Protección de datos personales para fines publicitarios. A propósito de la Disposición 4/2009 de la Dirección Nacional de Protección de Datos Personales.

Por Marcela I. Basterra.

SUMARIO: 1. Introducción. 2. El bien tutelado por el habeas data. 3. Los datos publicitarios en la ley 25.326. 4. La Disposición 4/2009 de la DNPDP. 5. Conclusiones.

1. Introducción.

Las nuevas tecnologías han avanzado de un modo significativo que ha inquietado, e introducido a los juristas en un análisis pormenorizado de la inserción de la informática en el ámbito jurídico[1].

La discusión recién ha comenzado y mientras continúe este proceso global, la protección jurídica de los derechos individuales a la luz de los avances tecnológicos es, sin duda, uno de los temas fundamentales.

Así, resulta innegable que el desarrollo de las nuevas tecnologías genera efectos en nuestra sociedad que tornan necesario el abordaje de determinados temas que, con anterioridad a esta "explosión informática", no eran siquiera imaginables. La velocidad con la que avanza la tecnología, en general, requiere que el legislador encuentre remedios jurídicos en tiempo oportuno.

La difusión de la informática en todos los aspectos de la vida social, ha dado nacimiento a nuevas posibilidades, nuevos intereses pero también nuevos peligros dando necesario nacimiento a una nueva disciplina jurídica.[2]

Se trata de salvaguardar los derechos de los individuos, en el caso particular en lo que hace a la preservación de su derecho a la intimidad, así lo expresa Vanossi[3] al alertar,

---

[1] Para ampliar el tema puede verse BASTERRA, Marcela I. "Protección de datos personales. Ley 25.326 y Dto 1558/01. Comentados. Derecho Constitucional Provincial. Iberoamérica y México". Ediar, UNAM, Buenos Aires., 2008.

[2] ETTORE, G., Manuale de direitto dell'Informática", Editorial Cedam, Padova, Italia, 1997, p. 3.

[3] VANOSSI, Jorge R, "El Derecho de Información" en Nuevos Derechos a la Información; Instituto de Investigaciones del Nuevo Estado de la Universidad de Belgrano, 1999, p. 21/22.

desde el principio, sobre la urgencia y la necesidad de la búsqueda rápida de soluciones desde el campo del derecho.

Recientemente, la Dirección Nacional de Protección de Datos Personales, dictó la Disposición Nº 4/09[4] mediante la cual establece que la opción para el ejercicio del derecho de retiro o bloqueo, prevista por la ley 25.326[5], deberá aparecer en toda comunicación que se efectúe con fines publicitarios, junto con el mecanismo previsto para su ejercicio.

En el presente analizaré la última disposición dictada por el órgano de control a la luz del derecho tutelado por la garantía del habeas data, considerando lo establecido por el artículo 27 de la ley de protección de datos personales.

2. El bien tutelado por el habeas data.

El hábeas data es una garantía que tiene por finalidad impedir que en bancos o registros de datos se recopile información respecto de la persona titular del derecho que interpone la acción, cuando la misma se refiere a determinados aspectos de su personalidad que se encuentran vinculados, en forma directa, con su intimidad.

Estos datos no deben estar a disposición del público en general, o ser utilizados en perjuicio de las personas por los organismos públicos o entes privados, sin derecho alguno que sustente dicho uso.

Concretamente, se trata de información relativa a la filiación política, ideas religiosas, militancia gremial, desempeño laboral, orientación sexual o aspectos de la salud de un individuo, entre otra.[6]

Esta garantía tiene a) una finalidad inmediata, que está comprendida por la posibilidad que tienen las personas de *"...tomar conocimiento de los datos a ella referidos y de su finalidad..."*; y b) de una finalidad mediata, en cuanto que, si dichos datos resultan *"falsos o discriminatorios podrá exigirse la supresión, rectificación, confidencialidad o actualización de los mismos"*.[7]

---

[4] Disposición Nº 4/2009, Publicada en el BO el 10/3/2009.

[5] Ley 25.326. Publicada en el BO el 2/11/2000.

