Principios Nacionales e Internacionales en el marco de la Protección de Datos Personales. Deficiencias. Recomendaciones.

María Eugenia Piccirilli[1] con colaboración del Dr. Eduardo Molina Quiroga[2], en el marco del proyecto UBACYT "Tensiones que genera la aplicación de las Tecnologías de la Información y las Comunicaciones (TICs) y los derechos a la protección de datos personales, intimidad e imagen".

1 Becaria UBACYT
eugenia.piccirilli@hotmail.com

2 Director del proyecto UBACYT

Abstract. Personal data is usually given in everyday situations. This paper will analyze if Argentina has an efficient legislation that protects the right to privacy, honor and intimacy. Moreover it will review the most important international foundations for gathering information without infringing these rights. Finally it will suggest some guidelines to improve the existing legislation.

Keywords: Personal data, Argentina, OEA, privacy, intimacy

Introducción. Prácticamente todos los días brindamos nuestros datos personales. El presente trabajo analizará si Argentina posee una legislación eficiente a la hora de proteger los derechos a la privacidad, honor, imagen e intimidad. Asimismo se evaluarán los principios internacionales para la recolección y tratamiento de datos. Finalmente recomendaremos algunas pautas para sortear las deficiencias legales.

Palabras claves: Datos Personales, Argentina, OEA, privacidad, intimidad.

adfa, p. 1, 2011.

1 Introducción

Cotidianamente brindamos nuestros datos personales, en ocasiones otorgando nuestra aquiescencia y otras veces sin tener un real conocimiento de ello.

Lo cierto es que son muchas las oportunidades en las que resulta inevitable proporcionar nuestra información (Renovación de nuestro DNI, viajes internacionales y de cabotaje, obtención de tarjeta SUBE, solicitud de beneficios sociales, controles impositivos, ingreso a un edificio que detenta extrema seguridad, entre otros).

En primer lugar los datos aislados parecieran ser innocuos, no obstante encierran potenciales conjeturas sobre cada uno de nosotros que pueden proporcionar distintos perfiles sobre nuestro comportamiento. Como consecuencia debemos indagar sobre la existencia o no de legislación eficiente que proteja nuestros datos personales, que vede su utilización ilegítima, excesiva, abusiva.

La ley 25.326 (sancionada y promulgada en el mes de octubre de 2000) sobre Protección de Datos Personales en Argentina establece una serie de principios y pautas para la recolección, cesión y transferencia de los datos personales con el fin de proteger al titular de los mismos, recogiendo los principios de la Directiva 95/46/CE de la Unión Europea. Sin embargo presenta algunas deficiencias que serán analizadas a lo largo de este trabajo.

Igual tarea ha desarrollado la Organización de los Estados Americanos con el objetivo de recomendar y hallar la armonización de las legislaciones nacionales.

Es importante remarcar que el derecho de acceso a la información y protección de datos personales está intrínsecamente relacionado con otros derechos reconocidos no sólo constitucionalmente sino internacionalmente como derechos humanos: libertad de expresión, educación, libre asociación, honor, imagen, privacidad, intimidad, identidad, verdad (Basterra Marcela, 2002). No deviene casual que muchas de estas prerrogativas sean pilares fundamentales del sistema democrático "(…) *la sociedad contemporánea respira a través de la información y de la comunicación, de modo tal que en un país donde rige ostensiblemente el dogma de la soberanía del pueblo, la censura no es solamente un peligro, sino un absurdo inmenso*" (Rodríguez María Belén c. Google Inc. s/ daños y perjuicios, Corte Suprema de la Nación Argentina, 28 de Octubre de 2014). Como consecuencia resulta de enorme trascendencia analizar cuáles son los principios que los protegen y de qué manera pueden ser compatibilizados y armonizados con el fin de que unos no excluyan a otros.

Como corolario formularemos recomendaciones a fin de forjar una efectiva protección de los derechos humanos reconocidos.

2 ¿Qué entendemos por datos personales?

La "palabra "dato" proviene del latín datum y significa "dado". Ello se relaciona generalmente con algo que se nos proporciona a fin de conocer otra cosa, "aquello que nos lleva a saber, constituyendo, por tanto, un "vehículo" para acceder al conocimiento" (Peyrano Guillermo, 2004).

A primera vista resulta verosímil enlazar el concepto de "datos personales" con elementos que identifican al individuo en una sociedad: DNI, nombre, apellido, fecha de nacimiento, CUIT/CUIL, estado civil, profesión, teléfono, correo electrónico.

Es indudable que la noción de datos personales contempla un espectro mucho más amplio y no sólo se limita a los datos que podríamos colocar en un simple formulario sino que debemos incluir fotografías, imágenes[i], filmaciones, grabaciones de voz, datos biométricos[ii] (huellas digitales, retina, iris, patrones faciales), comunicaciones realizadas, geolocalizaciones (Ej. GPS, registros satelitales).

Por otro lado la Ley 25.326 define en su artículo 2° a los datos personales como: "*Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables*", es decir todo tipo de elementos que permitan que se identifique a una persona de manera directa o indirecta.

Lo cierto es que a partir de diversos datos personales recabados es posible crear un perfil de la persona: "*incluyendo estado de salud, opiniones políticas y religiosas, asociaciones, interacciones e intereses, revelando tanto o más detalle que el que podría apreciarse a partir del contenido de las comunicaciones (…)"Comunicaciones abarca las actividades, interacciones y transacciones transmitidas por medios electrónicos, tales como el contenido, la identidad de las partes, información de rastreo de ubicación incluyendo direcciones IP, momento y duración de las comunicaciones, e identificadores de los equipos utilizados."* (Principios Internacionales sobre la aplicación de los Derechos Humanos a la vigilancia de las comunicaciones, 2014).

Ahora bien, no sólo debemos entender como derecho a la protección del dato personal en sí mismo sino que es menester concebirlo como elemento constituyente de la autodeterminación informativa: "*El control de la información personal está relacionado con el concepto de autonomía individual para decidir, hasta cierto límite, cuándo y qué información referida a una persona puede ser objeto de procesamiento automatizado, por lo que también se ha denominado a la protección del dato personal, autodeterminación informativa, e incluso libertad informática*."(Molina Quiroga Eduardo – Altmark, 2012)

El concepto de autodeterminación informativa converge con el derecho a la privacidad, a la autonomía individual, al acceso de información, al derecho de rectificación, supresión y actualización (Molina Quiroga Eduardo, 200). Es el derecho del individuo a elegir qué tipo y cantidad de su información personal puede ser procesada por un tercero "*El derecho de autodeterminación informativa consiste en la posibilidad que tiene el titular de los datos personales de controlar quiénes serán destinatarios de éstos y qué uso les darán, y se ejercita genéricamente a través de los derechos de acceso, rectificación y cancelación."* (Bazán Victor, 2005).

Nuestra Corte Suprema de Justicia ha resuelto en concordancia en "Urteaga, Facundo R. v Estado Mayor Conjunto de las Fuerzas Armadas s/amparo ley 16986 ", sent. del 15/10/1998, voto del juez Fayt- *"la protección legal que establece el hábeas data se dirige a que el particular interesado tenga la posibilidad de controlar la veracidad de la información y el uso que de ella se haga. En tal sentido, este derecho forma parte de la vida privada y se trata, como el honor y la propia imagen, de uno de los bienes que integran la personalidad. El señorío del hombre sobre sí se extiende a los datos sobre sus hábitos y costumbres, su sistema de valores y de creencias, su patrimonio, sus relaciones familiares, económicas y sociales, respecto de todo lo cual tiene derecho a la autodeterminación informativa"*.

