Memoria anual **2011**

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

Prólogo

A nuestro juicio, la elaboración de una memoria anual necesariamente conlleva la realización de un balance, no alcanza con plasmar en un documento el mero racconto de lo actuado durante el año cerrado, sino que es preciso evaluar, ponderar y contextualizar la actividad realizada.

El año 2011 fue de una actividad intensa, como se muestra documentadamente, pero asimismo profunda y trascendente por la naturaleza de los asuntos abordados por la URCDP.

Es posible afirmar que el año cerrado ha sido el de la consolidación de la URCDP. Una unidad joven, con tres años de constituida, que paulatinamente se ha incorporado al entramado institucional y social de nuestro país, a través de su respectivo reconocimiento.

Como testimonio de ello, la cantidad y variedad de consultas y denuncias formuladas por personas físicas y jurídicas ante la URCDP se incrementó sensiblemente en este período.

Del mismo modo, la interacción de la URCDP con otros organismos públicos ha dado origen a las más diversas resoluciones y dictámenes, así como su participación en varias modificaciones al orden jurídico a fin de asegurar debidamente el derecho a la protección de datos personales en diversas normas.

Asimismo, la naturaleza global de las redes de comunicación de información hace que el relacionamiento internacional sea un elemento imprescindible para materializar los principios que orientan la normativa vigente. Atento a ello, la URCDP ha continuado profundizando sus vínculos con autoridades de protección de datos de terceros países, cuerpos supranacionales y asociaciones internacionales vinculadas a la privacidad y a la protección de datos personales.

Todo ello con el fin último de que la tecnología y la privacidad no sean consideradas como polos opuestos, sino complementarios, de cuya síntesis en armonía, surja una mejor calidad de vida para nuestra sociedad.

Mag. Federico Monteverde

Índice

Prólogo – Presidente de la URCDP

1. El derecho humano a la protección de datos personales 5

2. Principales temas analizados en el 2011 10

a. Actuación inspectiva de la URCDP y manejo de información amparada por el secreto profesional, en el marco de inspecciones que se realicen.

b. Acuerdo de Cooperación Técnica entre la República Federativa del Brasil y nuestro país.

c. Administración Tributaria y Protección de Datos.

d. Comunicación de datos.

e. Postulación de Uruguay como Sede de la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad Protección de Datos.

f. Publicación de datos personales en la web.

g. Sanciones Administrativas – Adecuación en virtud de modificaciones introducidas a la Ley Nº 18.331, por la Ley Nº 18.719.

h. Transferencias internacionales.

i. Tratamiento de datos.

j. Videovigilancia – Circuitos cerrados de televisión (CCTV).

3. Avances en la normativa de protección de datos 15

a. Iniciativa para la Ratificación del Convenio N° 108 del Consejo de Europa.

b. Iniciativas nacionales relacionadas con la protección de datos personales:

i. Ley Nº 18.812, de 12 de octubre de 2011, por la que se regulan los datos personales incluidos en la Central de Riesgos Crediticios del Banco Central del Uruguay.

ii. Ley Nº 18.849, de 22 de diciembre de 2011, por la que crea el Registro Nacional de Huellas Genéticas.

c. Iniciativas internacionales relacionadas con la protección de datos personales:

i. Perú.

ii. Costa Rica.

iii. Jurisprudencia Internacional.

4. Jurisprudencia nacional 21

a. Sentencia del Tribunal de Contencioso Administrativo Nº 160, de 3 de marzo de 2011.

b. Sentencia del Juzgado Letrado de Primera Instancia en lo Penal de 18º Turno Nº 408, de 11 de marzo de 2011.

c. Sentencia del Tribunal de lo Contencioso Administrativo Nº 340, de 26 de abril de 2011.

d. Sentencia del Tribunal de lo Contencioso Administrativo Nº 353,de 26 de abril de 2011.

5. Presentación de la Memoria 2010 24

6. Difusión y capacitación de la Unidad Reguladora y de Control de Datos Personales 26

a. Sitio web.

b. Publicaciones realizadas.

c. Atención de consultas personalizadas.

d. Eventos nacionales.

e. Jornadas de capacitación interna en AGESIC

f. Relacionamiento internacional:

i. Seminario sobre "Acceso a la Información Pública y Protección de Datos". Antigua, Guatemala.

ii. Seminario "El impacto de las transferencias internacionales de datos en América Latina. Las políticas preventivas y la autorregulación en la implantación de la normativa de protección de datos". Cartagena de Indias, Colombia.

iii. 33º Conferencia Internacional de Protección de Datos y Autoridades de Protección de Datos y Privacidad. México D.F., México.

7. La URCDP en cifras. 31

a. Registro de Bases de Datos presentadas en 2011

b. Distribución territorial

c. Datos sensibles

d. Transferencias internacionales

e. Tipos de información

f. Cesiones o comunicaciones de datos

g. Tipo de soporte de registro de base de datos

h. Bases de datos inscriptas

i. Cantidad de visitas al sitio web

j. Consultas a la mesa de ayuda

k. Expedientes presentados por consultas y denuncias

l. Resoluciones sancionadas con apercibimiento o multas

m. Resoluciones y dictámenes realizados

n. Cantidad de informes realizados

8. La URCDP ante los nuevos retos en materia de protección de datos. 38

a. Proyectos a realizar en el 2012

b. Proyectos a largo plazo

9. Anexo normativo 40

a. Ley N° 18.812, 23 de setiembre de 2011.

b. Ley N° 18.849, de 2 de diciembre de 2011.

1.

El derecho fundamental a la protección de los datos personales

Desde el último tercio del siglo pasado se verifica un fenómeno singular en la sociedad: la preocupación por el encuentro de las Tecnologías de la Información y la Comunicación (TIC) con la información nominativa, hecho que comenzó a regularse primeramente en los países desarrollados (EEUU y Europa) para extenderse en forma reciente a otras regiones, entre ellas Latinoamérica.

Sin descartar los tratamientos de tipo tradicional o manual, no caben dudas que es el entorno tecnológico contemporáneo el que despierta y empuja hacia la construcción de este nuevo espacio jurídico. Se trata de un verdadero derecho subjetivo, que se ha ido delineando y llenando de contenido como disciplina jurídica alrededor de la protección de las personas. Tal derecho tiene por objeto enfrentar al uso irrefrenable de los datos personales, por parte de los distintos agentes sociales y económicos, públicos y privados, que utilizan este tipo de datos para sus cometidos.

Los tratamientos de las bases de datos personales que realizan terceras personas (afectando con ello a sus titulares) son, de esta manera, un asunto consustancial a la sociedad actual. El fenómeno es tan real que ha ido generando una toma de conciencia progresiva en cuanto a su necesario encuadre y regulación. Se trata de acogerlo, no de prohibirlo ni eliminarlo. Y es que cada "huella electrónica" que vamos dejando en nuestro trajinar diario por oficinas y lugares donde demandan nuestras señas caracterizantes, puede ser sin duda admisible y justificada, pero en muchos casos también inmotivada e innecesaria o no querida, o racionalmente limitable, convirtiéndose de este modo, aunque no lo queramos ni sepamos, en un elemento de rastreo y seguimiento de nuestras futuras acciones en la sociedad. La sociedad actual se caracteriza, entre otros rasgos, por el uso intenso de programas informáticos, técnicas de gestión y comunicación, etc., que permiten almacenar la información, conservarla, y someterla a una multiplicidad de reconversiones y utilidades (comerciales, tecnológicas, médicas, culturales, etc.), como nunca antes fue posible. La información que identifica a las personas, no escapa a este paradigma de la época.

¿Por qué hablar de "derechos fundamentales"? La respuesta adecuada a esta interrogante supone conocer, en principio, qué es un derecho fundamental, para luego explicar de qué manera se aplica esta categoría de análisis a las bases de datos personales, e incluso a los datos personales aislados, siempre que exista algún tratamiento externo que afecte en cierta medida a sus titulares.

Básicamente se trata de un derecho subjetivo, cualquiera sea, el que adquiere la nota de "fundamental" cuando resulta aplicable a los aspectos más trascendentes de la persona humana: su existencia, sus libertades, su dignidad personal. Por su importancia, este tipo de derechos se encuentra reconocido en los grandes tratados internacionales de DD.HH. y en las cartas constitucionales nacionales, además de merecer regulaciones legales y reglamentarias. Como categoría mayor de la ciencia y obrar jurídicos, se trata de un derecho que se nutre fuertemente de principios generales, que permean todo el régimen, y ayudan a un mejor conocimiento e interpretación de sus postulados.

De lo que se trata, en definitiva, es de preservar a todo individuo de las posibles vulneraciones de su intimidad, privacidad o cualquier otro valor a defender vinculado a su persona, con relación al tratamiento de sus datos personales.

En este sentido, el Derecho a la Protección de los Datos Personales es también un Derecho fundamental, del que se ha ido advirtiendo y aceptando su carácter autónomo paralelamente al avance de la tecnología y la globalización de las relaciones sociales. Por otra parte se trata de un Derecho que contribuye a la protección de otros derechos fundamentales, aunque posea por sí pleno valor y fuerza.

Así se lo tiene admitido por el más moderno y preclaro pensamiento jurídico, desde diferentes orígenes que, no obstante, muestran una tendencia prácticamente uniforme (tratados internacionales, leyes nacionales, jurisprudencia y doctrina), y que ha ido poniendo las piezas necesarias para consagrar este derecho tal cual se lo reconoce hoy día por un número siempre creciente de países y regiones.

Los grandes tratados internacionales de DD.HH., entre otros la Declaración Universal de 1948 (art. 12) y el Pacto de San José de Costa Rica de 1969 (art. 11), ya se habían abocado a la defensa de ciertos valores del individuo como su honra, dignidad y vida privada, proscribiendo "injerencias arbitrarias" perjudiciales a este tipo de derechos. Por razones cronológicas el fenómeno de la Sociedad de la Información que sobrevendría poco después, no estuvo presente expresamente en estos y otros textos jurídicos internacionales. Pero los mismos, dada su generalidad, igualmente resultan aplicables a la nueva esfera o clase de relacionamientos

propios del mundo más actual, los vínculos informáticos y telemáticos progresivamente impuestos y extendidos en la sociedad contemporánea. Los textos regionales europeos, más contemporáneos que los anteriormente citados, reconocen este derecho como autónomo e independiente de la privacidad, la honra y otros que integran la "familia" -junto al nombrado- de aquellos que encuentran su fundamento último en la dignidad del ser humano (art. 8° de la Carta de Derechos Fundamentales del año 2000).

Uno de los hitos de mayor prestigio en el camino de reconocimiento de este nuevo derecho, proviene de la célebre Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983 sobre la Ley del Censo de Población. En ella se expresa que la "autodeterminación informativa", también llamada "libertad informática", es una prerrogativa suficiente y distinguible de todo ser humano, quien tiene el derecho a conocer y controlar lo que hacen otros con sus propios datos. Lo más agudo de esta singular pieza jurídica consiste en advertir una visión social dentro del fenómeno examinado, lo que determina una necesaria trascendencia o superación de la fisonomía estrictamente individual de un derecho que, por fuerza natural, posee también otras dimensiones. Con justeza se señala en esta pieza jurisprudencial, que un individuo sometido a una constante vigilancia y expoliación de sus datos identificatorios, adoptará actitudes de autodefensa retrayéndose en su relacionamiento social perjudicando, con ello, al colectivo social al que pertenece, el que necesita de la participación saludable y efectiva de todos sus agentes.

Extrayendo alguno de los párrafos más sustantivos de esta sentencia, se aprecia que «la autodeterminación del individuo presupone –también en las condiciones de las técnicas modernas de tratamiento de la información– que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en su caso, a omitir, incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión adoptada... Esta libertad de decisión, de control, supone además que el individuo tenga la posibilidad de acceder a sus datos personales, que pueda, no sólo tener conocimiento de que otros procesan informaciones relativas a su persona, sino también someter el uso de éstas a un control, ya que, de lo contrario, se limitará su libertad de decidir por autodeterminación». ("El derecho fundamental a la protección de datos: perspectivas" Ricard Martínez Martínez, en http://www.uoc.edu/idp/5/dt/esp/martinez.pdf).

El Tribunal Constitucional español se ha pronunciado sobre este mismo derecho, perfilando claramente su carácter autónomo respecto de su más cercano pariente, el derecho de intimidad. En reconocido análisis que ha pasado a ser doctrina inspiradora para toda la región, el alto órgano judicial ha sostenido: «Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos, cuya concreta regulación debe establecer la ley, aquélla que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran». (Sentencia 292/2000).

Resulta importante ahora destacar las notas esenciales de este nuevo derecho, tal como ha venido a quedar configurado a partir de su peculiar proceso histórico evolutivo.

Como ya se adelantó, se trata de un derecho independiente de otros derechos subjetivos afines, como el respeto de la intimidad, la vida privada y familiar, rasgo que se advierte en los más modernos y actuales regímenes, donde la protección de datos personales ya no se encuentra solapada ni confundida con ningún otro, aunque pueda servirles de realización o garantía a muchos de ellos.