[6] HITTERS, Juan Carlos. Boletines nº 26, p. 1260, Cit. por QUIROGA LAVIÉ, El Amparo, El Habeas Data y El Habeas Hábeas, Editorial Rubinzal-Culzoni, Buenos Aires, 1995, p. 157.

[7] BASTERRA, Marcela. La garantía constitucional del habeas data. En AAVV Derecho Procesal Constitucional MANILI, Pablo L, coordinador. Editorial Universidad, Buenos Aires, 2005, p. 141/186.

El hombre presenta una dualidad de tendencias instintivas, por un lado el ser humano tiene necesidad de saber y por otra de ocultar.[8] El punto justo se encuentra en establecer el equilibrio entre la necesidad de saber y la necesidad de ocultar, estableciendo los límites para que dentro de un sistema de garantías como el nuestro el ejercicio de un derecho no vaya en detrimento del ejercicio de otro.

El derecho a manejar información y el derecho a preservar una esfera de intimidad tienen su fundamento en la propia naturaleza humana, por ello constituyen derechos fundamentales que deben ser garantizados y regulados por el Estado.

La informática es, sin duda, uno de los grandes descubrimientos del siglo que, utilizada por la administración pública y por las empresas privadas, proporciona, entre otras cosas, eficiencia y eficacia, celeridad a la hora de tomar decisiones o de recabar informaciones, el medio ideal para brindar servicios públicos y privados, como así también el medio propicio para guardar datos de las personas.

El encuentro entre informática y administración ha producido una nueva rama del saber, una nueva manera de trabajar. Debemos tener presente que el uso de la informática en manos tanto del Estado, como en manos de los particulares, crea diversos riesgos que pueden suponer una amenaza de agresión a la intimidad de los gobernados o usuarios de servicios.

En tal sentido, en una encuesta realizada en 1971 por el *"Younger Committee on Privacy"*, que cuenta Adoración de Miguel Castaño en su obra "Derecho a la Información frente al Derecho a la intimidad", en la que se preguntaba: ¿Objetaría que se dispusiese de información sobre su...? (los números son el porcentaje de respuestas afirmativas –o sea que sí se objetaría-), vida sexual 87%, ingresos 78%, historial médico 51%, opiniones políticas 42%, número de teléfono 34%, dirección 33%, opiniones religiosas 28%, etcétera.

Méjan[9] define a la intimidad como *"el conjunto de circunstancias, cosas, experiencias, sentimientos y conductas que un ser humano desea mantener reservado para sí mismo, con libertad de decidir a quien le da acceso al mismo según la finalidad que persiga, que impone a todos los demás la obligación de respetar y que solo puede ser obligado a*

[8] MEJAN, Luis Manuel "El derecho a la Intimidad y la Informática", Editorial Porrúa, México, 1996, Segunda edición, p. 5.

[9] Ibídem, p.81/87.

develar en casos justificados cuando la finalidad perseguida por la develación sea lícita".

Así, quedan sentados dos principios básicos. El primero consiste en que el hombre tiene valores individuales que no pueden ser sacrificados jamás en aras de ningún otro valor, tal es el derecho a su propia intimidad. El segundo, que existen casos y circunstancias de excepción en que el valor comunitario, el bien general, debe prevalecer sobre los intereses particulares.

La información resulta útil e importante, sin embargo es innegable que en determinadas ocasiones sentimos amenazada nuestra intimidad. Por ello, el artículo 43 de la Constitución Nacional otorga el equilibrio necesario en tanto garantiza el acceso a las fuentes de información, para conocer los datos que se tengan en relación a la persona, la posibilidad de conocer la finalidad con que se han recabado dichos datos, si los mismos se consideran falsos, discriminatorios o sensibles y prevé la posibilidad de solicitar la supresión, rectificación, actualización y confidencialidad de los datos. Queda, entonces tutelada la "intimidad informática de las personas".

Sin embargo, el artículo 43 de la Constitución Nacional nada dice en relación a los derechos protegidos por el habeas data. En efecto, la garantía se establece como la posibilidad de acceso a los datos personales, la finalidad que se dará a los mismos y la posibilidad, según los casos, de rectificación, supresión, confidencialidad y actualización de éstos.

