacio Legislativo y contó con la presencia del Sr. Prosecretario de la Presidencia de la República Dr. Diego Cánepa y los Miembros del Consejo Ejecutivo de la URCDP, Dr. Felipe Rotondo, Mag. Federico Monteverde e Ing. José Clastornik, así como la presencia de destacados participantes de la esfera pública y privada.

En su discurso, Monteverde señaló el incremento significativo de la cantidad de consultas y explicó que "la naturaleza global de las redes de intercambio de información hacen imprescindible que nuestra Unidad tenga relación con Unidades de otros países".

Por su parte, Clastornik realizó el lanzamiento oficial de la 34ª Conferencia Internacional de Autoridades de Protección de Datos Personales y Privacidad, destacando sus características en relación con la estructura programada en plenarios y paneles.

Presentación de la Memoria 2011

07

Difusión y capacitación de la Unidad Reguladora y de Control de Datos Personales

7. Difusión y capacitación de la Unidad Reguladora y de Control de Datos Personales

a. Sitio web

A los efectos de continuar brindando un adecuado conocimiento a la ciudadanía en lo relativo a las novedades y al ejercicio de sus derechos además del cumplimiento de sus obligaciones, la Unidad ha continuado la mejora de su página web oficial. Entre las novedades se destaca:

Migración del sitio web

Se ha llevado a cabo la migración del sitio web de la Unidad a una nueva herramienta de software que permite crear y gestionar portales Web.

La herramienta proporciona un punto único de acceso a los contenidos Web y aplicaciones, al tiempo que ofrece experiencias diferenciadas y personalizadas para cada usuario.

La migración y puesta en producción realizada le brinda a la Unidad Reguladora y de Control de Datos Personales una mayor autonomía en el manejo de la información brindada a la ciudadanía y beneficia, además, la mejora continua del portal.

b. Publicaciones realizadas

Folleto informativo

Se ha publicado un folleto de carácter informativo en referencia a qué es la URCDP y cuáles son sus cometidos. Asimismo, determina el concepto de dato personal, las formas en que se pueden ejercer los derechos y el avance de Uruguay en la materia.

E-Learning

Por otra parte, la Unidad Reguladora y de Control de Datos Personales (URCDP) ha desarrollado un curso online y gratuito sobre la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, dirigido a funcionarios públicos y ciudadanos, con el objetivo de dar a conocer el derecho a la protección de datos personales y los conceptos fundamentales de la ley, así como informar sobre los cometidos de la URCDP como órgano de control del cumplimiento de los derechos establecidos por la Ley.

El curso se encuentra formado por tres módulos: 1) el derecho a la protección de datos personales; 2) base de datos, responsables de las bases de datos, principios; y 3) quienes garantizan los derechos.

El curso es interactivo y puede ser realizado por cualquier ciudadano que desee conocer aspectos generales de la Ley. Esta iniciativa constituye un nuevo paso hacia el conocimiento de la protección de datos como derecho fundamental.

Guías temáticas

En el mismo sentido, la Unidad Reguladora y de Control de Datos Personales (URCDP) ha desarrollado cinco guías sectoriales educativas sobre la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, dirigidas a funcionarios públicos y ciudadanos.

Dichas guías se encuentran enfocadas a la capacitación de los sectores específicos: educación, salud, administración pública y telecomunicaciones. El objetivo es promover y desarrollar actividades de difusión de la normativa vigente, actualización y capacitación en materia de protección de datos personales en las mencionadas áreas.

Al respecto, la Guía N° 1 refiere a "Los datos personales y su protección", donde se define el concepto de dato personal, describiéndose los principios que orientan el uso de datos personales; identifica los datos que por sus características deben ser especialmente protegidos y refiere al marco legal en Uruguay.

La Guía N° 2 refiere a "Educación y datos personales". Se encuentra enfocada al sector de la Educación, principalmente a los padres, tutores y educadores. Tiene como finalidad concientizar acerca de la vulnerabilidad a la que los niños y jóvenes pueden estar expuestos al realizar un manejo incorrecto de sus datos personales, procurando educar, sin negar el acceso a Internet u otras tecnologías.

Se busca que los niños y jóvenes sean capaces de distinguir las señales de un engaño e identificar o evitar situaciones de riesgo. Cuando se trata de menores de edad se requiere la máxima atención y cuidado, ya que existen quienes entablan relaciones sociales, camuflando su verdadera identidad, con la finalidad de intercambiar fotos o videos de carácter sexual con personas de esa edad.

Asimismo se instruye sobre el grooming y el ciberbullyng a efectos que educadores y padres informen a niños y jóvenes sobre sus riesgos, tratando de evitarlos y tomando conciencia que pueden ser víctimas, pero también victimarios.

La Guía N° 3 sobre "Protección de datos en salud", refiere a la especial protección que merecen dichos datos, dado que describen los aspectos más sensibles sobre el individuo y pertenecen a la esfera más intangible de la persona.

Asimismo, desarrolla los derechos y obligaciones específicos de la salud, y las medidas de seguridad que deben implementar los centros asistenciales respecto a las historias clínicas, tanto escritas como electrónicas.

La Guía N° 4 sobre el "Manejo de datos personales en la administración pública", indica cuándo los organismos públicos pueden recabar, comunicar e intercambiar los datos de los ciudadanos, y el tema de la difusión de datos públicos en Internet.

La Guía N° 5 acerca del "Manejo de datos personales en operadores de telecomunicaciones", refiere a que las telecomunicaciones son merecedoras de especial atención, a los efectos de la protección de los datos personales. En este sentido, se establecen las exigencias a operadores y prestadores respecto a la protección de datos personales y se describe cómo se debe informar a los usuarios o abonados a efectos de prevenirlos sobre los riesgos de una posible violación de la seguridad de la red pública de comunicaciones electrónicas, e informando sobre las medidas a adoptar en ese caso.

Boletín Informativo

Asimismo, la URCDP publica de forma mensual un Boletín informativo con el objetivo de difundir las novedades y publicaciones, hacer conocer eventos y otras actividades concernientes y afines a sus competencias.

c. Atención de consultas personalizadas

Durante 2012 la URCDP ha realizado actividades diversas de difusión y capacitación en materia de Protección de Datos Personales. Para diferentes actores de la actividad nacional, personas físicas, asociaciones profesionales y organizaciones tanto públicas como privadas de todo el país.

En ese marco se realizó un taller dirigido al personal de las Obras Sanitarias del Estado (OSE), con la finalidad de informar, asesorar y capacitar en relación con todo lo vinculado con el derecho fundamental a la protección de datos personales.

La Unidad recibe en su sede a los ciudadanos en forma personalizada y además los atiende telefónicamente. Durante el año 2012 se han atendido personalmente alrededor de 1200 personas y 1700 llamadas telefónicas.

d. Eventos nacionales

El 4 de juniose presentó la Memoria Anual 2011 de la Unidad Reguladora y de Control de Datos Personales (URCDP), el Libro de Resoluciones y Dictámenes adoptados en 2011, y se lanzó oficialmente la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad como se ha mencionado anteriormente.

El 7 de junio se entrevistó a la Dra. María José Viega, en representación de la Unidad Reguladora y de Control de Datos personales en el programa "No toquen nada". En la entrevista se destacó que los datos personales son un derecho humano que muchas veces las prácticas empresariales no respetan. Recibir mensajes promocionales no deseados, estar en bases de datos crediticias sin saberlo, el spam telefónico o por correo electrónico y la videovigilancia son los principales motivos de denuncias de los ciudadanos.

Otro de los derechos de los ciudadanos que es vulnerado es el derecho al olvido: cuando pasa determinado plazo (cinco años con un máximo de diez), las instituciones crediticias deben borrar los datos. Viega afirmó que muchas veces las bases de datos obtienen la información a través de fuentes públicas y no son informados al titular.

Desde la creación de la Unidad Reguladora y de Control de Datos Personales el número de denuncias y consultas ha venido en aumento. La razón de ello es el mayor conocimiento de la población de la existencia de un mecanismo para denunciar violaciones a la ley de datos personales.

El 12 de julio el Mag. Federico Monteverde, integrante del Consejo Ejecutivo de la URCDP, concurrió en representación de la Unidad junto a la Dra. María José Viega Gerente de División Derechos Ciudadanos del área Ciudadanía Digital de AGESIC, a las instalaciones del canal 20 como invitados en el programa: "Punto Tecno".

La entrevista realizada por el Sr. Gerardo Sotelo, refirió a la importancia de la protección de datos personales de cara a la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, que se llevaría a cabo en Punta del Este.

El 18 de setiembre concurrió la Dra. Beatriz Rodríguez, Jefa de Protección de Datos de Derechos Ciudadanos, al Canal de la Intendencia de Maldonado, donde fue entrevistada por el periodista Gustavo Barceló sobre la 34ª Conferencia de Autoridades de Protección de Datos Personales y Privacidad. Ese mismo día concurre a los canales 7 y 11 de Maldonado, donde se le consulta por los datos personales en sí y sobre la Conferencia.

El 27 de setiembre el Diario El País publicó una nota que le realizara a la Dra. María José Viega, en representación de la URCDP el periodista Andrés Roizen, bajo el titular "Cien denuncias por año por mal uso de bases de datos". Refiere a que el gobierno comenzará a auditar empresas durante 2013, y que se encuentra trabajando en el tema y a partir de éste año se aumentarán los controles sobre cómo las firmas manejan y almacenan la información.

Se expresó además que la URCDP tiene potestad para aplicar distintos tipos de sanciones al constatar una infracción en el manejo de las bases de datos. Pueden oscilar entre un apercibimiento, una observación o una multa, hasta la suspensión temporal o la clausura de forma definitiva de la base de datos.

En el 2013 se comenzará con las auditorías de las bases de datos de las empresas, coordinando con las firmas durante la primera etapa. Con dichos controles se pretende chequear qué empresas cumplen o no con los requisitos y cuáles tienen inscriptas correctamente sus bases de datos. Se comenzará con un plan de auditorías, en principio no con la idea de sancionar, sino para colaborar con las empresas y ayudar a las que han tenido más denuncias para ver cuál es su problema.

El 1º de octubre fue publicada una nota de prensa del periodista Fabián de Muro en el suplemento Qué Pasa del Diario El País realizada a la Dra. María José Viega, en la que se menciona la importancia política y empresarial de las bases de datos, así como el aval de la Unión Europea, mediante la Adecuación que facilitará las transferencias de datos cuando se hacen compras por Internet.

Con el mismo objetivo de difundir la relevancia de la protección de datos personales, el 12 de noviembre el Dr. Felipe Rotondo, Presidente del Consejo Ejecutivo de la URCDP, concurrió al Programa "Ciudad Más" de Tevé Ciudad, donde enfatizó en cómo proteger y cómo lograr que se protejan los datos personales.

e. Jornadas de capacitación interna de AGESIC

Durante el año se fueron impartiendo diversas charlas sobre los temas a desarrollarse durante la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.

Los temas analizados fueron: Gobierno Electrónico, Gobierno Abierto, Sociedad de la Información, Smart Data, Herramientas Forenses, Herramientas de Cooperación, E-Salud, Marketing Comportamental, Geolocalización, Derechos Fundamentales, Reforma de la Protección de Datos en la Unión Europea, Protección de Datos en América Latina, entre otros.

Por otra parte se capacitó al personal de protección de datos en base a los diferentes temas abordados por las guías sectoriales: Protección de datos para responsables de acceso a la información pública, telecomunicaciones, educación y operadores de la salud.

f. Relacionamiento internacional

El 28 de enero de 2012 se celebró una nueva edición del "Día Internacional de la Protección de Datos", en conmemoración de la firma del "Convenio de Estrasburgo".

Con fecha 28 de enero de 1981 el Consejo de Europa aprobó el "Convenio 108" relativo a la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, constituyéndose en un hito histórico en la materia.

En nuestro país, dicha conmemoración adquiere un significado especial, ya que el Consejo de Europa invitó a Uruguay a suscribir este Convenio, en mérito a sus avances en la defensa del derecho a la protección de datos personales, convirtiéndose, de este modo, en el primer país no europeo invitado a suscribirlo.

Asimismo, es un día propicio para la reflexión individual y colectiva acerca de la importancia que tiene la defensa de este derecho humano en el marco de una sociedad que se desarrolla de forma justa y solidaria, con apego a los principios democráticos de un Estado de Derecho depositario de la tutela de la protección de datos personales, un derecho que nos atañe a todos.

El 20 de febrero, la Unidad visitó la Agencia Española de Protección de Datos. La Dra. María José Viega en representación de la URCDP, mantuvo un encuentro institucional con el Director de la Agencia Española de Protección de Datos (AEPD), José Luis Rodríguez Álvarez. En el marco de la visita institucional, además, se concurrió a la Agencia de Protección de Datos de Madrid y a la Agencia Vasca de Protección de Datos, y se previó un encuentro con otros miembros de la AEPD, como el Adjunto al Director y la Secretaria General, con el objeto de trasladar a la URCDP, en calidad de autoridad encargada de organizar en Uruguay la siguiente Conferencia Inter-

nacional de Autoridades de Protección de Datos y Privacidad, las opiniones y experiencias de la AEPD en la organización y desarrollo de la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en Madrid en 2009.

El 15 de mayo, el Ing. José Clastornik, Miembro de la URCDP, asistió a la "International Enforcement Meeting", en la ciudad de Montreal, Canadá. Entre los temas tratados en su exposición se encuentran: la discusión sobre los obstáculos y desafíos para el intercambio, la coordinación y la discusión sobre las posibles áreas de cooperación y coordinación, anuncio de la agenda tentativa, así como los temas a desarrollarse en los diversos paneles y los principales expositores confirmados a esa fecha a efectos del lanzamiento de la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.

En otra instancia, en el marco del XX Congreso y Feria Iberoamericana de Seguridad de la Información "Segurinfo 2012", realizado el 24 de mayo, se brindó una conferencia en relación con la Protección de Datos Personales, a cargo de la Dra. Esc. María José Viega.

A sala llena se presentaron los aspectos sustanciales de la regulación normativa nacional en la materia. Al finalizar hubo un interesante intercambio entre los asistentes, lo que denota el interés y avidez de conocimientos de quienes participaron en el evento.

Por último, se efectivizó la invitación y compromiso de la Unidad Reguladora y de Control de Datos Personales con el desarrollo de la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, que se realizaría en el mes de octubre en nuestro país.

El 20 de agosto de 2012, se realizó en San Pablo (Brasil) una mesa redonda organizada por Microsoft, con participación de representantes de Argentina, México, Perú, Colombia, Costa Rica, Chile, Brasil y Uruguay, representado por la Dra. María José Viega. El tema de debate fue el consentimiento frente a las nuevas tecnologías (biometría, big data, entre otros). El documento básico para la discusión fue el Trustworthy Computing Next, de Scott Charney (Corporate Vice President Trustworthy Computing Microsoft Corporation del 28 de febrero de 2012).

El 11 y 12 de setiembre la Dra. María José Viega en representación de la URCDP, asistió a: "Microsoft Global Privacy Summit" llevado a cabo en Redmond, EEUU. Dicho evento dio continuidad al celebrado en la Ciudad de San Pablo, contando con la participación de representantes de varios países latinoamericanos.

Durante el 23 y 24 de octubre se realizó la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad: "Privacidad y tecnología en equilibrio", en la ciudad de Punta del Este, Maldonado, en la que se reunieron los expertos en el tema, pertenecientes a la academia, el gobierno y la sociedad civil.

EL 29 y 30 de octubre la URCDP recibió la visita de la Autoridad de Protección de Datos de Costa Rica, representada por su Directora, Dra. Arlene González. Se realizó una pasantía en la cual se aportaron conocimientos y lecciones aprendidas sobre el proceso de inscripción de bases de datos y demás actividades desarrolladas por la Unidad a efectos de que pudiera conocer las buenas prácticas, antecedentes y dificultades vividas en el proceso de formación y desarrollo de la Unidad como un mecanismo para ilustrar sus futuras actividades en su país.

08

La URCDP en cifras

8. La URCDP en cifras

Este capítulo tiene como objetivo presentar de manera cuantitativa y gráfica datos que permitan realizar un análisis del estado de situación en Uruguay respecto a algunos aspectos de la protección de datos personales.

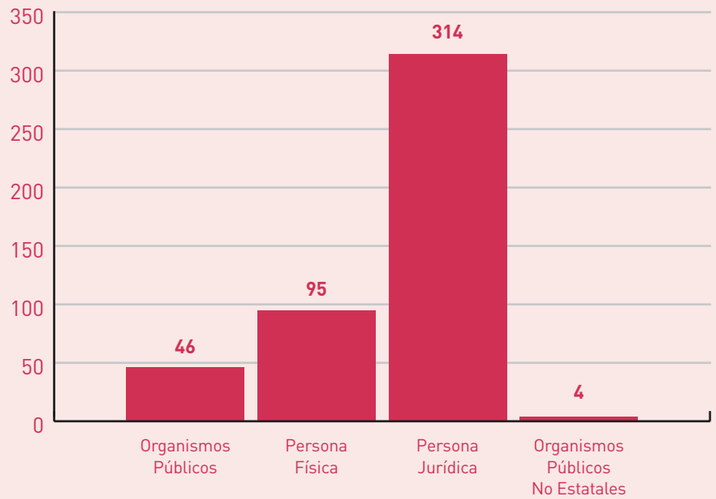
a. Registro de base de datos personales

Desde el inicio de su actividad, la URCDP puso a disposición de los sujetos obligados un sistema informático que permite el ingreso vía Internet de los Formularios de Registro de Bases de Datos Personales. A continuación se presentan y analizan los datos obtenidos como resultado del registro online de estos formularios durante el año 2012.

La tabla y el gráfico siguientes muestran las cantidades de base de datos según tipo de responsable presentados ante la URCDP durante el año 2012.

	Año 2012	
Tipo de responsable	**Cantidad de Bases de Datos**	**Cantidad de Responsables**
Personas físicas	95	84
Personas Jurídicas	314	218
Organismos públicos	46	9
Organismos públicos no estatales	4	3
Totales	**459**	**314**

Cantidad de Bases de Datos por tipo de responsable



Al igual que años anteriores se observa, por parte de las personas jurídicas, la voluntad de cumplir con la normativa vigente en cuanto a protección de datos y en particular con la obligación de inscribir las bases de datos personales que poseen.

En el gráfico siguiente se muestra la evolución en la cantidad de bases de datos total presentadas ante la Unidad. En el mismo se observa que durante 2012 el ritmo de inscripciones ha decrecido sensiblemente con respecto a años anteriores, lo cual sugiere que la mayor parte de los sujetos obligados ya han cumplido con la inscripción de las bases de datos.

b. Distribución territorial

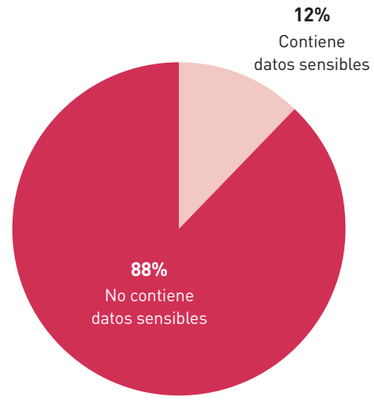
La siguiente tabla muestra la distribución territorial según la ubicación física de las base de datos agrupadas por departamentos, confirmándose una concentración en la capital de nuestro país, que coincide con la masa poblacional del Departamento.