Este derecho es multifacético en sus proyecciones porque contiene una serie de principios generales, pero también sigue paso a paso los distintos momentos de "la vida en sociedad" del dato personal (captura o recolección, procesamiento, cesión o comunicación a terceros, etc.). Se ocupa de preceptuar deberes y obligaciones, regula especialmente los llamados "datos especialmente protegidos", e incluye varias vías de tutela (privada, administrativa, jurisdiccional) al servicio de todo el régimen Está institucionalizado desde el momento en que se advirtió que su cumplimiento no sería efectivo si quedase librado a la mera voluntad o espontaneidad; ni tampoco sería práctico el otro extremo de inundar los tribunales con su defensa en toda hipótesis y oportunidad, mejorando y facilitando la tutela con la presencia de instituciones administrativas especializadas e independientes, las llamadas Autoridades u Órganos de Control. Éstas coadyuvan a la vigencia de este derecho utilizando sus poderes de intervención en la materia, sin desmedro de la intervención judicial como garantía mayor y cuando existe mérito para ello.

Es en esencia libertario y solidario, en la medida que defiende el espacio humano siempre reivindicable, dentro de una sociedad contemporánea cada vez más compleja, que tiende a socavar los derechos del individuo como tal, y contribuye, en forma decisiva, al compromiso del portador de

los datos con sus pares en sociedad según lo advirtiera el sutil enfoque de la sentencia alemana antes comentada.

Por tanto se trata de uno de esos derechos que anida y se despliega en favor de la propia esencia del ser humano, resultando anterior e independiente de toda previsión explícita que pudiera hacerse en el ordenamiento jurídico positivo. Esto no es más que traer a colación la doctrina jus-naturalista, recogida por nuestro constituyente a través del art. 72 de la Magna Carta nacional.

Respecto de esta doctrina en particular, el Profesor Alberto Ramón Real fue primero en señalar la importancia y analizar en profundidad esta precoz y original virtud del régimen constitucional uruguayo, expresando que "nuestra Constitución incorpora, genéricamente, al ordenamiento jurídico positivo, la esencia ideológica del jusnaturalismo clásico, es decir, la idea de derechos, deberes y garantías que derivan de la personalidad humana y de la forma republicana de gobierno y, por ende, positiviza las soluciones generalmente admitidas de la doctrina jusnaturalista" ("Los principios generales de Derecho en la Constitución Uruguaya. Vigencia de la estimativa jusnaturalista" (Revista de Derecho Público y Privado, tomo XL, Nº 238, abril 1958).

En el ordenamiento jurídico uruguayo el raciocinio jus-naturalista se aplica sin fisuras al derecho a la protección de los datos personales. El constituyente no previó expresamente este derecho dentro de las figuras que enumera el art. 7° de la Carta, ni tampoco en otros artículos del mismo cuerpo. No obstante, se integra al elenco de aquellos derechos "inherentes a la personalidad humana" e incluso también -si nos atenemos a la idea de la sentencia alemana anotada- que "derivan de la forma republicana de gobierno". Ambas son expresiones utilizadas por el art. 72 del máximo cuerpo normativo para dotar de vigencia a aquellos derechos que no gozan de una previsión expresa. El círculo se cierra con la aplicación inmediata del derecho en examen, previsto en el art. 332 de la Carta, sin necesidad de reglamentación al efecto.

La Ley Nº 18.331, de 11 de agosto de 2011 es la norma que regula los pormenores de este derecho, reconociendo a texto expreso el raciocinio jus-naturalista antes mencionado: "Artículo 1º: Derecho Humano.- 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".

Sin embargo, nada de esto significa que estemos ante un conjunto de prerrogativas que puedan imponerse en forma irrestricta en todos los casos y bajo cualquier circunstancia. En los sistemas jurídicos democráticos no existen derechos sin freno e ilimitados, excepto (al menos en nuestro ordenamiento) del derecho a la vida. Todos admiten ciertos contrapesos y límites, pero estos son una excepción, ya que deben emanar o encontrar fundamento en una ley dictada por razones de interés general (art. 7º de la Constitución Nacional).

En la vida real con frecuencia entran en conflicto dos o más derechos fundamentales. Es el caso del "derecho de información" y sus derivaciones asociadas a la libertad de pensamiento (expresión, comunicación, etc.), respecto del "derecho a la protección de los datos personales". Por ejemplo, ¿hasta qué punto debe admitirse que se expongan las intimidades de las personas en los medios periodísticos, en ausencia de un consentimiento otorgado por el afectado? La solución justa y adecuada en cada caso dependerá de ciertas labores de armonización interpretativa: jerarquía de los derechos en juego, sacrificio menor a realizar en la aceptación de uno u otro derecho; si se trata o no de una persona notoria de por sí; si se justifica el interés público de la noticia, etc. Existen criterios asentados en la doctrina especializada para resolver con justicia este tipo de casos, el más relevante -pero no el único- es la llamada "directriz de preferencia" que supone escoger en lo posible, dentro de las posibilidades interpretativas que brinda una norma, aquella más favorable o proteccionista del ser humano como tal.

A la hora de regular este derecho Uruguay ha adoptado el modelo europeo, el cual quedó totalmente delineado e impuesto en esa región según las previsiones contenidas en el Convenio Nº 108 de Estrasburgo de 1981, y la Directiva 95/46/CE de 1995. Siguiendo este modelo, la Ley Nº 18.331 se aboca a desbrozar el derecho fundamental en juego, en una serie de otras prerrogativas de tipo instrumental (también llamados derechos), que son por su orden las siguientes:

- El derecho de acceso en tanto facultad de toda persona afectada por un tratamiento de sus datos personales, de llegar a conocer el paradero de sus datos, ubicados en bases de datos y medios similares, así como saber lo que se está haciendo con ellos. A estos efectos se le confieren al afectado dos instancias sucesivas: la primera prejudicial (petición ante el responsable de la base de datos o tratamiento); la segunda de carácter judicial (acción de habeas data), sin perjuicio de las competencias de la Autoridad de Control para intervenir con cometidos de asesoramiento y control en la materia.
- Los derechos de rectificación, actualización, eliminación o supresión, ejercitables en circunstancias en que se aprecia la necesidad de alguna de estas correcciones o ajustes, ya sea por la pérdida de calidad de los datos registrados o el cumplimiento de su finalidad, ya sea por la preponderancia de un derecho a no verse molestado o avasallado de la forma que fuese (publicidad no deseada, afectación del honor, etc.).

- El derecho a impugnar valoraciones personales cuando las mismas provengan de tratamientos automatizados y se presenten bajo perfiles significativos de evaluación negativa en aspectos tales como rendimiento laboral, crédito, fiabilidad, conducta.

Estos derechos se suman a un conjunto de otras categorías y dispositivos jurídicos (principios generales, datos especialmente protegidos, obligación de registro de las bases de datos, régimen especial para las bases de datos de titularidad pública, estatuto del órgano de control, acción judicial especial), conformando un verdadero sistema jurídico regulatorio del derecho fundamental relativo a los datos personales.

La Unidad Reguladora y de Control de Datos Personales tiene por misión velar en el control y cumplimiento de este derecho y se ha trazado el objetivo de contribuir a divulgar su conocimiento entre la población, colaborando con la efectividad de su ejercicio, lo que puede apreciarse a través de sus dictámenes, resoluciones e informes.

.

2.

Principales temas analizados en 2011

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 2010.

a. Actuación inspectiva de la URCDP y manejo de información amparada por el secreto profesional, en el marco de inspecciones que se realicen.

El Consejo Ejecutivo se ha expedido en el sentido que en aquellas inspecciones y fiscalizaciones de bases de datos donde pudiera estar en juego la preservación del secreto profesional sobre ciertos datos, actuará con razonabilidad y ponderación. Consideró que dependiendo de las singularidades de cada caso, donde resulte esencial conocer información sometida a secreto profesional, se atenderá a la economía de medios y a la actuación certera y objetiva como principios de actuación, sin perjuicio de poder requerir el levantamiento judicial del referido secreto. Se entendió que en todo caso, la URCDP observará el derecho de defensa y contradictorio del sujeto inspeccionado o fiscalizado y que buscará su máxima colaboración con las medidas dispuestas.

b. Acuerdo de Cooperación Técnica entre la República Federativa de Brasil y Uruguay

La Dirección General de Comercio del Ministerio de Economía y Finanzas puso a consideración del Consejo Ejecutivo, previo a su firma, el Acuerdo de Cooperación Técnica entre las autoridades de la Defensa del Consumidor de la República Federativa de Brasil y Uruguay, en tanto dicho Acuerdo contiene dos cláusulas vinculables al régimen competencial de la Unidad y, de modo general, al derecho fundamental de la protección de datos personales.

El Consejo Ejecutivo entendió que dicho Acuerdo resulta conforme al régimen de protección jurídica de los datos personales vigente en el país, salvo su cláusula cuarta que refiere a contrapartida y reciprocidad.

c. Administración Tributaria y Protección de Datos

Varias instituciones educativas consultaron sobre la procedencia de la comunicación de datos requerida por parte de la Dirección General Impositiva, al amparo de lo establecido por el Código Tributario, en especial su artículo 68 apartado "E". Tal requerimiento implicaba el conocimiento de diversos datos personales relacionados con el grupo familiar del estudiante, datos identificatorios, responsable del pago, entre otros.

El Consejo Ejecutivo entendió que, conforme las normas y principios que rigen la Protección de Datos Personales, no era procedente la cesión de los datos específicos requeridos en esa oportunidad por la Administración Tributaria.

No obstante, precisó que resultaba procedente la cesión a que refiere la resolución dictada por la Dirección General Impositiva Nº 1486/2011, de 16 de septiembre de 2011, respecto a los datos contenidos en la declaración jurada solicitada por la Administración Tributaria, atinentes exclusivamente al "efectivo obligado al pago".

d. Comunicación de datos.

- El Consejo Ejecutivo se pronunció acerca de una consulta que refirió a una comunicación de datos entre el Ministerio de Trabajo y Seguridad Social (MTSS) y el Ministerio de Transporte y Obras Públicas (MTOP). Tal solicitud se fundó en el diseño, por parte del MTOP, de un Sistema de Información de Transporte de Carga Terrestre y Guías de Carga, para lo cual resulta necesario verificar que los profesionales registrados o que estén enviando información, pertenezcan a la empresa correspondiente. Es por ello que se solicitan los datos contenidos en las planillas de trabajo. El Órgano de Control entendió legítima la mentada comunicación entre los Organismos involucrados, sin necesidad de recabar el consentimiento de los titulares, en mérito a que se verifican en la especie las excepciones dispuestas por el artículo 9º literales B) y C). Se recomendó tener presente las demás disposiciones relativas a la protección de datos.
- Similar consulta planteó la Dirección General de Bomberos, preguntando sobre la legitimidad de que el Ministerio de Trabajo y Seguridad Social comunique los datos contenidos en las planillas de trabajo, con el objetivo de controlar que las empresas que cuentan con habilitación

de Bomberos, mantengan personal capacitado en el marco de los cursos de capacitación externa que brinda dicha Institución. También en este caso, el Consejo Ejecutivo estimó que resulta aplicable la excepción contenida en el artículo 9º literal C) de la Ley Nº 18.331 que habilita la comunicación de datos, en virtud de que la Dirección General de Bomberos está ejerciendo funciones propias del organismo y los datos provienen de otro organismo, por lo que no sería necesario recabar el consentimiento de los titulares.

- El Hospital de Clínicas consultó al Fondo Nacional de Recursos sobre la posibilidad de comunicar datos de los pacientes que reciben tratamiento por tabaco, , a efectos de que este último brinde la medicación necesaria. Para ello recaba el consentimiento de los pacientes y consigna la información en un formulario diseñado para tal fin. También se consulta sobre una base de datos por parte del Fondo Nacional de Recursos cuya información será utilizada para confeccionar estadísticas en forma disociada. El Consejo Ejecutivo entendió que, en el caso, se trata de organismos públicos actuando dentro de sus competencias y en cumplimiento de la Ley Nº 17.793, de 16 de julio de 2004, por lo que sería aplicable al presente, el literal C) del artículo 17 de la Ley Nº 18.331. Por otra parte, sería correcto y necesario el acceso por parte de personal autorizado del Fondo Nacional de Recursos a la base de datos creada a esos efectos, siempre que se cumpla con el principio de seguridad de los datos. Asimismo, se consideró legítimo que el Fondo Nacional de Recursos realice estadísticas disociándose los datos personales sometidos a tratamiento, conforme la normativa vigente. Se concluyó que en todo caso, deberán respetarse los principios que regulan la protección de datos, esencialmente los de seguridad y veracidad de los datos. El Consejo Ejecutivo entendió acorde a la normativa de protección de datos la comunicación de datos prevista por el Ministerio de Ganadería, Agricultura y Pesca al Ministerio del Interior en el marco del proyecto presentado como Fondo Concursable de AGESIC denominado "Fortalecimiento de la Seguridad del Movimiento de Semovientes". La Unidad entendió aplicable al caso la no necesidad de recabar el consentimiento de los titulares, porque se verifica la excepción relativa al ejercicio de las funciones propias de los Poderes del Estado.