Como consecuencia, en virtud de la amplia gama de elementos que encierra la noción de "dato personal" y "autodeterminación informativa" es que resulta trascendental analizar la normativa que lo regula y los principios rectores tanto a nivel nacional como internacional.

3 Principios y pautas para la recolección de datos personales – ley 25.326. Deficiencias.

En primer lugar corresponde analizar el contexto sancionatorio de la ley 25.326 que comienza con un proyecto presentado por el senador Eduardo Menem y girado luego a la Cámara de Diputados, siendo finalmente sancionado por la Cámara de Senadores en Octubre de 2000 y promulgado por el Poder Ejecutivo en dicho mes.

En el marco del tratamiento del proyecto de ley se suscitaron oposiciones de algunos senadores en torno al artículo 7 que prohíbe la recolección de datos sensibles pero luego introduce ciertas excepciones que revierten la regla general. Ello es tan sólo una aproximación que permite vislumbrar las deficiencias de la ley 25.326 que desde los comienzos encierra una normativa contemplativa de un sinnúmero de excepciones que desplazan las pautas primordiales (Fernández Delpech Horacio, 2003).

Ahora corresponde que nos adentremos en los principios y pautas establecidos por la Ley de Protección de Datos Personales Argentina (25.326):

Licitud: con el objetivo de que la recolección de datos personales devenga en lícita las bases de datos que los recopilen, sean públicas o privadas, deberán estar debidamente inscriptas (Art 3 Ley 25.326). La Dirección Nacional de Protección de Datos Personales es la autoridad de aplicación de la Ley 25.326 y es la encargada de procesar y conceder las inscripciones solicitadas[iii].

Finalidad: el motivo de la recolección de datos e inscripción de las bases no debe ser contraria a la ley ni a la moral pública (Art. 3 Ley 25.326). Lo cierto es que el

ordenamiento jurídico argentino repudia los actos que contraríen la ley, las buenas costumbres y la moral pública (art 953, 1047, 1071, 1501 Código Civil, entre otros)

Calidad del dato: los datos recolectados deben tener las siguientes características: ciertos, adecuados, pertinentes y no excesivos (Art 4 Ley 25.326). Ello significa que no podrán ser falsos y/o inexactos, deberán ser adecuados, pertinentes en concordancia con el fin para el cual han sido recolectados y ajustados estrictamente a lo necesario. Es decir que el dato debe expresar la realidad de la información del titular: "*efectivamente representan la realidad cuyo conocimiento supuestamente proporcionan*" (Peyrano Guillermo, 2006).

Por otro lado no sólo deben ser ciertos al momento de recogerse sino que la normativa también requiere su actualización y posterior sustitución o supresión ante la inexactitud de los mismos.

Asimismo los datos recolectados son válidos exclusivamente para la finalidad para la cual han sido recogidos y no para otras.

La Ley encomienda en su artículo 4° inc 7 la destrucción de los datos personales cuando haya cesado la necesidad y pertinencia correspondiente a los fines que originaron la recolección[iv]. El problema que se suscita aquí es que habitualmente, a medida que los servidores que almacenan los datos alcanzan una mayor capacidad, la destrucción legal no se convierte en realidad lo que sugiere cantidades inimaginables de datos recolectados lícitamente pero que han sido conservados contrariando la ley. Esto conlleva una deficiencia en la ley dado que habilita a retener información ilícitamente, por ello resulta importante ejercer un debido control sobre la duración en el almacenamiento de los datos.

Consentimiento: Si bien el art. 5 de la ley esgrime como regla general el "libre, expreso e informado" consentimiento del titular a fin de obtener sus datos personales, la normativa brilla por sus excepciones. Lo cierto es que se excluye la necesidad del consentimiento cuando los datos provengan de fuentes de acceso público irrestricto (en el art 3 de la ley 1845 de CABA se define como: "*boletines, diarios o repertorios oficiales, los medios de comunicación escritos, las guías telefónicas en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección o cualquier otro dato que indique de su pertenencia al grupo*"), cuando sean recolectadas para el ejercicio de las funciones propias de los poderes del Estado (entendemos que es una excepción tan amplia que llevaría a que todos los organismos estatales recojan los datos personales de los ciudadanos sin que ellos tomen conocimiento y mucho menos presten conformidad, amparándose en sus funciones).

Tampoco se requiere el consentimiento cuando la recolección de datos sea en virtud de una obligación legal. Con respecto a este punto enunciamos a modo ejemplificativo normas que no sólo permiten esto sino que en determinadas circunstancias lo exigen: Ley de Inteligencia Nacional título VI (art 18-22) en lo concerniente a Interceptación y captación de comunicaciones, Ley de Argentina Digital (art 62 inc g, h, i), Ley 19.798 de Telecomunicaciones (especialmente en su art 45 bis) y su reglamentación mediante Decreto 1563/2004, que habilita la intercepción y derivación hacia los diversos poderes del Estado.

Por otro lado en lo referido a los listados que sólo contengan nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio tampoco es necesario el consentimiento del titular. A primera vista este tipo de datos personales parecen comunes, no obstante no debemos subestimarlos dado que con ellos puede tenerse un mapa casi completo del comportamiento de un ciudadano. Es por ello que incluso un número de DNI puede permitir inmiscuirse en la esfera de la privacidad de una persona (del cual podrán desprenderse otros datos como ser: domicilio completo, lugar de trabajo, tenencia de cuentas bancarias, bienes muebles e inmuebles y/o servicios a su nombre, entre otras).

Asimismo el artículo 5° de la ley bajo análisis prevé dos últimas excepciones al consentimiento: cuando deriven de una relación contractual, científica o profesional del titular de los datos resultando necesarios para su desarrollo o cumplimiento; y cuando se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

Cesión y transferencia de datos personales: Con el objetivo de ceder o transferir internacionalmente datos personales recolectados, es fundamental que el titular preste su asentimiento. Sin perjuicio de ello nuevamente encontramos excepciones a la regla general que debilitan el principio general (Art. 11 y 12 de la ley 25.326).

El consentimiento para la cesión o transferencia no es exigido cuando se evidencien los supuestos del art 5° inc 2 de la ley 25.326 que ya hemos analizado, donde se sortea la venia del titular para la recolección de datos. Asimismo no será necesario cuando así lo disponga una ley, cuando la cesión se realice entre dependencias de los órganos estatales (en la medida del cumplimiento de sus competencias). Este segundo supuesto posibilita la adquisición de datos en favor de una entidad distinta a la que los recolectó en primer lugar con una expresa finalidad. Es decir que el ente cesionario de los datos los ha adquirido sin informar al titular, probablemente detentando un propósito distinto al que originó la obtención de los datos por parte del cedente. Entiendo que este punto no solo comprueba una cabal deficiencia en la normativa sino que contraria los principios analizados anteriormente.