País	Departamento	% distribución BDs 2012
Uruguay	Montevideo	74,29
	Maldonado	2,83
	Canelones	2,18
	San José	1,96
	Florida	1,53
	Colonia	1,31
	Artigas	1,31
	Soriano	1,09
	Tacuarembó	1,09
	Salto	0,87
	Paysandú	0,65
	Durazno	0,65
	Lavalleja	0,44
	Rivera	0,44
	Cerro Largo	0,22
	Río Negro	0,22
	Flores	0,00
	Treinta y Tres	0,00
	Rocha	0,00
Otros		8,93

c. Datos sensibles

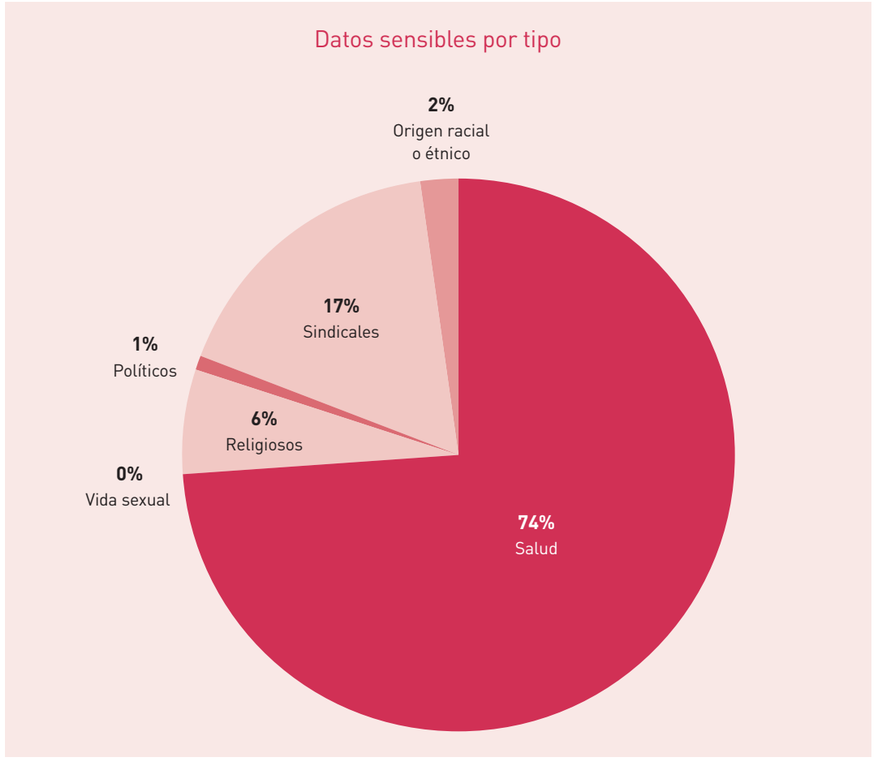
Interesa destacar la existencia de base de datos que contienen datos sensibles, de acuerdo con la respuesta afirmativa a la pregunta acerca de si guardan datos relacionados con:

- Salud
- Vida sexual
- Convicciones Religiosas
- Preferencias Políticas
- Afiliaciones Sindicales
- Origen racial o étnico



De los datos obtenidos, se observa que alrededor de un 12% de las bases de datos registran datos sensibles. Éste porcentaje ha aumentado de 9% registrado en 2011 a 12% en 2012.

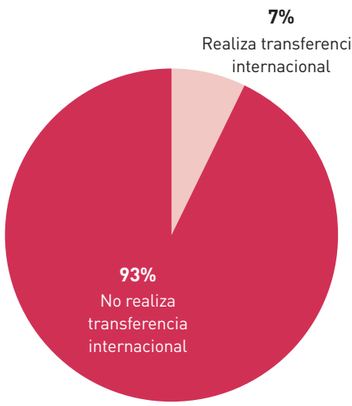
En el siguiente gráfico se presenta el desglose de las bases que guardan datos sensibles. Al igual que años anteriores se mantiene predominancia de datos de salud y sindicales. En Uruguay, las organizaciones sean públicas o privadas exigen a sus funcionarios la presentación de una constancia del último examen médico que habilita a trabajar. Si bien las empresas solo tienen acceso a la constancia y la fecha de último examen médico, éste es declarado como dato de salud al momento de completar el registro. En cuanto a los datos sindicales, las organizaciones sostienen que los datos sindicales son mantenidos con la única finalidad del descuento de la cuota de afiliación al sindicato.



d. Transferencias internacionales

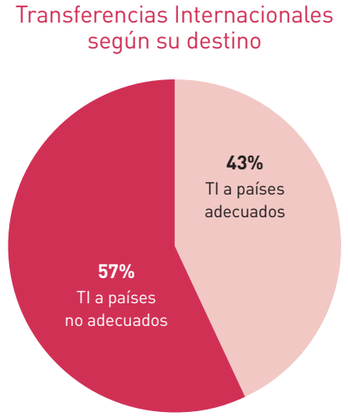
De acuerdo con el artículo 23 de la Ley N° 18.331, los datos personales transferidos internacionalmente están especialmente protegidos. Por esta razón, interesa conocer datos estadísticos sobre transferencias internacionales y en particular a qué países.

Del total de bases de datos presentadas durante el 2012, aquéllas que efectúan transferencias internacionales representan un 7,4% del total de las Bases.



Resulta de interés clasificarlas considerando si el país de destino es adecuado o no, de acuerdo con lo dispuesto por Resolución N° 17, de 12 de junio de 2009, del Consejo Ejecutivo de la URCDP.

Se constata que aproximadamente la mitad de las transferencias internacionales se realizan a países adecuados.



Los fuertes lazos con la República Argentina, único país de América Latina que ofrece en la actualidad un nivel adecuado de protección, permite comprender, tal como se demuestra en la siguiente tabla, que ésta ostente el primer lugar de todos los países hacia los que se transfieren datos personales.

La tabla presenta el ranking de los 5 países hacia donde se realiza la mayor cantidad de transferencias internacionales de datos desde Uruguay como país de origen:

Puesto	País
1	Argentina
2	EE.UU.
3	Brasil
4	España
5	Suiza

e. Tipos de Información

Las bases de datos personales pueden almacenar diferentes tipos de información según su finalidad. La gran mayoría de las bases de datos solo contienen datos identificatorios y de carácter personal. Sin embargo, hay muchas otras que, adicionalmente, almacenan otro tipo de información personal que son datos especialmente protegidos de acuerdo con la normativa vigente.

Los datos especialmente protegidos son los siguientes:

- Datos sensibles
- Datos relativos a la salud
- Datos personales transferidos internacionalmente
- Datos de Telecomunicaciones (conservación de los datos de tráfico en las comunicaciones electrónicas)
- Datos de bases de datos con fines de publicidad
- Datos relativos a la actividad comercial o crediticia

La tabla siguiente muestra datos que reflejan la situación con respecto a bases de datos que guardan diversos tipos de información, incluyendo algunos que están especialmente protegidos, tal como toda información comercial o crediticia:

Tipo de dato	% bases em 2012
Remuneraciones	17,07
Datos bancarios	11,85
Datos impositivos	10,80
Seguros	6,97
Deudas	6,97
Créditos, préstamos, avales	5,92
Estados contables	5,57
Historial créditos	4,88
Tarjetas de crédito	4,88
Hipotecas	4,18
Cuentas suspendidas y clausuradas	0,70

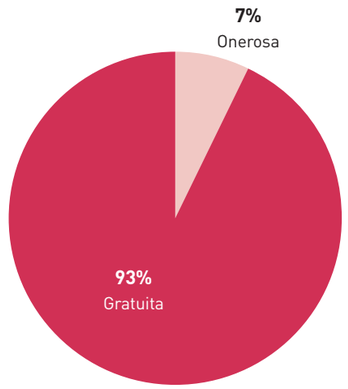
f. Cesiones o comunicaciones de datos

La proporción de bases de datos de las cuales se realizan cesiones o comunicaciones de datos representa el 24% del total de bases presentadas, tal como se presenta en el siguiente gráfico.

Comunicación de datos

De las bases de datos de las cuales se comunican o ceden datos interesa conocer en su desglose de acuerdo con la comunicación si se realiza de forma gratuita, onerosa o ambas.

Comunicación de datos por tipo



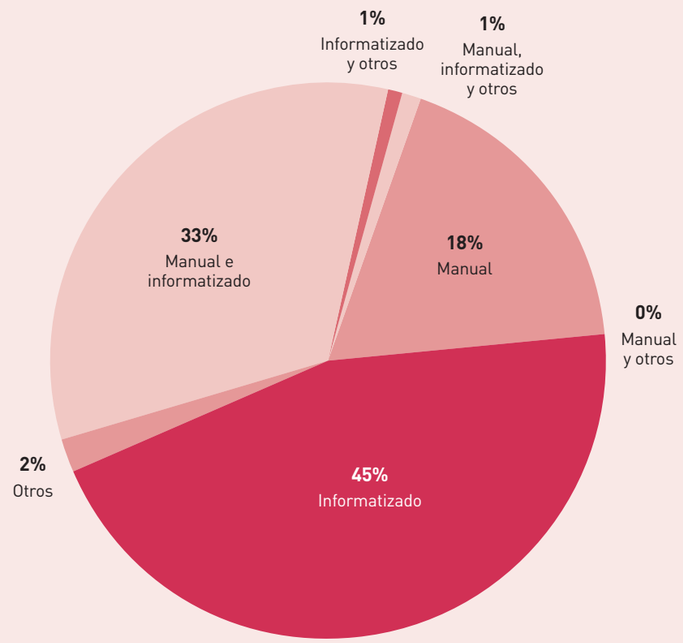
g. Tipo de soporte de registro de datos

Interesa en este punto destacar los soportes utilizados:

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

Tal como se puede observar en el gráfico, se verifica mayoritariamente el uso de soporte informatizado como forma de registrar datos.

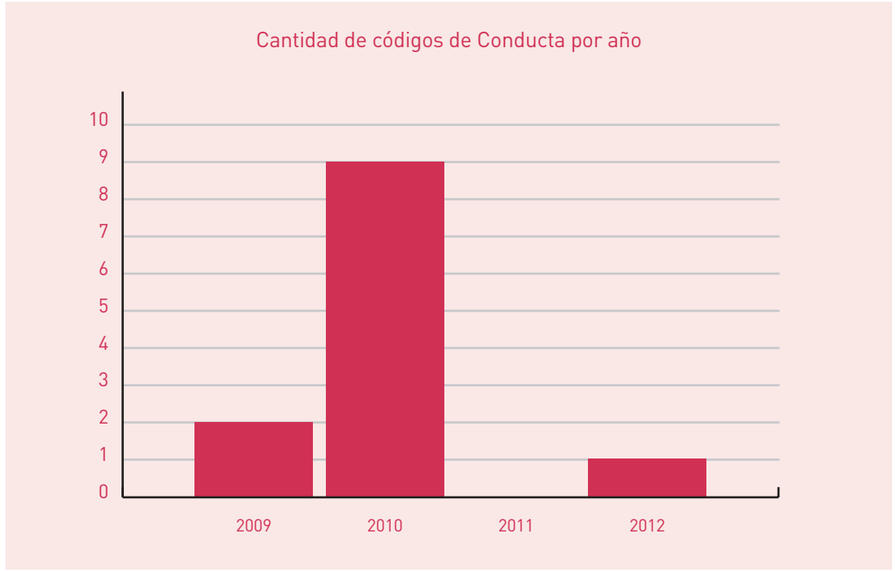
Soporte por registro



h. Códigos de conducta

Adicionalmente a la inscripción de base de datos personales los responsables pueden inscribir los códigos de conducta relativos al tratamiento de datos personales.

Durante el año 2012 se registró 1 código de conducta. A continuación se muestra la evolución de la cantidad de inscripciones de códigos de conducta desde el inicio de la actividad de la URCDP.

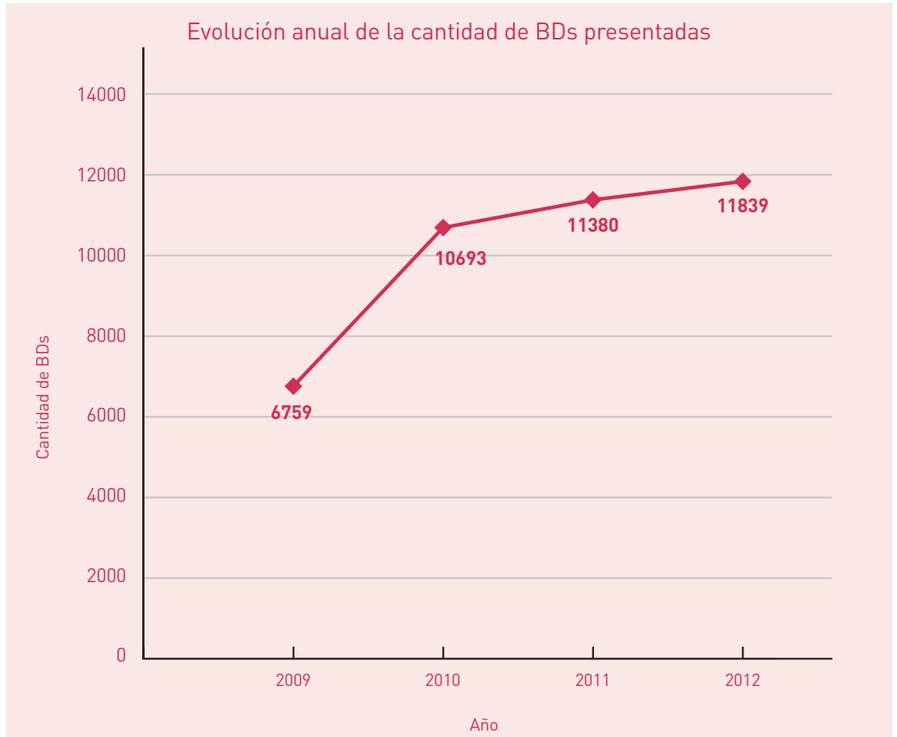


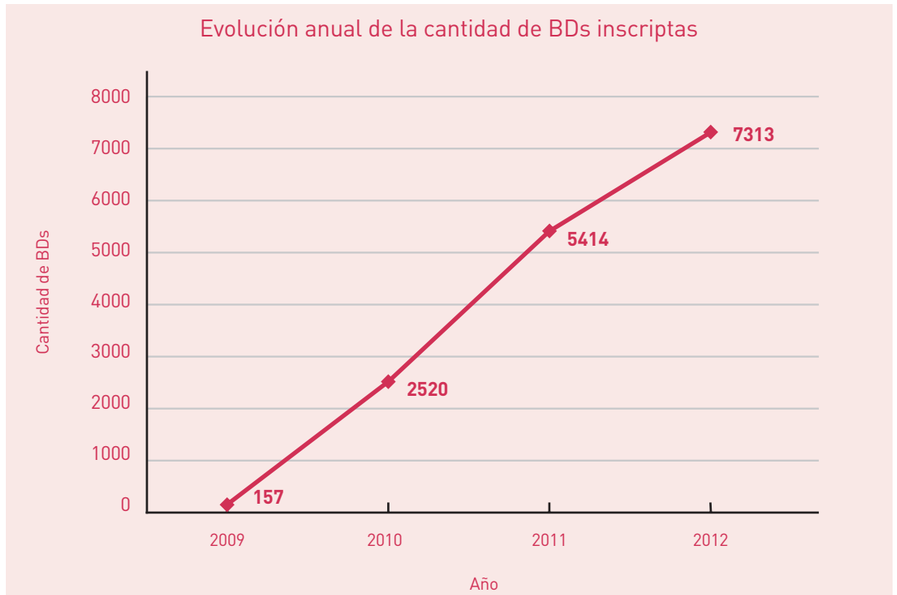
i. Bases de datos inscriptas en la URCDP

Las bases de datos presentadas ante la URCDP pasan por un completo control de cumplimiento de la normativa vigente. Este control consiste en una evaluación jurídica realizada por un abogado que analiza las características de la base de datos y eventualmente solicita aclaraciones al responsable; una evaluación notarial realizada por un escribano público que analiza la correcta representación de la empresa que solicita la inscripción de la base de datos y una evaluación técnica donde un ingeniero en computación realiza las recomendaciones de seguridad pertinentes para bases de datos que contengan datos especialmente protegidos o cuyas medidas de seguridad sean insuficientes.

Luego de realizados los controles, el Consejo Ejecutivo de la URCDP dicta la resolución donde se establece que la base de datos queda efectivamente inscripta en el Registro de Bases de Datos Personales.

