BASTERRA Marcela, "El consentimiento del afectado en el proceso de tratamiento de datos personales" JA -Lexis Nexis-. Número Especial, 28 de Abril de 2004, p. 6.

El Consentimiento del Afectado en el Proceso de Tratamiento de Datos Personales

Por Marcela I. Basterra

Sumario: I- El consentimiento exigido por la Ley de Protección de Datos Personales y Habeas Data. **II-** Características del Consentimiento en el ámbito de la Protección de Datos Personales **II.1** Libre **II.2** Expreso, por Escrito u otro medio equiparable. **II.2.a** Consentimiento de palabra o verbal **II.2.b** Consentimiento electrónico. **II.2.b.1)** Consentimiento dado a través de firma electrónica **II.2.b.2)** Consentimiento dado a través de correo electrónico. **II.2.c.** Consentimiento del afectado para los tratamientos de *"data mining"* o entrecruzamiento de datos. **II.2.d** Consentimiento Informado. **III.** Excepciones: Casos en los que la ley no exige del Consentimiento del titular para el tratamiento de sus Datos Personales. **III.1** Datos obtenidos de fuentes de acceso público irrestricto. **III.2** Datos recabados para el ejercicio de funciones propias de los poderes del Estado o derivados de una obligación legal. **III.3** Casos específicos exceptuados por la presente ley – nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio. **III.4** Datos que deriven de una relación contractual, científica o profesional. **III.5** Operaciones realizadas por entidades financieras – conforme al artículo 39 de la ley 21.526-. **IV.** Conclusiones

I- El consentimiento exigido por la Ley de Protección de Datos Personales y Habeas Data

El consentimiento exigido por la Ley Argentina de Protección de Datos Personales y Habeas Data, N° 25.326[1] - en adelante LPDP-, para el tratamiento de datos de carácter personal surge con claridad del artículo 5 de la ley es, sin duda, uno de los puntos cardinales de los principios que ordenan la presente normativa.

En materia de protección de datos, se convierte en un elemento esencial el consentimiento del afectado por el tratamiento. Todo Banco o Registro, público o privado, que desee tratar datos de personas físicas o jurídicas, como regla general deberá requerirles previamente su consentimiento para el tratamiento, salvo que los

[1] Sancionada el 04/10/200. Reglamentada por el decreto 1558 del 29/11/2001

datos se encuentren en alguno de los supuestos legales que eximen del mismo. Esto es lo que la Directiva Europea denomina en su sección segunda, artículo 7, legitimación del tratamiento[2], o sea que dicha legitimación va a estar condicionada al consentimiento que se haya prestado para el uso del dato personal.

Si definimos al derecho a la autodeterminación informática como la posibilidad de decidir qué datos queremos que se conozcan de nosotros y qué datos queremos mantener en reserva, protegidos dentro de la esfera del derecho fundamental a la intimidad, parece razonable que se exija tan alto grado de recaudo en materia de consentimiento. Toda vez que al prestar nuestra conformidad para el tratamiento del dato personal estamos eligiendo justamente cuáles son los datos que daremos a conocer y, con ello decidiendo el grado de protección elegido.

En la ley española de Tratamientos de datos personales[3], en el artículo 3 h) define el consentimiento del interesado como toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. Partiendo de esta definición, como contenido mínimo del consentimiento, son distintas las formas del mismo que se exigen en función de los datos objetos del tratamiento.

La ley argentina no contiene una definición sino que establece la ilicitud del tratamiento de datos personales sin consentimiento del interesado, el carácter "informado" del consentimiento conforme al artículo 6 y, taxativamente en cinco incisos detalla las circunstancias en las que no será necesario el consentimiento del titular de los datos.

El artículo 5º de LPDP establece: *"El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, juntamente con las advertencias previstas en el artículo 6º de la presente ley.*

No será necesario el consentimiento cuando:

a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

---

[2] Directiva 95/46/CE

[3] El 29 de octubre de 1992, se promulgó en España la ley Orgánica 5/92 de regulación del Tratamiento Automatizado de Datos de Carácter Personal, la que conocemos como LORTAD. En 1995 la Comunidad Europea asumió la necesidad un marco común para todos los países integrantes de la misma y, con esa finalidad se adoptó la directiva 95/46CE. El 13 de diciembre de 1999 se sanciona la Ley Orgánica de Protección de Datos de Carácter Personal la que deroga y sustituye a la anterior de 1992, cumpliendo con la finalidad de transposición de la Directiva Europea 95/46/CE.

c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

e)Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del art. 39 de la ley 21.526"

La importancia del consentimiento como eje del sistema de protección de los datos personales, ya era reconocido por la jurisprudencia, aún con anterioridad a la sanción de la ley 25.326. En efecto, la Sala D de la Cámara Nacional en lo Civil en el fallo *"Lascano Quintana, Guillermo Víctor c/Organización Veraz S.A. s/amparo"*[4] , ordena a la demandada eliminar información de su banco de datos privado destinado a proveer información a terceros porque carece del consentimiento de la actora a quien no se le solicitó en forma previa, tanto para procesar como para difundir la información. La información de marras se refiere a la calidad de presidente de una sociedad anónima del actor. En su defensa la empresa que comercializa el dato -Veraz- argumenta que aquel fue recogido del Boletín Oficial y luego insertado en el informe comercial de Lascano Quintana. La Cámara entendió que se estaba violando la intimidad de la persona utilizando sus datos personales y su vinculación con una persona jurídica sin su "consentimiento". Con claridad establece que: *"se lo considera un atributo del derecho general de la personalidad, o de un derecho personalísimo en sí mismo; es indudable que cada individuo tiene un poder reconocido, resultante de la noción de autodeterminación (libertad) de decidir él mismo, en primer lugar y ante todo, cuándo y en qué medida pueden ser divulgados lo hechos relativos a su propia existencia; esto se trata de un derecho de "dominio" de los datos personales. Y aún así, si se lo considera dentro de un derecho constitucional de propiedad, bastaría para comprenderlo, el amplio sentido"*

Sin embargo, este precedente en materia de habeas data y consentimiento es revocado por la C.S.J.N, cuando ya estaba sancionada la LPDP, la organización Veraz promueve recurso extraordinario, siendo denegado el mismo, la demandada ocurrió por queja ante la Corte Suprema, que por mayoría declaró procedente el remedio federal y dejó sin efecto la sentencia de cámara. *"Debe rechazarse la acción de habeas data tendiente a suprimir del legajo personal del actor en un banco de datos privado información*

[4] Sentencia de Cámara del 23/2/1999, puede verse en JA, del 20/10/1999
Sentencia de C.S.J.N del 06/03/2001, puede verse en La ley 06/06/2001, pág.5
Véase GOZAINI, Osvaldo,- Comentario al fallo –"El consentimiento para el uso de los datos personales"

relacionada con los juicios seguidos contra la sociedad anónima de la que el mismo es presidente, dado que no medió injerencia desmesurada en su privacidad, ponderada respecto de la finalidad que persigue dicho registro" (del voto del doctor Petracchi que adhiere al voto de la mayoría). *Es improcedente la acción de habeas data tendiente a suprimir del legajo personal del actor en un banco de datos privado información relacionada con los juicios seguidos contra la sociedad anónima de la que el mismo es presidente, si tales datos son verdaderos, no están desactualizados ni revisten carácter discriminatorio, reflejando una circunstancia objetiva que guarda estrecha relación con la finalidad del crédito* (del voto del doctor Boggiano).