- El Fondo de Solidaridad (FDS) consultó acerca de si se encuentra habilitado a informar la identidad de los beneficiarios de las becas que otorga la Institución y si la Universidad de la República (UdelaR) y UTU pueden los datos que permitan localizar a los egresados de dichos entes de enseñanza para la efectiva recaudación de los tributos. El Consejo Ejecutivo se expidió en el sentido que conforme las disposiciones de la Ley Nº 18.331 analizadas a la luz de los cometidos asignados por la Ley al Fondo de Solidaridad, la Universidad de la República y la ANEP – Consejo de Educación Técnico Profesional (UTU) están habilitados a comunicarle los domicilios de sus egresados, además de la respectiva nómina de los beneficiarios, fecha de egreso y carrera asociada. En cuanto a la posibilidad de informar la identidad de los becarios, entendió procede la divulgación de información, disociada de los titulares, al amparo de lo previsto por el literal D) del artículo 17 de la Ley Nº 18.331.

e. Postulación de Uruguay como Sede de la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.

Respecto al alto interés que reviste la Conferencia, que reúne anualmente a las máximas autoridades e instituciones garantes de la protección de datos y la privacidad, así como a expertos en la materia de todos los continentes y en mérito a que la experiencia recogida en ediciones anteriores ha sido muy proficua, el Consejo Ejecutivo decidió postular al país como Sede de la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad a celebrarse en el año 2012, durante la 33ª Conferencia que se desarrolló en el mes de octubre en México.

f. Publicación de datos personales en la web.

- El Consejo Ejecutivo tuvo oportunidad de expedirse sobre una consulta formulada por el Servicio de Registro de Estado Civil de la Intendencia de Montevideo que refería a si la colocación del índice archivo de las partidas de estado civil en su sitio web institucional, resultaba adecuada al régimen jurídico de protección de datos. La Unidad entendió que en el marco de la Ley Nº 18.331, la publicación con carácter general que pretende la consultante, de datos personales referidos a matrimonios, defunciones y cualquier otra especie, requiere de consentimiento previo de los afectados con las notas caracterizantes previstas en el artículo 9º de la Ley. Se destacó que quedan fuera de esta exigencia, los datos personales previstos en el artículo 9º literal c) de la misma Ley.
- La Intendencia de Rivera consultó si es acorde a la Ley de

Protección de Datos Personales, la publicación de ciertos datos en los servicios de consulta de deuda e impresión de factura de su página web. El Consejo Ejecutivo se pronunció por su legitimidad, con la salvedad que deberán eliminar los datos correspondientes a nombre y RUC del propietario, nombre y RUC del contribuyente, dirección y teléfono del contribuyente y datos de "información al contribuyente", en tanto no son necesarios para la finalidad consulta de deuda e impresión de factura. Se señaló, asimismo, que debe tenerse presente la cláusula de consentimiento para el caso que no se trate de datos requeridos para la función propia del Organismo.

- Obras Sanitarias del Estado (OSE) consultó acerca de si es válido que los usuarios de servicios de agua potable y saneamiento accedan al portal de OSE introduciendo su número de documento de identidad, considerando que ese dato conduce a otros que pueden ser de índole privada. El Consejo Ejecutivo se expidió indicando que sería correcta la utilización del número de cédula de identidad, si en forma complementaria se incluye un password de carácter personal del usuario.
- El Consejo Ejecutivo se pronunció sobre una denuncia relativa a la publicación de datos personales en el sitio web del Parlamento Nacional. Se trató de una versión taquigráfica de actuaciones realizadas en la Comisión de Hacienda de la Cámara de Senadores, donde se recogieran denuncias practicadas por un particular, denostativas de un órgano estatal y de algunos funcionarios del mismo. La Unidad sugirió a la autoridad correspondiente disponer la baja de su sitio web de los documentos motivantes de la denuncia, sustituyéndolos por otros de igual tenor donde figuren tachados o eliminados los nombres del órgano y funcionarios afectados (versión pública).

g. Sanciones Administrativas – Adecuación en virtud de modificaciones introducidas a la Ley Nº 18.331, por la Ley Nº 18.719.

En el marco su potestad sancionatoria, el Órgano de Control dictó una Resolución sobre cómo graduar las sanciones administrativas a imponer en caso de violaciones a la normativa proteccionista de datos personales, teniendo en cuenta los cambios verificados por la Ley Nº 18.719.

En este sentido, estableció que en la tarea de graduación, se contemplará que la infracción cometida encuadre en la categoría de muy leve, leve, grave o muy grave. A esos efectos se realizó una enumeración no taxativa de las eventuales conductas infractoras y su correlativa sanción a imponer. Se dispuso que se atienda a la gravedad, reiteración o reincidencia, para determinar qué sanción es razonable y proporcional al hecho cometido.

Se añadió que se apreciará el tipo de datos personales objeto de tratamiento, las medidas de seguridad, los derechos personales vulnerados, el volumen de los tratamientos efectuados, los beneficios obtenidos, sean económicos o de otra índole, el grado de intencionalidad, los daños y perjuicios causados a las personas interesadas y a terceras personas, y cualquier otra circunstancia que sea relevante para evaluar la conducta infraccional cometida.

Finalmente se indicó que deberán tenerse en cuenta eventuales eximentes de responsabilidad que puedan conjugarse, como la fuerza mayor o caso fortuito.

h. Transferencias internacionales.

Royal & Sunalliance Seguros (Uruguay) S.A. consulta acerca de la legalidad de transferir datos a Argentina a los efectos de realizar una encuesta a los corredores que trabajan para la empresa. El Consejo Ejecutivo decidió que podrá realizarse la mentada transferencia, atento a que Argentina posee declaración de país adecuado.

i. Tratamiento de datos.

- Obras Sanitarias del Estado (OSE) consultó acerca de la posibilidad de recolectar y tratar datos de salud del personal. Sobre este aspecto, el Consejo Ejecutivo entendió que no sería necesario el previo consentimiento informado, ya que se trata del ejercicio de una obligación legal. Éste sería necesario para ceder los datos fuera de OSE, a menos que se proceda a su disociación. Se recomendó tomar en consideración los principios consagrados en la Ley, en especial los de finalidad y reserva en la comunicación interna de datos.
- El Consejo Ejecutivo se expidió en una consulta formulada por la Junta Nacional de Drogas sobre la posibilidad de crear una base de datos con los usuarios de los centros de tratamiento. La Unidad consideró que el Organismo se encuentra habilitado a tales efectos, conforme lo previsto en el artículo 9º de la Ley Nº 18.331, en tanto se trata del ejercicio de una obligación legal. Se recomendó la inscripción de dicha base, así como la consideración de los principios legales en el tratamiento de datos especialmente protegidos, así como la adopción de medidas de seguridad.
- La Asociación Uruguaya de Empresas Aseguradoras (AUDEA) consultó sobre la implementación de una base de datos de seguros, la que sería el resultado de un proyecto desarrollado y promovido por el sector asegurador privado nucleado en la AUDEA, teniendo como objetivo central la prevención y combate del fraude en los seguros. El Consejo Ejecutivo resolvió que para la conformación de la referida base de datos, cada aseguradora que co-

munique estos datos a la AUDEA, deberá recabar el consentimiento e informar al titular sobre la finalidad de tal comunicación y de la existencia de dicha base. A efectos de cumplir con la Ley, se dispuso también que deba inscribirse la misma e implementar medidas de seguridad acordes.

j. Videovigilancia – Circuitos cerrados de televisión (CCTV).

- La URCDP tuvo oportunidad de pronunciarse sobre una consulta formulada por el Comité Uruguayo de Seguridad Bancaria (CUSEBA) acerca de si los CCTV instalados en las instituciones bancarias, se encuentran amparados por la excepción prevista en el literal b) del artículo 3º de la Ley Nº 18.331. El Órgano de Control entendió que dichos sistemas de videovigilancia, por imposición de la normativa del Ministerio del Interior y del Banco Central del Uruguay, en tanto se sustentan en razones de "seguridad pública", resultan exceptuados del régimen de la Ley Nº 18.331. No obstante, se consideró que deberán tener presente los principios rectores en materia de protección de datos personales, de veracidad, finalidad, seguridad y reserva, a la vez que se estableció deberán incorporar los logos de videovigilancia aprobados por la Unidad, en lugares visibles.

- La Dirección General de Casinos consultó sobre si es correcto interpretar a los efectos de la inscripción, que el responsable de las bases del Organismo es el Director General de Casinos, aún cuando delegue en Gerentes de Salas o Casinos y en el Departamento de Circuitos Cerrados de Televisión de la Dirección, a la vez que solicitó ser asesorado respecto a cómo garantizar el derecho de acceso a los interesados.El Consejo Ejecutivo resolvió que es la Dirección General de Casinos el organismo público responsable de sus bases de datos de videovigilancia en los términos y alcance previstos en la Ley Nº 18.331 y su Decreto reglamentario, aunque en el cumplimiento de sus facultades delegue en diferentes encargados de tratamientos según corresponda. En cuanto al ejercicio del derecho de acceso, el Consejo entendió que deberá garantizarse tal derecho, conforme lo previsto en el artículo 14 de la Ley, dando respuesta por escrito a los solicitantes, detallando la información existente en la referida base sobre su persona, sin vulnerar derechos de terceros.

3.

Avances en la normativa de protección de datos

a. Iniciativa para la Ratificación del Convenio N° 108 del Consejo de Europa

Con fecha 29 setiembre de 2011, el Poder Ejecutivo en acuerdo, aprobó un Proyecto de Ley para ratificar el Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Série des Traités Européens -STE- N° 108) aprobado en Estrasburgo en 1981 y su Protocolo Adicional relativo a las Autoridades de Supervisión y Flujos Internacionales de Datos (Série des Traités Européens -STE- N° 181) aprobado en Estrasburgo en 2001 .

Este proyecto de Ley, que supone un hito en Uruguay, es la culminación de un camino iniciado por la Unidad Reguladora y de Control de Datos Personales, desde que a la fecha nuestro país es el único no miembro de la Unión Europea invitado a adherir al Convenio N° 108 y su Protocolo Adicional N° 181.

El Convenio N° 108 del Consejo de Europa y su Protocolo Adicional N° 181, son instrumentos continentes de los principios rectores en materia de Protección de Datos, fuente de inspiración y consulta de la comunidad internacional.

Si bien se trata de documentos elaborados para los Estados miembros del Consejo de Europa, su artículo 23 prevé la posibilidad de que los Ministros del Consejo inviten a un Estado no miembro a adherir al mismo, lo que muestra la clara vocación universal de estos instrumentos jurídicos.

Antes de invitar un Estado a adherir a la Convención, los Ministros del Consejo tienen la posibilidad de evaluar la compatibilidad de la legislación interna del Estado con relación con las normas del Consejo de Europa, por lo que el país solicitante deberá contar con un adecuado nivel de protección de datos personales.

Uruguay posee un régimen jurídico en materia de protección de datos de origen constitucional y de consagración legal por la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 y sus Decretos Reglamentarios Nros. 664/08 y 414/09, de 22 de diciembre de 2008 y 31 de agosto de 2009 . Esta normativa es coincidente con la europea que ha sido su fuente inspiradora.

En este sentido, el 5 de febrero de 2010, la Unidad Reguladora y de Control de Datos Personales, emitió la Resolución N° 43/010 la cual resuelve: "Propiciar ante el Ministerio de Relaciones Exteriores la iniciación ante el Consejo de Europa de las gestiones necesarias a los efectos indicados en la presente resolución, de acuerdo con lo previsto por el art. 23 del Convenio N° 108 del Consejo de Europa (Convención Estrasburgo) y su Protocolo Adicional, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal."

Posteriormente, y en función de que el Consejo de Europa tiene su sede en Estrasburgo, la Embajada de Uruguay en Francia, envió una nota a la Secretaría General del Consejo de Europa, comunicando la intención de nuestro país de adherir al Convenio N° 108 y su Protocolo Adicional N° 181.

El 20 de julio de 2010, por intermedio de la Dirección General para Asuntos Políticos, Dirección Regional Europea, del Ministerio de Relaciones Exteriores, la Misión uruguaya en Francia informó sobre la respuesta de la Dirección Jurídica del Consejo de Europa para iniciar el proceso de adhesión, formalidades y documentación a ser agregada.

El 6 de agosto de 2010, la Dirección de Derechos Ciudadanos hizo llegar al Ministerio de Relaciones Exteriores la legislación nacional vigente en materia de Protección de Datos Personales en idioma inglés, a fin de ser enviada al Consejo de Europa junto con una nota del Señor Canciller de la República.