Ahora bien, dicha cesión deberá realizarse en la medida de las competencias del receptor de la información. Aunque pareciera ser un límite loable a la cesión no lo es dado que la entidad puede "flexibilizar" sus competencias con el fin de involucrarlas con los datos que desea obtener.

Es en estos casos en donde podemos advertir que dentro de las excepciones al consentimiento puede entrañarse la inobservancia a los parámetros y principios establecidos en la ley 25.326.

De igual manera el consentimiento para ceder los datos personales no es necesario cuando se trate de cuestiones de salud pública, de emergencia o para la realización de estudios epidemiológicos, siempre y cuando la identidad de los titulares de los datos sea debidamente preservada.

Asimismo el art. 11 de la ley bajo análisis autoriza a sortear el avenimiento del titular de los datos cuando "*se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables*". Entendemos que un listado de datos totalmente despojado de su relación con el titular no contraría los principios fundamentales establecidos en la ley, podría utilizarse por ejemplo para realizar estadísticas que no expongan a las personas de manera individual. No obstante ello, si realmente no pudiera vincularse la información a una persona determinada o determinable dejaría entonces de entrañar el real concepto de dato personal definido anteriormente. "*(…) no pueden caber dudas que en los datos personales resulta imposible prescindirse de la persona, no obstante lo cual, el carácter se mantendría en aquellos supuestos en los que si bien la realidad representada por el dato no es una persona, la información puede ser vinculada a la misma por asociación."* (Peyrano Guillermo, 2004)

Por otro lado, con respecto a la transferencia internacional debemos identificar dos variables que existen cuando se realiza la misma: que el país receptor cuente con legislación adecuada en materia de protección de datos, circunstancia en la cual no hay inconveniente alguno (ej. España) y otro que no tenga dicha legislación (ej. Brasil). Para este último caso la ley 25.326 prohíbe la transferencia salvo que: deba realizarse por motivos de cooperación judicial y/o entre organismos de inteligencia para luchar contra el crimen organizado, terrorismo y narcotráfico, cuestiones médicas, asuntos que hayan sido acordados por el país en tratados internacionales, transferencias bancarias. Ello significa que en estos casos no serán requeridos niveles de protección o seguridad, que de acuerdo a la misma ley son los que previenen la adulteración, sustracción, desviación no autorizada de los datos. Entonces cuando la transferencia de este tipo de datos se circunscribe a alguna excepción recién mencionada (destacamos que estaríamos hablando de datos que podrían ser sensibles[v] y de cabal trascendencia), cabe preguntarnos por qué no habría necesidad de requerir estándares de seguri-

dad para este tipo de información en el marco de una transferencia. ¿Acaso no resultan vulnerables los datos sensibles que cruzarían fronteras sin requisitos mínimos que aseguren su integridad e identidad y que justamente por requerirse su transferencia son delicados y significativos y merecen una especial protección?

Creemos que aquí hallamos una gran deficiencia de la ley que podría subsanarse con un mayor control y protección transfronterizo.

Por otro lado el decreto reglamentario de la ley 25.326 (1558/01) también incluye excepciones a la prohibición establecida por la normativa en relación a las transferencias. Ellas son: consentimiento del titular del dato y contrato de transferencia internacional de datos personales. La primera excepción es apropiada dado que el consentimiento del titular debe ser la regla primordial en la cesión y transferencia de datos personales. Con respecto a la segunda entendemos que una vez más las particularidades presiden la ley bajo análisis y dejan de lado la pauta general.

Información: El artículo 6 de la ley 25.326 dispone el deber de información ante el titular de los datos al momento de recabarlos. Deberá indicarse la finalidad de la recolección, la base de datos inscripta identificando la identidad y domicilio del responsable, carácter obligatorio o facultativo de facilitar los datos y las consecuencias de hacerlo de manera falsa o inexacta.

También deberá informarse al titular sobre su derecho de acceso, rectificación y supresión de datos.

Lo interesante del principio de información es que sin éste el derecho de acceso, incluso la propia protección de datos personales, resulta utópico. En otras palabras, si bien la ley establece una consulta pública y gratuita de los datos recolectados, lo cierto es que si el titular no cuenta con la información adecuada sobre qué bases poseen sus datos, y la identificación de sus responsables, no tiene posibilidad alguna de solicitar, ya sea ante la propia base o ante la Dirección Nacional de Protección de Datos Personales, el acceso a los mismos para así poder evaluar si los registrados reúnen las características de calidad (si son adecuados, exactos, pertinentes, no exceden la finalidad con la cual se recolectaron): "*Si un ciudadano no tiene información sobre quién ha obtenido información sobre él, qué tipo de información y con qué medios la ha obtenido, ya no podrá participar en la vida pública sin miedo*" (Sentencia de 15/12/1983 Tribunal Constitucional Alemán. Ref. 1 BvR 209/83)

Recordemos el concepto de autodeterminación informativa esbozado anteriormente que implica que sin la información necesaria el titular no solo está vedado de ejercer su derecho de rectificación o supresión sino que resulta menoscabado en su derecho a la autonomía individual: "*El que no pueda percibir con seguridad suficiente qué in-*

formaciones relativas a él son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse sustancialmente cohibido en su libertad de planificar o decidir por autodeterminación."(Molina Quiroga Eduardo – Altmark, 2012)

Insistimos, sin tener la debida información la posibilidad de ejercer los derechos que propugna la ley 25.326 y el artículo 43 de nuestra Carta Magna (acceso, rectificación, supresión) resulta casi imposible. Es por ello que el derecho de información es esencial para la protección de los datos personales, de la autonomía individual (art. 19 Constitución Nacional), de la privacidad, intimidad, en fin: de la autodeterminación informativa.

El artículo 15 de la ley de Protección de Datos Personales califica a la información que deberá proveer el responsable de la base de datos al titular como "*clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular*"

Es a raíz de dicha información que el titular posee las herramientas necesarias para ejercer realmente su autonomía individual, el derecho de rectificación, supresión, actualización, contemplados tanto a nivel constitucional como a nivel legal. En el supuesto caso en el que el titular requiera por ejemplo la rectificación y el responsable no cumpla con su obligación en el plazo de cinco días queda habilitado el titular a la interposición del recurso judicial de hábeas data.

Como si fueran pocas las excepciones que contempla la ley (nos remitimos a las ya analizadas en materia de recolección, cesión y transferencia de datos) en relación al ejercicio de los derechos del titular se plantean las siguientes limitaciones: en función de la protección de la defensa nacional, el orden, seguridad pública o derechos e intereses de terceros "*Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión*"(Art. 17 ley 25.326)

Ahora bien, resulta fundamental recordar que los derechos humanos constitucionalmente reconocidos pueden ser limitados únicamente mediante una ley precisa en virtud del interés general o por razones de utilidad social siempre y cuando el principio de proporcionalidad e idoneidad sea respetado (Molina Quiroga Eduardo – Altmark, 2012).

El artículo recién transcripto permite entonces limitar los derechos humanos sin el requisito de una ley específica, clara y proporcional sino que habilita una restricción mediante la simple decisión fundada de un particular.

Entonces ante esta total deficiencia de la ley 25.326 podemos concluir que permite que el ejercicio de los derechos por parte del titular dependa de las deliberaciones del responsable que recabó los datos y los posee de manera inexacta, falsa o desactualizada.