Vanossi al referirse a los bienes jurídicos tutelados expresa *"de nada sirve que llenemos los anaqueles con dispositivos legales que protejan otros aspectos como los bienes u otros desenvolvimientos de es misma persona, si no empezamos por proteger lo más inherente a esa propia persona, que es el derecho a su perfil y el derecho a su imagen"*[10].

Comparto la posición de Bazán[11], quien considera que esta novel garantía constitucional es el reflejo de la necesidad de abrir camino a un nuevo derecho o, al menos, a la reformulación de uno clásico cuyos contornos se han visto desbordados o erosionados por la realidad. Justamente, se refiere al derecho a la autodeterminación informativa. En tal sentido, el autor cita la sentencia del Tribunal Constitucional Federal Alemán, del

[10]VANOSSI, Jorge R, "El "Habeas Data": no puede ni debe contraponerse…" Op. Cit, p. 954.

[11] BAZAN, Víctor, "El Habeas Data y la Custodia al Derecho a la Autodeterminación Informativa". Boletín Asociación Argentina de Derecho Constitucional, Nº 142, p. 9.

15/12/1983, en la que se declaró parcialmente inconstitucional la ley germana del censo de población de 1982 donde se sostuvo que *"el habeas data brinda cauce de tutela a la libertad informática, que da pié a la existencia de un derecho autodeterminativo que va ganando adeptos en la doctrina y jurisprudencia europeas..."*.

Siguiendo a Pérez Lueño, pondera el mérito de la sentencia en haber entendido el derecho a la intimidad, en el caso, el derecho a la autodeterminación informativa, como la facultad de la persona de *"decidir básicamente por sí misma cuándo y dentro de que límites procede revelar situaciones dentro de la propia vida"*.

En consecuencia, considero que el habeas data tutela en forma directa el derecho a la intimidad informática y a la propia imagen, los que quedan subsumidos en un solo derecho que es el derecho a la autodeterminación informativa, que implica la posibilidad de decidir qué datos queremos proporcionar y cuáles deseamos mantener en reserva, alejados del acceso de los demás.

3. Los datos publicitarios en la ley 25.326.

La ley de protección de datos personales, en el artículo 27 establece un régimen especial para los registros, archivos, o bancos de datos con fines publicitarios, promocionales o comerciales, a los que también les son aplicables las regulaciones establecidas para los archivos destinados a proporcionar informes de carácter privado.

No obstante, la reglamentación de la norma admite operaciones de tratamiento de datos con fines publicitarios en determinados supuestos, sin que medie el consentimiento de sus titulares.

En tal sentido, el legislador permite que en la recopilación de domicilios, reparto de documentos, publicidad o venta directa, se procesen datos personales aptos para la conformación de "perfiles" de sus titulares con fines promocionales, comerciales o publicitarios, o bien, para determinar hábitos de consumo, a efectos de desarrollar la difusión de determinados productos y servicios y poner a disposición de los titulares de los datos recolectados ofertas a medida de sus preferencias y necesidades.

Según Francois Rigaux[12] *"... la noción de perfil, cuya utilización no está reservada a las investigaciones criminales, presenta una estricta analogía con el racismo. Servirse*

[12] RIGAUX, François, "*La protection de la vie privée..."* p. 597, citado por PEYRANO, Guillermo F., Régimen Legal de los Datos Personales y Hábeas Data. Comentario a la ley 25.326 y a la reglamentación aprobada por Dec. 1558/2001, Lexis Nexis, Depalma, Buenos Aires, 2002, p. 250.

de un perfil consiste en imputar a un individuo ciertos hechos de comportamiento que serían comunes al grupo al cual está considerado pertenece, y distinguirían los miembros del grupo dentro de la población global(..) se fragmentaría la sociedad en subcolectividades, obedeciendo ello a la selección de algunas normas de conducta determinantes, obedeciendo ello a la selección de algunas normas de conducta determinantes, y más caracterizadas que las del promedio de la población y cuyos rasgos específicos podrían ser imputados a cada uno de los miembros del grupo. Semejante previsión es generalmente proclive a motivar un comportamiento discriminatorio respecto del sujeto (...).