El 25 de marzo de 2011, la Embajada uruguaya en Francia remitió al Consejo de Europa una nota original del Señor Canciller Dr. Luis Almagro dirigida al Secretario General del Consejo de Europa, Don Thorbjorn Jagland, manifestando el interés de Uruguay en adherir al Convenio N° 108 y su Protocolo Adicional N° 181, adjuntando la legislación nacional mencionada. Todo conforme fuera indicado por la Dirección Jurídica del Consejo de Europa.

El 13 de abril de 2011, la Dirección General para Asuntos Políticos, Dirección Regional Europea del Ministerio de Relaciones Exteriores, informó el recibo de una nota del Secretario General del Consejo de Europa, Don Thorbjorn Jagland, mediante la cual se acusa recibo de aquella enviada por nuestro país expresando el deseo de adherir al Convenio N° 108 y su Protocolo Adicional N° 181. Se comunicó, asimismo, que de acuerdo con la práctica de la Organización, la Oficina de Tratados procederá a realizar consultas informales con los Estados Miembros del Consejo de Europa, a fin de

conocer sus opiniones respecto de la solicitud de Uruguay. Si la consulta resultaba positiva, la petición sería examinada por un Grupo Relator en materia de cooperación legal del Comité de Ministros y posteriormente enviada al Consejo de Ministros.

El 19 de julio de 2011, la Embajada uruguaya en Francia informó que la solicitud de invitación para ratificar el Convenio N° 108 y su Protocolo Adicional N° 181 fue aceptada.

El Proyecto de Ley para la ratificación del Convenio N° 108 y su Protocolo Adicional N° 181, se compone de Antecedentes en los que se relaciona la normativa nacional y las diversas iniciativas internacionales afines, para lograr un Convenio Universal en materia de protección de datos personales. Se transcriben algunos artículos del Convenio relativos a: Objeto y fin (1), Campos de Aplicación (3), Seguridad de los datos (7), Garantías complementarias para las personas concernidas (8), Flujo Transfronterizo de Datos (12), Integración y funciones del Comité Consultivo (18 y 19). Finalmente, se hace referencia al artículo 25 que establece la imposibilidad de formular reservas al Convenio.

Consta de dos artículos cuyo texto se transcribe a continuación:

"**ARTÍCULO 1°**.- Apruébanse los CONVENIO N° 108 DEL CONSEJO DE EUROPA PARA LA PROTECCION DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIAZDO DE DATOS DE CARACTER 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.

ARTICULO 2°.- Comuníquese, etc."

b. Iniciativas nacionales relacionadas con la protección de datos

Durante el año 2011, corresponde mencionar a nivel nacional, dos normas cuyo contenido se ocupa de la protección de datos. En orden cronológico según su fecha de publicación, ellas son:

i. Ley N° 18.812 de Datos de Carácter Personal Inscriptos en la Central de Riesgos Crediticios del Banco Central del Uruguay, de 23 de setiembre de 2011

Esta Ley se compone de cinco artículos. Tiene por objeto garantizar el derecho a la protección de los datos de carácter personal contenidos en la Central de Riesgo del Banco Central del Uruguay.

Se destaca la declaración realizada en su artículo primero, conforme la cual la Central de Riesgos se encuentra regulada por la Ley N° 18.331 de Protección de Datos Personales y Habeas Data, de 11 de agosto de 2008, con algunas especialidades que se establecen en las restantes disposiciones de la norma. A saber:

El plazo de registro es de quince años a partir del vencimiento de la operación (artículo 2).

No será necesario el previo consentimiento de los titulares para el tratamiento de datos personales en la Central de Riesgos (artículo 3).

El plazo de respuesta frente al ejercicio del derecho de acceso será de veinte días hábiles (artículo 4).

Las personas físicas y jurídicas del sistema de intermediación financiera que suministren la información contenida en la Central de Riesgos, serán las únicas responsables por su veracidad y actualización (artículo 5).

ii. Ley N° 18.849 de Registro Nacional de Huellas Genéticas, de 2 de diciembre de 2011

Esta norma se compone de 12 artículos. Su cometido es la creación de un Registro Nacional de Huellas Genéticas.

Se destaca:

El registro depende de la División de Identificación Criminal de la Dirección Nacional de Policía Técnica del Ministerio del Interior (artículo 1°).

Tiene por objeto facilitar el esclarecimiento de los hechos sometidos a investigación criminal; identificar y contribuir a ubicar personas extraviadas y asistir a la resolución de controversias judiciales (artículo 3°).

El registro no conservará muestras de ADN codificante y no codificante, solamente podrá registrar la información que provenga del mismo, la que tendrá carácter de reservada y confidencial (artículo 4°).

De principio, la extracción de ADN solo podrá ser realizada con consentimiento expreso e inequívoco de la persona, la que deberá estar en conocimiento del fin para el que la muestra será destinada. Se exceptúan los casos de muestras latentes obtenidas en escenas de comisión de delitos; los perfiles genéticos procesados por la justicia competente; la extracción dispuesta por Juez competente y las muestras correspondientes a funcionarios del Ministerio del Interior y Defensa Nacional que determine la reglamentación a dictarse.

c. Iniciativas internacionales relacionadas con la protección de datos

En el año 2011, Perú y Costa Rica se unieron al elenco de países latinoamericanos que cuentan con legislación en materia de protección de datos.

i. Perú

El 3 de julio de 2011, Perú publicó la Ley N° 29.733 de Protección de Datos Personales.

Compuesta por cuarenta artículos, esta norma consta de un Título Preliminar de Disposiciones Generales y siete Títulos restantes sobre: Principios rectores, Tratamiento de datos personales, Obligaciones del titular y del encargado del banco de datos personales, Bancos de datos personales, Autoridad Nacional de Protección de Datos Personales e Infracciones y Sanciones Administrativas, Disposiciones complementarias finales, respectivamente.

Sus Principios rectores son: legalidad (artículo 4°), consentimiento (artículo 5°), finalidad (artículo 6°), proporcionalidad (artículo 7°), calidad (artículo 8°), seguridad (artículo 9°), disposición de recurso (artículo 10) y nivel adecuado de protección (artículo 11).

Dispone que el tratamiento de los datos personales debe realizarse con pleno respeto de los derechos fundamentales de sus titulares y solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco, y en el caso de datos sensibles, además, debe extenderse por escrito (artículo 13).

Señala que las limitaciones al ejercicio del derecho fundamental a la protección de datos personales solo pueden ser establecidas por ley, y deberán estar justificadas en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos (artículo 13).

El artículo 14 se ocupa de las limitaciones al consentimiento en el tratamiento de datos personales.

En cuanto a los derechos de los titulares, esta norma establece el derecho de información (artículo 18), de acceso (artículo 19), de actualización, inclusión, rectificación y supresión (artículo 20), de impedir suministro (artículo 21), de oposición (artículo 22), de tratamiento objetivo (artículo 23), a la tutela (artículo 24) y a ser indemnizado (artículo 25).

Su artículo 32 crea la Autoridad Nacional de Protección de Datos en la órbita del Ministerio de Justicia.

En cuanto al sistema sancionador, el artículo 38 clasifica las infracciones en leves, graves y muy graves.

ii. Costa Rica

El 5 de setiembre de 2011, Costa Rica publicó la Ley N° 8.969 de Protección de la Persona frente al tratamiento de sus datos personales.

Se compone de treinta y cuatro artículos. Consta de seis Capítulos sobre: Disposiciones Generales, Principios y Derechos Básicos para la Protección de Datos, Transferencia de Datos Personales, Agencia para la Protección de Datos Personales, Procedimientos y Cánones, respectivamente.

Se trata de una ley de orden público, que tiene como objetivo garantizar el respeto de las personas a su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes (artículo 1°).

Establece como principios rectores: la autodeterminación informativa (artículo 4°), el previo consentimiento informado (artículo 5°) y la calidad de la información que deberá ser actual, veraz, exacta y adecuada (artículo 6°).

En cuanto a los derechos de los titulares, esta norma refiere al derecho a la información y al derecho de rectificación, ambos regulados por el artículo 7°.

Crea la Agencia para la Protección de Datos Personales (PRODAT) como desconcentrado del Ministerio de Justicia y Paz (artículo 15).

Con respecto al régimen sancionatorio, divide las infracciones en faltas leves, graves y gravísimas (artículo 28).

iii. Jurisprudencia internacional

En materia de jurisprudencia en protección de datos, no podemos dejar de comentar la sentencia dictada el 24 de noviembre de 2011 por el Tribunal de Justicia de la Unión Europea -asuntos acumulados c-468/10 y C-469/10- que se pronuncia por primera vez y en forma directa sobre el artículo 7°, letra f), de la Directiva 95/46/CE y en su mérito, sobre la incompatibilidad de las disposiciones nacionales que agregan requisitos a los solicitados por la citada norma comunitaria.

El litigio comenzó cuando la Federación de Comercio Electrónico y Marketing Directo (FECEMD), actualmente denominada ADIGITAL y la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), interpusieron un recurso de impugnación ante el Tribunal Supremo Español contra varios artículos del Real Decreto 1720/2007, que reglamenta la Ley Orgánica de Protección de Datos española.

En el marco de dicho proceso, el Tribunal Supremo Español, remitió las actuaciones en consulta al Tribunal de Justicia de la Unión Europea, sobre el artículo 7°, letra f), de la Directiva 95/46 de protección de datos y su compatibilidad con el artículo 10, apartado 2, letras a), supuesto primero, y b), párrafo primero, del mencionado reglamento.

El problema de fondo y por el cual se planteó la impugnación, radica en que según los recurrentes, la reglamentación española añade requisitos adicionales a los solicitados por la Directiva europea.

En términos de la sentencia comentada en sus numerales 16 a 22:

"La ASNEF, por una parte, y la FECEMD, por otra parte, interpusieron recurso contencioso-administrativo contra diversos artículos del Real Decreto 1720/2007.

16. Entre los preceptos impugnados se encuentra el artículo 10, apartado 2, letras a), supuesto primero, y b), párrafo primero, de dicho Real Decreto, a los que la ASNEF y la FECEMD imputan la infracción del artículo 7, letra f), de la Directiva 95/46.

17. En particular, la ASNEF y la FECEMD consideran que el Derecho español añade al requisito del interés legítimo como presupuesto del tratamiento de los datos sin consentimiento del titular un requisito que no está presente en la Directiva 95/46: que los datos consten en fuentes accesibles al público.

18. El Tribunal Supremo opina que el fundamento de los recursos interpuestos por ASNEF y FECEMD depende en gran medida de la interpretación que haga el Tribunal de Justicia del artículo 7°, letra f), de la Directiva 95/46. Así, señala que si el Tribunal de Justicia estimase que no corresponde a los Estados miembros añadir requisitos adicionales a los establecidos en esa disposición y que a dicha disposición puede reconocérsele efecto directo, el artículo 10, apartado 2, letra b), del Real Decreto 1720/2007 debería inaplicarse.

19. El Tribunal Supremo explica que, en el caso de que no exista consentimiento del interesado, para autorizar el tratamiento de sus datos de carácter personal, necesario para la satisfacción de un interés legítimo del responsable de ese tratamiento o de los terceros a quienes se comuniquen los datos, el Derecho español exige, además del respeto de los derechos y libertades fundamentales del interesado, que los datos figuren en los ficheros enumerados en el artículo 3, letra j), de la Ley Orgánica 15/1999. A este respecto considera que la Ley Orgánica 15/1999 y el Real Decreto 1720/2007 restringen el ámbito del artículo 7, letra f), de la Directiva 95/46.

21. No obstante, el Tribunal Supremo se pregunta si tal interpretación es conforme a la voluntad del legislador de la Unión.

22. En estas circunstancias, por considerar que la solución de los dos asuntos de que conoce depende de la interpretación de disposiciones del Derecho de la Unión, el Tribunal Supremo decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales, formuladas en idénticos términos en ambos asuntos:

«1) ¿Debe interpretarse el artículo 7, letra f), de la Directiva 95/46 [.] en el sentido de que se opone a una normativa nacional que, no mediando consentimiento del afectado y para permitir el tratamiento de sus datos de carácter personal que resulte necesario para satisfacer un interés legítimo del responsable o de los terceros a los que se vayan a comunicar, exige además de que no se lesionen los derechos y libertades fundamentales de aquél que los datos consten en fuentes accesibles al público?

2) ¿Concurren en el mencionado artículo 7, letra f), las condiciones que exige la jurisprudencia del Tribunal de Justicia [...] para atribuirle efecto directo?» "

En sentencia de fecha 24 de noviembre de 2011 (asuntos acumulados c-468/10 y C-469/10), el Tribunal de Justicia resuelve:

"1) El artículo 7, letra f), de 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, debe interpretarse en el sentido de que se opone a una normativa nacional que, para permitir el tratamiento de datos personales necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, exige, en el caso de que no exista consentimiento del interesado, no sólo que se respeten los derechos y libertades fundamentales de éste, sino además que dichos datos figuren en fuentes accesibles al público, excluyendo así de forma categórica y generalizada todo tratamiento de datos que no figuren en tales fuentes.