Sin perjuicio de lo antedicho es posible que en algunos supuestos un organismo estatal tome una decisión en miras de los intereses generales por sobre los individuales pero dicha resolución administrativa será objeto de control y revisión judicial de acuerdo a lo establecido por nuestra propia Corte Suprema de la Nación: "*la forma republicana de gobierno que adoptó la Nación Argentina a través del texto Constitucional requiere de la publicidad de sus actos; sin perjuicio, claro está, de aquellos que resulten de necesaria reserva o secreto, porque se vinculan con la seguridad interior o las relaciones internacionales del Estado, en cuyo caso debe primar la defensa de los intereses generales por sobre los individuales. Situación esta última que corresponde que sea evaluada, por el organismo oficiado, en cada caso concreto. Ello así sin descartar el posterior control judicial si correspondiere y no estuviere inserto en las facultades propias de los otros poderes del Estado y resultaren ajenas a la intervención del Poder Judicial*" (Ganora, Mario Fernando y otra s/ hábeas corpus 16/09/1999, según voto del Dr. Vázquez y Fernández Arias, Elena y otros c. Poggio, José 1960/09/19, Corte Suprema de Justicia de la Nación.)

Como consecuencia y con el fin de garantizar el derecho del titular al acceso, deberá existir fundamentación real y concreta por parte de la entidad que lo restrinja (Basterra Marcela, 2002).

Seguridad y Confidencialidad: la ley de protección de datos personales establece que los responsables de las bases deberán garantizar seguridad y confidencialidad, a fin de evitar adulteraciones, sustracciones, desviaciones o tratamientos no autorizados de los datos. Dichos requisitos son necesarios a la hora de inscribir una base de datos.

En lo concerniente a la confidencialidad es importante destacar que todas las personas que intervengan en el tratamiento de datos están sujetas a un contrato de confidencialidad por tiempo indeterminado[vi].

Por otro lado, en relación a la seguridad requerida la Disposición Nro 11/06 de la Dirección Nacional de Protección de Datos Personales dispone 3 niveles: Básico, Medio y Crítico. Los distintos niveles de seguridad refieren a la protección de distintos tipos de datos personales, es decir: en el nivel Básico se circunscribe a la seguri-

dad de los datos personales en sí, mientras que el nivel Medio apunta a las bases de datos que desarrollen actividades de prestación de servicios en la esfera pública como en la privada. Por último el nivel crítico exige mayores requisitos de seguridad dado que se trata de proteger a los datos sensibles (Art 2 de la ley 25.326: *Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.*). Los distintos niveles requieren mayores mecanismos de seguridad, es decir el Medio deberá contar con los expuestos por la disposición y los referidos al nivel Básico y el nivel Crítico deberá contar con los específicamente detallados pero también con los correspondientes al nivel Medio y Básico.

El concepto de "datos sensibles" mencionado anteriormente ha sido redefinido recientemente por la Organización de los Estados Americanos en el 86° período ordinario de sesiones desarrollado en Río de Janeiro Brasil el 23-27 de marzo de 2015 (Informe del Comité Jurídico Interamericano, 2015). Lo cierto es que resulta ser una noción que depende de su contexto, un dato no es sensible per se pero su uso puede derivar en discriminación afectando el derecho a la igualdad reconocido como un derecho humano, especificado en nuestra Carta Magna en el art 16. Es por ello que merecen un mayor nivel de protección.

El citado informe del Comité Jurídico Interamericano explica: "*La frase "datos personales sensibles" se refiere a una categoría más estrecha que abarca los datos que afectan a los aspectos más íntimos de las personas físicas. Según el contexto cultural, social o político, esta categoría podría abarcar, por ejemplo, datos relacionados con la salud personal, las preferencias sexuales, las creencias religiosas o el origen racial o étnico. En ciertas circunstancias podría considerarse que estos datos merecen protección especial porque, si se manejan o divulgan de manera indebida, podrían conducir a graves perjuicios para la persona o a discriminación ilegítima o arbitraria.*"

Como consecuencia es menester indicar que no hay una categoría específica a la que podamos identificar como dato personal sensible en sí. La doctrina entiende que un dato ordinario puede convertirse en un dato sensible por su uso o tratamiento discriminatorio *"(…) ejemplo muy sencillo: registrar el dato referido a la calidad de fumadora o no de una persona a los fines de destinarle ubicación en un restaurante no es lo mismo que hacerlo en un registro de seguros de vida."* (Travieso Juan Antonio, 2006).

Lo cierto es que la ley 25.326 regula su recolección en su artículo 7 cuando establece que ninguna persona está obligada a proporcionarlos y restringe su tratamiento: al interés general autorizado por una ley, fines científicos y estadísticos (siempre y cuando no puedan identificarse a los titulares).

Es importante comprender que el concepto de "dato sensible" no es estático sino evoluciona en consonancia con las disímiles circunstancias sociales, culturales, de tiempo y lugar.

Autoridad de aplicación: Por otro lado la ley y su reglamentación establecen como autoridad de aplicación a la Dirección Nacional de Protección de Datos Personales, cuyo fin es velar por el cumplimiento de la ley y el resguardo de los derechos del titular. Una de sus atribuciones es la imposición de sanciones a los infractores. Ahora bien, aquí también podemos advertir una gran falencia dado que la DNPDP ha ejercido su potestad primordialmente sobre las bases de datos y responsables privados, haciendo oídos sordos en lo concerniente al ámbito estatal "*En efecto las 137 inspecciones realizadas por la DNPDP entre 2008 y 2012 fueron realizadas a empresas privadas: nunca una dependencia estatal responsable de alguna base de datos fue objeto de una inspección por parte de la DNPDP entre esos años. Es posible verificar (…) en el análisis de las sanciones por violación de la ley impuestas por la DNPDP: las 36 sanciones aplicadas por la DNPDP entre 2005 y 2013 fueron impuestas a entidades privadas"* (Asociación por los derechos civiles, 2014).

Si bien el reglamento de la ley 25.326 (decreto 1558/01) establece que el director del organismo "*ejercerá sus funciones con plena independencia y no estará sujeto a instrucciones*", la realidad pareciera ser otra si analizamos la labor de la DNPDP.

Como corolario el lector puede observar que si bien la ley 25.326 establece principios progresistas y proteccionistas lo cierto es que las excepciones contenidas muchas veces derriban el amparo de los derechos personalísimos, siendo ello una importante deficiencia. De igual manera no sólo la ley en sí misma presenta falencias en relación a su redacción sino que en el marco operativo la autoridad de aplicación contribuye a una insuficiente protección de los derechos del titular.

4 Principios y recomendaciones en el marco de la OEA.

En el mes de octubre de 2011 el CONSEJO PERMANENTE de la Organización de los Estados Americanos, mediante la COMISIÓN DE ASUNTOS JURÍDICOS Y POLÍTICOS dio a conocer un documento presentado por el Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos sobre los principios y recomendaciones respecto de la protección de datos personales.

Recientemente (26 de marzo de 2015) la OEA ha dado a conocer un nuevo informe del Comité Jurídico Interamericano al cual ya hemos hecho referencia. Dicho instrumento no sólo redefine algunos conceptos sino que establece los principios rectores

en el marco de la privacidad y protección de datos personales ampliando lo establecido en el año 2011.