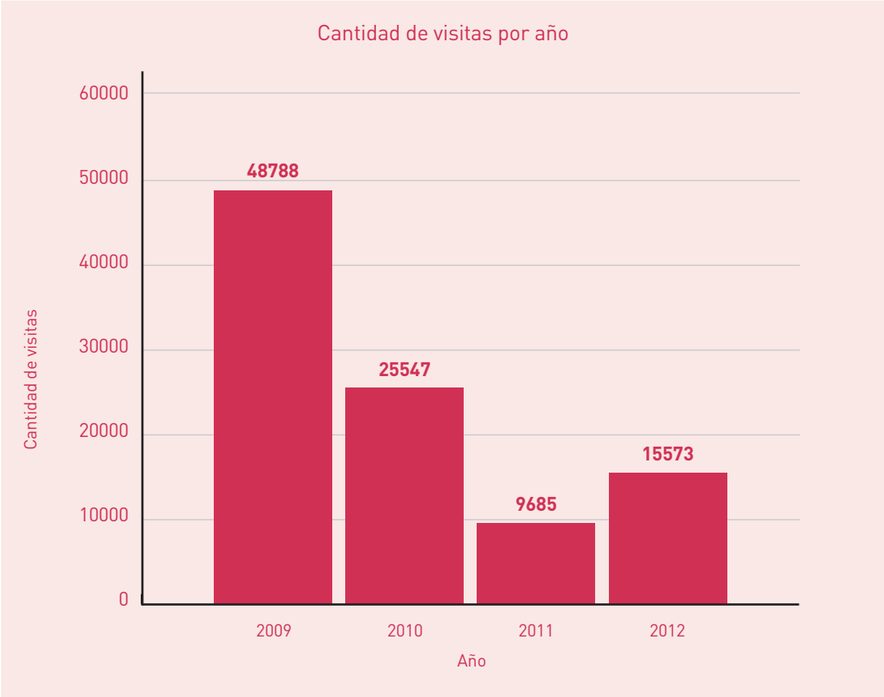
El gráfico siguiente muestra la evolución anual de la cantidad de base de datos inscriptas:



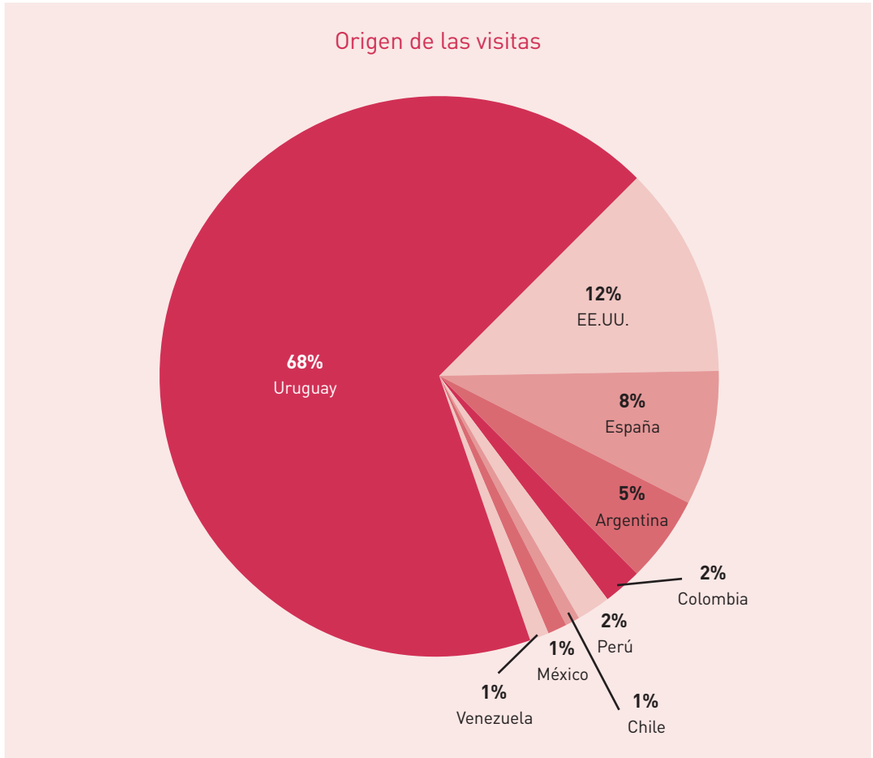


j. Cantidad de visitas al sitio web de la URCDP

Respecto a las visitas registradas en números, se constata una mayor cantidad de las mismas registradas durante 2009, año de inicio de actividades de la URCDP y durante el cual vencía el plazo para la inscripción de bases de datos personales existentes.



También se han registrado visitas al sitio de URCDP desde el exterior del país, principalmente de España y Estados Unidos.



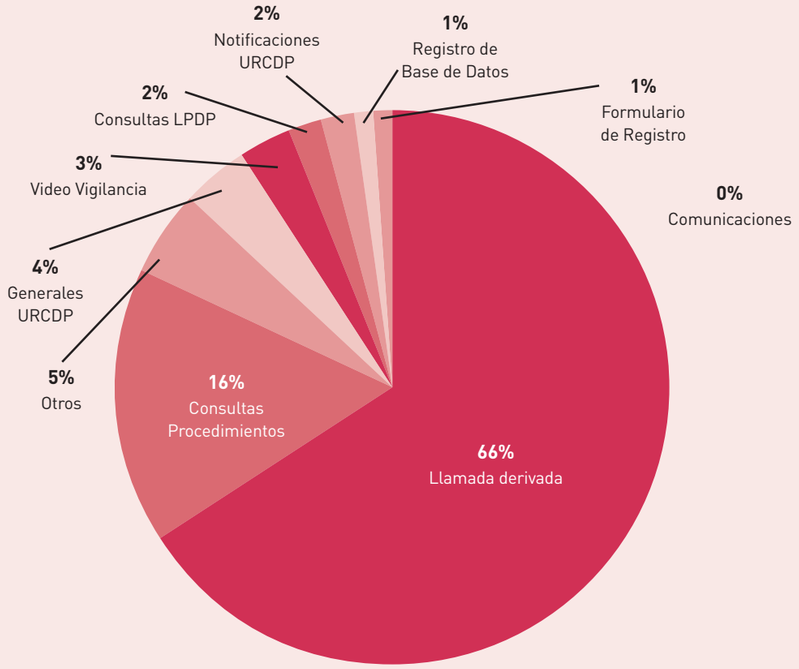
k. Consultas a la mesa de ayuda de la URCDP

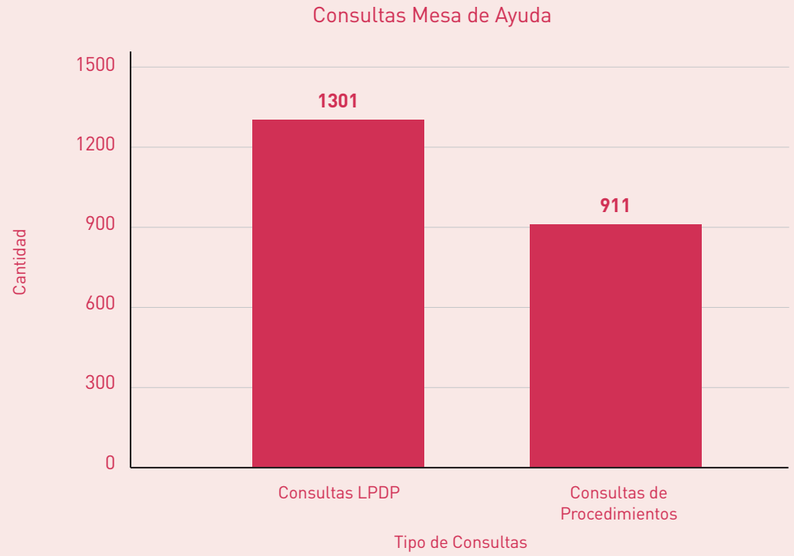
La mesa de ayuda de AGESIC atiende anualmente una importante cantidad de consultas formuladas a la URCDP. Las consultas son atendidas de manera personalizada en las oficinas de AGESIC, telefónicamente, vía mail y mediante el formulario de contacto de la Web de la URCDP.

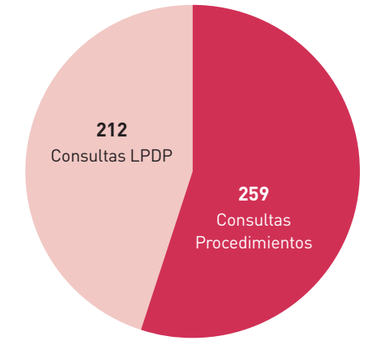
Durante 2012 se recibieron 2212 consultas. De estas consultas 1301 fueron sobre temas referidos a la Ley de Protección de Datos Personales y 911 fueron sobre procedimientos de inscripción de Base de Datos.

Las consultas son atendidas por profesionales jurídicos, notariales e informáticos en forma telefónica, vía e-mail, a través de la Web y en forma personal.

La Unidad atiende en forma permanente a los ciudadanos a través del área de asesoría de la Dirección de Derechos Ciudadanos de AGESIC.







l. Expedientes presentados por consultas y denuncias

Debido a la difusión realizada por la Unidad y el mayor conocimiento de la ciudadanía respecto de sus derechos en materia de protección de datos personales, durante 2012 hubo un aumento significativo en lo que se refiere a consultas y denuncias presentadas por parte de los ciudadanos respeto al año anterior.

Durante 2012 la Unidad recibió 38 consultas y 89 denuncias.

Los principales motivos de denuncia fueron: spam, inclusión en base de datos en instituciones crediticias, comunicación de datos personales, envío de tarjetas de crédito sin consentimiento y videovigilancia.

En lo referente a consultas realizadas ante la Unidad, los principales temas fueron: videovigilancia, datos de salud y publicaciones de datos en sitios web.

m. Resoluciones sancionadas con apercibimiento o multas

Dentro de los cometidos de la URCDP se encuentra aplicar sanciones administrativas a aquellas personas, empresas u organismos que realicen alguna violación a la Ley de Protección de Datos Personales.

Durante el 2012 fueron ejecutados: 2 observaciones, 1 apercibimiento, y 1 multa.

n. Resoluciones y dictámenes realizados

Durante 2012 se realizó el análisis de expedientes presentados tanto de Base de Datos como de denuncias y consultas.

Se expidieron 1081 Resoluciones y 31 Dictámenes.

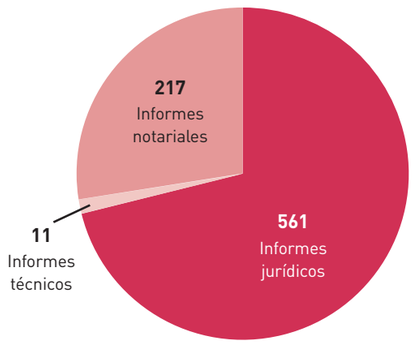
El ciudadano puede acceder a los mismos a través del sitio web de la Unidad, www.datospersonales.gub.uy

Resoluciones y Dictámenes

ñ. Cantidad de informes realizados

El estudio de los diferentes expedientes con lo que cuenta la Unidad ha producido 789 informes. Estos se dividen en informes jurídicos, informes notariales e informes técnicos.

Informes



Como se destaca en el gráfico, se realizaron 561 informes jurídicos, 217 notariales y 11 técnicos.

09

La URCDP ante los nuevos retos en materia de protección de datos Proyectos a realizar en el 2013

9. La URCDP ante los nuevos retos en materia de protección de datos. Proyectos a realizar en el 2013

Se proyecta continuar con la capacitación a los ciudadanos sobre protección de datos. Esta capacitación se realizará por sectores, para la primera etapa se determinaron cuatro: responsables de acceso, educación, salud, telecomunicaciones.

Se continuará con el funcionamiento permanente de la Unidad, con el apoyo de los servicios de AGESIC.

Se optimizará el registro de procesos de inscripción de bases de datos, para que el administrado tenga menos obligaciones y más celeridad en el procedimiento.

Se continuará con actividades de cooperación y participación en grupos de trabajos internacionales.

10

34ª Conferencia Internacional de Autoridades de Protección de Datos Personales y Privacidad

10. 34ª Conferencia Internacional de Autoridades de Protección de Datos Personales y Privacidad

El 23, 24 y 25 de octubre en Punta del Este (Uruguay), se realizó la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, denominada "Privacidad y Tecnología en equilibrio", con expositores de 50 países.

En la apertura y mensaje de bienvenida participaron el Ing. José Clastornik, Miembro del Consejo Ejecutivo de la URCDP; Jacob Kohnstamm, Miembro del Comité Ejecutivo de la Conferencia; el Dr. Felipe Rotondo, Presidente de la URCDP y el Mag. Federico Monteverde, Miembro del Consejo Ejecutivo de la URCDP.

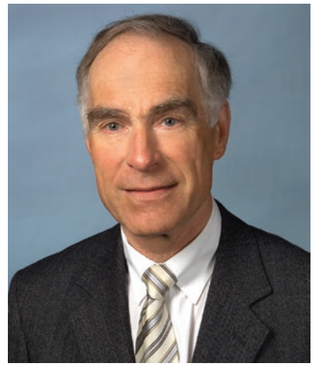
José Clastornik enfatizó en que el tema de los datos personales se ha encarado con responsabilidad y preocupación en Uruguay. Dijo que la creación de la Unidad Reguladora y de Control de Datos Personales y la declaración de Uruguay como país adecuado en protección de datos muestra un avance que este evento pretende ayudar a construir, además de generar valores compartidos.

Por su parte, Jacob Kohnstamm destacó el hecho de que el evento se haga por primera vez en América del Sur y de la oportunidad que significa poder compartir entre colegas el entusiasmo por la temática que se aborda. "Hablar y trabajar juntos es la clave entre nosotros", concluyó.

El Dr. Rotondo agradeció en nombre de Uruguay como país anfitrión y explicó que el abordaje del evento es una agenda de incidencia social en todos los ámbitos, y aclaró que se viven "tiempos de una sustitución acelerada con certeza de transitoriedad". "Lo que importa es el adecuado pasaje de la información al conocimiento" dijo, e ilustró la idea citando a Ortega y Gasset con su popular frase: "el hombre es él y su circunstancia".

Asimismo, explicó que "el avance de la tecnología debe darse en armonía con los derechos de las personas", y que las TIC tienen un rol decisivo en las formas de producción y en las nuevas formas de trabajo. Señaló que uno de los objetivos principales es promover, mediante incentivos adecuados, el desarrollo tecnológico, de nuevas y más eficaces formas de protección de nuestro "cuerpo electrónico".

a. Conferencia del Dr. Wolfgang Kilian[3]



Datos personales: el impacto de las nuevas tendencias en la sociedad de la información

1. Introducción

Durante más de cuarenta años[4] el desarrollo de los principios y reglamentos sobre la protección de datos personales ha acompañado a la sociedad de la información moderna.

El enfoque de la protección de datos se origina en la creencia filosófica de que cada individuo tiene sus propios atributos, cualidades, características, habilidades, relaciones y comportamientos distintos a los de los demás y sobre los cuales en principio debería tener derecho de disponer.

El aumento de los métodos relacionados a las TIC para identificar, analizar, evaluar y crear perfiles de individuos hace surgir una pregunta: ¿qué margen de toma de decisiones individuales existe con relación al uso de datos personales? ¿Debería protegerse a las personas de las solicitudes de datos personales

3 Traducción realizada de la conferencia original del Dr. Wolfgang Kilian para la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. Punta del Este, octubre 2012

4 James B. Rule/ Graham Greenleaf (ed.), Global Privacy Protection: The First Generation, Cheltenham, Reino Unido/ Northampton, MA, Estados Unidos (2008).

de autoridades estatales y de los grandes actores del mercado?

En el Antiguo Testamento, en el Segundo Libro de Moisés[5], se cuenta que cada vez que Moisés se presentaba ante el Señor para hablar con El, se quitaba el velo de su rostro hasta que salía. El texto ha sido interpretado en el sentido de que la comunicación personal con Dios es opuesta al uso de un velo.

En la sociedad de la información, el uso de seudónimos y el anonimato serían el velo. Facebook y Google prohíben los velos. Y también lo hacen las autoridades estatales.

¿Será que reclaman su devoción ante la sociedad de la información?

2. Nuevas tendencias en la sociedad de la información

En la actualidad la tecnología de la información y las comunicaciones podrían caracterizarse haciendo referencia a algunas palabras clave: Chips de memoria muy eficientes, convergencia de tecnología de las comunicaciones, capacidad de almacenamiento ilimitada, rápido procesamiento de datos a nivel de petabitios, dispositivos móviles multipropósito, redes sociales, reconocimiento facial automatizado, registros biométricos, cartografía de geolocalización, computación en la nube, técnicas de visualización, identificación por radiofrecuencia; tecnología de medición inteligente. Todos estos desarrollos se basan o están enfocados en los datos personales.

Algunos ejemplos:

Luego de los ataques terroristas en Nueva York en 2001, los esfuerzos para evitar episodios similares devengaron en enormes esfuerzos por desarrollar sistemas digitales de observación y alerta. La Dirección de Ciencia y Tecnología del Departamento de Seguridad Nacional de los Estados Unidos creó una inmensa "División de factores humanos / ciencia del comportamiento", que analiza "la biometría, motivación e intención, intención hostil, ingeniería de los factores humanos y las ciencias sociales, comportamentales y económicas para mejorar la detección, el análisis y la comprensión de las amenazas que representan individuos, grupos y movimientos radicales" [6].

En Europa se dieron enfoques similares: la Comisión Europea lanzó dentro del Séptimo Programa Marco (2007 - 2013) proyectos de investigación en seguridad que ascienden a 1,4 mil millones de euros. Un proyecto de investigación de seguridad [7] tiene como objetivo desarrollar un motor de búsqueda para realizar análisis automatizados de imágenes logradas a partir de videos de vigilancia obtenidos en espacios públicos, capaces de unir datos biométricos, de reconocimiento facial, datos de comunicaciones y de Internet. Se espera facilitar la identificación de sospechosos mediante sus comportamientos divergentes, tales como salir corriendo, conducir rápidamente, estar a la defensiva, sentarse en el suelo o perder el equipaje.

Los 27 Estados miembros europeos están obligados a través de la ley europea armonizada[8] a solicitar a sus proveedores de comunicaciones-tales como los proveedores de servicios de Internet, que almacenen los datos de tráfico de sus ciudadanos durante entre seis y veinticuatro meses. Las autoridades nacionales competentes pueden acceder a los datos almacenados en casos específicos. Algunos Estados miembros de la Unión Europea dudaron en trasladar la ley armonizada a las leyes nacionales dado que todos los ciudadanos son tratados como si fueran sospechosos de un delito.

En el ámbito privado Facebook, Google y otras empresas procesan cantidades increíbles de datos personales. Utilizan métodos para mejorar la precisión de mismo para lograr un marketing personalizado.

Facebook mantiene 100 petabitios de datos personales en línea [9]. La evaluación de los métodos aplicados por Google reciben el nombre de "Open Graph" o "Google Analytics".

El protocolo de Open Graph[10] permite que cualquier página web se vuelva un objeto rico en una gráfica social mediante la adición de metadata (etiquetas) como título, tipo y URL. Las etiquetas funcionan de manera similar al botón de "Me gusta" y permite procedimientos de devolución e interconectividad.

De esta manera es posible dirigirse individualmente a los consumidores y motivarlos. En 2011 el gobierno de los Estados Unidos registró 12271 solicitudes en Google donde se requería información sobre personas.

La empresa Volkswagen utiliza resultados de Google Graph en sus análisis de marketing.

Google Analytics es una plataforma de generación de informes conectada a productos relacionados como DoubleClick; AdWords y AdSense. Permite medir el impacto de las comunicaciones de los equipos móviles (Mobile Analytics), el contexto de los sitios web (Website Analytics), las interacciones de los visitantes en un cierto sitio web (Social Analytics) o el rendimiento de los avisos (Advertising Analytics).

3. Impactos

Los desarrollos técnicos están dando lugar a una infraestructura global que logra una mejor explotación de la información personal para los Estados, las instituciones privadas y las personas. La cantidad de datos personales generados, analizados y eva-

5 Éxodo 34, 33-35.

6 Departamento de Seguridad Nacional de los Estados Unidos, Departamento de Ciencia y Tecnología (ed.), High-Priority Technology Needs, Versión 3.0, Washington D.C., Mayo de 2009.

7 INDECT: Sistema inteligente de información que apoya la observación, búsqueda y detección para la seguridad de los ciudadanos en entornos urbanos (http://www.indect-project.eu).

8 Directiva 2006/24/CE sobre la retención de datos generados o procesados con relación a la disposición de servicios de comunicaciones electrónicas disponible públicamente o de redes de comunicaciones públicas, DO L 105/54 del 13 de abril de 2006.