2) El artículo 7, letra f), de la Directiva 95/46 tiene efecto directo".

Esto significa, que las normativas europeas nacionales no pueden exigir requisitos adicionales a los solicitados por la Directiva. En la especie, el artículo 7°, letra f), establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos; y que los derechos y libertades fundamentales del interesado.

De lo que se desprende que el Reglamento español sobre protección de datos se ha excedido al exigir, además, el requisito de que los datos objeto de tratamiento figuren en fuentes accesibles al público.

Por otra parte, el artículo 7°, letra f), de la Directiva 95/46 tiene efecto directo, puesto que, se trata de una disposición suficientemente precisa para poder ser invocada por un particular y aplicada por los órganos jurisdiccionales nacionales.

Estos fundamentos son más que suficientes para que el Tribunal Supremo Español declare nula la restricción añadida por el legislador en el artículo 10, apartado 2, letras a), supuesto primero, y b), párrafo primero del Real Decreto 1720/2007 sobre protección de datos personales, lo que sería un golpe al bloque normativo del país. Por otro lado, su no anulación implicaría un nivel diferente de protección por parte de España frente a los restantes Estados miembros, lo que podría acarrear problemas de flujo de información.

4.

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.

a. Sentencia del Tribunal de lo Contencioso Administrativo Nº 160, de 3 de marzo de 2011.

En esta sentencia, el Tribunal de lo Contencioso Administrativo confirma el acto administrativo por el que se observa a una empresa de emergencia móvil y se amonesta a un médico por contradicciones surgidas del registro de la historia clínica del paciente.

Esta sentencia trata las consecuencias derivadas de la dificultad de entender la caligrafía de un médico, al elaborar una historia clínica en plena asistencia médica, que termina con el fallecimiento del paciente.

La sentencia indica que era tal la dificultad, que la accionante agregó una versión mecanografiada de la historia, pero existía una gran diferencia entre la historia manuscrita y la versión mecanografiada proveniente de omisiones derivadas de la imposibilidad de comprender la caligrafía de quien realizó la traducción.

Del caso expuesto, surge la importancia de que las historias clínicas contengan información que sea clara y veraz dando cumplimiento, de esa forma, al principio de veracidad regulado en la Ley de Protección de Datos.

b. Sentencia interlocutoria del Juzgado Letrado de Primera Instancia en lo Penal de 18º Turno Nº 408, de 11 de marzo de 2011.

En esta sentencia se resuelve si Facebook constituye o no un medio de comunicación comprendido en la Ley de Prensa Nº 16.099, de 13 de noviembre de 1989.

Específicamente se analiza la posibilidad de cometer un delito de difamación a través de una red social. En el caso concreto, en diciembre de 2010 se publicaron en www.facebook.com expresiones que señalaban que la denunciante a través de su criadero de perros, había hurtado un cachorro de perro de raza Bulldog Francés.

En este caso el Magistrado entiende que no es de aplicación el régimen muy especial de la Ley Nº 16.099. Se aclara que las manifestaciones que considera agraviantes fueron anunciadas en las cuentas de FACEBOOK de CC y del Grupo de Amigos de Bulldog Francés, a las que solo tendrían acceso las personas vinculadas a los mismos debidamente inscriptas en la red social, con su autorización para ingresar, o los allegados a los que previamente conocieron las aseveraciones, grupo por demás comprimido, reducido. Esto conllevó a subrayar por la interesada que se trata de aquellos con idéntica o afín actividad de crianza de perros de raza. Aclara que remotamente nos enfrentamos a acontecimientos vertidos en un diario, televisión, radio o semejantes, con un alcance enorme, universal, ilimitado de receptores, "medio de comunicación público"

El interés de la sentencia radica en la utilización que se hace de datos personales sin consentimiento del titular, lo que ésta en ningún momento evalúa.

c. Sentencia del Tribunal de lo Contencioso Administrativo Nº 340, de 26 de abril de 2011.

En esta sentencia el Tribunal de lo Contencioso Administrativo confirma el acto administrativo dictado por Obras Sanitarias del Estado (O.S.E) que sancionó a un funcionario con suspensión de diez días sin goce de sueldo, por utilizar los sistemas informáticos del organismo para realizar descargas de videos y similares para fines personales y puso en peligro la confidencialidad de la información del ente estatal.

La sentencia confirma la Resolución del Directorio de O.S.E. aplicando la sanción por entender que incurrió en la falta prevista en el Reglamento Interno de Personal. Esto en tanto cometió intencionalmente actos incompatibles con el buen desempeño de sus funciones o que significan abandono continuado de las mismas, sin que el hecho ocasione perjuicios a la entidad, por los hechos relacionados con el uso de Internet por parte de tres administradores de la red del Centro de Informática de la Administración; más la posible descarga de archivos DVD. El actor reconoció haber utilizado su equipo informático para actividades ajenas a la función, al haberse detectado en el mismo archivos correspondientes a carátulas de películas de DVD, de películas infantiles que ven sus hijos menores, así como archivos MP3 de música.

La importancia de esta sentencia radica en que se valora que la conducta del funcionario puso en peligro la seguridad de la información del organismo, lo cual constituye una posible infracción a la Ley de Protección de Datos Personales.

d. Sentencia del Tribunal de lo Contencioso Administrativo Nº 353, de 26 de abril de 2011.

Por esta sentencia el Tribunal de lo Contencioso Administrativo confirma la Resolución dictada por el BROU, por la cual se destituye a un funcionario por brindar información bancaria a terceras personas.

Esta sentencia confirma la Resolución del Directorio del Banco de la República que dispuso proceder de acuerdo con la propuesta del Gerente General en el sentido de destituir a un funcionario bajo imputación de culpa grave.

Las actuaciones se iniciaron a partir de una denuncia efectuada por una persona que, al concurrir al banco y solicitar un estado de cuenta, constató que se habían cobrado dos cheques en dólares pertenecientes a su cuenta corriente, los cuales no habían sido emitidos por ella o por su esposo quien es cotitular de la cuenta.

En virtud de la denuncia formulada se decretó la instrucción de una investigación administrativa tendiente al esclarecimiento de los hechos descriptos. Se interrogó al ahora accionante, puesto que surgió evidencia de que había realizado consulta de saldos de la cuenta corriente de la clienta denunciante. El accionante manifestó que consulta los estados de cajas de ahorro cuando los mismos son solicitados por los clientes vía telefónica, se cerciora de los datos personales y brinda la información respectiva.

Interrogado el accionante por la razón de la consulta remota a la cuenta corriente de la denunciante, afirmó "es que tiene un amigo que tiene una casa de cambios, que realiza transacciones con cheques, a veces lo llama y pregunta antes de descontarlo sobre si la cuenta es buena, en ese caso le informo si el saldo es bueno y si tiene buen promedio". La Administración entendió que existen elementos probatorios con relevancia jurídica para responsabilizar administrativamente al accionante, y se resolvió instruirle sumario administrativo.

Las conductas imputadas al funcionario, identificadas como consultas a cuentas corrientes y cajas de ahorro, el hecho de brindar información de saldos a terceros, no son propias de la función que cumple el accionante en el Banco. En las indicadas circunstancias, el actor cometió una falta administrativa prevista en el Estatuto del Funcionario del BROU ya que brindó información a terceros sobre cuentas de clientes de la Institución, provocando descrédito en ésta y violando prohibiciones estatutarias que le hacen pasible de ser sancionado administrativamente.

Se destaca en esta sentencia la importancia que posee el principio de reserva, el cual alcanza a las instituciones financieras de nuestro país donde se hace operativo a través de sus agentes, que deben ser estrictos en la observancia de dicho principio. De allí que las transgresiones a la reserva de las actuaciones en el ejercicio de su función, acarree responsabilidades tanto en el fuero penal y civil como en el administrativo, por los daños causados ante la violación de su deber jurídico de guardar secreto.

5.

Presentación de la Memoria 2010

El 12 de mayo del 2011 se realizó en la Torre Ejecutiva el lanzamiento de la Memoria Anual 2010. Se contó con la presencia del Prosecretario de la Presidencia Dr. Diego Cánepa y el Lic. Iñaki Vicuña Nicolás, Director de la Agencia Vasca de Protección de Datos.

El Dr. Diego Cánepa señaló y destacó la importancia de la actuación llevada a cabo por la Unidad, la que se ve reflejada en la publicación de la memoria contribuyendo a la transparencia, elemento sustancial de la protección de datos personales y manifestó vivamente su apoyo a la gestión de la Unidad.

Por su parte, el Lic. Iñaki Vicuña Nicolás, se refirió a la importancia del cumplimiento de un derecho fundamental como es el de la protección de datos para las autoridades nacionales. A su vez destacó el afianzamiento de las relaciones de cooperación entre la Unidad y la Agencia Vasca de Protección de Datos, comunicando el deseo de seguir trabajando en conjunto y aprovechar las experiencias de las dos entidades.

El evento contó con la participación de autoridades de diferentes organismos públicos, así como con la presencia de integrantes de los Poderes Legislativo, Ejecutivo y Judicial.

Cabe destacar la presencia de empresarios de diferentes sectores de la actividad privada nacional, lo cual denota la importancia que tiene para estos el tema de la protección de los datos personales en el desarrollo de sus actividades.

6.

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 oficial.

Entre las novedades se destacan:

i. Jurisprudencia: El ciudadano puede acceder a sentencias de diferentes Tribunales y Juzgados respecto a temas relacionados con la protección de datos personales.

Se incluyen sentencias referentes a:

- La condena por hurto mediante la presentación de un CD que contenía registros fílmicos de las cámaras de seguridad de un comercio.
- Si la red Social Facebook constituye o no un medio de comunicación comprendido en la Ley de Prensa N° 16.099.
- La condena por uso ilegal de marca derivado del hurto de software que incluía bases de datos de la empresa.
- Un reclamo por daños y perjuicios derivados de la inclusión en una base de datos de deudores.
- El procesamiento por delitos sexuales por publicación de material pornográfico en un sitio web.
- Acción de Habeas Data realizada contra el Banco Central del Uruguay.
- Acción de Habeas Data llevada a cabo a efectos de acceder a la información contenida en las cesiones de las boletas de derechos de mejor postor y transferencias de créditos bancarios.

Encontramos, además, sentencias dictadas por la Suprema Corte de Justicia respecto a:

- Denegación de recurso de casación por entenderse que se informó al titular debidamente y se acreditó la existencia del previo consentimiento informado.
- Denegación de recurso de casación por entenderse que no existió consentimiento informado de un paciente en un procedimiento médico.

Por último, se incluyen sentencias dictadas por el Tribunal de lo Contencioso Administrativo que refieren a:

- La observancia de una empresa de emergencia móvil donde se amonesta a un médico por contradicciones en una historia clínica de un paciente.
- La decisión de la División Recursos Humanos del BROU por la cual se dispuso el registro en el legajo de un funcionario de informes sobre acciones realizadas por éste en contra del Banco.
- La anulación de un acto administrativo que denegó el acceso a determinados datos incorporados al Sistema Central de Riesgos del Banco Central del Uruguay.
- Se confirma acto administrativo de la DGI por el que se entendió que la consultante es contribuyente de los tributos IVA e IRIC, por los servicios brindados a personas en el exterior, entre los que se encuentran el alojamiento web, espacio en disco, base de datos y colocación de banners de publicidad.

ii. Denuncias: El ciudadano puede acceder a la información necesaria a la hora de hacer una denuncia ante la Unidad. En esta sección puede acceder a los formularios para realizar las denuncias en forma personal, así como desde el mismo sitio web.

b. Publicaciones realizadas

El 28 de enero de 2011, fecha en el que se celebró el "Día Internacional de la Protección de Datos", se realizó la presentación y publicación del libro "Resoluciones, Dictámenes e Informes 2010". En la mencionada publicación, se puede acceder a las resoluciones y dictámenes del Consejo Ejecutivo de la URCDP sobre temas de interés en la materia, así como a los informes realizados para esos temas. Ésta se encuentra publicada en formato papel y digital. En formato digital se encuentra en el sitio web de la Unidad, del cual se puede descargar.

Los documentos incluidos en esta edición fueron seleccionados con la finalidad de profundizar las temáticas tratadas en años anteriores. Según el Presidente del Consejo Ejecutivo de la URCP, Mag. Federico Monteverde: "ampliando el abanico de las mismas, en una muestra de la creciente preocupación y el desenvolvimiento teórico y práctico que la protección de este derecho fundamental tiene en nuestra sociedad".