Inmediatamente los estudiaremos a fin de interpretarlos armónicamente con los ya analizados de la normativa local argentina.

En primer lugar el informe aclara que los principios regirán tanto en el ámbito público como privado, al igual que lo establecido en la ley 25.326

Propósitos legítimos y justos: el procesamiento de datos debe ser con fines legítimos y por medios justos y legales, no puede devenir en un delito penal ni contrariar las obligaciones impuestas por las leyes que "*deben respetarse en todo el proceso de recopilación, compilación, almacenamiento, utilización, divulgación y eliminación de datos personales, no solo en el momento de su recopilación.*" (Informe del Comité Jurídico Interamericano, 2015) Podemos asimilar este principio al de licitud y finalidad que establece la ley 25.326.

Con respecto a la legitimidad la OEA lo identifica con el requisito de legalidad es decir que la recopilación y tratamiento de datos deberá realizarse en el marco de una norma fundamental que disponga el consentimiento del titular y una limitación a la obtención de los datos, la cual posee una intrínseca relación con el propósito.

Los medios justos y legales excluyen la recolección de datos por medio de engaños, fraudes o falsas alegaciones. El Informe de la OEA establece de manera acertada que el término de "justicia" es contextual (al igual que el concepto de dato sensible que analizamos anteriormente) y se vincula con los requisitos jurídicos de cada estado y con las expectativas razonables de los titulares de los datos en su relación con el controlador de datos.

Por otro lado el principio del propósito (remitiéndonos al informe presentado por el Consejo Permanente de la OEA en el año 2011) debe ser específico, explícito y legítimo, "*debe ser acorde a las expectativas razonables de la persona afectada en el momento en que se obtuvo u otorgó el consentimiento (…) Para determinar si un nuevo propósito o divulgación es compatible con el propósito original para el cual se obtuvieron los datos, podría ser necesario determinar si el nuevo uso proyectado de los datos personales es justo y legítimo*".

Claridad y Consentimiento: deberán especificarse los fines de la recolección al momento de realizarla y la regla general es el consentimiento del titular para ello.

Este principio tiene relación con la información que debe brindarse al titular, la transparencia que debe reinar en la recolección y en definitiva con la autodeterminación informativa de la persona. Específicamente para que haya transparencia el titular

de los datos debe conocer la identidad del controlador de los mismos, el objetivo de recolección, la forma de almacenamiento y procesamiento de datos, toda transferencia que pueda realizarse, las personas a quienes se podrán revelar los datos, el mecanismo y legislación que protege a los datos del titular, que entidad reguladora autoriza a procesar esos datos. Toda esta información deberá ser brindada al titular de manera clara y sencilla al momento de la recolección (teniendo en cuenta el contexto, la edad y la capacidad del titular), si estos datos fueran otorgados por un tercero el controlador debe hacer saber todo ello al titular en un plazo razonable: "*Sin claridad, el consentimiento de la persona con respecto a la recopilación de los datos no puede ser válido."* (Informe del Comité Jurídico Interamericano, 2015).

Pertinencia y Necesidad: los datos deberán ser "verídicos, pertinentes y necesarios" para los fines expresados en su recopilación. Ello significa que los datos deberán ser ciertos, exactos, actualizados, limitados, relacionados al propósito que motiva la obtención (es lo que en la legislación nacional entendemos como no excesivos) y necesarios, es decir que los datos recabados deben contribuir objetivamente al fin que promueve la recolección.

Es importante destacar que la recolección debe ser proporcional en relación al fin y a la injerencia en la intimidad de la persona.

Uso limitado y retención: los datos deberán conservarse el tiempo estrictamente necesario y deberán utilizarse únicamente para lograr el fin perseguido y de conformidad con la legislación nacional. Recordemos que este principio está reconocido en la ley Argentina dado que prevé la destrucción de los datos cuando cesan los fines que motivaron su recolección.

Deber de confidencialidad: "*Los datos personales no deben divulgarse, ponerse a disposición de terceros ni emplearse para otros propósitos que no sean aquellos para los cuales se obtuvieron, excepto con el conocimiento o consentimiento de la persona en cuestión o bajo autoridad de la ley*" (Informe del Comité Jurídico Interamericano, 2015) Un elemento esencial para la autodeterminación informativa es la confianza del titular en el controlador de datos, la cual está determinada muchas veces por el compromiso de confidencialidad.

Protección y Seguridad: La protección de los datos personales requiere de medidas de seguridad que garanticen la integridad, confidencialidad y disponibilidad de los datos, las cuales dependerán de la sensibilidad de la información. Esto se relaciona totalmente con los principios establecidos en nuestra legislación y la disposición 11/06 de la DNPDP. Debe existir protección contra accesos no autorizados, pérdida, destrucción, uso, alteración o divulgación.

Fidelidad de los datos: Este principio tiene que ver con el ya enunciado respecto de la certeza, exactitud y actualización de los datos. Es importante que la información recabada mantenga su fidelidad a lo largo del período de conservación.

Acceso y Corrección/Supresión/Rectificación: Estos derechos no sólo se reconocen en el marco de la OEA sino que, de acuerdo a lo analizado anteriormente, la legislación argentina también los pregona. El derecho al acceso no ha sido entendido sólo en relación a los datos personales sino que la OEA también ha elaborado una ley modelo para los estados interamericanos sobre el acceso a la información pública en el año 2010, entendiéndola como un fortalecimiento de la democracia (Ley Modelo Interamericana sobre el acceso a la información pública, 2010). Este derecho contempla que cualquier persona pueda solicitar información sobre los datos personales que se han recabado del cual es titular, de cómo y por qué se procesan. Vinculándose con el principio ya expuesto de transparencia, la información brindada al titular debe ser clara, sencilla, comprensible y en un plazo razonable.

A diferencia de la ley 25.326 que dispone que el acceso gratuito (cada seis meses) la OEA establece tanto gratuidad como onerosidad del trámite, siempre y cuando el cargo impuesto no sea excesivo. Queda librada a la interpretación de cada estado qué monto puede resultar excesivo y cual no. Asimismo el estado podrá limitar el número de consultas por año, cuestión que ya ha previsto la ley argentina en su artículo 14.

Al igual que la normativa argentina, la OEA deja abierta la posibilidad de denegar del acceso o corrección siempre y cuando esté dispuesto por la legislación nacional: por ejemplo ilicitud en informar, interferencia con detenciones y prevención de ilícitos, revelación de información confidencial.

Sin perjuicio de ello la OEA reconoce la herramienta judicial del Hábeas Data, contenido en el art. 43 de nuestra Constitución Nacional Argentina. El procedimiento para ejercer estos derechos deberá ser fácil, eficiente y rápido.

Datos personales sensibles: Aquí el informe refiere a las definiciones ya mencionadas a lo largo del presente trabajo indicando que dichos datos deben ser tenidos en cuenta en un contexto determinado y merecen una especial protección junto con medidas de seguridad dado que son susceptibles de causar daños considerables a las personas ante su uso indebido.