9 En una plataforma Hadoop de la Fundación Apache Software. 1 petabitio = 1000 (elevado a la 5) bitio = 1 miogigabitio = 1000 terabitio.

10 La especificación se encuentra disponible en el Acuerdo de Fundación de la Red Abierta, versión 0.9 ("OWFa 0.9", ver: http://openwebfoundation.org/legal/the-0-9-agreements (visitado el 22 de julio de 2012).

luados está aumentando tremendamente. Al mismo tiempo, la vigilancia electrónica pública y privada, el rastreo de comunicaciones por Internet o satelitales, y la identificación facial o ubicación automáticas se entrometen cada vez más en la vida pública y privada de las personas. ¿A quién le gusta ser controlado, calificado, ubicado, etiquetado, descubierto, reconocido, localizado o identificado electrónicamente en todos lados y a la hora que sea para diversos fines? Se cuenta con contramedidas técnicas como quitar las cookies o la aplicación de funcionalidades de no rastreo y procedimientos de "opt-in" o de "opt-out", pero muchas veces no están disponibles o los proveedores los bloquean.

Asimismo, las medidas de rastreo o no rastreo llevan a cascadas técnicas de programación limitadas solamente por la cantidad de dinero de la que se dispone para inversiones y planes de negocios.[11]

A pesar de que los gobiernos pueden pensar que tales instrumentos técnicos sirven al bien común al aumentar el cumplimiento de la ley, otros consideran estos enfoques como un paso siniestro hacia la vigilancia general mediante métodos sofisticados.

La Unión Europea comparte la competencia con los 27 Estados miembros para promover un área de "libertad, seguridad y justicia" (Art. 4(2)(j) TFUE). Las actividades de vigilancia a nivel europeo son parte de la cooperación de las instituciones policiales y judiciales en asuntos penales (Art. 83; 84; 85 TFUE).

Una Decisión Marco del Consejo de Europa de 2008[12] promueve la eficiencia en asuntos penales "así como también su legitimidad y el cumplimento de los derechos fundamentales, en especial en lo que respecta a la privacidad y a la protección de los datos personales"[13]. Los Estados miembros podrán ofrecer medidas preventivas adicionales a las establecidas en la Decisión Marco para proteger los datos personales.[14]

Los ciudadanos de América y Europa muestran una creciente preocupación por el impacto de las tecnologías de vigilancia inteligentes sobre sus libertades personales. Que la investigación social paralela lanzada en Europa[15] calme las protestas y los levantamientos, depende de sus objetivos, alcances y resultados. Dado que los desarrollos en las tecnologías de la información y las comunicaciones son globales y de ninguna forma se detendrán mediante la intervención legal, las manifestaciones tienen impacto sobre la sociedad y sobre los individuos.

Una sociedad que sabe que, en teoría, todos los acontecimientos y comportamientos individuales relacionados en el espacio y en el tiempo podrían ser monitoreados y explotados, sufrirá adaptaciones en su desarrollo. El modo y la medida de dichas adaptaciones dependerán de cuáles comportamientos se clasifican como "normales" y cuáles como "desviados". Los "comportamientos desviados", si se describieran en un lenguaje formalizado, podrían codificarse en un algoritmo y aplicarse para tomar decisiones automatizadas.

La teoría del comportamiento desviado consta de varios enfoques. De acuerdo con la explicación más aceptada [16] un "comportamiento desviado" es el que

resulta de una interacción entre personas y la sociedad que conduce a estigmatizaciones y prejuicios.

Si las autoridades estatales declaran a un comportamiento como "desviado", las personas son etiquetadas y en consecuencia perseguidas.

¿Qué conceptos legales deberían proponerse para regular y controlar el impacto de los desarrollos técnicos? ¿Cómo podrían hacerse cumplir a nivel global los conceptos legales para los ámbitos público y privado?

Me gustaría centrarme en algunos aspectos teóricos. Primero mencionaré varios principios generales, y luego, en términos de su aplicación, propondré distinguir claramente entre el procesamiento de datos personales en el sector público y en el privado.

4. Principios generales

El grado en que un ser humano puede controlar el uso de datos relacionados con él mismo o tiene derecho a controlarlos, depende del marco cultural, político y legal que lo rodea. Cerca de 89 Estados[17] han aprobado algún tipo de disposición sobre la protección de datos para proteger la privacidad del hogar y la confidencialidad de las comunicaciones y para preservar las acciones autodeterminadas. El modo, grado y contenido de esas normas reflejan en su di-

11 Google recientemente pagó una multa récord de 22,5 millones de dólares por la resolución de una controversia con la Comisión Federal de Comercio de los Estados Unidos porque Google había aplicado la opción de cookies de rastreo para burlar la opción de "privado" del buscador Safari de manera de acceder a datos de comunicaciones de usuarios (www.ftc.gov/opa/2012/08/google.shtm). Otro ejemplo: Apple prohibió una aplicación llamada "Clueful", desarrollada por la empresa alemana "BitDefender GmbH"; se esperaba que "Clueful" controlara alrededor de 60.000 aplicaciones de la tienda de Apple para saber si los iPhones y iPads accedían a directorios de direcciones, calendarios, diarios íntimos y fotos de usuarios (Frankfurter Allgemeine Zeitung del 24 de julio de 2012, p.29). Actualmente es posible descargar "Clueful" desde la Web como programa de código abierto (www.cluefulapp.com).

12 Decisión Marco del Consejo del 27 de noviembre de 2008 (2008/977/JHA) sobre la protección de los datos personales procesados en el marco de la cooperación policial y judicial en asuntos penales, DO L 350 del 30 de diciembre de 2008, p.60 (DMC)

13 Enumeración 3 de la DMC 2008/977/JHA.

14 Enumeración 8 de la DMC 2008/977/JHA.

15 Ver los proyectos de investigación de la UE SMART: Medidas escalables para las tecnologías automáticas de reconocimiento (www.smartsurveillance.eu), lanzado en 2011; RESPECT: Normas, expectativas y seguridad mediante tecnologías convenientes con privacidad mejorada (http://respectproject.eu), lanzado en 2012; SURVEILLE: Vigilancia: aspectos éticos, limitaciones legales y eficiencia (http://www.surveille.eu), lanzado en 2012; IRISS: Aumento de la resiliencia en las sociedades vigiladas (http://irisproject.eu/?page_id=7).

16 Howard Saul Becker, Outsiders: studies in the sociology of deviance, Nueva York 1973.

17 Graham Greenleaf, Global Data Privacy Laws, febrero de 2012. (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034).

versidad la elección de políticas de los distintos regímenes legales.

Originalmente las leyes de protección de datos se centraban en la relación entre el Estado y el ciudadano.

La idea regulatoria estaba basada en la suposición de que un Estado que almacena registros de sus ciudadanos, está de esta manera, limitando sus libertades personales. Por lo tanto, en una sociedad democrática, el mantener registros debe legitimarse expresamente. Los archivos públicos deben de estar accesibles para su inspección y control individuales.

En la esfera privada los bienes públicos como la seguridad o la prevención de delitos no están en juego. Empresas y personas compiten por gobernar los datos en el mismo campo de juego. Dado el surgimiento de los mercados electrónicos de datos personales (datos de domicilio; perfiles personales; calificaciones; archivos de fotos; datos biométricos), un concepto realista de la protección de datos en la esfera privada debe considerar las situaciones mercantiles.

En general, el procesamiento de datos personales para uso público y privado requiere de algunos principios únicos y una normativa marco adicional que respete el derecho a la personalidad y a la autodeterminación informativa como derecho fundamental.

Los principios generales están establecidos en el Convenio 108 del Consejo de Europa sobre Protección de Datos (1981)[18].

Los ocho principios de este Tratado internacional, los cuales son también respetados por la ley de la Unión Europea [19], proclaman que será posible obtener y procesar datos personales de una manera justa y legal con finalidades específicas. Deberán ser adecuados, pertinentes, no excesivos y precisos, y no podrán almacenarse durante más tiempo que el necesario para su procesamiento. Los principios son aplicables a lo largo de los sectores y no son específicos para ninguna tecnología o negocio en particular. La mayor parte de los principios hacen referencia a la publicación de la Casa Blanca estadounidense de 2012 en lo que respecta a la privacidad de los datos de los consumidores [20]. Para el caso del sector público ya en un informe de los Estados Unidos del año 1973 podían encontrarse algunos principios [21].

Por debajo de ese nivel bastante abstracto de principios generales encontramos en el mundo una serie de enfoques regulatorios que van desde la autorregulación a las normativas marco y las reglamentaciones estatales detalladas y sectorizadas. El modo y los efectos difieren en el ámbito público y en el privado.

5. Ámbito público

En la esfera pública predominan las reglamentaciones obligatorias. Los intereses estatales son variados pero siempre prioritarios. La decisión de qué datos personales se deben recolectar y procesar y con qué propósitos, es una cuestión política que rara vez puede verse influida por una única persona.

Todo tipo de medidas tomadas por las autoridades estatales como administrar, detectar, etiquetar y perseguir individuos, implica una intrusión en las libertades personales. En las democracias las libertades están garantizadas por las Constituciones [22] y por los convenios internacionales. Cuando prevalece el Estado de Derecho, el procesamiento de datos personales debe ser transparente y legítimo en lo que respecta a la finalidad y al procedimiento. Si se ha tomado una decisión democrática en la cual se han respetado completamente los valores constitucionales [23], el ciudadano debe dar prioridad a los intereses públicos (prevención de delitos; sistema tributario; seguridad social; seguridad nacional; salud pública).

Los datos personales, necesarios en pos de los intereses públicos legítimos, están fuera del alcance de la disposición de los individuos en base al derecho a la privacidad de los datos o de la personalidad. La competencia para supervisar y garantizar el cumplimiento de las leyes existentes de manera eficiente la tienen o deberían tenerla autoridades independientes (comisionados de protección de datos; tribunales).

6. Ámbito privado

El ámbito privado está definido por la autonomía individual, las transacciones del mercado y las relaciones contractuales.

Cuando los mercados funcionan adecuadamente, es posible asumir la existencia de un poder de negociación igualitario de los actores, y los contratos sirven para reconciliar intereses divergentes. Si existen fallas en el mercado (competencia desleal o inexistente; fuerte poder de mercado, débil cumplimiento de la ley), una de las partes del contrato tendrá una posición de negociación más débil. Para identificar cuál es la situación prevalente, deben tomarse en cuenta la estructura y el comportamiento del mercado, la competencia y el cumplimiento de la ley.

Las transacciones mercantiles se basan en el intercambio de derechos de propiedad sobre bienes comerciables. De acuerdo con los sistemas de Derecho Civil, el derecho a la personalidad está definido principalmente como un derecho inmaterial que, a no ser que se aplique el sistema de Derecho Anglosajón, no puede transferirse pero puede utilizarse. Sin embargo, bajo ambos regímenes de derecho, algunos elementos del derecho a la personalidad incluyen bienes comerciables, como por ejemplo la comercialización de fotos[24] o de una licencia de derechos de autor. Existe la posibilidad de dudar de si los "datos personales" podrían considerarse como algún tipo de "propiedad" de una persona.

6.1. Propiedad en los datos personales

Falta una teoría legal convincente que indique cómo ubicar los "datos personales" en relación con los mercados electrónicos. La mayor parte de las contribuciones legales relativas a los datos personales se centran en la relación entre el estado y el ciudadano y brindan enfoques de la protección de la "privacidad" basados en principios como la libertad, la confidencialidad de las comunicaciones o el libre desarrollo de la personalidad. Estos principios no son directamente aplicables a las situaciones mercantiles.

Históricamente, la noción legal de "propiedad" incluye todas las manifestaciones (ius utendi, fruendi, possidendi, etc.) de los bienes tangibles. Los "datos personales", que toman la forma de información relacionada a una persona física y la identifican, son, en contraste, bienes intangibles y, de acuerdo con el Derecho Romano, las tradiciones y las creencias filosóficas rara vez son clasificadas como "propiedad". Aún en el caso de partes tangibles del cuerpo de una persona (tejidos, órganos) el asignar la noción de "propiedad" está negado por tradición[25].

El uso de bienes inmateriales, si no ha sido asignado a una persona ni está especialmente protegido por la ley, depende solamente de procesos socioeconómi-

18 Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), Estrasburgo 1981 (http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm).

19 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 estos datos, DO L 281/31 del 23 de noviembre de 1995.

20 Consumer Data Privacy in a networked world: A Framework for protecting privacy and promoting innovation in the global digital economy, La Casa Blanca, Washington, febrero de 2012 (http://www.whitehouse.gov/sites/default/files/privacy-final.pdf). Algunos principios ya habían sido propuestos en el Libro Verde 2010 por parte del Grupo de trabajo de políticas de Internet del Departamento comercial de los Estados Unidos. (www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf)

21 Departamento de Salud, Educación y Servicios Sociales (HEW) de los Estados Unidos, Registros, computadoras y los derechos de los ciudadanos (Records, Computers, and the right of Citizens), Instituto Tecnológico de Massachusetts. Cambridge / Mass. / Estados Unidos 1973.

22 Art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea, DO C 83/389 del 30 de marzo de 2010.

23 El Tribunal Supremo Constitucional de Alemania resolvió que la Constitución alemana incluirá una "garantía de la confidencialidad e integridad de los sistemas de información" (BVerfGE 120, 274 del 27 de febrero de 2008).

24 Tribunal Civil Federal Supremo de Alemania, 1 de diciembre de 1999, BGHZ 143, 214 - Marlene Dietrich.

25 Una excepción es John Locke, quien reconoció ser propietario de su propia persona (Segundo Tratado sobre el gobierno civil, 1690, Capítulo V, Art. 44).

cos y no conduce a sanciones legales. Solamente en algunos casos la ley reconoce en una persona derechos inmateriales y la inviste con ellos. Los derechos de autor pueden citarse de la misma manera que una ilustración.

Dado que se ha creado un mercado electrónico de datos personales, lo cual significa que existe en Internet la respectiva oferta y demanda, la cuestión es si los datos personales digitales tienden a transformarse en bienes de mercado independientemente de su estructura y origen. En términos reales, las direcciones digitales, los perfiles personales, las imágenes y calificaciones personales o los datos biométricos, que originalmente pudieron considerarse como inalienables y propias de una persona, en la actualidad se comercializan[26]. Si no cedemos algún tipo de "derecho de propiedad" sobre sus datos a las personas, es de esperarse la apropiación indebida por parte de los actores del mercado.

La ley de protección de datos existente inviste a la persona principalmente con el derecho a disponer, corregir, eliminar y consentir con respecto a sus datos personales, a ser informado sobre el uso de tales datos y a negarse ante el uso de cookies relativas a sus datos[27]. En lo que concierne a la esfera privada, este grupo de derechos podría concebirse como la parte comerciable del derecho a la personalidad. Este grupo de derechos podría reformularse como aspectos de un "derecho de propiedad" general en un nuevo bien de información.

Sería recomendable reconocer a los "datos personales" o al "derecho a disponer de los datos personales" como "bienes de información" y crear, además de las categorías de bienes tangibles e intangibles, una tercera categoría legal de bienes comerciables o, de manera alternativa, extender el concepto de derechos morales por analogía.

En Alemania, la protección de los datos personales está anclada al derecho a la personalidad general de la manera en que se expresa en la Constitución. Este derecho a la personalidad general no está definido como un derecho exclusivo, sino como el llamado "derecho marco" ("Rahmenrecht"[28]), cuyas consecuencias legales dependen de una valoración que se hace de los intereses contrapuestos. Los mismos pueden surgir si están en juego la libertad de expresión, la libertad de prensa o la libertad de información.

Pero el principal problema en lo civil en un entorno digital no es el establecer preferencias entre valores constitucionales contrapuestos. El problema principal radica en la cuestión estructural de cómo el derecho civil puede asignar adecuadamente al propietario de los datos, el derecho de disponer, con relación a los datos personales comerciables.

La mayoría de los conflictos en el pasado tenían que ver con la publicación de fotografías y material privado en medios accesibles al público[29]. En esos casos, una vez evaluados los intereses, es posible que se disponga la falta de legalidad de las publicaciones si prevalecen los intereses privados. Por consiguiente podrían entablarse acciones por daños y perjuicios. Pero en caso de corresponder aplicar el derecho contractual, el derecho de responsabilidad civil es complementario al primero.

6.2. Aspectos del mercado

En el ámbito privado una persona es un participante del mercado donde se comercializan datos personales comerciables. Registrarse para cualquier servicio a través de Internet requiere transferir datos personales. El uso de motores de búsqueda implica datos sobre el registro de las personas y sus intereses que son enviados automáticamente a sitios adicionales.

De acuerdo con los términos estándar de los proveedores de servicios ellos ceden la "propiedad" de los datos personales en quien se suscribe, pero al mismo tiempo insisten en su uso y distribución libres. Y eso es una contradicción.

La mayor parte de los desarrollos de TIC actuales tratan con estructuras, implementaciones y aplicaciones en el sector privado. Empresas internacionales poderosas ofrecen almacenamiento electrónico y servicios de comunicación y realizan un uso secundario de los datos personales. Por lo tanto, ya surgieron los mercados electrónicos de datos personales.

Y como consecuencia, los suscriptores pierden el control sobre sus datos. Los proveedores de servicios son quienes obtienen todos los beneficios de adquirir datos personales comerciables. Los proveedores pueden externalizar las pérdidas (distorsión; robo de identidad[30]; pérdida de control). Los grandes retornos generados por la comercialización de los datos personales[31] ofrecen a los proveedores de servicios un incentivo adicional para realizar la recolección y explotación sistemática de los datos personales. Hasta ahora, en la práctica, no es posible hacer cumplir las limitaciones en cuanto a los propósitos para los que se utilizan los datos, la cantidad de los mismos, su vencimiento o su eliminación. El acceso a la información relevante es difícil y usualmente los proveedores de servicios tienen sus oficinas en otros países. En resumen, debemos admitir que los mercados electrónicos de datos personales tienen sus fallas.

Económicamente, no permiten la distribución eficiente de los derechos de propiedad. Desde el punto de vista legal, la aplicación de la ley de protección de datos existente, en especial el cumplimiento de la condición de consentimiento informado, ha demostrado ser muy difícil en el ámbito privado. En Europa y en los Estados Unidos, los intentos por impulsar los mercados electrónicos están dando como resultado nuevas actividades legislativas referentes a la privacidad de los datos. La Unión Europea recientemente propuso una norma para crear más confianza en el entorno en línea y para darle a las personas el control de sus propios datos[32]. El borrador de la norma incluye el derecho de la persona a preferir que sus datos personales sean "olvidados"[33] y el derecho a la "portabilidad de los datos"[34]. Con respecto al Convenio 108 del Consejo de Europa, se han propuesto enmiendas similares[35].