Nótese de todos modos que, el fallo de la Corte no desnaturaliza el principio general de la exigencia del consentimiento para el tratamiento personalizado de datos. Sólo que al existir la ley este es un tipo de datos para los que no se necesita consentimiento, puesto que el cargo en una Empresa a nuestro criterio estaría abarcado dentro de la previsión del artículo 5 inc. c) de la ley "ocupación" y en el inciso a) del mismo artículo dado que es un dato extraído del Boletín Oficial, es decir de una fuente de acceso irrestricto al público.

II- Características del Consentimiento en el ámbito de la Protección de Datos Personales

II.1 Libre

El consentimiento a que se refiere el precepto legal es el elemento determinante para que sea lícita la recolección de datos o la fase del tratamiento[5] del dato en el momento en que el consentimiento sea requerido.

Se trata de una declaración de voluntad del titular de un dato de la que en forma inequívoca se infiera que el mismo ha autorizado al tratamiento de un dato personal.

Cuando la ley exige como requisito que el consentimiento sea "libre" consideramos siguiendo a Peyrano[6] que claramente se está refiriendo a los principios generales del derecho que rigen en materia de consentimiento. Como todo acto voluntario deberá ser

---

La ley, Suplemento de Derecho Constitucional, 15 de junio de 2001, pág. 1

[5] Entiéndase por "Tratamiento de datos", tal como surge de la definición del artículo 2° de la LPDP, cuarta definición a *"Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y, en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias"*.

consentido con los elementos determinantes de la validez del consentimiento; discernimiento, intención y libertad -artículo 897 del CC-. Por lo tanto afectarán al consentimiento las mismas causales que en los casos de los actos voluntarios, tales como la inmadurez, la alteración de las facultades mentales, el dolo, el error y la violencia.

II.2 Expreso, por Escrito u otro medio equiparable

Así entonces, cuando la ley establece este segundo requisito es claro que tuvo en miras el carácter "expreso" del consentimiento que contempla el C. C. en su artículo 917 –verbalmente, por escrito o por signos inequívocos- solo que en este caso particular es notorio que la ley LPDP privilegia el consentimiento por escrito.

Efectivamente, el art. 5º impone como condición que el consentimiento sea prestado *"por escrito o por otro medio que permita se le equipare, de acuerdo con las circunstancias"*. La firma por parte del afectado, del documento que directamente contiene la información para el tratamiento de sus datos o del propio formulario por medio del cual se recogen, con las menciones requeridas por el artículo 5 de la Ley, es el medio más efectivo de prueba del consentimiento del afectado.

Gozaíni[7] ha entendido que el recaudo de la firma aparece ineludible, circunstancia que elimina la posibilidad de aplicar los sistemas o mecanismos que establece el art. 15 inc. 3 º de la ley, cuando se refiere a la información que debe emitir cuando se plantea el derecho de acceso a los archivos -"La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin"- Por tanto, si la autorización se solicita a través de la pantalla, por vía telefónica, por carta personalizada, por correo electrónico, o por cualquier otra vía indirecta, la autorización presunta tendrá que estar ratificada con la firma del titular de los datos.

Compartimos sólo en parte este criterio, en sentido que en determinados casos concretos se exija la firma del titular de los datos con posterioridad si no surge fehacientemente que se prestó el consentimiento. Sin embargo, no consideramos que "siempre y en todos los casos" así sea, toda vez que lo que debe surgir en forma inequívoca es el consentimiento y siendo la propia ley en el artículo 15 inciso 3 que específicamente

[6] PEYRANO, Guillermo F. "Régimen Legal de los Datos Personales y Habeas Data", comentario a la ley 25.326, Editorial Lexis Nexis- Depalma, Buenos Aires, abril de 2000, p.72

[7] GOZAINI, Osvaldo, Op. cit, nota al pié n°4, pág. 6

establece otras formas que no son escritas y el decreto reglamentario de la misma-1558/2001- en la reglamentación del propio artículo 5, aclara *"La Dirección Nacional de Protección de Datos Personales establecerá los requisitos para que el consentimiento pueda ser prestado por un medio distinto a la forma escrita, el cual deberá asegurar la autoría e integridad de la declaración"* nosotros interpretamos que lejos de tornarse inaplicable al precepto legal del artículo 15.3 de LPDP, -en contrario- compatibiliza o armoniza con principio general del artículo 5 y la reglamentación de la misma norma.

II.2.a Consentimiento de palabra o verbal

Este tipo de consentimiento no parece ser el que la ley "equipare según las circunstancias" al consentimiento dado por escrito, toda vez que específicamente así lo establece -que sea escrito-. Sin bien no surge tampoco prohibición de aceptar el consentimiento de manera verbal la norma parece por demás clara con lo cual en caso de aceptar el consentimiento verbalmente, a nuestro criterio sólo tendía validez si además hay alguna manera de demostrar fehacientemente que el consentimiento fue dado.

La ley en el punto consideramos debe ser de interpretación restrictiva, toda vez que es uno de los recaudos más importantes establecidos por el legislador en aras de la preservación de un derecho de raigambre constitucional, el derecho a la autodeterminación informativa o a la intimidad de los datos.

Puede surgir alguna duda en lo que respecta a los supuestos de consentimiento por vía telefónica. En España, por ejemplo se resuelve por aplicación analógica de las normas de contratación contenidas en el Real Decreto 1906/1999, por el que se regula la contratación telefónica o electrónica con condiciones generales, en el desarrollo del art. 5.3 de la Ley 7/1998, parecería lógico entender que existe consentimiento expreso, equiparable al escrito, por ejemplo, cuando el mismo se realice de palabra y quede constancia en registros magnéticos e informáticos, de los que posteriormente se tome constancia escrita.

Siendo así, este tipo de consentimiento debería ser admisible y válido para legitimar el tratamiento de datos ya que si bien será –siempre- más prudente acudir al consentimiento escrito en sentido estricto, nada obsta a que en principio se acepte debiendo posteriormente ser ratificados.

También estaríamos ante un caso especial cuando el consentimiento es prestado en actividades de prospección comercial telefónica o de recolección de datos por emisoras

de radio, cuando el oyente participa revelando datos personales de *motu* propio. En estos supuestos, si por la inmediatez que exige la naturaleza de estas relaciones de comienzo del tratamiento no es posible una información exhaustiva previa, la solicitud de consentimiento para la recolección de datos debería ser sustituida por la información posterior inmediata y por escrito de la inclusión en el registro, archivo o banco. En todo caso, en ciertos supuestos, como puede ser por ejemplo los concursos radiofónicos, la recolección de datos personales, de palabra, se verá amparada por la excepción al consentimiento del artículo 5. d) de la LPDP, al incluirse dentro de una relación contractual (que en el caso de los concursos se iniciaría con la comunicación radiofónica de las propias bases del concurso) [8].

II.2.b Consentimiento electrónico

Las nuevas tecnologías nos han traído aparejado la necesidad de resolver algunas cuestiones, tal como la del consentimiento ectrónico. Así podemos hablar de dos formas de consentimiento electrónico; 1) la firma electrónica y 2)el correo electrónico

II.2.b. 1)Consentimiento dado a través de firma electrónica

La ley argentina deja abierto el concepto a la aplicación de la "firma digital" como una forma de prestar el consentimiento al referirse a "los medios que se equiparen". Si bien podría considerarse que estamos ante un "instrumento particular no firmado" de los previstos por el art.1190 del C. C., resultaría complementaria la sanción de una ley que acepte expresamente la firma digital como una forma de expresión del consentimiento, lo que por otra parte redundaría en el desarrollo del comercio electrónico[9]

En otros países, que nos llevan en la materia una ventaja de más de una década el tema ya está legislado puesto que sabemos es un realidad ineludible y, en la medida que pongamos remedios jurídicos acorde a las necesidades que se vayan presentando más alto será el grado de protección de que gocemos.