Es entonces que esta garantía constitucional no se circunscribe únicamente a la protección de la intimidad y el honor, sino que, como lo expuse anteriormente, tutela el derecho a la intimidad, pero no en forma genérica, sino a una especie de intimidad, "la intimidad informática" que implica la autodeterminación informática y, a través de ella, el derecho a la imagen o el propio perfil.

El legislador, con el objeto de preservar el derecho a la intimidad de los titulares de los datos en cuestión, dispone que para la recopilación de este tipo de información se requiere que la misma esté disponible en documentos accesibles al público, o que haya sido facilitad por sus titulares u obtenida con su consentimiento.

El consentimiento exigido por la ley 25.326 para el tratamiento de datos de carácter personal surge con claridad del artículo 5º de la ley y es, sin duda, uno de los puntos cardinales de los principios que ordenan la normativa[13].

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 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[14], o sea que dicha legitimación va a estar condicionada al consentimiento que se haya prestado para el uso del dato personal.

---

[13] Véase 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.

[14] Directiva 95/46/CE.

Entonces, 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.

Justamente, al prestar nuestra conformidad para el tratamiento del dato personal estamos eligiendo 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[15], 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 6º y, taxativamente en cinco incisos detalla las circunstancias en las que no será necesario el consentimiento del titular de los datos.

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 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.

Efectivamente, el artículo 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

[15] 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.

se recogen, con las menciones requeridas por el legislador, es el medio más efectivo de prueba del consentimiento del afectado.

Sin embargo, entiendo que no siempre y en todos los casos debe exigirse la firma del titular de los datos con posterioridad, si no surge fehacientemente que se prestó el consentimiento, sino solo en determinados casos concretos.

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

A mayor abundamiento, 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 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*)[16] 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

[16] 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. 73/75

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 artículo 4.1 y 4.3 de la LPDP.

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 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 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 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.

Ahora bien, el principio de limitación de la recolección, que requiere el consentimiento del sujeto para la incorporación de cada dato (que no sea con límites, como en el caso), si se lo llevara a la práctica en forma estricta, condenaría a los bancos de datos a la desaparición".

Los derechos a la autodeterminación informática, a la intimidad y a la propia imagen[17]

[17] BASTERRA, Marcela "Habeas Data: Derechos Tutelados" LL, Doctrina Judicial, 1999-3, p. 77.

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.

Así, con idéntico objetivo además de evitar ofertas no deseadas, el legislador reconoce en el artículo 27, inciso segundo y tercero, respectivamente, el derecho de acceso de estos titulares, el cual podrá ser ejercido sin límite de tiempo y en forma gratuita y, los derechos retiro y bloqueo de los datos a ellos referidos de los archivos respectivos.

Fel primer inciso no surge claramente la voluntad del legislador en lo que respecta a, si el consentimiento del titular de los datos tratados, cuando no se encuentren en fuentes de acceso público, debe prestarse igualmente, tanto para la formación de perfiles determinados con fines publicitarios, comerciales y promociónales, como para establecer hábitos de consumo.

La duda fue despejada por el inciso 1° de la reglamentación al artículo 27 en tanto dispone que *"podrán recopilarse, tratarse y cederse datos con fines de publicidad sin consentimiento de su titular, cuando estén destinados a la formación de perfiles determinados que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios"*.

Cabe mencionar que ni las fuentes españolas de nuestra ley de protección de datos personales realizan esta distinción, así como tampoco existen en el debate parlamentario indicios de que ésta haya sido la intención del legislador nacional.

Ahora bien, con relación a los derechos de los titulares a los registros de este tipo de informaciones, el inciso segundo se refiere al derecho de acceso, el cual podrá ser ejercido sin limitaciones temporales ni económicas a fin de conocer los datos que sobre su persona se tengan recolectados con fines publicitarios, comerciales o promocionales.

Esta prescripción, elimina, respecto de este tipo de archivos, la limitación temporal del artículo 14, inciso 3° en tanto dispone que el derecho de acceso sólo puede ser ejercido

en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo.

Por su parte, los derechos de retiro o bloqueo del nombre del titular de los bancos de datos previstos en el inciso 3°, también pueden ser ejercidos en cualquier momento y, como bien explica Peyrano[18], constituyen variantes del procedimiento de "disociación de datos" definido en el artículo 2° de la LPDP, dado que su resultado produce la desvinculación de las informaciones de sus titulares.