Responsabilidad: *"La protección efectiva de los derechos individuales de protección de la privacidad y de los datos se basa tanto en la conducta responsable de los controladores de datos como en las personas y en las autoridades gubernamentales del caso"* (Informe del Comité Jurídico Interamericano, 2015). Lo cierto es que recae sobre el controlador de datos la responsabilidad de demostrar al titular y al resto de las

personas que cumplimenta las directivas que establece la legislación aplicable en materia de protección de datos personales.

Flujo transfronterizo de datos y responsabilidad: El informe encomienda a la cooperación de los Estados Miembros a fin de asegurar la responsabilidad de los controladores de datos por el cumplimiento de los principios enunciados.

La recomendación de la OEA establece que la transferencia internacional de datos deberá realizarse con adecuados niveles de seguridad (de acuerdo a las leyes vigentes), protección y responsabilidad entre los estados o controladores ya sean importadores o exportadores. Dicho principio es asimilable a lo ya analizado por la normativa argentina.

No obstante, de no otorgar un país el mismo nivel de protección legislativo, se podría realizar la transferencia siempre y cuando reine el consentimiento de la persona afectada, la misma sea necesaria y en beneficio de la persona, cuando sea imprescindible para evitar un daño sustancial o la muerte de la persona o un tercero, para proteger el interés público o el exportador se responsabilice por la protección de los datos.

Publicidad de las excepciones: Si los estados establecieran en su legislación excepciones a los principios mencionados, por razones de soberanía nacional, seguridad interna o externa, combate a la criminalidad, deberán ponerlas en conocimiento del público. Entendemos que ello es un aspecto fundamental para una efectiva protección de los derechos del titular.

Condiciones para el procesamiento de datos: Finalmente resulta importante remarcar el principio establecido por el informe de la OEA del año 2011 que refería al procesamiento de datos. El instrumento de la OEA identifica al consentimiento libre, inequívoco e informado como condición primordial. Luego entiende como circunstancia para el procesamiento al interés legítimo del controlador o ejercicio legítimo de la actividad de los órganos estatales, el cual siempre deberá ponderarse en relación a los derechos e intereses del titular del dato. Asimismo para el procesamiento de datos el controlador puede utilizar distintos procesadores que podrán ser utilizados por terceros. En virtud de ello es fundamental que el controlador asegure un nivel de protección acorde al que exige la legislación vigente.

Por otro lado mediando una razón legítima o perjuicio sustancial el titular puede objetar el procesamiento de datos. No podrá hacerlo si son necesarios para el cumplimiento de un deber del contralor en el marco de la legislación vigente o si la persona expresó su consentimiento. Ahora bien entendemos que el supuesto del consentimien-

to debiera contemplar la posibilidad de revocarlo, con el fin de luego poder objetar el procesamiento de datos.

5 Recomendaciones

A lo largo de este trabajo hemos podido evidenciar una gran cantidad de principios y recomendaciones progresivas, importantes y autosuficientes.

Sin embargo, muchas veces las excepciones que subyacen terminan consolidándose como la regla general desarticulando el sistema protectorio que proclaman.

Como consecuencia enumeramos algunas posibles recomendaciones que lograrían sortear algunas de las deficiencias de la Ley 25.326 en concordancia con sus principios y en armonía con lo establecido por la OEA.

- Es primordial lograr un tratamiento igualitario respecto de las bases públicas y privadas, (incluso si fuera desigual enfatizando sobre las primeras). Es decir si bien ambos ámbitos son importantes y deben estar regulados y controlados, entendemos que las bases públicas tienden a recabar mayor información (cuantitativa y cualitativa –datos sensibles-) sobre los ciudadanos resultando ser las que detentan mayores excepciones a la hora de requerir el consentimiento del titular. Debemos exhortar a las autoridades de aplicación a que vigoricen el control sobre las bases de datos públicas.
- Resulta fundamental la notificación fehaciente, clara y exacta al titular al momento de recabar los datos: especialmente sobre cuáles han sido recolectados, su finalidad, el procesamiento de los mismos, herramientas administrativas y judiciales para ejercer sus derechos. En los casos en donde el consentimiento no es necesario y se sortea a modo de excepción, sugerimos implementar idéntica notificación luego de la recolección, a fin de que el titular realmente tenga las herramientas y el conocimiento para ejercer los derechos de acceso, supresión, actualización o rectificación. De lo contrario estaríamos reconociendo derechos cuyo ejercicio se torna ilusorio y la autodeterminación informativa sería utópica. "*El que no pueda percibir con seguridad suficiente qué informaciones relativas a él son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse sustancialmente cohibido en su libertad de planificar o decidir por autodeterminación*" (Molina Quiroga Eduardo – Altmark, 2012).
- Asimismo recomendamos que el consentimiento deba solicitarse en todas las circunstancias y no podrá eludirse a excepción de una ley que así lo disponga. Si bien pareciera que tan sólo reiteramos lo dispuesto por la ley 25.326 y la OEA lo cierto es que en dicha normativa la regla general termina por ser la excepción. No deberán admitirse otro tipo de resoluciones, decretos o decisiones que limiten este requisito.
- Es menester contar con una autoridad competente que sea completamente independiente, imparcial y cuente con un fuerte empoderamiento a fin de ejercer un real e integral control sobre las bases, sus responsables, los procedimientos de recolección,

tratamiento y conservación. La misma deberá concientizar al titular de sus derechos, deberá informar y brindar asesoramiento a fin de que pueda ejercer su derecho de autodeterminación informativa.

- Destrucción datos: recomendamos la realización de controles periódicos por parte de la autoridad de aplicación que certifique la vigencia de la finalidad que permitió la recolección y analice si debe procederse a la destrucción de los datos o es factible que subsistan por un tiempo mayor.
- Sugerimos arbitrar un sistema de supervisión pública en el cual intervengan los propios ciudadanos a fin de consolidar la transparencia en el acceso y procesamiento de datos, fortaleciendo la democracia. Ello podrá realizarse mediante el mecanismo de consulta popular o programas impulsados por la autoridad competente a fin de requerir comunicaciones periódicas de los responsables, por ejemplo sobre el tratamiento de datos.
- Es importante reforzar el control judicial suficiente (Ganora, Mario Fernando y otra s/ hábeas corpus 16/09/1999 y Fernández Arias, Elena y otros c. Poggio, José 1960/09/19, CSJN) a modo de revisión jurídica respecto de la recolección y tratamiento de los datos personales con el fin de ponderar su utilización y la protección de los derechos fundamentales del individuo en casos donde el titular no haya podido ejercer sus prerrogativas (Basterra Marcela, 2002).
- En concordancia con el control judicial, deviene esencial la primacía del debido proceso y el adecuado derecho de defensa a fin de posibilitar el correcto ejercicio de los derechos del titular.
- Si fuera estrictamente necesaria la intercepción de comunicaciones y demás mecanismos que vulneran totalmente los Derechos Humanos (privacidad, intimidad, imagen, honor), sólo deberán proceder mediante orden judicial fundada, es decir no podría realizarse mediante un decreto ni resolución administrativa y su objetivo no deberá extralimitarse más allá de la lucha contra los delitos. Continuando con dicha línea de pensamiento, es importante recordar que el art 18 de la ley 19.798: "*La correspondencia de telecomunicaciones es inviolable. Su* ***interceptación solo procederá a requerimiento de juez competente."*** *El destacado me pertenece.*

En este último caso deberá disponerse la notificación al titular siempre y cuando el juez no disponga lo contrario mediante resolución fundada.