Se destacan entre los temas tratados: Ratificación ante el Consejo de Europa del Convenio Nº 108 y su Protocolo Adicional; derecho de acceso que posee un titular de datos personales y las formas en que puede ejercer su derecho el ciudadano; transferencias internacionales de datos, aprobación y regulación de logos de videovigilancia; actualizaciones de bases de datos, datos personales con relación al manejo por parte de instituciones crediticias, información que se debe brindar en un concurso público; convenios entre instituciones; tratamiento por parte del Ministerio de Desarrollo Social (MIDES) de los datos de sus beneficiarios; destrucción de la información recabada para un fin determinado; requerimiento de previo consentimiento informado de referencias laborales en el momento de la recepción de Curriculums Vitae en un proceso de selección de personal; integración de datos de actos de salud de emergencias médicas, datos sensibles y referencias personales de empresas de seguridad, entre otros.

Con esta publicación se busca crear conciencia sobre la importancia de este derecho a todos los integrantes de la sociedad.

c. Atención de consultas personalizadas

Durante el 2011 la URCDP ha realizado diversas actividades de difusión y capacitación en materia de Protección de Datos Personales. Éstas se practicaron con diferentes actores de la actividad nacional, personas físicas, asociaciones profesionales y organizaciones tanto públicas como privadas de todo el país.

En ese marco se realizaron cursos en el Ministerio de Desarrollo Social (MIDES) y en la Dirección General de Registro de Estado Civil, con el fin de informar a los funcionarios sobre la normativa de protección de datos personales.

Se colaboró con el Sistema Informático Integral de Asuntos Sociales (SIIAS) del Ministerio de Desarrollo Social, en la confección de los artículos referidos a la protección de datos personales que debían ser incluidos en el Decreto Reglamentario de ese organismo.

Respecto a entidades y empresas privadas se realizaron reuniones con los integrantes del Estudio Ferrere, la Asociación Uruguaya de Aseguradores y con Meb Uruguay.

d. Eventos nacionales

El 8 de febrero de 2011, el Mag. Federico Monteverde, integrante del Consejo Ejecutivo de la URCDP, concurrió en representación de la Unidad junto al Ing. Santiago Paz de AGESIC, a las instalaciones de Televisión Nacional como invitados en al programa "La noticia y su Contexto".

En otra instancia de capacitación y difusión con entidades del Estado se participó de los eventos organizados por el Programa de Gestión Unificada de Registro e Información (GURI) del Consejo de Educación Inicial y Primara. Las charlas estuvieron a cargo de integrantes de la Dirección de Derechos Ciudadanos de AGESIC, las que se realizaron en los departamentos de Colonia, Maldonado y Rivera. Los eventos contaron con la concurrencia de inspectores nacionales, regionales y locales, así como docentes y asesores del programa representantes de los departamentos sede y limítrofes.

Es válido destacar la importancia de la mencionada capacitación ya que fue brindada a maestros que transmitirán la necesidad de proteger los datos personales a sus alumnos, quienes desde la niñez conocerán cuáles son sus derechos y obligaciones al respecto.

La Unidad participó de la Primera Sesión Académica del Instituto de Derecho Informático de la Universidad de la República, ocasión en la que el Dr. Felipe Rotondo, en calidad de Presidente del Consejo Ejecutivo de la URCDP realizó una exposición denominada "Central de Riesgos del Banco Central del Uruguay, ventajas y desventajas de su libre acceso".

La exposición enfatizó los derechos de acceso a la información pública y protección de datos personales y el proyecto de Ley que se encontraba a estudio en el Parlamento Nacional que modifica aspectos regulados por la Ley N° 18.331 de Protección de Datos Personales y Habeas Data, hoy Ley N° 18.812.

A su vez se dictaron dos charlas sobre Protección de Datos, una realizada en las instalaciones de Microsoft y otra en la Unidad Reguladora de Servicios de Comunicaciones (URSEC) por el Mag. Federico Monteverde. En la mencionada en último término fue acompañado por un integrante de la Dirección de Derechos Ciudadanos de AGESIC.

e. Jornadas de capacitación interna en AGESIC

Siguiendo la línea de mejora continua establecida en los años anteriores, la Unidad organizó del 9 al 13 de mayo un taller para la formación de sus funcionarios sobre protección de datos dictado por el Lic. Iñaki Vicuña Nicolás, Director de la Agencia Vasca de Protección de Datos. El motivo de la realización del mencionado taller fue la incorporación y aprendizaje de las mejores prácticas surgidas de la experiencia vasca en la materia. En dicho evento se contó con la participación de miembros del Consejo Ejecutivo e integrantes de diferentes áreas de AGESIC.

Luego de realizado el taller se comenzaron a poner en práctica las lecciones aprendidas y se trabajó en la estandarización de los procesos de gestión de la URCDP.

El proyecto culminó con la realización de los manuales de trabajo de los procesos de registro de base de datos, consultas y las denuncias que se realizan frente a la URCDP.

f. Relacionamiento internacional

Continuando con el objetivo de crear vínculos de trabajo y cooperación con diferentes autoridades tanto académicas como institucionales que trabajan en el tema de la protección de datos, la URCDP ha participado en los siguientes eventos internacionales.

i. Seminario sobre Acceso a la Información Pública y Protección de Datos. Antigua. Guatemala.

El 5 y 7 de abril de 2011 se realizó en Antigua Guatemala el Seminario sobre Acceso a la Información Pública y Protección de Datos; en el que se trató la protección de datos en las cédulas y documentos de identificación de las personas, contando con la participación de los siguientes países: Bolivia, Chile, Costa Rica, Guatemala, España, Panamá, Honduras, Venezuela, Colombia, El Salvador, Ecuador, México, Paraguay, Perú, República Dominicana y Uruguay.

Por nuestro país participaron el Dr. Felipe Rotondo, Presidente de la Unidad Reguladora y de Control de Datos Personales, quien expuso sobre "La incidencia del derecho de acceso a la información pública y la protección de datos personales en los sectores de defensa y seguridad pública, banca, telecomunicaciones, función pública, y sanidad, entre otros; y la Dra. Esc. María José Viega, Directora de Derechos Ciudadanos de AGESIC, quien presentó "Modelos de autoridades de control en Transparencia y Protección de Datos Personales: una autoridad o doble autoridad".

ii. Seminario El impacto de las transferencias internacionales de datos en América Latina. Las políticas preventivas y la autorregulación en la implantación de la normativa de Protección de Datos. Cartagena de Indias. Colombia.

Desde el 14 al 16 de junio se realizó en la ciudad de Cartagena de Indias, Colombia, el Seminario de la Red Iberoamericana de Protección de Datos Personales. Este año el tema fue "Las transferencias internacionales de datos. Políticas preventivas y la autorregulación en la implantación de la normativa de protección de datos".

En esta oportunidad Uruguay estaría representado por el Dr. Felipe Rotondo como Consejero de la URCDP y la Dra. Graciela Romero de Derechos Ciudadanos de AGESIC.

Sus exposiciones se realizaron por videoconferencia desde Montevideo. La Dra. Graciela Romero desarrolló el tema "Instrumentos para la aplicación de la normativa de protección de datos en la perspectiva de los países latinoamericanos: la experiencia de Uruguay" y por su parte el Dr. Felipe Rotondo presentó la "Autorregulación: aplicaciones en materia de protección de datos, con especial referencia a Uruguay".

iii. 33ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. México D.F. México.

33ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad

Privacidad: La Era Global

Ciudad de México, 2 y 3 de noviembre 2011

La 33ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad se realizó en la ciudad de México, D.F, los días 2 y 3 de noviembre. La URCDP estuvo representada por el Director Ejecutivo de AGESIC e integrante del Consejo Ejecutivo de la Unidad y la Dra. Esc. María José Viega, Directora de Derechos Ciudadanos de AGESIC.

Como es ya tradición en este evento mundial se nuclearon las máximas autoridades en la materia.

Para Uruguay y en especial para la URCDP esta instancia del evento tuvo una importancia significativa ya que nuestro país fue designado sede de la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad para el 2012, la cual se realizará en octubre en Punta del Este.

Cabe mencionar que con anterioridad al evento principal se realizaron las Conferencia The Public Voice y la Conferencia de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), así como también la reunión de la Red Iberoamericana de Protección de Datos, en las cuales Uruguay participó.

7.

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.

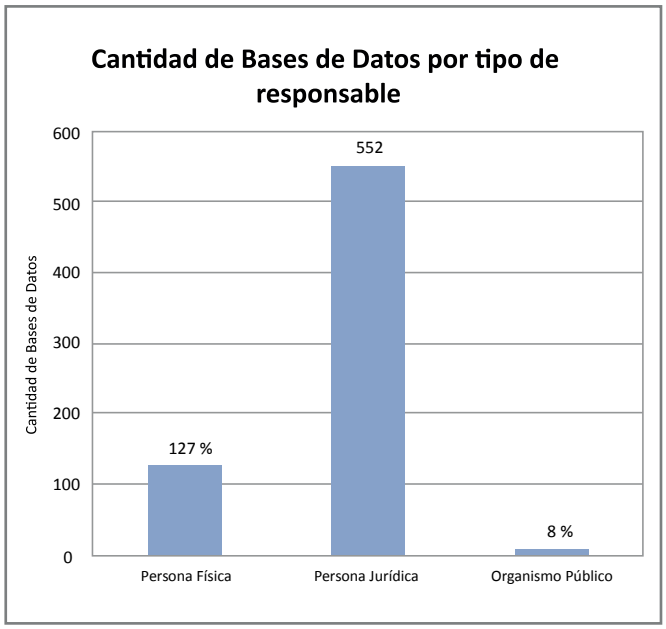
1. Registro de base de datos personales

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 2011.

La tabla y el gráfico siguientes muestran las cantidades de base de datos según tipo de responsable presentados ante la URCDP durante el año 2011.

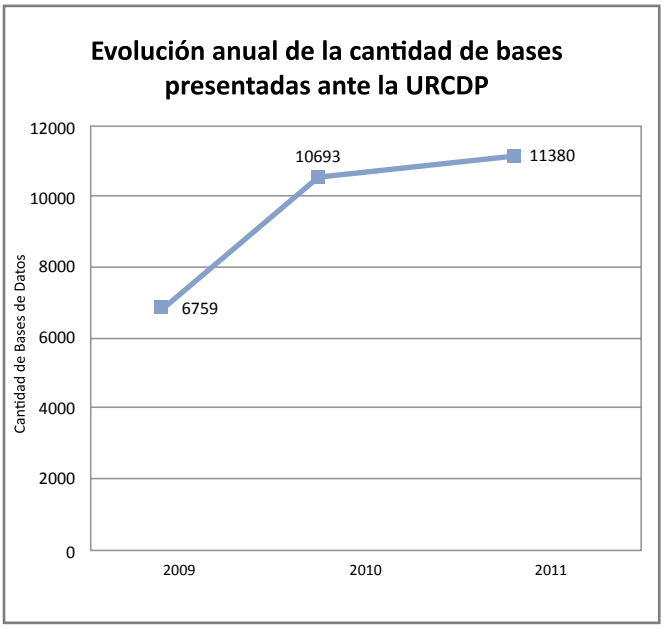
Año 2011

Tipo de responsable	Cantidad de Bases de Datos	Cantidad de Responsables
Personas físicas	127	110
Personas Jurídicas	552	263
Organismos públicos	8	4
Totales	687	377

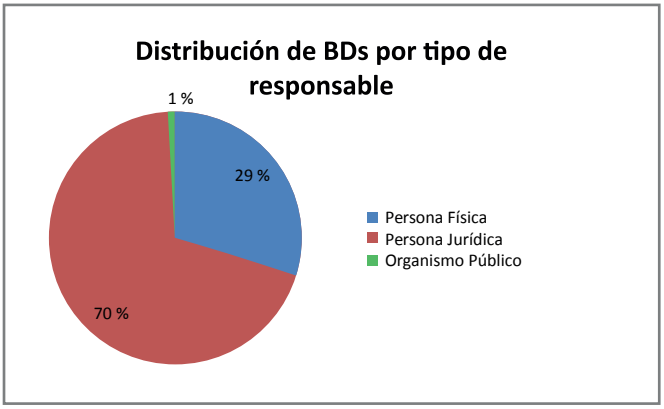


Al igual que años anteriores se observa una fuerte adhesión por parte de las personas jurídicas lo que muestra, por parte de las empresas privadas, voluntad de cumplir con la normativa vigente en cuanto a protección de datos y en particular con la obligación de inscribir las bases de datos personales 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 el año 2011 el ritmo de inscripciones ha decrecido sensiblemente con respecto a años anteriores, debido a que nos encontramos con un muy alto índice de cumplimiento de la normativa vigente.



En el gráfico por tipo de responsable se muestra que la mayoría de las bases de datos presentadas corresponden a personas jurídicas. Resulta significativo evidenciar que las empresas privadas muestran gran interés por cumplir con la normativa vigente en protección de datos personales.