En España rige El Real Decreto Ley 14/1999, sobre Firma electrónica, la define como el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. Dentro del concepto de firma electrónica el

[8] Amplíese de ÁLVAREZ CIVANTOS, Oscar J. "Normas para la implementación de una eficaz protección de datos de carácter personal en empresas y entidades", Editorial Comares, Granada, España, 2002, p.61-62

[9] Véase UICICH, Rodolfo D., "Habeas Data. Ley 25.326", Comentada y anotada, Ad-Hoc, Buenos Aires, octubre de 2001, p.57

mismo texto legal distingue dos subtipos o categorías, la firma electrónica avanzada y la no avanzada, definiendo la primera como la firma electrónica que permite la identificación del signatario y ha sido creada por medios que este mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo, y a los datos a que se refiere, lo que permite que sea detectable cualquier modificación ulterior de estos. Firma electrónica no avanzada es, lógicamente, la que se define por oposición a la avanzada.[10]

El consentimiento para el tratamiento de datos, que una persona concede tanto por medio de la firma electrónica avanzada, como de la que no lo es, se puede equipara al consentimiento expreso y por escrito a que se refiere el art.. 7.2 de la Ley 15/1999. La diferencia estriba en que el valor que la Ley concede a la firma electrónica avanzada es el mismo que el de la firma manuscrita, mientras que el consentimiento que se realice mediante firma electrónica no avanzada, tendrá únicamente el valor que le asignen los tribunales en la apreciación de la prueba.

Los Tribunales vienen concediendo efectos probatorios a los documentos realizados en forma electrónica, en aplicación de lo dispuesto por el artículo 299 de la Ley 1/2000 de Enjuiciamiento Civil, de 7 de enero, al manifestar: *"También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos cifras y operaciones matemáticas, llevadas a cabo con fines contables o de otra clase, relevantes para el proceso"*[11]

La consideración de la firma electrónica no avanzada como suficiente para concretar el concepto de consentimiento expreso y por escrito, determina que se admita como tipo de consentimiento válido para amparar el tratamiento de datos que exigen un nivel alto de seguridad, nos parece – al menos- peligroso.

---

[10] En cuanto a los efectos que tienen cada uno de estos tipos de firma el art. 3 del Real decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica establece: 1. "La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta, según los criterios de apreciación establecidos en las normas procesales. Se presumirá que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicados en este apartado, cuando el certificado reconocido en que se base, haya sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que esta se produzca se encuentre certificado con arreglo a lo establecido en el art. 21. 2. A la firma electrónica que no reúna todos los requisitos previstos en el apartado anterior, no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica".

[11] ÁLVAREZ CIVANTOS, Oscar J. Op. cit, nota n°8, p. 64

La firma electrónica avanzada es un medio de garantizar las transacciones que se realicen a través de Internet, que permite probar la identidad del remitente, la integridad del contenido que este envía y la confidencialidad del mismo, evitando que su contenido se conozca por terceros. No obstante, deja sin solucionar una cuestión de trascendental relevancia como es la del recibo del mensaje por el destinatario, que de esta forma podría alegar la no recepción del mensaje esta es, sin duda una de las debilidades que actualmente presenta este sistema[12]

II.2.b. 2) Consentimiento dado a través de correo electrónico

El consentimiento, realizado por medio de mensaje de correo electrónico, en el que se determine la aceptación del tratamiento de los datos personales, así como el alcance del tratamiento que se acepta, se englobará al igual que sucedía para el caso anterior, en el concepto de consentimiento expreso y por escrito -la mención al alcance del tratamiento es importante y se podrá realizar, o bien mediante una enumeración de las condiciones del tratamiento que se acepta, o bien remitiendo al texto informativo, caso este último que traería consigo mayores dificultades probatorias-.

Es necesario, como lo planteáramos en el caso de la firma digitalizada que se sancione una ley de comercio electrónico que sea aprobada en los mismos términos reflejados en los principios generales de la actual LPDP, pudiendo tener el valor equiparable en ambos casos.

De importancia en ese ámbito puede resultar la reseña de la Sentencia de la Sala de Social del Tribunal de Justicia de Madrid del 13/03/2001 que admitió un mensaje de correo electrónico sin firma como prueba para avalar la procedencia del despido de un directivo de la empresa en el que el mismo presentaba su dimisión irrevocable, aunque no fue reconocido como enviado ni escrito por aquel. Para el Tribunal *"el correo electrónico es un medio de comunicación utilizado que la nueva tecnología facilita, siendo su uso cada vez más habitual y que, desde luego, es útil y eficaz"* el Tribunal Superior de Justicia establece que *"hubo dimisión porque la actuación del actor fue clara y terminante al respecto, siendo tales las notas exigidas por la jurisprudencia, y la expresión de aquélla voluntad irrevocable a través del e-mail enviado por él, patente queda y no deja duda al respecto".* El problema que presenta el consentimiento por medio de correo electrónico se sitúa en el ámbito de la prueba. En este sentido, Juan

[12] ÁLVAREZ CIVANTOS, Oscar J. Op. cit, nota n°8, p. 65

Bonilla Blasco[13], pone de manifiesto que son dos las cuestiones fundamentales que suscita todos envíos de correos electrónicos, la autoría y la autenticidad de los mismos, los cuales no serán siempre de fácil determinación, y que no quedarán garantizados hasta tanto la empresa/persona jurídica o persona física no integre los instrumentos técnicos necesarios, para permitir la presunción de que el correo electrónico es enviado por la persona a cuyo nombre se ha configurado y con el contenido por él dispuesto. Esta necesidad podría verse, en gran parte, cumplimentada por la introducción de todas y cada una de las medidas de seguridad en el caso que se sancione una ley al respecto o, que como dice el decreto reglamentario en su artículo 5, podría partir de una disposición de la Dirección Nacional de Protección de Datos Personales – en adelante DNPDP- la que está facultada por la propia ley y el reglamento a "establecer medios distintos a la forma escrita (…)siempre que se asegure la autoría e integridad". La validez del consentimiento prestado a través de correo electrónico podría ser aceptada por la presunción de control que sobre el mismo corresponde al titular del e-mail. La posibilidad de que alguien suplante su personalidad, será remota si de cumple con todas las medidas de seguridad que estarían establecidas en la ley o reglamentación, sólo de esta manera consideramos viable dar cumplimiento a la posibilidad que nuestra ley "abre" en su artículo 15.3 y en la reglamentación del artículo 5; mientras no haya un marco normativo claro y preciso, específico en torno a la firma electrónica y al correo electrónico como formas de consentimiento, no estarán dadas -a nuestro criterio- las condiciones de seguridad necesarias para la protección de los datos personales en el alto grado de protección que es sin duda el fin último de la ley.

II.2.c. Consentimiento del afectado para los tratamientos de *"data mining"* o entrecruzamiento de datos.

Con el advenimiento de estas nuevas tecnologías nos encontramos con verdaderos obstáculos o problemas que, sin duda afectan a la solicitud del consentimiento para el tratamiento de los datos de los afectados, dando lugar a nuevas técnicas de tratamiento como las que se basan en el cruce de datos personales procedentes de distintos ficheros para extraer perfiles de consumo utilizable con fines publicitarios. Estas técnicas han proliferado de manera notoria con la llegada de internet, pero ya eran usables en empresas de gran volumen, en las que existe diversificación de productos e incluso en

[13] BONILLA BLASCO, Juan, "Los efectos jurídicos del correo electrónico en el ámbito laboral", Revista Relaciones Laborales de Agosto 2001, Madrid, España.

grupos de empresas de sectores distintos. A la infraestructura de equipos dispuesta para realizar el cruce de datos se le denomina *Datawarehouse* y al tratamiento concreto que se efectúa con dichos datos *data mining* o "minería de datos". La propia denominación del tratamiento nos permite descubrir su finalidad que no es otra que indagar distintas bases de datos, donde las personas consintieron el tratamiento de los suyos con el objeto de obtener, a su vez, una nueva base de datos como resultante del entrecruzamiento de los datos de los anteriores. A estos efectos, por regla general los tratamientos de *data mining* se efectúan en sistemas informáticos distintos a los del resto de la empresa, incluyendo en los mismos los datos procedentes del reto de ficheros para su interrelación (*Datawarehouse*)[14] Estas técnicas normalmente están dando lugar a conductas al margen de la normativa sobre protección de datos personales.