7. Reconceptualización de la Ley de protección de datos

7.1. Principios generales

El Convenio 108 del Consejo de Europa, la Ley de protección de datos de la Unión Europea, los Principios rectores de la ONU de 1990[36], los Lineamientos

26 Un sola dirección vale alrededor de 5,00 euros de acuerdo con un estudio realizado en Alemania en 2012 relativo a las direcciones de los habitantes proporcionadas por las comunidades locales.

27 Enumeración 66 y Art. 2 inciso 5 de la Directiva de la UE 2009/136/CE DO L 337/11 del 18 de diciembre de 2009.

28 BGH NJW 2012, 2197 (2199).

29 ECHR, Solicitud N° 59320/00, Sentencia del 24 de setiembre de 2004, Caroline of Hannover c. Alemania (http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-61853).

30 En los Estados Unidos en el año 2010 se procesaron 1300 casos de robo de identidad (The White House Paper on Consumer Privacy Protection 2012, p. 42).

31 El valor del mercado de Facebook asciende a 625 mil millones de dólares estadounidenses (Frankfurter Allgemeine Zeitung, 2 de octubre de 2012, p. 19) y el mismo resulta principalmente de la venta de datos personales con fines publicitarios.

32 Comisión Europea, Propuesta de Regulación General para la Protección de Datos, COM(2012)11 final del 25 de enero de 2012, enumeración 6.

33 COM(2012)11 final, Art. 17.

34 COM(2012)11 final, Art. 18.

35 Consejo de Europa, Borrador del Informe T-PD(2012) RAP 28 del 24 de setiembre de 2012.

36 Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales, 14 de diciembre de 1990 (http://www.unhcr.org/refworld/docid/3ddcafaac.html).

de la OCDE[37] y el Marco de privacidad del Foro de Cooperación Económica Asia-Pacífico[38] establecen principios generales como la transparencia, la proporcionalidad, la finalidad y el procesamiento justo, entre otros. Dichos principios son necesarios pero no son suficientes. Asimismo, cumplen diversas funciones en el sector público y privado.

7.2 Sector público

El derecho a la protección de los datos personales en el sector público no es un derecho absoluto y debe considerarse en su función en la sociedad[39]. La legislación obligatoria referente a la seguridad nacional y otros intereses públicos tienen la prioridad. Esto puede generar conflictos como ha demostrado el debate sobre la retención de datos de comunicaciones personales con fines estatales que ha tenido lugar en Australia y Europa. Los procedimientos democráticos, siempre que sean controlados por tribunales, instituciones independientes[40] y agencias de cumplimiento de ley podrían restringir los usos indebidos. En general, se observa que cada vez hay más reglamentos vinculantes en el sector público que reemplazan la toma de decisiones individual sobre cuestiones de privacidad de datos.

7.3 Sector privado

7.3.1 Derecho a la propiedad

De acuerdo con la legislación sobre protección de datos, los datos personales deberían estar bajo el control de las personas. A partir de que los datos personales se han convertido en bienes comerciables, la pregunta es quién se beneficia con los principios de protección de datos generales en los mercados. Esto está sujeto a la asignación legal del derecho de disponer, que debe basarse en un derecho de propiedad. Por lo tanto, el modo de las transacciones relativas a los datos personales en mercados a través de contratos depende de la asignación de derechos de propiedad a los participantes del mercado. Existen diversas opciones.

Una opción es reconocer los aspectos comerciales del derecho de personalidad como una "propiedad" en el sentido jurídico. Los datos personales como bien inmaterial tienen una estrecha relación con la propiedad intelectual. Un buen ejemplo de un instrumento que asigna el derecho de propiedad intelectual a la persona sobre sus datos personales es el Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio (TRIPS) de la Organización Mundial del Comercio. En el Artículo 39 (2)(b)(c) se establece que una persona, que tenga la posibilidad legítima de impedir que la información, que tenga valor comercial, se divulgue a terceros, sea adquirida o utilizada por terceros sin su consentimiento, puede reclamar competencia desleal.

Otra opción es extender el concepto de "propiedad" a todos los bienes comerciables independientemente de su estructura física. La definición de "mercaderías" en el Artículo 2 de la Convención internacional sobre los contratos de compraventa de mercaderías (CISG) no limita las "mercaderías" a bienes tangibles. El término "mercaderías" (en inglés: "goods", en portugués: "mercadorias", en francés: "marchandises", en alemán: "waren", en polaco: "towar") comprende a todos los objetos comerciables siempre que no estén expresamente excluidos, como la electricidad (Art. 2(f) CISG).

Una tercera opción es agregar una nueva categoría legal de "bien de información" a la ya histórica distinción entre bienes "tangibles" o "intangibles" (inmateriales)[41]. Esto podría ajustarse mejor a las necesidades de un individuo en la sociedad de la información que crear una analogía de las clasificaciones que se encuentran en los convenios internacionales, las cuales se aplican a las transacciones entre empresas[42]. Un enfoque de derechos de propiedad también podría aclarar y legitimizar los métodos de "privacidad por diseño". Las tecnologías que mejoran la privacidad así como la desactivación de las cookies o la aplicación de métodos criptográficos[43] son complementos técnicos para el reconocimiento de los derechos existentes.

7.3.2 Falla del mercado

Una condición esencial para el intercambio justo de mercaderías comerciables es el funcionamiento del mercado pertinente. Los proveedores de servicios en Internet como Facebook, Google, Apple, Amazon, etc. son actores mundiales que tienen un fuerte peso en el mercado de comercialización de datos personales. Falta una competencia efectiva. Los suscriptores transmiten sus datos personales por una serie de razones conocidas y desconocidas sin poder realizar una elección justa en Internet aún cuando deberían tener la posibilidad legítima de impedir que la información bajo su control se divulgue, sea adquirida o sea utilizada por terceros sin su consentimiento, siempre que dicha información tenga valor comercial y que la persona en cuestión haya tomado las medidas necesarias para mantenerla en secreto[44].

¿Qué estrategias jurídicas existen? La legislación antimonopólica es un recurso para limitar el uso indebido del poder del mercado. En este sentido, la legislación podría adaptarse para alentar nuevos modelos de negocio que ofrezcan servicios de Internet para el pago de cuotas que a la vez garanticen que no se procesarán más datos personales. La promoción de la competencia es un medio para generar opciones entre las alternativas para las personas. Solamente se procesarían adicionalmente datos personales para fines bien definidos si existiese un consentimiento explícito. Una institución de control independiente (comisionado de protección de datos) debería salvaguardar los intereses de las personas.

A menos que a las personas se les ofrezcan opciones contractuales justas para la transacción de datos personales comerciables, las fallas del mercado pueden tener como resultado la clasificación de personas como "consumidores"[45]. Por lo tanto, la reglamentación obligatoria de protección a los consumidores adquiere importancia para el cumplimiento de la ley de protección de datos.

La nueva reglamentación marco de la legislación de protección de datos, tal como fue planificada por la

37 C(80)58/FINAL del 23 de setiembre de 1980 (http://www.oecd.org/privacy).

38 Foro de Cooperación Económica Asia-Pacífico (http://www.apec.org/Groups/Committee-on-TradeandInvestment/>/media/Files/Groups/ECSG/05_ecsg_privacyframework.ashx).

39 ECJ, 9 de noviembre de 2010, C-92/09 y C-93/09, Casos conexos Volker and Markus Schecke GbR/Hartmut Eifert c. Land Hessen, DO C 13/6 del 15 de enero de 2011.

40 Ver: Hans-Jörg Albrecht et al./Max-Planck Institut für ausländisches und internationales Strafrecht (ed.), Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten, 2. erweiterte Fassung, Freiburg i.Br. Julio de 2011.

41 Mi propuesta correspondiente (en cuanto a los programas) fue la adoptada por el Tribunal Civil Federal de Alemania: BGHZ 102, 135 (140).

42 Recientemente, el Tribunal de Justicia de Europa dictaminó que el principio de agotamiento de derechos (principio de la primera venta) se aplica incluso a una copia única descargada de un programa y no necesariamente material (ECJ, C-128/11, 3 de julio de 2012, Oracle c. UsedSoft http://eurlex.europa.eu).

43 Aplicaciones como AdBlockPlus, BetterPrivacy, DuckDuckGo, JavaScript Blocker, NotScript, ScriptNo, Tor, entre otras.

44 La formulación corresponde al Artículo 39 (2)(b)(c) del Acuerdo TRIPS.

45 La Ley sobre la privacidad de los consumidores de la Casa Blanca (The White House Consumer Privacy Bill) de 2012 se denomina: La privacidad de los datos de los consumidores en un mundo en red (Consumer data privacy in a networked world).

Unión Europea, puede interpretarse como la forma de ofrecer una ley moderna para la protección de consumidores. El borrador de la reglamentación incluye cláusulas legales obligatorias relativas al consentimiento informado, el derecho a revocar, olvidar y borrar físicamente datos personales, así como la posibilidad de exportarlos a otro proveedor de servicios.

La reglamentación más universal europea tiene diferencias con la Ley de privacidad de los consumidores promulgada por la Casa Blanca este año en Washington. La Ley de privacidad de los consumidores "se refiere únicamente a cómo gestionan las entidades del sector privado, los datos personales en un contexto comercial"[46]. Tiene como fin "hacer que los códigos de conducta sean la base de protección de privacidad mutuamente reconocida"[47]. Estos Códigos de conducta no requerirán una legislación especial.

La Ley depende de un "proceso multipartito"[48] para procedimientos de autocertificación.

Este enfoque de lo particular a lo general tiende a igualar el interés principal de las personas con los intereses competitivos de las otras "partes interesadas". El impacto de las fallas del mercado en la gestión de datos personales no se ha considerado. El respeto por la defensa del control de las personas ocasionalmente afecta dicho modelo de procedimiento. En lugar de un tribunal, la Comisión Federal de Comercio (FTC) debe establecer si la compañía cumple con el código aplicable y puede imponer multas en el caso de incumplimientos.

8. Expectativas para el futuro

La sensibilización pública a nivel mundial en relación a los problemas de privacidad de datos es bastante alta[49]. La privacidad de los datos no es para nada un valor obsoleto. Los principios básicos, tales como se establecen en el Convenio del Consejo de Europa sobre la protección de datos, pueden identificarse fácilmente como un tipo de legislación moderna de protección a los consumidores.

Los principios se han ido aceptando en diversas regiones, incluso en Azerbaiyán, China, India, la República de Macedonia o Moldavia. Estos principios pueden brindar una base apropiada para el marco de privacidad de datos legales a nivel mundial. Hasta el momento, el Convenio es el único instrumento vinculante internacional sobre la privacidad de datos y 44 países lo han ratificado. Su acceso es abierto a países no europeos.

Los impactos de dichos principios básicos varían considerablemente cuando se aplican al sector público y privado.

En cuanto al sector público, fácilmente puede generarse un conflicto de intereses entre los estatales y los principios básicos de privacidad de datos. La correspondiente legislación pública obligatoria debería estar sujeta al escrutinio democrático.

En lo que concierne al sector privado, el concepto futuro de privacidad de datos en mercados electrónicos debe tener en cuenta el hecho de que varias formas de datos personales se han transformado en bienes comerciables. Las personas no tienen la posibilidad de escoger opciones realistas en los mercados monopólicos u oligopólicos. La asignación del derecho de propiedad en los datos personales comerciables ofrece un método para que las personas tengan el control de sus propios datos comerciables. Por lo tanto, el control también podría gestionarse de manera más eficaz por sociedades que ejerzan sus derechos. A nivel económico, podrían supervisar la posición de negociación de una persona respecto a la finalización de contratos de proveedores de servicios de Internet.

En este sentido, es necesario que los principios básicos de privacidad de datos sean específicos mediante un marco legal adicional. Se asumirá que una persona que actúe como consumidor en el entorno digital está razonablemente bien informado respecto de los aspectos técnicos pero no de los aspectos legales. Particularmente, en el caso de las personas que utilizan teléfonos inteligentes para celebrar contratos en Internet, deberá brindarse información pertinente y concreta.

La información podría asegurarse mediante marcas de calidad o etiquetas confiables independientes.

Se ha generado un problema grave debido al aumento significativo del flujo transfronterizo de datos personales. A menos que no pueda alcanzarse un nivel de protección adecuado mediante ajustes de las cláusulas de privacidad de datos de lo general a lo particular o viceversa, la persona podrá verse privada de sus derechos en los casos en que el controlador de los datos no resida en el país de dicha persona. La mayoría de los servicios de computación en la nube, motores de búsqueda y otros servicios basados en Internet tienen su sede de negocios en los Estados Unidos de América. Por ello, el cumplimiento de la legislación es una cuestión difícil. Rara vez, una persona tiene la opción real de acudir a un tribunal. Los recursos y las querellas colectivas podrían ofrecer un mecanismo más eficaz.

Para resolver los problemas de privacidad existentes en los mercados electrónicos, una entidad internacional debería asumir la responsabilidad de elaborar una ley modelo a nivel internacional para el sector privado. La ley modelo debería destacar el potencial singular de los principios generales y abarcar los siguientes mecanismos transfronterizos:

- Cláusulas relativas a los reconocimientos mutuos de reglas de privacidad de datos basadas en leyes públicas obligatorias o autorregulaciones aplicables.
- Cláusulas relativas a la notificación pronta y eficiente a autoridades en otro país.
- Cláusulas relativas a la asistencia en la investigación en casos de cumplimiento de privacidad de datos.
- Cláusulas relativas al alto nivel de protección de los consumidores en cuanto a los consentimientos informados de procesamiento de datos personales.
- Cláusulas para estimular el cumplimiento de las leyes desde el punto de vista de la legislación internacional privada.

En lugar de la OMC, la OMPI u otro organismo gubernamental, la CNUDMI es quien tiene la experiencia específica sobre el tratamiento de entornos electrónicos en contextos comerciales[50]. Podría encomendarse a la CNUDMI. La ley modelo debería tener en cuenta que un nivel alto de privacidad de datos no constituye una restricción en el comercio de servicios (Art. XIV (e)(ii) OMC-AGCS).

La ley modelo debería brindar un primer paso hacia un Convenio de las Naciones Unidas sobre la Privacidad de Datos.

b. Reseña de las Conferencias, Plenarios y Paneles de la 34ª Conferencia

En el marco de la 34ª Conferencia de Autoridades de Protección de Datos y Privacidad se realizaron dos Conferencias magistrales a cargo del Ing. José Clastornik, Miembro del Comité Ejecutivo de la URCDP, del Dr. Brad Smith Consejero General y Vicepresidente Ejecutivo de Asuntos Legales y Corporativos de Microsoft y el Dr. Wolfgang Kilian, Profesor de la Universidad de Hannover.

El Ing. José Clastornik inició la conferencia afirmando que Uruguay desde hace ya bastante tiempo no es sólo un país natural sino que también tiene grandes avances en tecnología o en todo lo vinculado con lo digital. Esos avances se ven en múltiples instancias, por ejemplo en la digitalización de las telecomunica-

46 The White House Consumer Privacy Bill, p. 5 nota 1.

47 The White House Consumer Privacy Bill, p. 32.

48 Las partes interesadas son "compañías individuales, grupos de la industria, defensores de la privacidad, grupos de consumidores, víctimas de delitos, académicos, socios internacionales, el Fiscal General del Estado, representantes de cumplimiento federal, civil y penal y otros grupos pertinentes" (The White House Consumer Privacy Bill 2012, p. 23).

49 Ver: Comisión Europea (ed.), Special Eurobarometer 359, Attitudes on Data Protection and Electronic Identity in the European Union, 2011 (http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf).

50 Ver: la Ley Modelo sobre Firmas Electrónicas y la Ley Modelo sobre Comercio Electrónico de la CNUDMI; y el Borrador de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales.

ciones, en los indicadores de inclusión digital, - que son los más altos de la región-, en proyectos como el Plan Ceibal, que significa la implementación del sueño de Negroponte “un computador para cada niño, cada liceal y cada maestro”, entre otros.

A su vez, se trabajó con el Plan Ceibal en todo lo que tiene que ver con el acceso de la familia. Con su diseño, se pretendió que no fuera necesario un desplazamiento mayor a 300 metros de la casa de cualquier niño, para tener un lugar de acceso libre a Internet. La conectividad se garantiza desde la propia estructura, la que a su vez pasa por determinados filtros de contenidos.

Se verifican múltiples desafíos. Entre ellos, se presentan aquéllos que tienen relación con temas tales como Big Data, Profiles, Intercambio de Información, Integración de Información, y estos son parte de todos los proyectos de Gobierno Electrónico, ya sea que se esté trabajando en comercio electrónico, en firma digital, en salud electrónica, en identificación digital. Se afirma, además, que seguramente van a continuar apareciendo más desafíos relacionados con la privacidad y la seguridad de la información.

El resolver y plantear soluciones a esos desafíos, es lo que le da confianza a todo el sistema. La base de sustento de todos estos desafíos, es generar confianza y ello se construye de acuerdo a cómo se trabaje en relación con la privacidad, la protección de datos personales y la seguridad de la información.

La idea desde el inicio ha sido trabajar con una visión de todo el problema, es decir, con una visión holística, que además trate de generar balances. Por ejemplo si en e-Gov se trabaja con Gobierno Abierto, Datos Abiertos y Transparencia, debe hacerse lo propio para proteger la confidencialidad y la reserva de determinada información, y ese equilibrio debe existir dentro de todos los proyectos de Gobierno Electrónico.

También es necesario la generación de equilibrios dentro de lo que es la aplicación de tecnología y la regulación, o sea que estos de alguna forma son multidimensionales, considerando las capacidades de uso y de crecimiento que otorgan las tecnologías versus los derechos de las personas. Este balance de alguna forma tiene que ser entendido en forma dinámica, porque las características con las que se trabaja hoy, no son las mismas que se verificarán a futuro. La estabilidad del sistema requiere que se comprenda ese dinamismo.

En Uruguay se trabajó desde el inicio con esta visión holística y de equilibrio. AGESIC comenzó efectivamente a funcionar en 2007 y en 2008 se crearon varias de las unidades reguladoras; en donde se destaca la creación de la Unidad Reguladora y de Control de Datos Personales (URCDP).

Los cuatro ejes en que se trabaja la temática del e-Gov en AGESIC son: a) transformación del Estado, b) buen uso de la tecnología, c) empowerment de la ciudadanía digital, y d) la generación de confianza que permita el desarrollo continuo en el tiempo de los proyectos que están en implementación.

En un principio, lo que probablemente fuera más tentador para una Agencia como la que se planteó, habría sido trabajar sólo en tecnología, pero ello no hubiera permitido ver la gran figura y los mecanismos de balance que hay que considerar. Por eso se promocionó la formulación de un marco legal nuevo que abarcara la privacidad y la protección de datos personales, junto con la creación de una Unidad Reguladora que extendiese el marco legal existente –en aquel momento sólo para datos comerciales-, hacia una visión más comprensiva que incluyese los datos personales en su conjunto.