2. Distribución territorial

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

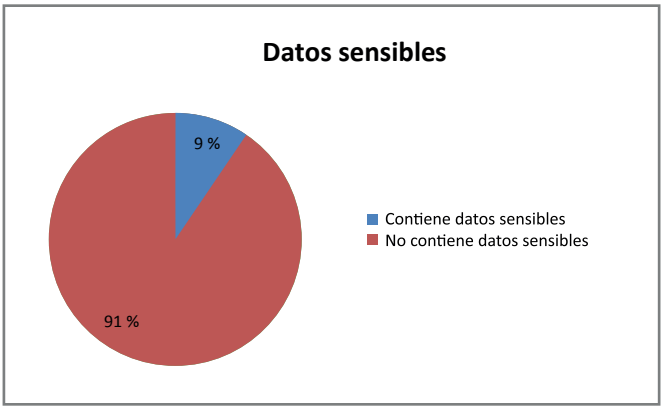
País	Departamento	% distribución BDs 2011
Uruguay		
	Montevideo	67,34
	Salto	9,58
	Canelones	3,63
	Maldonado	3,63
	San José	3,48
	Soriano	2,32
	Colonia	2,03
	Paysandú	1,89
	Lavalleja	0,87
	Cerro Largo	0,58
	Flores	0,29
	Rivera	0,29
	Tacuarembó	0,29
	Durazno	0,15
	Treinta y Tres	0,15
	Rocha	0,00
	Florida	0,00
	Río Negro	0,00
	Artigas	0,00
Otros		3,48

3. Datos sensibles

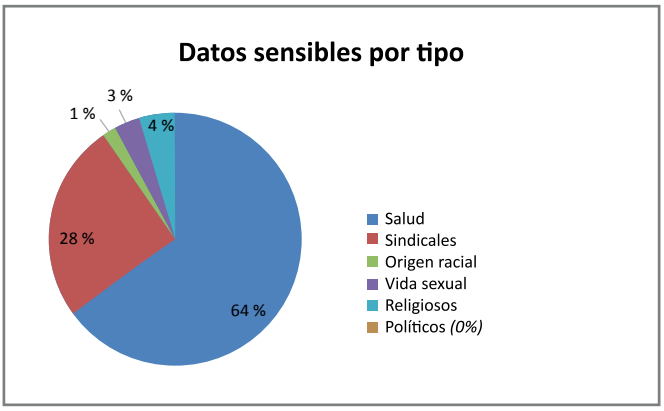
Interesa destacar la existencia de bases de datos que contienen datos sensibles, de acuerdo con la respuesta afirmativa a la pregunta acerca de si guardan datos relacionados con:

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

De los datos obtenidos, se aprecia que alrededor de un 9% de las bases de datos registran datos sensibles. Este porcentaje de bases de datos que contienen datos sensibles con respecto al total se mantiene muy similar a la de los dos años anteriores.



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 a 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 se trata de una clase de datos mantenidos con la finalidad del descuento de la cuota de afiliación al sindicato, entre otros.



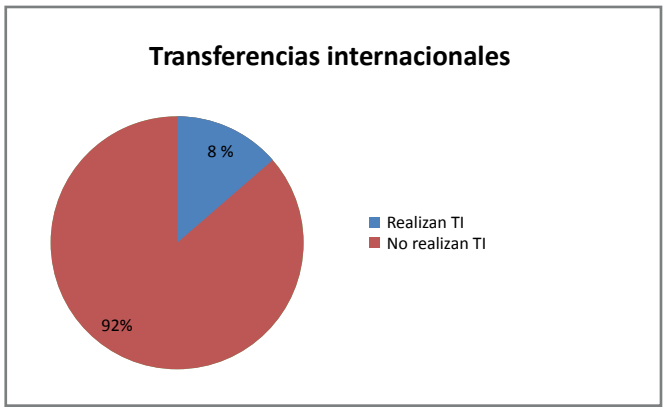
4. Transferencias internacionales

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 2011, aquellas que efectúan transferencias internacionales representan un 8% 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 la 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 éste ostente el primer lugar de todos los países hacia los que se transfieren datos personales.

La tabla presenta un ranking de los 3 países hacia donde se realiza la mayor cantidad de transferencias internacionales de datos desde Uruguay como país de origen:

Puesto	País
1	Argentina
2	España
3	Estados Unidos

5. 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:

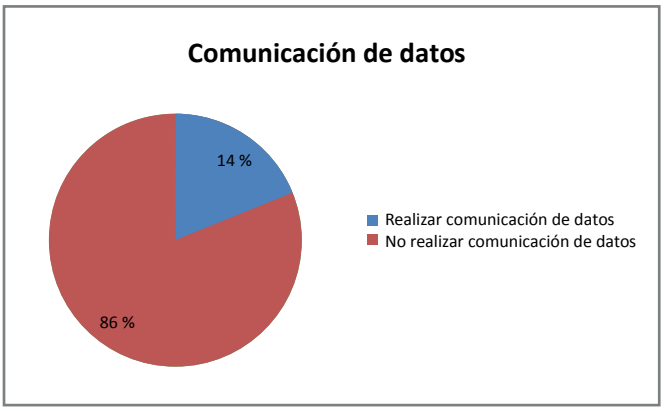
- Datos sensibles
- Datos relativos a la salud
- Datos personales transferidos internacionalmente
- Telecomunicaciones (conservación de los datos de tráfico en las comunicaciones electrónicas)
- Datos de bases de datos con fines de publicidad
- Datos relativos a la actividad comercial o crediticia

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, tales como salud, información crediticia, telecomunicaciones y publicidad:

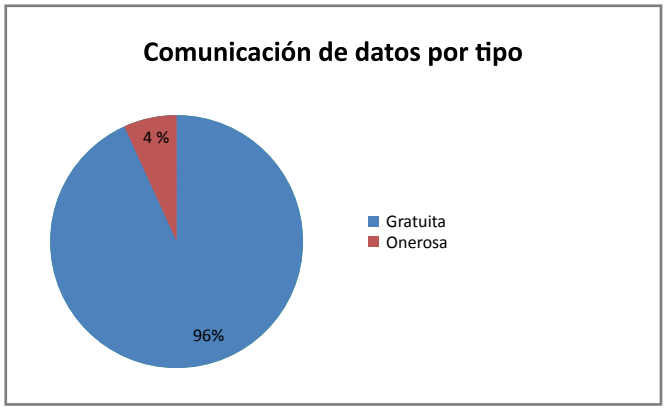
Tipo de dato	% bases en 2011
Datos bancarios	9,75
Salud	6,84
Seguros	3,64
Créditos , préstamos, avales	3,06
Historial de créditos	2,77
Hipotecas	1,75
Telecomunicaciones	1,16
Publicidad	1,02

6. Cesiones o comunicaciones de datos

La proporción de bases de datos de las cuales se realizan cesiones o comunicaciones de datos representa el 14% del total de bases presentadas, tal como se presenta en el siguiente gráfico.



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 formas gratuitas, onerosas o ambas.

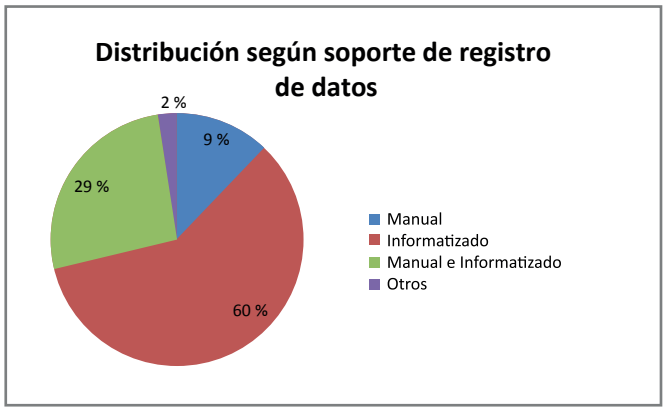


7. Tipo de soporte de registro de datos

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.

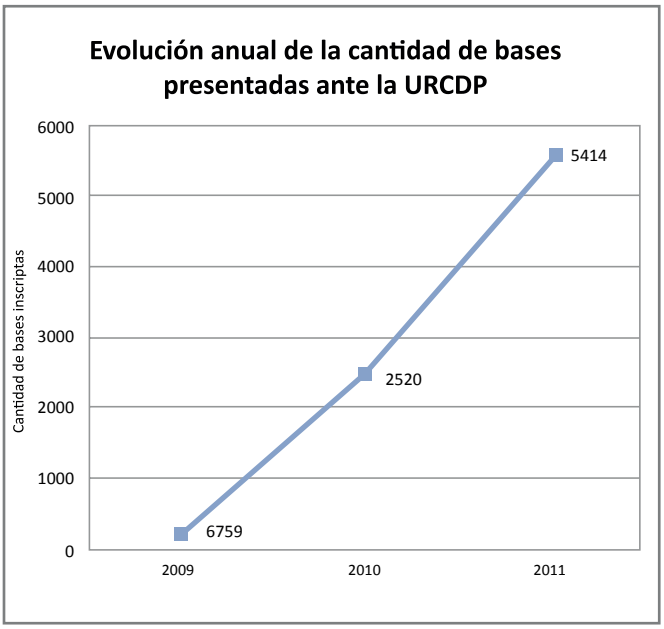


8. Bases de datos inscriptas en la URCDP

Las bases de datos presentadas ante la URCDP pasan por un completo control de cumplimiento de la normativa vigente. El mismo 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.

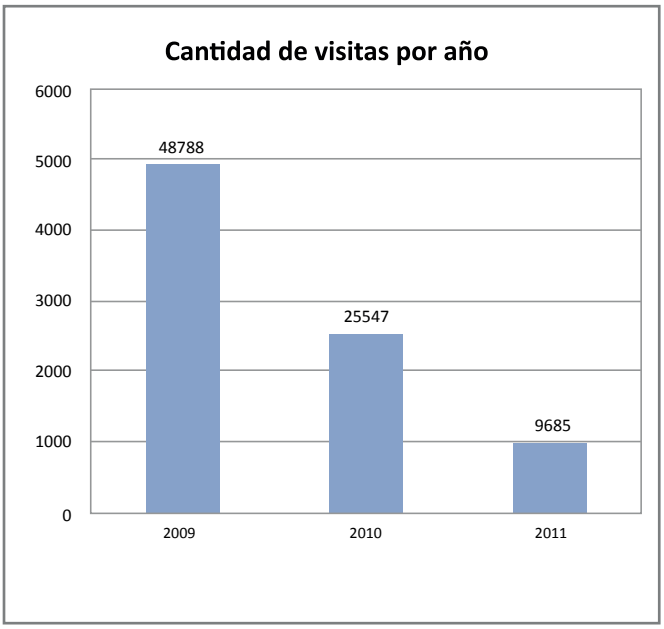
Luego de realizados los controles, el Consejo Ejecutivo de la URCDP dicta la resolución donde se establece que la base de datos queda efectivamente inscripta en el Registro de Bases de datos Personales.

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



9. 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 el año 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.

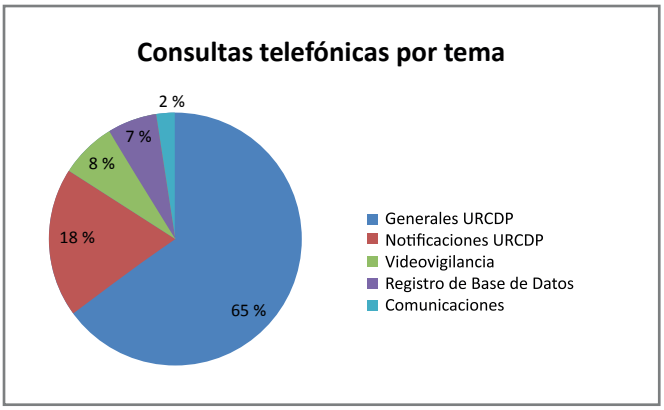


También se han registrado visitas al sitio web de URCDP desde el exterior del país, principalmente España y Argentina. Se constata además, durante los últimos meses del año 2011, visitas desde orígenes remotos tales como Taiwán, Turquía, Rusia, entre otros, lo cual probablemente se deba a la reciente designación de Uruguay como la sede para la sede de la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad para el año 2012.

10. 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.

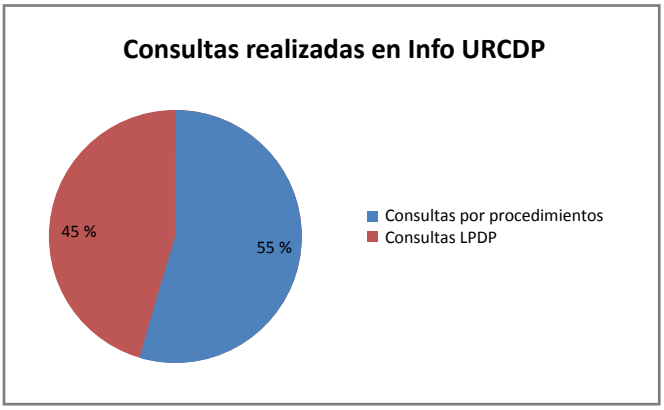
En 2011 se recibieron 1582 consultas telefónicas, las cuales se clasifican por tema en la gráfica siguiente:



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

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.

Durante 2011 se recibieron 268 consultas.