- Los mecanismos que establezcan posibles limitaciones a los derechos humanos deberán ser mediante ley"*(…) sólo la ley puede justificar la intromisión en la vida privada de una persona, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen"* (Halabi, Ernesto c/ P.E.N. - ley 25.873 dto. 1563/04 s/ amparo ley 16.986) y deberán ser de interpretación restrictiva, así lo entiende nuestra Corte Suprema de la Nación cuando dice: "*Que en esa línea esta Corte ha requerido que toda restricción, sanción o limitación a la libertad de expresión debe ser de interpretación restrictiva (conf. doctrina de Fallos: 316:1623) y que toda censura previa que sobre ella se ejerza padece una fuerte presunción de inconstitucionalidad*." (Rodríguez, María Belén c/ Google Inc. s/ daños y perjuicios), es decir que ante la duda deberá estarse por la no limitación. Por otro lado, las disposiciones legales que establezcan limitaciones deberán ser sometidas a revisiones periódicas por la autoridad competen-

te o el poder judicial a fin de evitar lesiones a los derechos fundamentales (Molina Quiroga Eduardo – Altmark, 2012).

Las leyes que así lo dispongan deberán ser precisas, específicas y no podrán contener términos ambiguos ni oscuros:[1] *"(…) para restringir válidamente la inviolabilidad de la correspondencia, supuesto que cabe evidentemente extender al presente, se requiere: a) que haya sido dictada una ley que determine los "casos" y los "justificativos" en que podrá procederse a tomar conocimiento del contenido de dicha correspondencia; b) que la ley esté fundada en la existencia de un sustancial o importante objetivo del Estado, desvinculado de la supresión de la inviolabilidad de la correspondencia epistolar y de la libertad de expresión; c) que la aludida restricción resulte un medio compatible con el fin legítimo propuesto y d) que dicho medio no sea más extenso que lo indispensable para el aludido logro. A su vez, fines y medios deberán sopesarse con arreglo a la interferencia que pudiesen producir en otros intereses concurrentes." (*Halabi, Ernesto c/ P.E.N. - ley 25.873 dto. 1563/04 s/ amparo ley 16.986.). En el hipotético caso en que la legislación se ampare en términos como "interés general", "seguridad nacional" u "orden público" es importante recordar que el Estado posee como limitación el respeto de los derechos fundamentales de los individuos: *"la Corte Interamericana de Derechos Humanos tiene dicho que el poder del Estado para garantizar la seguridad y mantener el orden público no es ilimitado, sino que "su actuación está condicionada por el respeto de los derechos fundamentales de los individuos que se encuentren bajo su jurisdicción y a la observación de los procedimientos conforme a Derecho (...) con estricta sujeción a los procedimientos objetivamente definidos en la misma"* (Halabi, Ernesto c/ P.E.N. - ley 25.873 dto. 1563/04 s/ amparo ley 16.986 y Corte Interamericana de Derechos Humanos. Serie C, n° 100, caso "Bulacio v. Argentina", sentencia del 18 de septiembre de 2003.)

Asimismo la limitación a los derechos fundamentales deberá ser proporcional al interés perseguido. Es decir que no podrá exceder lo estrictamente necesario a fin de lograr el objetivo propuesto.

- La denegación al ejercicio del derecho de acceso, supresión, actualización o rectificación no podrá limitarse por una decisión fundada del responsable de la base de datos, deberá ser limitada por una ley específica o por una autoridad judicial mediante resolución fundada. Resultaría inconcebible que la persona que detenta los datos de otro ciudadano pueda denegar el ejercicio de sus derechos cuando es el propio controlador quien posee datos inexactos, falsos o desactualizados.
- Deviene necesario compatibilizar los derechos de raigambre constitucional y ante una posible colisión deberá someterse directamente al fuero judicial a fin de efectuarse una ponderación de los mismos, es decir establecer una "jerarquía axiológica móvil" (Gil Dominguez Andrés, 2011) en el caso concreto. Ello significa otorgar a un derecho una primacía temporaria y sólo para ese caso con el fin de resolver la controversia.

- Para el supuesto en el que la transferencia se prohíba si no se evidencian niveles de protección adecuados para los datos, pero sí se permita en razón de cooperación judicial (terrorismo, crimen organizado) deberán igualmente garantizarse parámetros mínimos de seguridad que protejan al dato de adulteraciones, sustracciones o desviaciones no autorizadas.

6 Conclusión

A lo largo del presente trabajo hemos analizado los principios y pautas establecidos en el ámbito de la Argentina y la Organización de los Estados Americanos encontrándonos con nociones muy similares.

Es por ello que concluyo que la normativa argentina es progresista y proteccionista.

Sin perjuicio hallamos grandes deficiencias, desde la letra pura de la ley que contempla una gran cantidad de excepciones que derriban la regla general como desde el funcionamiento real del órgano encargado de velar por los derechos personalísimos de los titulares de los datos personales.

Si bien aún nos queda un largo camino por recorrer la ley 25.326 contempla casi todos los principios que recomienda la Organización de los Estados Americanos. Es por ello que resulta importante enriquecer y armonizar la legislación nacional con los principios y recomendaciones internacionales fortaleciendo la cooperación entre estados, unificando y actualizando la protección de los derechos humanos.

Como ya hemos manifestado a lo largo del presente trabajo, en muchas circunstancias la problemática no radica en los principios y derechos reconocidos sino en las excepciones que reinan en la legislación y que permiten avasallar los derechos proclamados.

Deviene fundamental tomar en consideración y realizar una efectiva aplicación de las recomendaciones sugeridas en el presente trabajo con el fin de no tornar ilusoria la protección de los datos personales.

Como conclusión debemos exhortar a los poderes políticos y legislativos a analizar de manera crítica la normativa establecida, teniendo en consideración las prácticas habituales y proyectar una nueva normativa tendiente a zanjar las dificultades, con ayuda de las recomendaciones propuestas en el presente con el fin de enriquecer la legislación nacional y los principios internacionales haciendo efectiva la protección de la autodeterminación informativa.