La construcción de esa gran figura, se efectiviza no sólo desde AGESIC, sino desde todos y entre todos. Si se mira esa gran figura, se puede apreciar que desde la creación de la Unidad Reguladora, ésta ha trabajado en todo lo que es la reglamentación de la Ley, el registro de las bases de datos y todo lo que de alguna forma se comparte con otras unidades reguladoras. En definitiva, se ha trabajado tratando de generar una visión de conjunto, cuidando que ello sea así porque es un tema importante y distintivo, que colabora a darle estabilidad a todo el sistema.

Ahora bien, es necesario cuestionarse cuáles son los desafíos que se presentan para el futuro, cuáles serán los paradigmas que aún no se conocen y en las cuales indudablemente habrá que trabajar.

Respecto a los equilibrios, es imprescindible crear toda una infraestructura legal y normativa, en donde es preciso tener presente que si bien la tecnología puede ser parte del problema, también puede serlo de la solución. Por ejemplo, en el área de la interoperabilidad, -un área muy compleja para el Estado porque es donde se está juntando toda la información, se trabaja tecnológicamente con dos tipos de soluciones que están en desarrollo simultáneo. Una que está basada en los deberes y obligaciones de cada organización, estructurando una plataforma de interoperabilidad que permita que los deberes y obligaciones de cada organización se traspasen a los deberes y obligaciones de la que reciben el dato, de forma tal que los datos se manejen con las mismas garantías y obligaciones. Éste es un esquema basado en deberes y obligaciones de las instituciones.

Una segunda forma de visualizarlo es tener una sede electrónica de la persona, donde ésta defina cuáles son los usos admisibles para los contenidos y cuáles datos disponibiliza para ser compartidos con otras instituciones. En este sentido, la referencia no es a los deberes y obligaciones de las instituciones, sino al derecho ciudadano a la privacidad de los datos.

Son dos formas de encarar soluciones. Son complementarias y probablemente se necesite utilizar ambas, dependiendo del tipo de problema que se tenga que resolver. El punto es que no todo, tal vez, se tenga que resolver mediante una regulación normativa, sino que habrá también que utilizar la tecnología como un instrumento más para resolver los problemas.

En definitiva tres puntos centrales en nuestra forma de trabajar, son los que se han desarrollado hasta ahora:

- La Gran Pintura/ Visión Holística - The big picture/ holistic view.
- Dinamismo/ Balance por Diseño - Dynamic/ balance by design.
- Tecnología: Problema/Solución – Tecnology: Problem/solution.

Esto es parte de la política en ejecución y es lo que de alguna forma se pretende trasmitir desde el momento en que se aceptó en nombre de Uruguay la realización de la 34º Conferencia de Autoridades de Protección de Datos. Interesa trabajar en una visión holística, mirando la gran pintura en su conjunto, que no tiene sólo una parte regulatoria y legal, sino también tecnológica. Se considera, asimismo, que se debe trabajar en los equilibrios y balances. Para que sea estable la solución, tiene que existir un equilibrio que permita que lo mueva el viento, que sea dinámico en su funcionamiento, pensando en la tecnología no sólo como parte del problema sino también como parte de la solución.

La conferencia se estructuró además en base a Plenarios y Paneles destacándose de cada uno de ellos lo siguiente:

Plenario I – El Impacto de las nuevas tendencias en la Sociedad de la Información

Este Plenario analizó el impacto de las nuevas tecnologías en la protección de datos personales. Se abordaron qué expectativas puede ofrecer la Sociedad de la Información a las normas y prácticas relacionadas con la protección de datos personales. Se apuntó a conocer más a fondo los rasgos definitorios de las mismas. ¿Cuánto existe de limitante y perjudicial, y cuánto de aperturista y saludable en esta básica relación? Para nuestras competencias la Sociedad de la Información es el espacio en el que crecen y se multiplican prácticamente todos los temas de la disciplina. De ahí que detenerse en una comprensión del escenario mayor, tanto como en sus aportes y restricciones al movimiento internacional de la Privacidad son imperativos vigentes.

La Conferencia central estuvo a cargo de Wolfgang Kilian, Profesor de la Universidad de Hannover (Alemania). Moderó Raúl Echeberría, Director Ejecutivo de LACNIC (Uruguay) y fueron expositores: Carolina Cosse, Presidente de ANTEL (Uruguay), Christopher Wolf, Fundador de "El futuro de Internet" (EEUU), José Luis Piñar, de la Universidad CEU (España), Federico Monteverde, Miembro de la URCDP (Uruguay)

El Mag. Federico Monteverde integrante del Consejo Ejecutivo de la URCDP comenzó su exposición con la pregunta ¿Qué es la tecnología? Dijo que es el conjunto de teorías y técnicas que permiten el aprovechamiento práctico del conocimiento científico. En la base misma de su definición se encuentra el conocimiento científico.

Continuó expresando que en la sala hay especialistas de diferentes áreas que brindan distintas perspectivas. Federico Monteverde les invita a realizar un viaje intelectual a través de la ciencia para hacer una lectura de la sociedad contemporánea en el marco del tiempo cósmico, en el cual 13 mil millones de años de historia del universo se reducen a un siglo. En ese marco, en los últimos segundos se ha dado la construcción del paradigma tecnológico organizado a partir de las tecnologías de la información, en lo que hoy conocemos como sociedad de la información

Enuncia que hace sólo 7 segundos se desarrolló el estándar de comunicaciones que permite el acceso a Internet y la World Wide Web. Desde entonces la cantidad de computadores creció sin cesar hasta superar los mil millones y hoy los datos transferidos a través de Internet superan el 98 % de todos los datos transferidos en forma electrónica. La información almacenada en medios digitales se calcula en medio millón de gigabytes y en el próximo segundo cósmico ascenderá a treinta y cinco mil millones de gigabytes. Esta cantidad de información ya ha transformado la forma de hacer negocios, la organización del Estado, y el día a día de las personas, cuyos datos personales son procesados, circulan por la red, y son almacenados en bases de datos, afectando su privacidad.

Indica que frente a esta evolución cabe preguntarse cómo mantener el equilibrio entre privacidad y tecnologías, cuáles son las bases sólidas sobre las cuales construir una sociedad moderna y equitativa. ¿Podemos hablar de una crisis de la privacidad provocada por las tecnologías? Los tiempos de crisis pueden ser tiempos de creatividad. Significa que se puede llegar a una síntesis entre los peligros y la creatividad. Se trata de un proceso doloroso pero altamente positivo de nuestras visiones que funcionan como un crisol de nuevas actitudes éticas.

Manifiesta que la tecnología trae el progreso pero se debe tener al hombre como medida de todas las cosas. Siendo así la tecnología deberá ser liberadora. Ésta es la clave para equilibrar el pie de la balanza entre la tecnología y la privacidad.

El cree que es imprescindible ocuparse del tema porque la privacidad es un derecho humano fundamental y para su defensa nunca es tarde y siempre vale la pena. El Convenio Nº 108 tiene solo 7 segundos cósmicos de haber sido aprobado y la Directiva de la Unión Europea apenas 4 segundos.

Concluye que cada persona debe continuar el viaje, y caminar significa una constante pérdida y recuperación del equilibrio. De las acciones que se tomen dependerá el equilibrio entre tecnología y privacidad en los próximos segundos cósmicos.

Plenario II – Protección de Datos Personales y Gobierno Electrónico

En épocas de nueva gestión pública basada en Tecnologías de la Información, las Administraciones estatales continúan siendo grandes recopiladores de datos personales, recogiéndolos y tratándolos al servicio de sus cometidos.

Acceso a la información pública, intercambios y reutilización de la información que dispone un determinado sector de la Administración; política de datos abiertos, transparencia del mercado financiero, inspecciones del Fisco, son algunos de los escenarios e instrumentos que plantean tensiones, abriendo interrogantes sobre cuándo y cómo legitimar una colecta inicial, pero también una cesión o comunicación posteriores de datos personales, en contextos de administración electrónica.

La protección de datos debe tener en cuenta el desarrollo del Gobierno Electrónico para no descuidar su marco jurídico.

Moderó Trevor Hughes CEO de la IAPP (EEUU) y fueron expositores Pierre Trudel, Universidad de Montreal (Canadá), Fred H. Cate, Universidad de Indiana (EEUU) y Vagner Diniz, Gerente W3C (Brasil).

Plenario III- Modelos de Regulación de Privacidad

La protección de datos personales cuenta con regulaciones específicas en diversas partes del mundo que han obedecido a diferentes motivaciones acordes con la realidad socio-económica, política y jurídica de cada país o región.

Es posible identificar modelos de regulación basados en distintos enfoques y perspectivas, ya sea enfatizando el derecho a la protección de datos como un derecho fundamental o protegiendo los derechos de los consumidores.

Es así que resulta fundamental el análisis de las buenas prácticas y de los diversos modelos de privacidad con el objetivo de evaluar e intercambiar expe-

riencias, enriqueciéndose con los aspectos positivos de cada uno de ellos.

Moderó Jacob Kohnstamm, Presidente del Grupo de Trabajo del Artículo 29 (Holanda) y fueron los expositores Julie Brill, Comisionada de la Federal Trade Commision (USA), Allan Chiang, Autoridad de Protección de Datos de Hong Kong, Giovanni Buttarelli, Adjunto del Supervisor Europeo (Italia), Bruno Giancarelli, Jefe del Sector de Relaciones Internacionales de la Comisión Europea.

Plenario IV- La nueva Normativa Europea

El impacto del uso de la tecnología es de tal magnitud, que obliga a introducir cambios que faciliten una protección adecuada y un efectivo control de los datos personales, así como la preservación de la intimidad en medio de una realidad básicamente digital y globalizada.

La nueva legislación busca ampliar y reforzar los derechos de las personas (derecho al olvido, a la portabilidad de los datos, privacidad por defecto, consentimiento expreso e inequívoco, nuevo sistema de multas por incumplimiento, etc.), así como a mejorar la economía mediante la supresión de cargas administrativas y simplificación de procedimientos.

Con estos objetivos en los próximos años muy probablemente se aprobará un nuevo reglamento que se transformará en el marco general para la protección de datos personales, armonizando así la legislación de la Unión Europea. También se proyecta la realización de una nueva directiva que regulará la protección de los datos personales tratados con fines de prevención, detección, investigación o persecución de delitos y su respectiva actividad judicial.

Este plenario tuvo como objetivo la discusión y análisis de estos cambios, sopesando las ventajas y desventajas a la luz de la realidad actual.

Moderó Peter Hustinx, Supervisor Europeo (Holanda) y fueron expositores José Luis Rodriguez, Director de la Agencia Española de Protección de Datos (España), Richard Allan, Responsable de Facebook para Europa (Inglaterra), Isabelle Falque-Pierrotin, Comisionada Presidenta de CNIL (Francia), Bruno Gencarelli, Jefe de sector de Relaciones Internacionales de la Comisión Europea

Plenario V- Protección de Datos Personales en América Latina. Ampliando horizontes

¿Desde qué óptica se incorporó este derecho en la región? ¿Por cuál sistema se ha optado? ¿Cuál es el rol de las entidades garantes? Éstas fueron algunas de las preguntas analizadas en este plenario.

El nacimiento y desarrollo del derecho a la protección de datos personales se formaliza en el seno europeo a partir del último tercio del siglo pasado, mediante normas supranacionales y de derecho interno de cada país.

Estas normas permitieron que la Unión Europea avanzara rápida y considerablemente en la construcción de un sistema garante de los datos personales coherente y armonizado, que poco a poco ha sido internalizado por otros continentes como un derecho autónomo.

América Latina no ha estado ajena a la tuición de este derecho. Con base constitucional o sin ella, numerosos países fueron progresivamente regulando el derecho a la protección de datos a través de normas locales o nacionales, en conjunción con las tradiciones jurídicas propias (habeas data, amparo).

¿Desde qué óptica se ha visto e incorporado este derecho en la región? ¿Por cuál sistema se ha optado? ¿Cuál es el rol de las entidades garantes, ya no solo las judiciales sino también las autoridades administrativas independientes de control? Son algunos de los temas que pretendieron debatirse en este panel.

Moderó María José Viega, Directora del Instituto de Derecho Informático de la Universidad de la República (IDI), Directora de Derechos Ciudadanos de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) (Uruguay) y fueron expositores Pablo Segura, Coordinador Legal de la Dirección Nacional de Protección de Datos Personales (Argentina); Danilo Doneda, Coordinador General de Supervisión y Control de DPDC; Ministerio de Justicia (Brasil); José Alejandro Bermudez, Superintendencia de Industria y Comercio (Colombia); Felipe Rotondo, Presidente de la URCDP (Uruguay); Arlene González, Autoridad de Protección de Datos de Costa Rica (Costa Rica); José Alvaro Quiroga León, Jefe de la Autoridad Nacional de Protección de Datos Personales (Perú); Ángel Trinidad, Comisionado del IFAI (México).

El Dr. Felipe Rotondo como Presidente de la Unidad Reguladora y de Control de Datos Personales de Uruguay, destacó que Uruguay avanza en materia de protección de datos. La Ley es de agosto de 2008 y fue aprobada por la unanimidad de los integrantes del Parlamento Nacional, sin oposición ciudadana de índole alguna, y sigue básicamente los lineamientos de la Unión Europea y del Convenio N° 108.

En abril de 2009 se integró el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales (URCDP) del cual el Dr. Rotondo es integrante. Se trata de un órgano desconcentrado privativamente y que funciona en el ámbito de la Presidencia de la República, concretamente en la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC). Posee competencias propias que el jerarca no le puede quitar ni abocar, entre ellas las de regulación, registro, autorización de transferencias internacionales, control y la potestad sancionatoria. Por otra parte, los miembros no pueden ni deben aceptar órdenes de ningún tipo, ni instrucciones de carácter técnico.

La motivación que Uruguay ha tenido a efectos de regular en este tema refiere a:

- Reconocer el derecho como inherente a la personalidad humana (art. 72 de la Constitución) y brindarle medios específicos de garantía. Lo que hace la Ley es reconocer un derecho preexistente en la Constitución desde 1918.

- Afrontar los desafíos que presenta la implementación del Gobierno Electrónico, o para ser más específico, la gobernanza electrónica.

Por otra parte, en lo que hace relación con el plano del relacionamiento internacional, se destacaron los siguientes aspectos:

- La adecuación con la Unión Europea (La Decisión de Ejecución de la Comisión es del 21 de julio de 2012).
- La adhesión al Convenio N° 108.

Por otra parte, se señaló particularmente que las especificidades de la Ley N° 18.331 son:

- La extensión a las personas jurídicas en cuanto corresponda.
- La expresa consagración del derecho de inclusión, además de los derechos ARCO.
- Las características del consentimiento. Debe ser escrito en caso de datos sensibles y el silencio se debe considerar como negativo, o sea si pasados 10 días si no se expresa se considera que no lo otorga.
- El Habeas Data judicial. Esta acción es específica y sumaria.

Finalmente se efectuaron referencias a lo que se entiende son los desafíos actuales de la URCDP, a saber:

- Contribuir a generar conciencia del derecho y sus garantías. Se consideró que se entiende que el ciudadano uruguayo tiene bastante conciencia respecto a la protección de sus datos personales sin perjuicio que de todas maneras la Unidad seguirá trabajando en este sentido.
- Incidir en la aplicación equilibrada en relación con otros derechos y determinados intereses públicos.
- Concretar un mayor control con el adecuado apoyo técnico.
- Lograr un mayor nivel de cooperación con las demás autoridades, en especial en América Latina, el que se verá facilitado con la aprobación de nuevas leyes.

En cuanto a los paneles se destacan los puntos más relevantes de cada uno de ellos:

Panel A - Gobierno abierto

Las nuevas tecnologías ofrecen oportunidades para el intercambio de información, la participación ciudadana y la colaboración. Cada vez más, los gobiernos procuran aprovechar estas tecnologías para hacer pública más información, de manera que permita a los ciudadanos entender lo que sus gobiernos hacen e influir en las decisiones.

Los gobiernos se encuentran cada vez más alineados en fortalecer su compromiso con la transparencia, luchar contra la corrupción, empoderar a los ciudadanos y aprovechar a las nuevas tecnologías para un gobierno más eficaz y responsable. En este sentido, recolectan y almacenan datos personales, y los ciudadanos tienen derecho a solicitar información sobre las actividades gubernamentales, promoviendo un mayor acceso a la información.

La adopción de políticas y estrategias de Datos Abiertos es quizás uno de los enfoques más innovadores para aprovechar las nuevas tecnologías en materia de disponibilidad de información. Proporcionar activamente información de alto valor, incluidos los datos primarios, de manera oportuna, en formatos que el público pueda encontrar, comprender y utilizar fácilmente, y que simplifiquen su reutilización.

Sin embargo, la enorme cantidad de información y su capacidad de reutilización obliga a realizar un balance entre la confidencialidad de la información, la existencia de un marco jurídico adecuado para hacer pública la información y los principios que hacen a un buen gobierno.

El presente panel tuvo como objetivo analizar el impacto que tiene esta mayor apertura en el gobierno, con relación a la confidencialidad y datos personales, y qué tipo de medidas se deberían adoptar para lograr el referido balance.

Moderó Iñaki Vicuña, experto en Protección de Datos Personales (España) y fueron expositores David Banisar, Asesor Legal Artículo 19 (EEUU), Christopher Graham ICO (Reino Unido), Javier Ruiz Díaz, Open Rights Group (Reino Unido).

Panel B - Geolocalización pública y privada

¿Dónde vamos a cenar? Ésta es una pregunta que quizás no nos hagamos más. Si pensamos en prospectiva, en poco más estaremos usando con cierto grado de masividad la geolocalización en actividades cotidianas: para llegar al trabajo evitando las zonas de mayor congestión, para buscar un buen restaurante o un cine que nos ofrezca la película de nuestro agrado, para conocer el clima reinante a medida que nos vamos desplazando de una zona a otra, o incluso para hacer público el lugar exacto en el que nos encontramos y compartirlo con nuestros contactos.

Las aplicaciones de geolocalización aparecen cada vez con mayor fuerza a la medida de nuestras necesidades. Permiten obtener todo tipo de información en tiempo real a través de un simple dispositivo conectado a Internet. Sin embargo, hay que tener presente que todas estas actividades repercuten en nuestra privacidad, aspecto que muchas veces desconocemos. Por ello es importante analizar cuáles son los riesgos que estos servicios presentan, y cómo podemos evitarlos.

Moderó Christopher Olsen de la Federal Trade Commission (EEUU) y fueron expositores Peter Schaar, Comisionado de la Autoridad de Protección de Datos de Alemania, Endre Gyozo Szabo, Vicepresidente de la Autoridad de Protección de Datos de Hungría, Pat Walshe, Director of GSMA (Reino Unido), Beatriz Rodríguez, Miembro del Instituto de Derecho Informático de la Universidad de la República (IDI) y de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) (Uruguay).

Panel C - E-Salud

Las Tecnologías de la Información inciden en todos los aspectos de nuestra vida, y la salud no es la excepción. La seguridad de las historias clínicas sigue siendo un tema clave. En tal sentido la reciente normativa busca instaurar medidas preventivas de rango general.