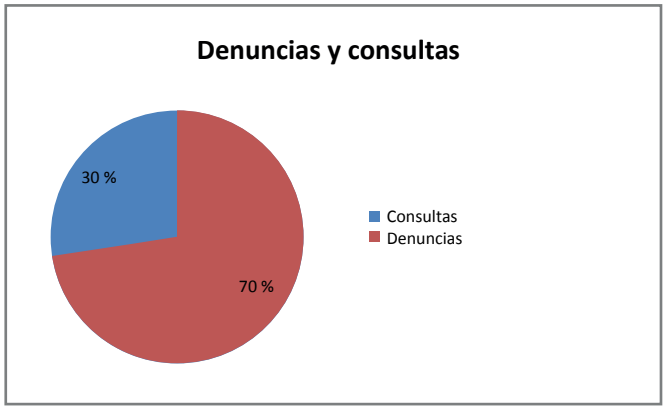
De estas consultas podemos destacar que 132 fueron sobre temas referidos a la Ley de Protección de Datos Personales y 136 fueron sobre procedimientos de inscripción de Base de Datos.

11. 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 el 2011 hubo un aumento significativo en lo que se refiere a consultas y denuncias presentadas por parte de los ciudadanos respeto al año anterior.

En 2011 la Unidad recibió 42 consultas y 106 denuncias.

Los principales motivos de denuncia fueron: Spam, inclusión en base de datos en instituciones crediticias, derecho al olvido debido a la inclusión en un sitio web oficial de una sanción que ya caducó, comunicación de datos personales y videovigilancia.



En lo referente a consultas realizada ante la Unidad, los principales temas fueron: solicitud de datos por parte de un organismo del Estado a particulares, utilización de datos personales por parte de un sindicato, publicación de datos en cartelera de institución de enseñanza, utilización de datos en procedimientos bancarios, transferencia de datos entre organismos del Estado y videovigilancia.

12. Resoluciones sancionadas con apercibimiento o multas

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

Durante el 2011 fueron realizadas 8 observaciones y aplicada una multa.

13. Resoluciones y dictámenes realizados

Durante 2011 se realizó el análisis de expedientes presentados de Bases de Datos, denuncias y consultas.

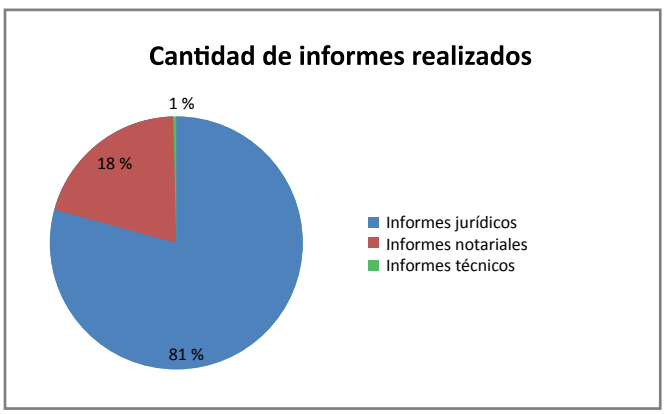
Se expidieron 1734 resoluciones y 32 dictámenes.

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

14. Cantidad de informes realizados

El estudio de los diferentes expedientes con los que cuenta la Unidad ha producido 13529 informes. Estos se dividen en informes jurídicos, informes notariales e informes técnicos.

Como se destaca en el gráfico, se realizaron 11000 informes jurídicos, 2398 notariales y 131 técnicos.



8.

La URCDP ante los nuevos retos en materia de protección de datos

1. Proyectos a realizar en el 2012

Para el año 2012, la URCDP trabajará para concretar los objetivos delineados en el ejercicio anterior y profundizar las líneas fundamentales de su gestión, en todos los casos con vistas al debido respeto de la normativa y los principios en materia de protección de datos personales.

En ese sentido, entre los ejes de su acción ha estado y sigue estando el "generar en la ciudadanía la conciencia de que la protección de datos personales es un derecho ciudadano", por lo cual se proseguirá con el dictado de charlas de difusión sectorial y capacitación para diversos sectores sociales. Con ello se contribuye al conocimiento de los contenidos del derecho y de los medios de su protección, sean administrativos o jurisdiccionales y, más aún, a hacer saber los procedimientos que cada persona o entidad debe asumir para proteger sus propios datos, especialmente al utilizarse medios electrónicos de información y comunicación.

Por otro lado, habiéndose definido un procedimiento inspectivo, procede realizar su práctica, sin perderse de vista que –en todo caso – corresponde mantener una actitud de colaboración hacia el administrado.

Otras actividades

- Organizar la "34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad" a realizarse en octubre de este año en Punta del Este.
- Perfeccionar el expediente electrónico correspondiente al trámite de consultas y denuncias
- Continuar con la mejora de la gestión y el registro de base de datos, en particular la simplificación del procedimiento.

2. Próximos pasos

- Continuar con el funcionamiento permanente de la Unidad, con el apoyo de los servicios de la AGESIC.
- Revisar el proceso registro de bases de datos, con el objetivo de reducir la carga del administrado, propiciando y adoptando las medidas necesarias para ello.
- Profundizar la estrategia de vinculación internacional y nacional, según corresponda, con el fin de:

  a. Concretar la obtención de la Declaración de Adecuación de la Unión Europea.

  b. Ratificación el Convenio 108 y su Protocolo Adicional.

  c. Coordinar, cooperar y participar en grupos de trabajo internacionales.

9.

Anexo normativo

1. Ley N° 18.812 de 23 de setiembre de 2011 . Datos de carácter personal inscriptos en la Central de Riesgos Crediticios del Banco Central del Uruguay.

Artículo 1º. (Registros).- Declárase que la Central de Riesgos Crediticios que administra el Banco Central del Uruguay está regulada por la Ley Nº 18.331, de 11 de agosto de 2008, con las modificaciones y precisiones establecidas en los artículos siguientes.

Será competencia exclusiva del Banco Central del Uruguay la instrumentación y puesta en funcionamiento de dicha base de datos.

Artículo 2º. (Plazo de registro).- Los datos personales relativos a personas físicas podrán permanecer inscriptos en la Central de Riesgos Crediticios a cargo del Banco Central del Uruguay por un plazo máximo de quince años contados a partir del vencimiento de la operación.

Artículo 3º. (Consentimiento de los titulares de datos personales).- El tratamiento de datos personales en la Central de Riesgos Crediticios a cargo del Banco Central del Uruguay no requerirá del previo consentimiento del titular (literales B) y C) del inciso tercero del artículo 9º y literal B) del inciso tercero del artículo 17 de la Ley Nº 18.331, de 11 de agosto de 2008).

Artículo 4º. (Derecho de acceso).- El plazo máximo para proporcionar la información prevista en el artículo 14 de la Ley Nº 18.331, de 11 de agosto de 2008, para el caso de la Central de Riesgos Crediticios a cargo del Banco Central del Uruguay, será de veinte días hábiles.

Artículo 5º. (Responsabilidad).- Las personas físicas y jurídicas del sistema de intermediación financiera que suministren la información contenida en la Central de Riesgos Crediticios a cargo del Banco Central del Uruguay serán las únicas responsables por la veracidad y actualización de la misma.

2. Ley N° 18.849 de 2 de diciembre de 2011 . Registro Nacional de Huellas Genéticas.

Artículo 1º. Créase en el Ministerio del Interior y como dependencia de la División Identificación Criminal de la Dirección Nacional de Policía Técnica, el Registro Nacional de Huellas Genéticas.

El Registro Nacional de Huellas Genéticas conservará y custodiará la información genética obtenida de conformidad con las disposiciones de la presente ley, a efectos de su utilización mediante los procedimientos y con los fines establecidos en la misma.

Artículo 2º. Por huella genética digitalizada se entenderá el registro alfanumérico personal elaborado exclusivamente sobre la base de información que comprenda un mínimo de trece marcadores genéticos validados a nivel internacional, que carezca de asociación directa en la expresión de genes no codificante, que aporte solo información identificatoria y que resulte apto para ser sistematizado y codificado en una base de datos informatizada.

Artículo 3º. El Registro Nacional de Huellas Genéticas tendrá por objeto:

A) Facilitar el esclarecimiento de los hechos sometidos a investigación criminal, particularmente en lo relativo a la individualización de las personas responsables y sobre la base de la identificación de un perfil genético del componente de ácido desoxirribonucleico (ADN) no codificante.

B) Identificar y contribuir a ubicar personas extraviadas, desaparecidas o fallecidas.

C) Asistir a la resolución de controversias judiciales en relación a la identidad de autores o supuestos autores de hechos delictivos.

Artículo 4º. La información contenida en el Registro Nacional de Huellas Genéticas tendrá carácter secreto y confidencial. El Registro no conservará en su poder muestras de ácido desoxirribonucleico (ADN) -codificante y no codificante-, deberá obligatoriamente proceder a la eliminación del material genético y solamente podrá registrar la información que provenga del estudio del mismo.

Solo podrá ser requerida -con fines identificatorios- a la Dirección Nacional de Policía Técnica en el curso de una investigación criminal, por parte de los Jueces competentes, en el mismo régimen del Archivo Dactiloscópico de Identificación Criminal (Ley Nº 4.847, de 11 de mayo de 1914).

Bajo ningún supuesto dicha información podrá ser utilizada como base o fuente de discriminación, estigmatización, vulneración de la dignidad, intimidad, privacidad u honra de persona alguna.

Artículo 5º. La extracción de ácido desoxirribonucleico (ADN) solamente podrá ser realizada cuando la persona lo consienta expresa e inequívocamente y en conocimiento del fin para el que se ha de destinar.

Exceptúanse del principio que se consagra por el inciso precedente pudiendo incorporarse a los registros correspondientes sin consentimiento previo:

A) Las muestras latentes obtenidas de escenas de hechos delictivos, para ser comparadas contra muestras recolectadas de las víctimas, de personas indagadas y con los perfiles almacenados en el Registro Nacional de Huellas Genéticas.

B) Los perfiles genéticos de los procesados por la Justicia competente.

C) La extracción que se disponga por Juez competente.

D) Las muestras correspondientes a los funcionarios del Ministerio del Interior y del Ministerio de Defensa Nacional que determine la reglamentación que dictará el Poder Ejecutivo.

Artículo 6º. El Registro Nacional de Huellas Genéticas constará de tres Secciones:

A) Sección Archivo Genético de Latentes obtenidos a partir de indicios y evidencias recolectados en las escenas de los hechos delictivos, sin identificar, a los fines de posteriores confrontaciones.

B) Sección Archivo Genético de Identificación Criminal en donde estarán almacenados en forma sistematizada y codificada (anónima), los perfiles genéticos de los procesados por la Justicia competente.

C) Sección Archivo Genético de Identificación de los Funcionarios de los Ministerios del Interior y de Defensa Nacional, conforme a lo dispuesto por el artículo 5º literal D) de la presente ley.

Artículo 7º. La Suprema Corte de Justicia a través del Instituto Técnico Forense podrá implementar, en el ámbito de su competencia y conforme a las disposiciones de la presente ley, una base común de datos a cuyos efectos el Ministerio del Interior deberá proporcionar toda la información que le sea solicitada.

Artículo 8º. El Laboratorio Biológico de la Dirección Nacional de Policía Técnica es la autoridad científica competente para efectuar los estudios y análisis de las muestras cuyos resultados serán integrados al Registro Nacional de Huellas Genéticas de la División Identificación Criminal.

Artículo 9º. El Poder Ejecutivo, conforme a las disposiciones de la presente ley, reglamentará las prioridades de toma de muestras y procesamiento de ácido desoxirribonucleico (ADN) no codificante con fines exclusivos de identificación criminal, de acuerdo con sus planificaciones estratégicas y recursos materiales y humanos.

Artículo 10. Por razones de interés general, la Dirección Nacional de Policía Técnica, como único organismo autorizado, previa orden de Juez competente, podrá intercambiar datos de su Registro Nacional de Huellas Genéticas con otros organismos internacionales que actúen en el mismo ámbito y con iguales fines de investigación criminalística. Se actuará bajo el mismo régimen empleado para las huellas dactilares contenidas en su Archivo Dactiloscópico de Identificación Criminal (Ley Nº 4.847, de 11 de mayo de 1914), siempre que dicha información recaiga sobre personas con sentencia de condena pasada en autoridad de cosa juzgada.

Artículo 11. El Poder Ejecutivo reglamentará, previo informe de la Dirección Nacional de Policía Técnica, la creación o modificación orgánica de los Departamentos o Secciones necesarios para la organización y funcionamiento del Registro Nacional de Huellas Genéticas, en su División Identificación Criminal, que aseguren el cumplimiento de sus cometidos técnicos y administrativos.

Artículo 12. El Poder Ejecutivo reglamentará la presente ley dentro de los noventa días de su promulgación.

info@datospersonales.gub.uy
www.datospersonales.com.uy

Andes N° 1365 piso 8, Montevideo, Uruguay
(+598) 2 901 2929 interno 1352