7 Referencias

1. Asociación por los derechos Civiles (ADC): El Estado recolector – Un estudio sobre la Argentina y los datos personales de los ciudadanos. Disponible en: http://www.adc.org.ar/wp-content/uploads/2014/09/El-estado-recolectorInformeADC.pdf (2014)
2. Basterra, Marcela I: Reconocimiento constitucional del Habeas Data. Publicado en Colección de Análisis Jurisprudencial Derecho Constitucional - Director: Alberto Ricardo Dalla Via, Editorial LA LEY (2002).
3. Bazán Víctor: El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado. Revista Estudios Constitucionales. Disponible en: http://www.redalyc.org/articulo.oa?id=82030204 (2005)
4. Bulacio v. Argentina, Corte Interamericana de Derechos Humanos sentencia del 18 de septiembre de 2003
5. 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, Diario Oficial n° L 281 de 23/11/1995 p. 0031 – 0050, Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML
6. Disposición Nro 11/06 de la Dirección Nacional de Protección de Datos. Disponible en: http://www.jus.gob.ar/media/33445/disp_2006_11.pdf
7. Fernández Arias, Elena y otros c. Poggio, José. CSJN, 1960/09/19
8. Fernández Delpech Horacio: Los datos sensibles en la ley de protección de datos personales. Disponible en: http://www.hfernandezdelpech.com.ar/PUBLICAtrabajosLosDatosSensEnLaLeyProteDatosPer.htm. (2003)
9. Ganora, Mario Fernando y otra s/ hábeas corpus. CSJN 16/09/1999 - (JA 2000-II-43)
10. Gil Dominguez Andrés: Estado Constitucional de Derecho, psicoanálisis y sexualidad. C: Neoconstitucionalismo y ponderación y El Estado Constitucional de Derecho como paradigma constitucional argentino. Ed. Ediar (2011)
11. Halabi, Ernesto c/ P.E.N. - ley 25.873 dto. 1563/04 s/ amparo ley 16.986
12. Informe del Comité Jurídico Interamericano (2015). CJI/doc. 474/15. Disponible en: http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf
13. LEY MODELO INTERAMERICANA SOBRE ACCESO A LA INFORMACIÓN PÚBLICA (2010) Según Resolución AG/RES. 2607 (XL-O/10) Disponible en: http://www.oas.org/es/sla/ddi/docs/AG-RES_2607_XL-O-10_esp.pdf
14. Molina Quiroga Eduardo, Altmark Daniel: Tratado de Derecho Informático. C: Protección de Datos Personales. Ed. La Ley 2012 (2012)
15. Molina Quiroga: Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material, Id Infojus: DACC030027 (2003)

16. Peyrano Guillermo F: Nuevas problemáticas del tratamiento de datos personales. Publicado en LEXIS NEXIS - JURISPRUDENCIA ARGENTINA (JA 2004 II, fásciculo N° 1), Id Infojus: DASF060063 (2004)
17. Peyrano Guillermo F: El tratamiento de datos personales extraídos de informaciones periodísticas, y su acceso a través de Internet. La protección de los datos personales y el derecho a la autodeterminación informativa, ante las nuevas formas de procesar y comunicar la información. Publicado en la obra "Estudios de Derecho - Estudios de Derecho Privado - Estudios de Derecho Público - Derecho Público y Procesal. Editorial Universidad Católica Andrés Bello, Caracas Venezuela (2004)
18. Peyrano Guillermo F: Consolidación de principios para la protección de datos personales y de reglas procesales en la acción de hábeas data: Veracidad exigida a la información y carga de la prueba. Efectos personales de la sentencia. Lexis Nexis-Jurisprudencia Argentina, JA 2006-IV, fascículo Nº7 (2006)
19. Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones Traducción por *Comisión Colombiana de Juristas*, *Access*, *Fundación Karisma*, *Fundación Vía Libre*. Disponible en: https://es.necessaryandproportionate.org/text (2014)
20. Relatorías de libertad de expresión emiten declaración conjunta acerca de internet. R50/11, (2011) Disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=848
21. Resolución OEA/Ser.G CP/CAJP-2921/10 rev.1 corr. 1. Sobre Principios y Recomendaciones respecto de la Protección de Datos Personales (2011) Disponible en: http://www.oas.org/dil/esp/CP-CAJP-2921-10_rev1_corr1_esp.pdf
22. Rodríguez María Belén c. Google Inc. s/ daños y perjuicios, Corte Suprema de la Nación Argentina, 28 de Octubre de 2014. (R. 522. XLIX)
23. Sentencia de 15/12/1983 Tribunal Constitucional Alemán (Ref. 1 BvR 209/83) en las demandas de inconstitucionalidad contra la Ley sobre el recuento de la población, de las profesiones, de las viviendas y de los centros de trabajo (Ley del Censo de 1983) de 25/03/1982 (publicada en el Boletín de Legislación Federal –BGBI- I, pág. 369), el Tribunal Constitucional Federal –Sala Primera- dicto dicha sentencia, con la participación del Presidente Benda y de los Jueces Simón, Hesse, Katzenstein, Niemeyer, Heussner, Niedermaier, Henschel (según extracto publicado por la revista Derecho Público Contemporáneo Nº 7, de la Agrupación de Abogados de la Contraloría General de la República de Colombia, basado en algunas partes de la sentencia traducida por Manuel Daranas, para el Boletín de Jurisprudencia Constitucional Nº 33, de 1984)
24. Travieso, Juan Antonio Moreno, María del Rosario: La protección de los datos personales y de los sensibles en la ley 25.326. Publicado en LA LEY2006-D, 1151 (2006)
25. Urteaga, Facundo R. v Estado Mayor Conjunto de las Fuerzas Armadas s/amparo ley 16986 , sentencia del 15/10/1998, (Voto del Juez Fayt)

8 Notas

[i] El dictamen de la Dirección Nacional de Protección de Datos Personales nro 001/13 estableció que "*La imagen de una persona es un dato personal en tanto es un dato útil para identificarla. Las imágenes digitales de las personas en un sistema fílmico (como serían los sistemas actuales de video vigilancia que se almacenan en un servidor) conforman un banco de datos*" y Disposición nro 10/15 "*Que una imagen o registro fílmico constituyen, a los efectos de la Ley N° 25.326, un dato de carácter personal, en tanto que una persona pueda ser determinada o determinable*." Disponible en http://www.jus.gob.ar/datos-personales/documentacion-y-capacitacion/dictamenes-pdp/d2013.aspx

[ii] El Dictamen N° 16/11 de la Dirección Nacional de Protección de datos personales entiende al dato biométrico como un dato personal y somete su protección a la ley 25.326. Disponible en http://www.jus.gob.ar/datos-personales/documentacion-y-capacitacion/dictamenes-pdp.aspx

[iii] Registro de bases de datos en la DNPDP http://www.jus.gob.ar/datos-personales/areas-de-la-pdp/registro.aspx

[iv] Los requisitos que debe cumplir el procedimiento de destrucción de datos se encuentran en documento que debe detentar el responsable llamado "Manual de Seguridad de Datos Personales". Allí deberá diferenciar la destrucción de datos en formato papel o electrónico. Para ambos deberá incluir los siguientes requisitos: qué sectores serán los responsables, qué métodos se utilizarán y qué constancia deberá emitir si se le solicitara la destrucción a una empresa.

[v] De acuerdo al INFORME DEL COMITÉ JURÍDICO INTERAMERICANO de la OEA redactado el 26 de marzo de 2015. La definición de los datos sensibles no es exacta dado que debe interpretarse en un contexto, la misma "*abarca los datos que afectan a los aspectos más íntimos de las personas físicas. Según el contexto cultural, social o político, esta categoría podría abarcar, por ejemplo, datos relacionados con la salud personal, las preferencias sexuales, las creencias religiosas o el origen racial o étnico.*" Podríamos incluir aquí datos que refieran a imputaciones por delitos, antecedentes penales, investigaciones criminales, entre otros, que merezcan una protección especial debido al perjuicio que pudiera ocasionar su divulgación o uso indebido.

[vi] El convenio de confidencialidad deberá ser firmado por los empleados, terceros u otras personas que accedan a las bases de datos personales.