Asimismo, hay quienes implementan sistemas de tarjeta sanitaria electrónica, lo cual supondrá un gran avance. No obstante también implica algunos resguardos respecto a su seguridad.

Ante este panorama, se consideró necesario confrontar experiencias, buenas prácticas y analizar qué medidas se están tomando para garantizar la seguridad en lo que refiere a los datos de salud, considerados -según consenso- datos personales de carácter sensible.

Moderó Jesús Rubí, Subdirector AGDP (España) y fueron expositores Carlos Delpiazzo, Instituto de Derecho Informático de la Universidad de la República (IDI) (Uruguay). Deven McGraw, Center for Democracy and Technology (EEUU), Philip Evans, Boston Consulting Group (EEUU), Sarah Wynn-Williams, Manager of Privacy And Public Policy Facebook (Nueva Zelanda).

Panel D – Herramientas de Concientización y Difusión: ¿Preparado para una vida 3.0?

Algunos hablan de evolución, otros de revolución. Lo cierto es que la Web que conocemos se encuentra próxima a cambiar. La información será capaz de relacionarse entre sí, clasificarse y ordenarse sin necesidad de la intervención humana. Los agentes inteligentes leerán información y devolverán conocimiento. Para su funcionamiento, se requerirá del usuario mayor transparencia y apertura. Resulta crucial, entonces, analizar los nuevos desafíos que esta Web presenta a la privacidad y protección de datos, así como conocer las iniciativas y estrategias que las autoridades y la sociedad civil pretenden desarrollar.

Moderó este panel: Chantal Bernier, Comisionada Adjunta Protección de Datos de Canadá y fueron expositores Larry Magid, Connect Safely (EEUU), Pablo Pérez San José, INTECO (España), Steve Wood, ICO (Reino Unido), Clara Guerra, Comisión de Datos Personales de Portugal.

Panel E - Herramientas forenses: lo que nuestros dispositivos dicen de nosotros

Por un momento pensemos cuántas comunicaciones electrónicas realizamos, cuántos documentos electrónicos y archivos multimedia almacenamos en diversos dispositivos. Todo puede ser relevado llegado el caso.

Las herramientas forenses, como el E-Discovery, permiten identificar, colectar, preparar y preservar información electrónica, en el marco de un proceso legal.

Además de la arista técnica, todo proceso de este tipo implica aspectos legales referidos a la protección de los datos personales y la seguridad de la información.

Moderó Monique Altheim, Especialista en E-Discovery (Bélgica) y fueron expositores Yoram Hacohen, Autoridad de Información y Tecnología (Israel), Jeimy Cano, Prof. Universidad de los Andes (Colombia), Gustavo Betarte, Prof. Facultad de Ingeniería de la Universidad de la República (Uruguay), William Barker, NIST (EEUU), Oscar Puccinelli, Profesor de Derecho Constitucional, Universidad Nacional de Rosario (Argentina).

Panel F - Herramientas de Cooperación: el camino posible y efectivo

La cooperación internacional entre las DPA constituye una herramienta imprescindible que debe acompasar el constante avance de las tecnologías, ya que con ello se afianza el cumplimiento de la normativa de protección de datos.

Las brechas de seguridad ya no suceden en el ámbito doméstico, sino que tienden a su internacionalización. En la era de las grandes bases de datos, y ante la falta de convenciones de alcance mundial, la cooperación internacional aparece como uno de los pocos caminos de tránsito posible y efectivo.

La actual tendencia hacia una legislación global de PDP, la experiencia de un diálogo siquiera incipiente entre autoridades ubicadas en diversos continentes, son también aspectos relevantes a considerar en la estrategia de implementar una protección ubicua del derecho.

Moderó Blair Stewart, Vice Comisionado de Nueva Zelanda y fueron expositores John B. Morris, Director de Políticas de Internet de la Administración Nacional de Telecomunicaciones e Información (NTIA – Estados Unidos), Lina Ornelas, Profesora Investigadora Asociada, Centro de Investigación y Docencia Económica, A.C. CIDE (México), Diana Alonso Blas, Data Protection Officer at Eurojust (Holanda), Rafael García Gozalo, Coordinador del Departamento Internacional, AEPD (España).

Panel G - Marketing comportamental en línea

Varias razones llevan a los sitios Web a usar tecnologías de marketing comportamental: la posibilidad de personalizar información, buscar posibles compradores de bienes o servicios en línea o recolectar datos demográficos. Es, además, una forma de mantener actualizados a los determinados sitios según los intereses de los usuarios, mediante la captura de datos de los comportamientos de éstos en Internet.

Sus perfiles se crean analizando páginas visitadas, cantidad de tiempo en cada página, enlaces consultados, búsquedas e interacciones. ¿Es deseable que se guarden trazas de los sitios Web visitados por los usuarios desde la óptica de la protección de datos personales? Estos elementos de detección se encuentran hoy previstos en el proyecto de reforma de la nueva Directiva de la Unión Europea.

Moderó Justin Brookman, Director de Privacidad del Center for Democracy and Technology (EEUU) y fueron expositores Florence Raynal CNIL (Francia). Ashley Winton, White & Case (Reino Unido), James Mullock, Socio de Osborne Clarke (Reino Unido), Edith Ramirez, Comisionada de FTC (EEUU).

Panel H - Biometría

Asistimos a nuevas formas de identificación automatizada de personas. Hoy en día la tecnología de reconocimiento facial no solo se utiliza como instrumento de combate a la criminalidad, el fraude en los pasaportes y soporte al orden público, sino también para acelerar el proceso de identificación de amigos y conocidos en las fotografías que se publican en redes sociales.

Cada vez son más las empresas que invierten en tecnologías para el reconocimiento facial con distintos propósitos, pero realmente poco se escucha sobre las medidas de seguridad y de protección a la privacidad de los usuarios ante su implementación.

¿Cómo juega el deber de informar y la obtención del consentimiento en este sistema de identificación?

Una vez más la biometría nos enfrenta con tres aspectos fundamentales: libertad, seguridad y privacidad, temas que se analizaron en este panel, a la luz del estado actual de esta técnica biométrica.

Moderó Wojciech Wiewiorowski, Autoridad de Protección de Datos de Polonia y fueron expositores Lillie Coney, Associate Director EPIC (EEUU), Gus Hosein, Privacy International (Inglaterra), Sigrid Arzt, Comisionada del Instituto Federal de Acceso a la Información y Protección de Datos- IFAI (México), Ruben Amato, Director de la Dirección Nacional de Identificación Civil (Uruguay).

Panel I - ¡Smart Data! ¡Tus datos piensan!

Sistemas inteligentes que combinan sensores y objetos en red con sofisticado análisis de datos. Colectan y divulgan información de diversa índole con prescindencia de la intervención humana, según consignas predeterminadas. Esta tecnología ya se encuentra entre nosotros.

Conocer en profundidad su funcionamiento y aplicaciones, discutir la necesidad, o no, de entregar nuestros datos a una inteligencia artificial, y entender las consecuencias jurídicas de esa conducta, son algunos de los retos que se abordaron en este panel.

Moderó James Dempsey, Centre for Democracy and Technology (EEUU) y fueron expositores Steffano Nolfi, Instituto de Ciencias Cognitivas. Consejo Nacional de Investigación (Italia), Ken Anderson, Asistente del Comisionado de Privacidad de Ontario (Canadá), Rainer Knyrim, Socio Preslmayr Attorney at Law Viena (Austria), y Noah Lang, Vicepresidente de Reputation.Org (EEUU).

Panel J – Consentimiento informado ¿Regla o excepción?

El consentimiento del titular es un tema clave en el sistema jurídico aplicado a la protección de datos personales. ¿Qué requisitos deben cumplirse para que sea lícito? ¿En qué situaciones no es necesario recabarlo?

Estos y otros aspectos han dado lugar a diferentes enfoques y opiniones. La transparencia es una condición para la disposición de las facultades de control y legitimidad de un auténtico consentimiento. Por ende, el deber de información es un corolario ineludible. No obstante, surge como tema de discusión si será éste un requisito que deba cumplirse en todos los casos.

Las leyes de protección de datos y el reciente dictamen sobre la definición del consentimiento adoptado por el Grupo de Protección de Datos del Artículo 29 darán paso a la reflexión y brindarán oportunidad de compartir lecciones aprendidas.

Moderó María Verónica Pérez Asinari, Oficina del Supervisor Europeo de Protección de Datos (Argentina) y fueron expositores Pablo Palazzi, Universidad de San Andrés (Argentina), Willem Debeuckelaere, Presidente de la Autoridad belga de Protección de Datos de Bélgica, Erin Egan, Directora de privacidad de Facebook (EEUU), Eduardo Ustarán, Socio de Field Fisher Waterhouse (Inglaterra).

Panel K – Derechos Fundamentales

La protección de los datos personales entendido como "derecho fundamental autónomo" ha pasado a ser un pilar indiscutido en toda sociedad justa y democrática. El esfuerzo por trazar puentes de adaptación entre las TIC y este derecho, continúa provocando la reflexión de los expertos.

En simultáneo con ello se observa la necesidad de armonizar el conjunto de derechos y libertades fundamentales actuantes en la Sociedad de la Información. En un mundo donde el uso de la network se expande sin cesar, la transparencia de los asuntos públicos, la libertad de expresión y el derecho al olvido, integran un conjunto de temas siempre factibles de atención especializada.

Moderó Marcelo Bauzá, Miembro del Instituto de Derecho Informático de la Universidad de la República y AGESIC (Uruguay) y fueron expositores Ahti Saarenpaa, Profesor de Derecho e Informática. Universidad de Laponia (Finlandia), Giuseppe Busia, Autoridad de Protección de Datos de Italia, Deborah Hurley, Asesora independiente en políticas de Información y comunicación (EEUU), Jörg Polakiewicz, Jefe de Política de DDHH y Departamento de Desarrollo del Consejo De Europa (Francia).

Panel L - Piratería y privacidad: desafíos cruzados

La Stop Online Piracy Act es una legislación pensada para detener la piratería en línea. Frente a la sospecha de utilización sin autorización de material sujeto a derechos de autor, esta norma habilita a la justicia a revisar, perseguir y desconectar a cualquier sospechoso. Así, se podrá inhabilitar el acceso a un dominio, retirar publicidad, bloquear los pagos online, congelar fondos y eliminar enlaces.

Su esquema de funcionamiento, amenaza derechos fundamentales tales como la protección de datos y la libertad de expresión. La protección de datos, en tanto vigilancia ejercida sobre la Web en búsqueda de material no autorizado, se traducirá necesariamente en espionaje a los usuarios. La libertad de expresión también es un aspecto clave, en la medida en que los sitios deberán aplicar mecanismos de auto-censura, tendientes a filtrar la actividad de sus usuarios para no verse sancionados. Esta situación, además, vacía por completo de contenido las disposiciones de la Digital Millenium Copyright Act al respecto.

Este panel tuvo objetivos la discusión y búsqueda de lineamientos que debería contener una posible regulación consensuada en la materia.

Moderó Christopher Docksey, Office of the European Data Protection Supervisor (Bélgica) y fueron expositores Markham Ericson, Representante de la Net Coalition (EEUU), Bogdan Manolea, Vicepresidente European Digital Rights (Bélgica), Renato Jijena Leiva, Profesor de Derecho Informático. Universidad Católica de Valparaiso (Chile), Bruno Magrani, Investigador y Profesor Asociado de la Fundación Getulio Vargas (Brasil).

Panel M - Explorando caminos: Investigaciones y proyectos

La privacidad, lejos de agotarse, encuentra recurrentemente nuevos lineamientos y propuestas que permiten su afianzamiento y expansión.

En este espacio se recogieron algunas iniciativas que se encuentran en desarrollo en la actualidad. Se trata de investigaciones y proyectos que por su carácter novedoso resultan de utilidad conocer, socializando su posible aplicación por diferentes actores. La Conferencia recibió con beneplácito la presentación de estas propuestas que nos permiten seguir avanzando en el desarrollo de la privacidad.

Fueron expositores Sophie Kwasny, Jefa de la Unidad de Protección de Datos del Consejo de Europa (Francia), David Wright, Gerente de Three Lateral Research and Consulting (Reino Unido), Artemi Rallo, Investigador (España), Iván Salgado Lomas, Asesor de la Dirección General de Registro de Datos Públicos (Ecuador).

11

Anexo normativo

11. Anexo normativo

Ley Nº 18.996 de Rendición de Cuentas 2011, de 21 de noviembre de 2012, artículo 43

Artículo 43.- Incorpórase al texto de la Ley N° 18.331, de 11 de agosto de 2008, el siguiente artículo:

"ARTÍCULO 9º bis.- A los efectos de lo dispuesto por el literal I) del artículo 4º, por el literal A) del inciso tercero del artículo 9º y por los artículos 11, 21 y 22 de la presente ley, se consideran como públicas o accesibles al público, las siguientes fuentes o documentos:

El Diario Oficial y las publicaciones oficiales, cualquiera sea su soporte de registro o canal de comunicación.

Las publicaciones en medios masivos de comunicación, entendiendo por tales los provenientes de la prensa, cualquiera sea el soporte en el que figuren o el canal a través del cual se practique la comunicación.

Las guías, anuarios, directorios y similares en los que figuren nombres y domicilios, u otros datos personales que hayan sido incluidos con el consentimiento del titular.

Todo otro registro o publicación en el que prevalezca el interés general en cuanto a que los datos personales en ellos contenidos puedan ser consultados, difundidos o utilizados por parte de terceros. En caso contrario, se podrá hacer uso del registro o publicación mediante técnicas de disociación u ocultamiento de los datos personales.

La Unidad Reguladora y de Control de Datos Personales, de oficio o a solicitud de cualquier interesado, se expedirá sobre el derecho a la protección de datos personales, en situaciones relacionadas con los apartados precedentes literales A) y B) del inciso primero del artículo 34 de la presente ley"

Ley Nº 19.030 de 27 de diciembre de 2012

PODER EJECUTIVO

MINISTERIO DE RELACIONES EXTERIORES

Ley 19.030

Apruébanse el Convenio N° 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y el Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos.

PODER LEGISLATIVO

El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General,

DECRETAN

Artículo Único: Apruébanse el Convenio N° 108 del Consejo de Europa para la protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal de 28 de enero de 1981 adoptado en Estrasburgo y el Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos adoptado en Estrasburgo, el 8 de noviembre de 2001.

Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal

Estrasburgo, 28.I.1981

Texto

Los Estados miembros del Consejo de Europa, signatarios del presente Convenio,

Considerando que el fin del Consejo de Europa es llevar a cabo una unión más íntima entre sus miembros, basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales;

Considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados;

Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras;

Reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos;

Convienen en lo siguiente:

Capítulo I - Disposiciones generales

Artículo 1. Objeto y fin

El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»).

Artículo 2. Definiciones

A los efectos del presente Convenio:

a. datos «de carácter personal» significa cualquier información relativa a una persona física identificada o identificable («persona concernida»);

b. fichero « automatizado» significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado;

c. por «tratamiento automatizado» se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión;

d. autoridad «controladora del fichero» significa la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán.

Artículo 3. Campos de aplicación

1. Partes se comprometen a aplicar el presente Convenio a los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores público y privado.

2. Cualquier Estado podrá en el momento de la firma o al depositar su instrumento de ratificación, aceptación, aprobación o adhesión, o en cualquier otro momento ulterior- hacer saber mediante declaración dirigida al Secretario general del Consejo de Europa:

a. Que no aplicará el presente Convenio a determinadas categorías de ficheros automáticos de datos de carácter personal, una lista de la cuales quedará depositada. No deberá sin embargo incluir en esa lista categorías de ficheros automatizados sometidas, con arreglo a su derecho interno, a disposiciones de protección de datos. Deberá, por tanto, modificar dicha lista mediante una nueva declaración cuando estén sometidas a su régimen de protección de datos categorías suplementarias de ficheros automatizados de datos de carácter personal;

b. que aplicará el presente Convenio, asimismo, a informaciones relativas a agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo compuesto directa o indirectamente de personas físicas, tengan o no personalidad jurídica;

c. que aplicará el presente Convenio, asimismo, a los ficheros de datos de carácter personal que no sean objeto de tratamientos automatizados.

3. Cualquier Estado que haya ampliado el campo de aplicación del presente Convenio mediante una de las declaraciones a que se refieren los apartados 2, b) o c), que anteceden podrá, en dicha declaración, indicar que las ampliaciones solamente se aplicarán a determinadas categorías de ficheros de carácter personal cuya lista quedará depositada.

4. Cualquier parte que haya excluido determinadas categorías de ficheros automatizados de datos de carácter personal mediante la declaración prevista en el apartado 2, a), anterior no podrá pretender que una Parte que no las haya excluido aplique el presente Convenio a dichas categorías.

5. Igualmente, una Parte que no haya procedido a una u otra de las ampliaciones previstas en los párrafos 2, b) y c), del presente artículo no podrá pretender que se aplique el presente Convenio en esos puntos con respecto a una parte que haya procedido a dichas aplicaciones.

6. Las declaraciones previstas en el párrafo 2 del presente artículo tendrán efecto en el momento de la entrada en vigor del Convenio con respecto al Estado que las haya formulado, si dicho Estado las ha hecho en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, o tres meses después de su recepción por el Secretario general del Consejo de Europa si se han formulado en un momento ulterior. Dichas declaraciones podrán retirarse en su totalidad o en parte mediante notificación dirigida al Secretario general del Consejo de Europa. La retirada tendrá efecto tres meses después de la fecha de recepción de dicha notificación.

Capítulo II - Principios básicos para la protección de datos

Artículo 4. Compromisos de las Partes

1. Cada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.

2. Dichas medidas deberán adoptarse a más tardar en el momento de la entrada en vigor del presente Convenio con respecto a dicha Parte.

Artículo 5. Calidad de los datos

Los datos de carácter personal que sean objeto de un tratamiento automatizado:

a. Se obtendrán y tratarán leal y legítimamente;

b. se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;

c. serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;

d. serán exactos y si fuera necesario puestos al día;

e. se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Artículo 6. Categorías particulares de datos

Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales.

Artículo 7. Seguridad de los datos

Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Artículo 8. Garantías complementarias para la persona concernida

Cualquier persona deberá poder:

a. conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;

b. obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;

c. obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;

d. disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo.

Artículo 9. Excepción y restricciones

1. No se admitirá excepción alguna en las disposiciones de los artículo 5, 6 y 8 del presente Convenio, salvo que sea dentro de los límites que se definen en el presente artículo.

2. Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:

a. Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales;

b. Para la protección de la persona concernida y de los derechos y libertades de otras personas.

3. Podrán preverse por la ley restricciones en el ejercicio de los derechos a que se refieren los párrafos b), c) y d) del artículo 8 para los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas.

Artículo 10. Sanciones y recursos

Cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.