En principio, cualquier técnica de *data mining* exigirá el consentimiento previo del sujeto afectado, no sólo para efectuar ese tratamiento, sino también para su uso con la finalidad concreta a la que se pretenda destinar. El hecho de que exista consentimiento del afectado para el tratamiento de sus datos en otros casos no significa que se pueda efectuar un tratamiento paralelo, que supondría una vulneración del principio de finalidad del tratamiento contenido en el art. 4.1 y 4.3 de la LPDP Artículo 4º (Calidad de los datos). "*1.Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. 3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención".*

Las ventajas que presenta las técnicas de *data mining* en el sector publicitario y de marketing son importantes y son el fundamento de la proliferación de dichas técnicas. Las técnicas hoy en día tienden hacia la personalización y esta personalización conlleva el conocimiento exhaustivo de cada cliente, conocer el nivel de gasto asumible por el cliente, sus condiciones económicas, medios de vida, situación familiar, hábitos de consumo y otros datos igualmente relevante, permitirán conocer el producto que debe ofrecérsele. Día a día las modernas tecnologías conducen a sistemas que permiten una mayor personalización de las ofertas. Actualmente, las técnicas de *data mining* han ganado mucho con la llegada y evolución de la red. La cantidad de datos de un usuario que puede conjurar un portal de comercio electrónico es inmensa, partiendo de los datos voluntariamente introducidos por el usuario registrado, y pasando por los hábitos de navegación que demuestre en su utilización diaria de los servicios del portal. La

[14] Amplíese de ÁLVAREZ CIVANTOS, Oscar J. Op. cit, nota n°8, p. 73/75

personalización le permite seleccionar de forma voluntaria los contenidos que son de su interés, pero asimismo permitirá a la empresa propietaria del portal conocer mejor que productos pueden ser del interés del usuario. Sin embargo, muy pocos portales informan de la existencia de ficheros de *data mining* y de la finalidad de los tratamientos que efectúan con los datos de los usuarios registrados. Esta situación, en principio constituiría una grave violación a la ley 25.326 en los puntos pre referidos. Se tendría que tratar de casos en los que sea notorio que se trata de formar perfiles con miras únicamente a ofrecer un bien o servicio, del que se infiera que no es posible sea utilizado con finalidad discriminatoria alguna. Así y todo, la empresa que lleva cabo el cruce de datos o *"data mining"*, debería – a nuestro criterio- notificar el resultado al titular de los datos y en caso de no contar con su consentimiento o que el mismo sea revocado, automáticamente sacar el dato del correspondiente registro.

III.3 Consentimiento Informado

En concordancia con la regulación del artículo 5; el artículo 6 de la LPDP establece la obligación previa de informar a quien va a prestar el consentimiento para el tratamiento de sus datos personales; así la norma establece: -art.6 - *" Información. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:*

a)La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios;

b)La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;

c)El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente:

d)Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;

e)La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Se entiende por consentimiento informados a la expresión de voluntad brindada sólo después de haber tomado conocimiento de las circunstancias que rodean al caso. La LPDP tiene – a nuestro criterio- carácter meramente enunciativo no resulta taxativo toda vez que, en situaciones concretas la información se hará bajo determinadas circunstancias que no son las mismas en todos los casos.

En efecto, el carácter de la información no será para todas las personas de igual manera. el propio artículo 5 en su reglamentación deja sentado con claridad que: *"El consentimiento informado es el que está precedido de una explicación, al titular de los datos, en forma adecuada a su nivel social y cultural, de la información a que se refiere el art. 6° de la ley 25.326"*

El carácter informado del consentimiento está dado por los presupuestos de mínima que debe conocer quien va a prestar su consentimiento para que se de tratamiento a sus datos personales los mismos son:

a) La finalidad para la que serán tratados y quienes pueden ser sus destinatarios o clase de destinatarios. Esto es como consecuencia de los principios de especificación del fin y de restricción del uso. En forma escueta el texto vetado ya incluía la exigencia de informar a los interesados sobre la finalidad del registro; ahora se le ha agregado el importante de quiénes pueden ser los destinatarios de la información, cuestión clave que puede resultar determinante para que el titular de los datos preste o no su consentimiento.[15]

b) La existencia del archivo, registro, banco de datos electrónico o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable. Este requisito es sin duda a los efectos de evitar que el tratamiento del dato personal se lleve a cabo de una manera ilícita o contraria a la finalidad para la cual el titular dio su consentimiento, pueda saber quien es el responsable, que a su vez será contra quien tendrá las acciones judiciales correspondientes. Con amplitud la ley se refiere tanto a bancos de datos informatizados como los que no recurren a la tecnología informática, que aunque cada vez menos frecuentes todavía existen. La cláusula ya estaba prevista en el texto vetado, con el agregado importante del deber de informar al titular de los datos sobre "el tratamiento a que se los someterá (a los datos), así como quiénes han solicitado informes sobre su persona. Parece sobreabundante ya que en el inciso a) del artículo 6, la primera información dada deberá ser la *"finalidad para que serán tratados"* (los datos)

c) El tercer requisito para informar previo a la solicitud del consentimiento es carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos personales sensibles.

Esta previsión ya estaba contenida en la ley vetada con la siguiente redacción: "el carácter obligatorio o facultativo de sus respuestas a las preguntas que se les formularen, por parte del sector público, y que ello es facultativo si las preguntas las realiza el sector privado". La modificación pone de manifiesto que el legislador ha considerado que no siempre las respuestas a las preguntas formuladas por los registros privados son facultativas; en el caso de que estuviere establecida la obligatoriedad de las respuestas

[15] QUIROGA LAVIÉ, Humberto, "Habeas Data", Editorial Zavalía, Buenos Aires, 2001, p.83

en relación con las preguntas del sector privado, ello deberá estar fijado por ley y no por decreto reglamentario[16].

d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos. La inclusión parece acertada pues permitirá ilustrar a los titulares de los datos acerca de las consecuencias que tendrá, en relación con sus personas, contestar de una u otra los requerimientos de los registros. Tal como lo explica Moraga Díaz[17] que actualmente enfrentamos una situación verdaderamente crítica, ya que aproximadamente un 90% obtiene datos de personas identificables y, tan sólo un 10% es informado sobre la intención de los mismos y su finalidad.

e) Por último la ley establece que se deberá explicar al titular del dato requerido los derechos más importantes que la ley prevé e torno al tratamiento de datos personales, ellos son 1) el derecho de acceso que está establecido en el artículo 14 de la LPDP y 2) los derechos de rectificación y supresión de datos, tal como surge del artículo 16 de LPDP; ambas normas dentro del capítulo III "Derecho de los titulares de los datos". Esta norma se inserta en el sistema garantista vigente en todo el mundo a favor de los derechos humanos: todas las personas deben saber cuáles son sus derechos y las vías procesales concretas para defenderlos.