En efecto, retirar el nombre del titular implica equilibrar la información, dado que la supresión del nombre del titular del registro o archivo de datos, implica que el mismo (dato) dejará de ser personal. Esto es se disociará, dejando de pertenecer a una persona determinada o determinable.

De otro lado, el derecho de bloqueo del nombre es una operación de carácter transitorio, prevista como medida cautelar en la acción de habeas data, que no implica la eliminación del dato bloqueado de la base de datos, sino, simplemente que no podrá proporcionarse. Al tiempo que, el bloqueo de los datos significa una forma de sometimiento a "confidencialidad" de los mismos, que en el caso en estudio alcanza al nombre del titular de éstos.

El decreto 1558/01, dispone *"las cámaras, asociaciones y colegios profesionales del sector, que dispongan de un Código de Conducta homologado por la Dirección Nacional de Protección de Datos Personales, al que por estatuto adhieran obligatoriamente todos sus miembros, junto con la autoridad de aplicación, implementarán, dentro de los noventa días siguientes a la publicación de esta reglamentación, un sistema de retiro o bloqueo a favor del titular del dato que quiera ser excluido, de las bases de datos con fines de publicidad. El retiro podrá ser total o parcial, bloqueado exclusivamente, a requerimiento del titular, el uso de alguno o algunos de los medios de comunicación en particular, como el correo, el teléfono, el correo electrónico u otros".*

Si bien esta prescripción se refiere al bloqueo y retiro de los "medios de comunicación" de los datos objeto de tratamiento, y no del "nombre" del titular de los mismos, como lo establece el inciso 3°, tal disposición debe ser interpretada como complementaria de esta última, y no como la instrumentación de un sistema cuya finalidad difiere de la perseguida por la norma reglamentada.

[18] PEYRANO, Guillermo F. "Régimen legal de los datos personales..." Op. Cit., p. 253.

En ese sentido, el párrafo tercero de la reglamentación determina que "e*n toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, internet u otro medio a distancia a conocer, se deberá indicar, en forma expresa y destacada, la posibilidad del titular del dato de solicitar el retiro o bloqueo, total o parcial, de su nombre de dicha base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó la información".* Este es el único caso en que la LPDP se refiere en forma expresa al derecho de acceder a la fuente de información.

Por otra parte, la ley no ha fijado un plazo específico para que el responsable o usuario del banco de datos con fines de publicidad cumpla con el retiro o el bloqueo solicitado, según corresponda. Entiendo que, entonces, debe aplicarse el plazo de 5 días previsto en el artículo 16 inciso 2, en tanto se refiere al derecho de rectificación, actualización o supresión.

Si bien es cierto que la ley faculta a las empresas a llevar a cabo actividades de marketing, en forma correlativa hace que los titulares de los datos se hagan cargo de los instrumentos necesarios para la salvaguarda del derecho a la autodeterminación informativa, el que incluye, por supuesto, no estar en esas bases de datos e incluso el derecho a no ser molestado con ofertas indeseadas, posteriormente a haber expresado claramente su voluntad de no recibir más información.

Así, quienes realizan marketing no pueden valerse de cualquier dato, debiendo cumplir con los principios de finalidad, información y notificación, previstos en los artículos 4º y 6º de la ley de protección de datos personales, respectivamente.

4. La Disposición 4/2009 de la DNPDP.

La Disposición dictada recientemente por el órgano de control en materia de protección de datos personales, establece que *"en las comunicaciones con fines de publicidad directa, el banco de datos emisor debe incorporar un aviso que informe al titular del dato sobre los derechos de retiro o bloqueo total o parcial, de su nombre de la base de datos, el mecanismo que se ha previsto para su ejercicio, con más la transcripción del artículo 27, inciso 3, de la Ley Nº 25.326 y el párrafo tercero del artículo 27 del Anexo I del Decreto Nº 1558/01*"[19]

[19] DNPDP, Disposición 4/2009, artículo 1º.

Asimismo, en el artículo 2º dispone que, cuando se efectúen envíos de comunicaciones de publicidad directa no requeridas o consentidas previamente por el titular del dato personal, el banco de datos debe advertir, de modo destacado el hecho de que se trata de una publicidad o, cuando se trate de publicidad enviada mediante correo electrónico, en el encabezado se debe insertar el término único "publicidad".