Artículo 11. Protección más amplia

Ninguna de las disposiciones del presente capítulo se interpretará en el sentido de que limite la facultad, o afecte de alguna otra forma a la facultad de cada Parte, de conceder a las personas concernidas una protección más amplia que la prevista en el presente Convenio.

Capítulo III - Flujos transfronterizos de datos

Artículo 12. Flujos transfronterizos de datos de carácter personal y el derecho interno

1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento.

2. Una Parte no podrá, con el fin de proteger la vida privada prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte.

3. Sin embargo, cualquier Parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2:

a. En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente;

b. cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo.

Capítulo IV - Ayuda mutua

Artículo 13. Cooperación entre las Partes

1. Las Partes se obligan a concederse mutuamente asistencia para el cumplimiento del presente Convenio.

2. A tal fin,

a. cada Parte designará a una o más autoridades cuya denominación y dirección comunicará al Secretario general del Consejo de Europa;

b. cada Parte que haya designado a varias autoridades indicará en la comunicación a que se refiere el apartado anterior la competencia de cada una de dichas autoridades.

3. Una autoridad designada por una Parte, a petición de una autoridad designada por otra Parte:

a. Facilitará informaciones acerca de su derecho y su práctica administrativa en materia de protección de datos;

b. tomará toda clase de medidas apropiadas, con arreglo a su derecho interno y solamente a los efectos de la protección de la vida privada, para facilitar informaciones fácticas relativas a un tratamiento automatizado determinado efectuado en su territorio con excepción, sin embargo, de los datos de carácter personal que sean objeto de dicho tratamiento.

Artículo 14. Asistencia a las personas concernidas que tengan su residencia en el extranjero

1. Cada Parte prestará asistencia a cualquier persona que tenga su residencia en el extranjero para el ejercicio de los derechos previstos por su derecho interno que haga efectivos los principios enunciados en el artículo 8 del presente Convenio.

2. Si dicha persona residiese en el territorio de otra Parte, deberá tener la facultad de presentar su demanda por intermedio de la autoridad designada por esa Parte.

3. La petición de asistencia deberá hacer constar todos los datos necesarios relativos concretamente a:

a. El nombre, la dirección y cualesquiera otros elementos pertinentes de identificación relativos al requirente;

b. el fichero automatizado de datos de carácter personal al que se refiere la demanda o la autoridad controladora de dicho fichero;

c. el objeto de la petición.

Artículo 15. Garantías relativas a la asistencia facilitada por las autoridades designadas

1. Una autoridad designada por una Parte que haya recibido información de una autoridad designada por otra Parte, bien en apoyo de una petición de asistencia bien como respuesta a una petición de asistencia que haya formulado ella misma, no podrá hacer uso de dicha información para otros fines que no sean los especificados en la petición de asistencia.

2. Cada parte cuidará de que las personas pertenecientes a la autoridad designada o que actúen en nombre de la misma estén vinculadas por obligaciones convenientes de secreto o de confidencialidad con respecto a dicha información.

3. En ningún caso estará autorizada una autoridad designada para presentar, con arreglo a los términos del artículo 14, párrafo 2, una petición de asistencia en nombre de una persona concernida residente en el extranjero, por su propia iniciativa y sin el consentimiento expreso de dicha persona.

Artículo 16. Denegación de peticiones de asistencia

Una autoridad designada, a quien se haya dirigido una petición de asistencia con arreglo a los términos de los artículos 13 ó 14 del presente Convenio, solamente podrá negarse a atenderla si:

a. La petición es incompatible con las competencias, en materia de protección de datos, de las autoridades habilitadas para responder;

b. la petición no está conforme con lo dispuesto en el presente Convenio;

c. atender a la petición fuese incompatible con la soberanía, la seguridad o el orden público de la Parte que la haya designado, o con los derechos y libertades fundamentales de las personas que estén bajo la jurisdicción de dicha Parte.

Artículo 17. Gastos y procedimientos de asistencia

1. La ayuda mutua que las Partes se concedan con arreglo a los términos del artículo 13, así como la asistencia que ellas presten a las personas concernidas residentes en el extranjero con arreglo a los términos del artículo 14, no dará lugar al pago de gastos y derechos que no sean los correspondientes a los expertos y a los intérpretes. Dichos gastos y derechos correrán a cargo de la Parte que haya designado a la autoridad que haya presentado la petición de asistencia.

2. La persona concernida no podrá estar obligada a pagar, en relación con las gestiones emprendidas por su cuenta en el territorio de otra Parte, los gastos y derechos que no sean los exigibles a las personas que residan en el territorio de dicha Parte.

3. Las demás modalidades relativas a la asistencia referentes, concretamente a las formas y procedimientos así como a las lenguas que se utilicen se establecerán directamente entre las Partes concernidas.

Capitulo V - Comité consultivo

Artículo 18. Composición del Comité

1. Después de la entrada en vigor del presente Convenio se constituirá un Comité Consultivo.

2. Cada Parte designará a un representante y a un suplente en dicho Comité. Cualquier Estado miembro del Consejo de Europa que no sea Parte del Convenio tendrá el derecho de hacerse representar en el Comité por un observador.

3. El Comité Consultivo podrá, mediante una decisión tomada por unanimidad, invitar a cualquier Estado no miembro del Consejo de Europa, que no sea Parte del Convenio, a hacerse representar por un observador en una de las reuniones.

Artículo 19. Funciones del Comité

El Comité Consultivo:

a. Podrá presentar propuestas con el fin de facilitar o de mejorar la aplicación del Convenio;

b. podrá presentar propuestas de enmienda del presente Convenio, con arreglo al artículo 21;

c. formulará su opinión acerca de cualquier propuesta de enmienda al presente Convenio que se le someta, con arreglo al artículo 21, párrafo 3;

d. podrá, a petición de una Parte, expresar su opinión acerca de cualquier cuestión relativa a la aplicación del presente Convenio.

Artículo 20. Procedimiento

1. El Secretario general del Consejo de Europa convocará al Comité Consultivo. Celebrará su primera reunión en los doce meses que sigan a la entrada en vigor del presente Convenio. Posteriormente se reunirá al menos una vez cada dos años y, en todo caso, cada vez que un tercio de los representantes de las Partes solicite su convocatoria.

2. La mayoría de los representantes de las Partes constituirá el quórum necesario para celebrar una reunión del Comité Consultivo.

3. Después de cada una de dichas reuniones, el Comité Consultivo someterá al Comité de Ministros del Consejo de Europa una memoria acerca de sus trabajos y el funcionamiento del Convenio.

4. Sin perjuicio de lo dispuesto en el presente Convenio, el Comité Consultivo fijará su reglamento anterior.

Capítulo VI - Enmiendas

Artículo 21. Enmiendas

1. Podrán proponerse enmiendas al presente Convenio por una Parte, por el Comité de Ministros del Consejo de Europa o por el Comité Consultivo.

2. Cualquier propuesta de enmienda se comunicará por el Secretario general del Consejo de Europa a los Estados miembros del Consejo de Europa y a cada Estado no miembro que se haya adherido o se le haya invitado a que se adhiera al presente Convenio, con arreglo a lo dispuesto en el artículo 23.

3. Además, cualquier modificación propuesta por una Parte o por el Comité de Ministros se comunicará al Comité Consultivo, el cual presentará al Comité de Ministros su opinión acerca de la enmienda propuesta.

4. El Comité de Ministros examinará la enmienda propuesta y cualquier opinión presentada por el Comité Consultivo y podrá aprobar la enmienda.

5. El texto de cualquier enmienda aprobada por el Comité de Ministros conforme al párrafo 4 del presente artículo se remitirá a las Partes para su aceptación.

6. Cualquier enmienda aprobada con arreglo al párrafo 4 del presente artículo entrará en vigor el trigésimo día después de que todas las Partes hayan informado al Secretario general de que la han aceptado.

Capítulo VII - Cláusulas finales

Artículo 22. Entrada en vigor

1. El presente Convenio quedará abierto a la firma de los Estados miembros del Consejo de Europa. Se someterá a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario general del Consejo de Europa.

2. El presente Convenio entrará en vigor el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha en que cinco Estados miembros del Consejo de Europa hayan expresado su consentimiento para quedar vinculados por el Convenio, con arreglo a las disposiciones del párrafo anterior.

3. Para cualquier Estado miembro que expresare ulteriormente su consentimiento para quedar vinculado por el Convenio, éste entrará en vigor el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha del depósito del instrumento de ratificación, aceptación o aprobación.

Artículo 23. Adhesión de Estados no miembros

1. Después de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa podrá invitar a cualquier Estado no miembro del Consejo de Europa a que se adhiera al presente Convenio mediante un acuerdo adoptado por la mayoría prevista en el artículo 20, d), del Estatuto del Consejo de Europa y por unanimidad de los representantes de los Estados contratantes que tengan el derecho a formar parte del Comité.

2. Para cualquier Estado adherido, el Convenio entrará en vigor el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha del depósito del instrumento de adhesión en poder del Secretario general del Consejo de Europa.

Artículo 24. Cláusula territorial

1. Cualquier Estado podrá designar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el territorio o los territorios a los cuales se aplicará el presente Convenio.

2. Cualquier Estado en cualquier otro momento posterior, y mediante una declaración dirigida al Secretario general del Consejo de Europa, podrá ampliar la aplicación del presente Convenio a cualquier otro territorio designado en la declaración. El Convenio entrará en vigor, con respecto a dicho territorio, el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha de recepción de la declaración por el Secretario general.

3. Cualquier declaración hecha en virtud de los dos párrafos anteriores podrá retirarse, en lo que respecta a cualquier territorio designado en dicha declaración, mediante notificación dirigida al Secretario general. La retirada será efectiva el día primero del mes siguiente a la expiración de un período de seis meses después de la fecha de recepción de la notificación por el Secretario general.

Artículo 25. Reservas

No podrá formularse reserva alguna con respecto a las disposiciones del presente Convenio.

Artículo 26. Denuncia

1. Cualquier parte podrá en cualquier momento denunciar el presente Convenio dirigiendo una notificación al Secretario general del Consejo de Europa.

2. La denuncia será efectiva el día primero del mes siguiente a la expiración de un período de seis meses después de la fecha de recepción de la notificación por el Secretario general.

Artículo 27. Notificaciones

El Secretario general del Consejo de Europa notificará a los Estados miembros del Consejo y a cualquier Estado que se haya adherido al presente Convenio:

a. Cualquier firma;

b. el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;

c. cualquier fecha de entrada en vigor del presente Convenio, conforme a sus artículos 22, 23 y 24;

d. cualquier otro acto, notificación o comunicación relativo al presente Convenio.

En fe de lo cual los infrascritos, debidamente autorizados al efecto, afirman el presente Convenio.

Hecho en Estrasburgo el 28 de enero de 1981 en francés y en inglés, los dos textos igualmente fehacientes, en un ejemplar único que quedará depositado en los archivos del Consejo de Europa. El secretario general del Consejo de Europa remitirá copia certificada conforme del mismo a cada uno de los Estados miembros del Consejo de Europa y a cualquier Estado invitado a la adhesión al presente Convenio.

Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos

Estrasburgo, 8/XI.2001

Preámbulo

Las Partes en el presente Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, abierto a la firma en Estrasburgo, el 28 de enero de 1981 (en lo sucesivo denominado «el Convenio»);

Convencidas de que las autoridades de control que ejercen sus funciones con total independencia son un elemento de la protección efectiva de las personas con respecto al tratamiento de datos de carácter personal;

Considerando la importancia del flujo de información entre los pueblos;

Considerando que, con la intensificación de los intercambios de datos de carácter personal a través de las fronteras nacionales, es necesario garantizar la protección efectiva de los derechos humanos y de las libertades fundamentales y, en particular, del derecho al respeto de la vida privada, en relación con tales intercambios, han convenido en lo siguiente:

Artículo 1. Autoridades de control

1. Cada Parte dispondrá que una o más autoridades sean responsables de garantizar el cumplimiento de las medidas previstas por su derecho interno que hacen efectivos los principios enunciados en los Capítulos II y III del Convenio, así como en el presente Protocolo.

2. a este efecto, las autoridades mencionadas dispondrán, en particular, de competencias para la investigación y la intervención, así como de la competencia para implicarse en las actuaciones judiciales o para llamar la atención de las autoridades judiciales competentes respecto de las violaciones de las disposiciones del derecho interno que dan efecto a los principios mencionados en el apartado 1 del artículo 1 del presente Protocolo.

b. Cada autoridad de control atenderá las reclamaciones formuladas por cualquier persona en relación con la protección de sus derechos y libertades fundamentales respecto de los tratamientos de datos de carácter personal dentro de su competencia.

3. Las autoridades de control ejercerán sus funciones con total independencia.

4. Las decisiones de las autoridades de control que den lugar a reclamaciones podrán ser objeto de recurso ante los tribunales.

5. De conformidad con lo dispuesto en el Capítulo IV, y sin perjuicio de lo dispuesto en el artículo 13 del Convenio, las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus obligaciones, en particular mediante el intercambio de toda la información útil.

Artículo 2. Flujos transfronterizos de datos de carácter personal hacia un destinatario que no está sujeto a la jurisdicción de una Parte en el Convenio.

1. Cada Parte dispondrá que la transferencia de datos de carácter personal hacia un destinatario sometido a la jurisdicción de un Estado u organización que no sea Parte en el Convenio sólo podrá efectuarse si dicho Estado u organización garantiza un nivel de protección adecuado a la transferencia de datos prevista.

2. No obstante lo dispuesto en el apartado 1 del artículo 2 del presente Protocolo, cada Parte podrá permitir la transferencia de datos de carácter personal:

a. si está prevista en su legislación interna a causa de:

- intereses específicos de la persona interesada, o de
- intereses legítimos prevalecientes, en particular, intereses públicos importantes, o

b. si la persona responsable de la transferencia ofrece garantías, que, en particular, pueden resultar de cláusulas contractuales, y éstas son juzgadas suficientes por la autoridad competente de conformidad con el derecho interno.

Artículo 3. Disposiciones finales

1. Las disposiciones del artículo 1 y 2 del presente Protocolo serán consideradas por las Partes artículos adicionales al Convenio y todas las disposiciones del Convenio se aplicarán en consecuencia.

2. El presente Protocolo estará abierto a la firma de los Estados signatarios del Convenio. Después de adherirse al Convenio en las condiciones previstas en el mismo, las Comunidades Europeas podrán firmar el presente Protocolo. El presente Protocolo está sujeto a ratificación, aceptación o aprobación. Cualquier signatario del presente Protocolo no podrá ratificar, aceptar o aprobar el mismo a menos que haya ratificado, aceptado o aprobado, con anterioridad o simultáneamente, el Convenio o se haya adherido al mismo. Los instrumentos de ratificación, aceptación o aprobación del presente Protocolo se depositarán en poder del Secretario General del Consejo de Europa.

3. a) El presente Protocolo entrará en vigor el primer día del mes siguiente a la expiración de un período de tres meses después de la fecha en que cinco de sus signatarios hayan expresado su consentimiento para quedar vinculados por el Protocolo, de conformidad con lo dispuesto en el apartado 2 del artículo 3.

b) Respecto de cualquier Estado Signatario del presente Protocolo que posteriormente expresen su consentimiento para quedar vinculado por el mismo, el Protocolo entrará en vigor el primer día del mes siguiente a la expiración de un período de tres meses después de la fecha de depósito del instrumento de ratificación, aceptación o aprobación.

4. a) Después de la entrada en vigor del presente Protocolo, cualquier Estado que se haya adherido al Convenio podrá adherirse asimismo al Protocolo.

b) La adhesión se hará efectiva mediante el depósito en poder del Secretario General del Consejo de Europa de un instrumento de adhesión, que entrará en vigor el primer día del mes siguiente a la expiración de un período de tres meses después de la fecha de su depósito.

5. a) Cualquier Parte podrá en cualquier momento denunciar el presente Protocolo mediante notificación dirigida al Secretario General del Consejo de Europa.

b) Dicha denuncia entrará en vigor el primer día del mes siguiente a la expiración de un período de tres meses después de la fecha de recepción del dicha notificación por el Secretario General.

6. El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a las Comunidades Europeas y a cualquier otro Estado que se haya adherido al presente Protocolo:

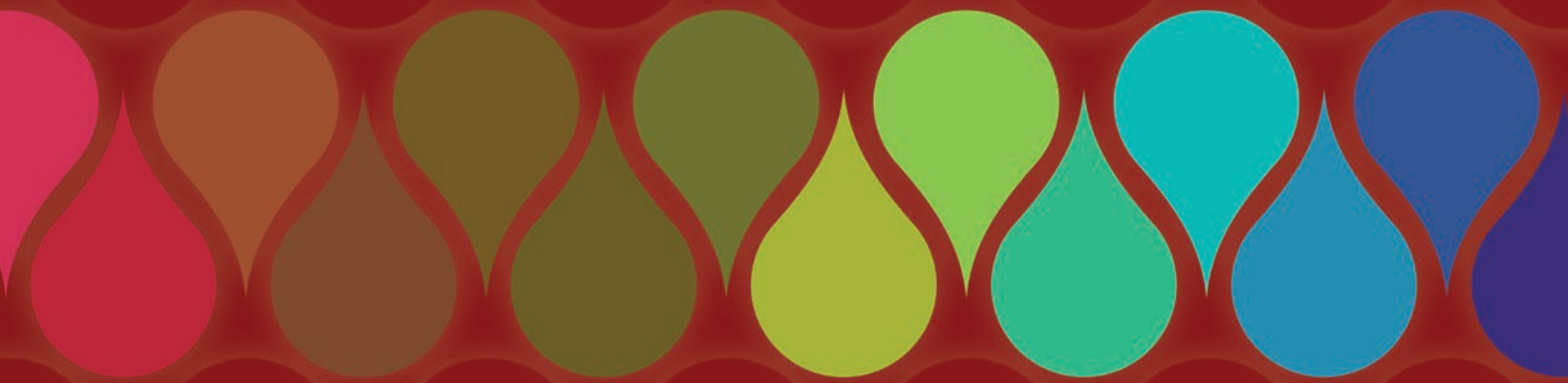
a. cualquier firma;

b. el depósito de cualquier instrumento de ratificación, aceptación o aprobación;

c. cualquier fecha de entrada en vigor del presente Protocolo de conformidad con el artículo 3;

d. cualquier otra acción, notificación o comunicación relativa al presente Protocolo.

En fe de lo cual, los abajo firmantes, debidamente autorizados para ello, firman el presente Protocolo. Hecho en Estrasburgo, el 8 de noviembre de 2001, en francés e inglés, siendo ambos textos igualmente auténticos, en un único ejemplar, que se depositará en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copias certificadas a cada Estado miembro del Consejo de Europa, a las Comunidades Europeas y a cualquier Estado invitado a adherirse al Convenio.



UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

Andes 1365 Piso 8 | Montevideo, Uruguay
(+598) 2901 2929 int. 1352
info@datospersonales.gub.uy
www.datospersonales.gub.uy