Padilla[18], a su turno, opina que alguna voz aislada se ha alzado para advertir que la ley ha omitido crear una protección especial para los datos de los menores "que hoy están muy expuestos". Preocupación que compartimos con el autor quien cita a modo de ejemplo un norma de protección a los niños que es la ley estadounidense *"The Children´s Online Privacy Protection"* que brinda a los padres las herramientas para controlar qué información es colectada de sus hijos menores de trece años en sitios o páginas comerciales de la *World Wide Web*. Sus operadores deben notificar a los padres acerca de sus prácticas; obtener su consentimiento antes de reunir información personal de sus hijos; darle la opción respecto de si esa información podrá ser cedida a terceros; no requerir a los menores otra información que la razonablemente necesaria para participar en una actividad, y mantener la confidencialidad, seguridad e integridad de la información dispuesta en el inciso siguiente.

[16] QUIROGA LAVIÉ, Humberto, Op. cit, nota n°15, p.84

[17] MORAGA DIAZ, Magdalena del V., "La defensa a la intimidad", en AA.VV, "La defensa de la intimidad y los datos personales a través del habeas data", Obra coordinada por GOZAÏNI, O., Editorial Ediar, Buenos Aires, 2001, p.227

[18] PADILLA, Miguel M, "Banco de datos y acción de Habeas Data", Editoril Abeledo Perrot, Buenos Aires, 2001, p.156

III. Excepciones: Casos en los que la ley no exige del Consentimiento del titular para el tratamiento de sus Datos Personales

El principio de limitación de la recolección, que requiere el consentimiento del sujeto para la incorporación de cada dato, si se lo llevara a la práctica en forma estricta, condenaría a los bancos de datos a la desaparición"[19].

Los derechos a la autodeterminación informática, a la intimidad y a la propia imagen[20] que son los que esencialmente tutela la garantía de habeas data, no escapan al principio general de que no existen derechos absolutos sino que todos son susceptibles de reglamentación, mientras la misma sea razonable y no altere o desvirtúe la esencia del derecho. De manera tal, que aplicado al caso la regla general de la necesidad del consentimiento del titular de los datos personales para poder dar tratamiento a los mismos, también tiene sus excepciones en la presente ley, a nuestro criterio significan un límite razonable toda vez que no lesionen otro derecho, también fundamental como es el derecho a la información.

En el reciente fallo (25/05/2003) de la Cámara Comercial, Sala E, *"Jones, Carlos Raúl c/Organización Veraz s/amparo"*[21], ley 25.326, articulo 26.1 y 26.2, el tribunal adhiere a este criterio, que es en definitiva el seguido por la ley 25.326 *"Cabe rechazar la acción de habeas data intentada contra cierta empresa destinada a suministrar informes atinentes a la solvencia de las personas –Organización Veraz S.A.- a fin de que esta suprima de su base de datos e informe la ilicitud de la fuente informativa, de ciertos datos sobre la persona del accionante relacionados con la calificación de deudor irrecuperable, toda vez que la falta de consentimiento suyo en la publicación de los datos cuestionados no resulta suficiente causa para ordenar su supresión, ya que la ley 25326, art. 26 ha legitimado la prestación de los denominados "informes comerciales" para evaluar la solvencia y el riesgo crediticio, cuando se recojan datos de carácter patrimonial de fuentes accesibles al público p procedentes de informaciones facilitadas por el interesado o con su consentimiento y, además, autoriza la recolección de datos sobre morosidad facilitados por el acreedor o por quien actúe por su cuenta o interés (inc.1 y 2)".*

Las excepciones están taxativamente enunciadas en el artículo 5 y son las siguientes:

[19] PUCCINELLI, Oscar R., "El habeas data en Indoiberoamérica", Editorial Temis, Bogotá, Colombia, 1999, p.11 y ss.

[20] BASTERRA, Marcela I. "Hábeas data: derechos tutelados"; La Ley- Doctrina Judicial, 1999-3-77

III.1 Datos obtenidos de fuentes de acceso público irrestricto

La primera de las excepciones comprendidas en la LPDP alcanza a los datos que sean obtenidos "de fuentes de acceso público irrestricto".

En cuanto al significado de la expresión que debe entenderse por "fuente de acceso público irrestricto" se ha expresado que se trata de "aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación"[22]

Son los bancos, bases, ficheros o registros, que contengan datos que pueden ser libremente consultados y recogidos por los interesados, sin necesidad la autorización o consentimiento del titular del dato obtenido.

En principio parece razonable –como excepción- no requerir el consentimiento para tratar un dato que ya tiene estado público. Sin embargo, el tema amerita algunas aclaraciones.

Son fuentes de fácil acceso aquellas que no tienen impedimentos formales ni sustanciales para que cualquier interesado las consulte. La información disponible puede ocupar varios campos e, inclusive, ingresar en situaciones personales que eventualmente estarían privados de circulación (por ejemplo: archivos del Banco Central de la República Argentina; Registro Público de Comercio; Inspección General de Justicia; Registro Nacional de Antecedentes Personales, entre otros). En su momento, bastará con informar el lugar del cual se extrajeron los datos personales comunicados, y la Autoridad de control establecerá si es o no una fuente de fácil acceso[23]

Peyrano[24] destaca que la caracterización de estas "fuentes" puede dar lugar a equívocos. Primero, porque las mismas pueden encontrarse tanto en bancos de datos públicos, como en bancos de datos privados, ya que en ambos casos puede darse la circunstancia de no existir limitaciones para su consulta, no necesariamente tienen que ser datos "públicos" sino de "acceso público irrestricto", que no es lo mismo. En segundo lugar, recordemos que la existencia de ciertas restricciones, tanto al acceso a las "fuentes", como a determinados datos obrantes en las mismas, puede darse sin que la fuente pierda la condición que la caracteriza como "de acceso público irrestricto", a los efectos de la

---

[21] Sentencia del 25/05/2003. Cámara Comercial , Sala E, Dres. Arecha-Ramírez-Guerrero.

[22] MESTRE, Javier A., "Comentarios a la legislación sobre protección de datos", http://v2.vlex.com/vlex2/front/asp/canales , cit por PEYRANO, Guillermo F. Op. cit, nota n°6, p. 79

[23] GOZAINI, Osvaldo, Op. cit, nota al pié n°4, p. 7

[24] PEYRANO, Guillermo F. Op. cit, nota n°6, p. 79

posibilidad de consulta de la generalidad de los datos recolectados en la misma. Es habitual que las oficinas públicas que formen archivos de datos de carácter personal que a su vez requieren para acceder a sus registros determinadas calidades personales en los consultantes tales como un título o habilitación profesional (escribano, abogado, etc). El acceso obviamente se encuentra "restringido", si bien tal restricción no obedece en muchos casos de modo primordial a la "reserva" que puedan merecer los datos archivados por su calidad intrínseca, sino mayormente a razones operativas, y la limitación en cuestión no le hace perder a la fuente ni a los datos en ella contenidos, el carácter de datos obrantes en fuentes de acceso público irrestricto, toda vez que carecería de lógica otorgar un status distinto a esas bases y a sus registraciones.

Por tanto puede válidamente afirmarse que la expresión "fuentes de acceso público irrestricto", si bien alude a bases, ficheros o registros en los que en principio obran datos a los que se puede acceder sin limitaciones y que, en su generalidad, contienen informaciones que no precisan del consentimiento de sus "titulares" para las operaciones de tratamiento, puede comprender también en el caso concreto bancos o archivos que reconozcan ciertas restricciones en el acceso a los mismos –sin perder su condición-, como igualmente que dichos archivos pueden contener determinados registros que necesiten de la prestación del consentimiento de la persona a la que refieren. Este consentimiento no sería necesario en virtud del registro, base o banco de datos, sino en virtud de la calidad del dato, por ejemplo si en el registro de "acceso público irrestricto" constara uno de los denominados datos sensibles, cuyo tratamiento surge del juego de los artículos 2 (definición de dato sensible) y 7 (que establece que ninguna persona estará obligada a brindar datos sensibles)[25]

[25] PEYRANO, Guillermo (Amplíese op. cit p.80/81), aclara que de la circunstancia de constar en las mismas se deriva que en principio (y sólo en principio), estos datos personales pueden ser calificados como "datos públicos", ya que "el público" puede tener libre acceso a los mismos (con las salvedades apuntadas ut supra). O sea que la noción de "datos públicos" resulta independiente de la de "bancos públicos de datos", por cuanto esta última refiere a la pertenencia de los archivos y no a la calidad de los datos registrados en los mismos. Así al analizarse el art. 1º de la LPDP, en lo relativo a los "bancos públicos de datos personales", se ha expresado que "el carácter de públicos devendrá de su pertenencia a la organización estatal, sea ésta nacional, provincial o municipal, sin interesar que los datos almacenados en esos archivos sean de libre acceso, o tengan carácter reservado por determinadas circunstancias", lo que evidenciaría la imprecisión terminológica de la ley, en tanto y en cuanto en el art. 17, al establecer las "Excepciones" a los derechos de los titulares de los datos, alude a "bancos de datos públicos", cuando en realidad debió expresar "bancos públicos de datos", a los que en verdad se está refiriendo, ya que como se ha visto, los "datos públicos" pueden encontrarse almacenados tanto en archivos públicos como en archivos privados. Para el autor de las consideraciones precedentes queda evidenciada la relatividad del concepto "fuentes de acceso público irrestricto", como justificante de la excepción a la obligatoriedad del consentimiento de los titulares de los datos.

III.2 Datos recabados para el ejercicio de funciones propias de los poderes del Estado o derivados de una obligación legal

La previsión que el legislador hace en el segundo inc.2.b del artículo 5 sin duda debe interpretarse en forma armónica con la norme del artículo 23 inc. 2º la que establece: *"El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquellos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad".*

El fundamento de esta norma está dado en que es necesario establecer un equilibrio entre el derecho a la intimidad informática de las personas y, por otra parte el deber del Estado de cumplir con las obligaciones emergentes del poder de policía estatal.

Parece razonable que en circunstancias en que esté en juego la defensa nacional y la seguridad pública los organismos estatales encargados de salvaguardar las mismas, puedan, con fundamento en la ley estar exceptuados de solicitar el consentimiento del titular del dato. La actividad estatal no significa que todos los organismos estén libres de requerir autorización, sino, que sólo podrá exceptuarse en los términos estrictos que la propia ley establece.

Gozaini[26], advierte que la recolección de este tipo de datos muchas veces cuenta con autorizaciones implícitas, tal el caso de las inscripciones en registros públicos para constituir un derecho; para certificar acciones de alguna naturaleza; al ingresar en establecimientos hospitalarios, etc. circunstancia que, según el autor obligará a considerar el alcance que tiene el consentimiento presunto, frente al requerimiento expreso e informado que solicita la ley. Agrega que el dato personal que se presta como consecuencia de una actividad que tiene implícito un interés particular, elimina la necesidad de lograr una autorización expresa posterior a dicha manifestación

Nosotros consideramos que el consentimiento tácito o presunto es ilícito toda vez que contraría al principio del consentimiento "expreso, libre, por escrito u equivalente" que contempla específicamente la LPDP. Las únicas excepciones aceptadas son las taxativamente especificadas en esta norma y, en todos los demás casos en que un titular otorgue un dato personal en circunstancias particulares, tal como el de los sanatorios u

[26] GOZAINI, Osvaldo, Op. cit, nota al pié n°4, p. 8

hospitales, tales institutos si tienen un banco o registro de datos deben darle a estos el tratamiento que la presente ley establece en toda su normativa.

Sólo con una interpretación restrictiva de la ley se logrará la efectiva protección del derecho a la autodeterminación informática.

En el caso particular deben darse los requisitos que la propia ley en la presente excepción establece para que no se transforme la misma en un "arma de doble filo", cuando justamente el exceptuado puntualmente para recopilar datos sin consentimiento es el estado a través de los organismos específicos establecidos en la ley.

Por cierto, – a nuestro criterio-, para que alcance esta excepción se deben dar los siguientes requisitos: 1) Sólo procede para el caso en que se recopilen datos con fines de defensa nacional, seguridad pública o represión de delitos la que debe tener fundamento estrictamente en una misión asignada por ley. Quedaría excluida la recopilación de datos basados en estos motivos si se alude a un mandamiento genérico de la ley. 2) Los bancos de datos a los que la ley concretamente puede autorizar en un caso concreto a recabar datos sin consentimiento serán las fuerzas armadas, fuerzas de seguridad, organismos policiales y organismos de inteligencia. 3) solo se recopilaran los datos que se necesiten para el cumplimiento de la misión que la misma ley que autorice el tratamiento determine. Dado que las leyes de deben interpretar en forma armónica y no analizando aisladamente sus normas, resulta claro que determinados datos jamás podrán ser autorizados al tratamiento tales como la orientación sexual u otros aspectos de la intimidad de las personas, origen racial o étnico, los datos referidos a la salud sólo podrán tratarse si se aplica la disociación del dato, esto es sin que sea identificable la persona a la cual pertenece ese dato. 4) Otro requisito determinante es el tiempo por el que pueden ser recolectados estos datos. Sería por el que específicamente establezca la ley autorizante, pero siempre en consonancia con el principio general de la LPDP establecido en el artículo 4.7 y esto es por el tiempo que sea necesario para el cumplimiento estricto de los fines de recolección, luego serán inmediatamente destruidos. Ni la propia ley habilitante en caso concreto podría no cumplir con este principio establecido en la ley 25.326. 5) Por último, como surge específicamente de la normativa del artículo 23 –último párrafo- será necesario que en esos casos concretos los archivos de datos fundados en esta disposición sean clasificados por categorías en función de su grado de fiabilidad.

III.3 Casos específicos exceptuados por la presente ley – nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio.

Antes de la sanción de la ley 25.326 la jurisprudencia había iniciado un camino tendiente a delimitar los casos en los que no se necesita el consentimiento del titular de los datos a tratar, por considerar que hay datos fuera de la protección de la esfera de intimidad, anteponiendo, en el caso ante una colisión de valores, otros como la transparencia del mercado, las operaciones de crédito, el derecho a la información, etc.

En el caso *"Estado Nacional Dirección General Impositiva c/ Colegio Público de Abogados de la Capital Federal s/medidas cautelares"*[27] la D.G.I. reclamó al Colegio Público la información relativa al número de documento, fecha de nacimiento y fecha de matriculación de los letrados matriculados, negándose la institución a dar tal información por considerar que ello afectaba el ámbito de autonomía individual de los abogados inscriptos y porque ponía en peligro real o potencial la intimidad de los mismos. El máximo tribunal hizo lugar a las pretensiones de la D.G.I. reiterando los argumentos expresados en la causa *"Guthein, Federico c/Alemann, Juan"*[28], advirtiendo que el derecho de controlar la información personal que de un individuo figura en los registros, archivos o bancos de datos no es absoluto estableciendo límites.

En similar sentido la Suprema Corte de justicia de Mendoza en el precedente *"Huertas Juan C. c.Co.De.Me"*[29] ha señalado que " la recolección de datos de un registro de morosos es lícita, aún sin mediar consentimiento del interesado, cuando los datos aparecen en el padrón electoral, son los propios de cualquier operación de crédito, y la entidad que los contiene no lucra con el servicio de prestar información sólo a sus asociados. Afirmando categóricamente que los datos referidos al nombre, dirección, documento de identidad y actividad desempeñada, no corresponde al ámbito de las acciones privadas protegidas por el artículo 19 de la constitución nacional, ni a la información colectiva sobre datos sensibles utilizada con fines discriminatorios por motivos de raza, religión, ideología, opinión política o gremial, sexo, etc.

Es claro entonces que esta es la orientación que toma la LPDP y que compartimos, son datos que no vulneren la intimidad estando en bancos o registros de fácil acceso.

---

[27] CSJN, Sentencia del 13/2/1996; véase en JA, 1996-II-295; LL, 1996.B-35

[28] CSJN, Sentencia del 15/4/1993, G-556-XXIII,

[29] SCMendoza, Sentencia del 15/04/1999, publicada en la Ley Gran Cuyo,1999-600. Con comentario de BAZÁN, Victor, "Habeas Data, Registro de cumplimiento o Incumplimiento de Obligaciones patrimoniales, y Saneamiento del crédito: la copa medio llena o medio vacía. La Ley, T.1999-F, p.295.

Es necesario, asimismo no confundirlos con los datos del inciso a) de fuentes de acceso público irrestricto, puesto que estos datos no provienen de una fuente de acceso irrestricto, sino de una fuente de fácil acceso que no es lo mismo. Coincidimos con Gozaíni[30] En que es conviene tener presente que la fuente es importante porque al deducir el derecho de acceso se debe indicar el lugar y la persona de la cual se obtiene la información. Esta es la situación que tienen los datos de "fuentes de acceso público irrestricto"; en cambio, cuando se trate de listados como los que mencionan, no existe obligación alguna de expresar la fuente de captura.

Los datos a que alude este apartado son entre otros los que se podrán extraer de la Guía telefónica, del Anses, registros de asociaciones de profesionales, etc.

El elemento que habilita en estos casos a la recolección de los presentes datos llamados "nominativos" es que no parecen aptos para generar "perfiles" que implique conductas discriminatorias.

III.4 Datos que deriven de una relación contractual, científica o profesional

Esta excepción comprende, entonces a) los datos derivados de una relación contractual b) los datos cuyo tratamiento sea con fines científicos; c) los datos derivados de una relación profesional y, para los tres supuestos la propia ley agrega un requisito aplicable a todos y cada uno de ellos; para que proceda la excepción de consentimiento, debe "resultar necesarios para su desarrollo o cumplimiento".

Para que una relación contractual quede perfeccionada, necesariamente se deberán dar a conocer datos personales, dado que se tornan imprescindibles para concretar el vínculo. En aquellos contratos en los cuales solo se dan los denominados datos "nominativos"- nombre, documento de identidad, domicilio, CUIT, profesión, fecha de nacimiento- no habría mayores consecuencias. Además porque estos datos están exceptuados del consentimiento por el inciso c, del artículo 5 de la ley. Es el caso de los contratos tales como por ejemplo; de compraventa o locación de inmuebles entre otros.

El problema se presenta cuando es una relación contractual en la que necesariamente el titular presta datos que en muchos casos entran en la categoría de "sensibles" tal el supuesto que se da en los contratos como los de seguros de vida; locación de servicios; donde la persona deja voluntariamente datos que, de otro modo, no divulgaría, o podría pretender su reserva o confidencialidad.

[30] GOZAINI, Osvaldo, Op. cit, nota al pié n°4, pág. 8

Coincidimos en el caso con Gozaini[31] en cuanto que en este último supuesto la excepción del consentimiento no es necesario, pero únicamente en la etapa de recolección; porqué si a partir de esta información se buscan finalidades diferentes (por ejemplo: cuando una persona adquiere un inmueble en un barrio privado, y tras el contrato le llegan ofertas de seguridad, bienes, accesorios, etc.), quien obtuvo esos datos y los transfirió, está violando la LPDP que en su artículo 24 establece: "Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el art. 21 de la ley".

O sea, que si una base de datos almacena, conserva o transfiere datos, está obligada a cumplir todas las exigencias de la ley. No así si se tratara, por ejemplo simplemente de un archivo de un Estudio de abogados que tiene los datos de sus empleados y es para uso estricto del estudio. Esto sería equiparable a abrir la computadora personal o la agenda de alguien. Es la propia ley en la reglamentación del artículo 1° de la ley 25.326 que establece que la misma no alcanza a los archivos de datos que sean para estricto uso personal.

La obtención de datos personales provenientes de una "relación científica", por ejemplo si se realizan estudios sobre personas que padecen una determinada enfermedad, elimina por su propia naturaleza la necesidad de requerir el consentimiento para el almacenamiento de esos datos, siempre que se de la disociación entre el dato y el titular de los mismos. Por ejemplo, se debe saber cuántas personas que son portadores y/o enfermos de HIV entran cada mes o por año a hospitales/ clínicas/ sanatorios, con fines científicos o de estadísticas, no se debe saber el nombre y apellido del portador y/o enfermo, salvo que el mismo portador del virus otorgue su consentimiento.

En consonancia con esto el tratamiento de los datos referidos a la salud está contemplado en el artículo 8 º de la LPDP el que establece que: "Los establecimientos sanitarios públicos o privados y los profesionales vinculados a la ciencia de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieran estado bajo tratamiento de aquellos, respetando los principios del secreto profesional" [32]

Está autorizado por la ley el tratamiento de los datos personales de aquellos pacientes a los que se les haya dado asistencia médica cuando ello resulte necesario para la prevención o para el diagnóstico medico y para el tratamiento clínico, tanto en relación

[31] GOZAINI, Osvaldo, Op. cit, nota al pié n° 4, pág. 9

[32] Específicamente el tema de datos referidos a la salud puede consultarse; PEYRANO, Guillermo F. Op. cit, nota n° 6, p. 106-111, QUIROGA LAVIÉ, Humberto, Op. cit, nota n°15, p.87

a salud física como mental siempre y cuando quede, asimismo sujeto al secreto profesional establecidos en la presente ley o en otra ley nacional.

Relacionada con esta disposición se encuentra la previsión hecha por la ley en la normativa del artículo 11[33], inciso 3 en relación a la cesión en la que además de exceptuar el consentimiento para la cesión – sea la misma nacional o internacional- de datos en los supuestos del artículo 5° ,inciso 2, específicamente prevé que el consentimiento no es exigido cuando...”se trate de datos personales relativos a la salud, y sean necesarios por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismo de disociación adecuados”.

A su turno, la ley también se encarga de puntualizar que tratándose de la transferencia internacional de datos, la prohibición no regirá, aunque no se reúna los niveles adecuados de protección en el supuesto de que se trate del “intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior”. El que a su vez, ampara la cesión del dato cuando se produjere una disociación entre el titular y el dato; esto es que los titulares de los datos sean inidentificables.

En cuanto a la tercera categoría, o sea los datos obtenidos en ejercicio de una actividad profesional, consideramos se refiere a la información que guardan los médicos, psicólogos, psicoanalistas, odontólogos, etc, de sus pacientes o los abogados, escribanos, contadores y cualquier prestador de servicios de sus clientes los que deben mantener en secreto y confidencialidad siendo para su estricto uso profesional y personal, siempre que no se pase a otra etapa del tratamiento de datos no será necesario el consentimiento del titular, en caso de pasar la mera recolección, sí será necesario el consentimiento del mismo.

[33] La norma del artículo 11(cesión) analiza la relación entre el consentimiento en los casos de cesión nacional o internacional de datos. Al respecto establece que: “1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legitimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo. 2. El consentimiento para la cesión es revocable. 3. El consentimiento no es exigido cuando: a) Así lo disponga una ley; b) En los supuestos previstos en el artículo 5º inciso 2º; c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias; d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados; e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables. 4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo

III.5 Operaciones realizadas por entidades financieras – conforme al artículo 39 de la ley 21.526-

La Ley de entidades financieras[34] en su artículo 39 establece que; "Las entidades comprendidas en esta ley no podrán revelar las operaciones que realicen, ni las informaciones que reciban de sus clientes. Sólo se exceptúan de tal deber los informes que requieran: a)Los jueces en causa judiciales con los recaudos establecidos por las leyes respectivas; b) El Banco Central de la República Argentina en ejercicio de sus funciones; c) Los organismos recaudadores de impuestos nacionales, provinciales o municipales sobre la base de las siguientes condiciones: - Debe referirse a un responsable determinado; - Debe encontrarse en curso una verificación impositiva con respecto a ese responsable, y - Debe haber sido requerido formal y previamente; d)Las entidades deberán guardar absoluta reserva sobre las informaciones que lleguen a su conocimiento".

El fundamento de exceptuar el consentimiento en el presente supuesto estaría dado por la necesidad de no producir ningún tipo de afectación al tráfico mercantil y a la información crediticia tal como aparece hoy en el mercado[35] sin desproteger, por otro lado, a las operaciones financieras que deben estar amparadas en el secreto bancario establecido también por ley.

En cuanto al concepto de las "entidades financieras" que quedan exceptuadas por la normativa en cuestión sirva de aclaración- en caso de duda- la reglamentación del propio artículo 5 del decreto reglamentario 1558/2001 en el que se establece "A los efectos del art. 5°, inc. 2° e) de la ley 25.326 el concepto de entidad financiera comprende a las personas alcanzadas por la ley 21.526 y a las empresas emisoras de tarjetas de crédito, los fideicomisos financieros, las ex entidades financieras liquidadas por el Banco Central de la República Argentina y los sujetos que expresamente incluya la autoridad de aplicación de la mencionada ley"

Asimismo, el propio reglamento de la ley se encarga de remarcar que "no será necesario el consentimiento para la información que se describe en los incs. a), b), c) y d) del artículo 39 de la ley 21.526"

Quedan comprendidas dentro de esta ley- a nuestro criterio- las personas o entidades privadas o públicas, oficiales o mixtas, de la Nación, de las Provincias de los Municipios, de la Ciudad Autónoma de Buenos Aires que realicen intermediación habitual entre la oferta y la demanda de recursos financieros. Quienes deberán desempeñar sus actividades conforme a los principios generales que rigen las operaciones financieras de este tenor.

---

de control y el titular de los datos de que se trate. Para ampliar el tema puede verse PEYRANO, Guillermo F. Op. cit, nota n° 6, p. 134-141

[34] Ley 21.536, sancionada y promulgada el 14 de febrero de 1977.

Así en coherencia con lo dispuesto en el párrafo precedente la reglamentación en su artículo 5° agrega que, " En ningún caso se afectará el secreto bancario, quedando prohibida la divulgación de datos relativos a operaciones pasivas que realicen las entidades financieras con sus clientes, de conformidad con lo dispuesto en los arts. 39 y 40[36] de la ley 21.526".

Al respecto la Jurisprudencia de la Cámara Nacional en lo Comercial, Sala A que*: "Toda entidad bancaria puede –sin violar el secreto bancario- ofrecer información acerca de los datos identificatorios de su cliente; no así respecto de las operaciones por éste realizadas por cuanto ella es reservada, ya que desde el momento en que el cliente circula cheques, debe aceptar que los portadores de éstos están habilitados para indagar respecto de la identidad e identificación del librador"*[37]

IV. Conclusiones

Consideramos que las mismas, entonces, deben versar en torno a cuáles son los datos que siempre y en todos los casos requieran del consentimiento del interesado. La LPDP determina la necesidad de una u otra forma del consentimiento, del siguiente modo:

1) Datos de carácter personal que revelen la ideología, vida sexual, origen étnico o racial, convicciones filosóficas o morales, afiliación sindical, religión o creencias[38]: Para estos datos se exigirá el consentimiento expreso y por escrito, salvo cuando los ficheros que pertenezcan a la Iglesia católica, asociaciones religiosas y las organizaciones políticas y sindicales quienes pueden llevar sus registros por autorización de la propia LPDP, para el caso de recolección, porque para la fase de cesión del dato, si se produjera, sería – a nuestro criterio- necesario el consentimiento[39].

2) Datos de carácter personal que hagan referencia, a la salud [40]; para estos datos se

---

[35] WETZLER MALBRÁN, Germán, "Algunos Aspectos de la Información Crediticia" La Ley, 2002- F-, pág.1369

[36] La Ley de Entidades Financiera. Artículo 40.- *"Las informaciones que el Banco Central de la República Argentina reciba o recoja en ejercicio de sus funciones tendrán carácter estrictamente confidencial. Tales informaciones no serán admitidas en juicio, salvo en los procesos por delitos comunes y siempre que se hallen directamente vinculadas con los hechos que se investiguen. El personal del Banco Central de la República Argentina deberá guardar absoluta reserva sobre las informaciones* que lleguen a su conocimiento. *Las informaciones que publique el Banco central de la República Argentina sobre las entidades comprendidas en esta ley sólo mostrarán los totales de los diferentes rubros, que como máximo podrán contener la discriminación del balance general y cuenta de resu*ltados mencionados en el art. 36"

[37] CNCom, sala A, mayo 5/983 *"Lon, Fanny c. Noguera Canto, Juan"*, cit. por GOZAINI, Osvaldo, Op. cit, nota al pié n° 4, pág. 10

[38] Art. 2 de la LPDP, 2 párrafo "datos sensibles"

[39] Art. 7.3 de la LPDP

[40] Art. .2 LPDP

requerirá el consentimiento expreso del afectado o la autorización concedida por una ley fundada en razones de interés general[41].

Los datos relativos a la salud que sean objeto de tratamiento por parte de los organismos público o privados y los profesionales relacionados con la salud física o mental de los pacientes deben realizarse respetando el principio de secreto profesional[42]

A modo de ejemplo, y por la polémica que ha suscitado el tema en países europeos o en los Estados Unidos ¿Es lícito la publicación de listas de violadores o pederastas? ¿o implicaría la publicación de un "dato sensible" –salud y/o vida sexual- de las personas? En principio, sería directamente aplicable el régimen al que hemos hecho referencia por afectar de lleno a datos sobre salud y vida sexual -el caso de los malos tratos sería más discutible aunque también podrían atribuírsele caracteres de dato médico-psicológico-. Para este tipo de publicación, se requeriría, por tanto, el consentimiento expreso del propio pederasta o bien el que una ley autorizara dicha publicación. De no hacerse así, se estaría incurriendo en una flagrante vulneración de la normativa vigente. Claro está siempre queda la interpretación judicial que si bien propiciamos que en relación al tema del consentimiento debe ser de carácter restrictivo, ello no obsta a que en cada caso concreto realice una ponderación de valores en juego

3) Datos de carácter personal no incluidos en los grupos anteriores: Para la recolección de los datos de carácter personal no incluidos en los dos grupos anteriores el tipo de consentimiento requerido será el mismo al que hace referencia el propio concepto del artículo 5 de la Ley, es decir un consentimiento libre, expreso e informado, mediante el cual el interesado manifieste su aquiescencia con el tratamiento de datos personales que le concierne.

4) Las excepciones a la exigencia del consentimiento de datos personales son los que taxativamente enuncia la LPDP en la normativa del artículo 5 y 23.inc. 2. Y, en relación a la cesión de datos también las excepciones establecidas en el artículo 11 de la LPDP.-

[41] Art. 7 LPDP
[42] Art. 8 LPDP