Por último, el artículo 3º agrega que el banco de datos emisor deberá verificar que los mecanismos previstos para el ejercicio del derecho de retiro o bloqueo cuentan con suficiente capacidad operativa para responder al eventual ejercicio de tal derecho por parte de los titulares de los datos.[20]

Tal como lo señalé, el artículo 27 de la ley de protección de datos personales, en el inciso tercero establece que en cualquier momento, el titular de los datos, tiene el derecho de solicitar el retiro o bloqueo de su nombre de los bancos de datos con fines publicitarios.

A mayor abundamiento, la disposición 7/2005 de la Dirección Nacional de Protección de Datos Personales, al reglamentar las sanciones, establece como falta expresamente "n*o cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido por el titular. Entiéndese incluida en este supuesto la negativa a retirar o bloquear el nombre y dirección de correo electrónico de los bancos de datos destinados a publicidad cuando su titular lo solicite de conformidad con lo previsto en el último párrafo del artículo 27 de la Ley 25.326"*[21]

Además, cabe destacar que, aunque no se ha reglamentado la forma en que el titular de los datos puede ejercer los derechos de pedido y bloqueo, en principio, corresponde la forma escrita. Sin embargo, entiendo que ello no obsta a la posibilidad de utilizar medios similares a aquél medio por el cual se recibe la publicidad.

En efecto, un particular que recibe un correo no deseado o *spam*, puede solicitar por e-mail el retiro o bloqueo correspondiente.

Estos mensajes *spam,* habitualmente de tipo comercial, no solicitados y en cantidades masivas son enviados por distintas vías. La más utilizada entre el público en general es la basada en el correo electrónico, no obstante que otras tecnologías de internet, que han

---

[20] DNPDP, Disposición 4/2009, artículo 3º: *"En las comunicaciones a que aluden los artículos precedentes, el banco de datos emisor deberá verificar que los mecanismos previstos para el ejercicio del derecho de retiro o bloqueo cuentan con suficiente capacidad operativa para responder al eventual ejercicio de tal derecho por parte de los titulares de los datos".*

[21] DNPDP, Disposición 7/2005, Publicada en el BO el 11/11/2005.

sido objeto de spam, incluyen mensajes, grupos de noticias *usenet*, motores de búsqueda y blogs. Además, el spam también puede tener como objetivo los teléfonos móviles a través de mensajes de texto y los sistemas de mensajería instantánea.

Cabe traer a colación el caso "*Tanús Gustavo Daniel y otro c/ Cosa Carlos Alberto y otro s/ habeas data (art. 43 c.n"*[22], en el que la justicia ordenó cesar el envío de *spam* debido a que los demandados incumplían con las disposiciones de la ley de protección de datos personales[23].

Los actores, Gustavo Tanús y Pablo Andres Palazzi iniciaron la demanda en el año 2003 ante el resultado negativo que tuvieron los pedidos efectuados a los demandados, Carlos Cosa y Ana Carolina Elizabeth Magraner para que no les enviaran más correo *spam.*

Como medida cautelar, el juez ordenó que los accionados se abstuvieren de enviar mensajes a las casillas de los actores así como, transferir o ceder a terceros la dirección de su correo electrónico u otro dato personal que se vincule a ellos.

De la prueba realizada en el juicio se demostró que los actores habían recibido el correo *spam* y que solicitaron poder acceder a sus datos obrantes en las bases de datos de los demandados y ser removidos de ellas, pero obtuvieron resultados infructuosos.

El juez de primera instancia resolvió sobre la base de las disposiciones del artículo 27 de la ley 25.326 y el decreto reglamentario Nº 1558/01, en tanto regulan el funcionamiento de las bases de datos de marketing y permiten que los titulares de datos que reciban publicidades de parte de éstas soliciten su remoción.

Asimismo, el juez entendió que los demandados, al ofrecer un servicio de correo electrónico ocultando el remitente, violaban las disposiciones de la LPDP ya que de ese modo se dificulta el acceso al responsable de las bases de datos, conforme lo establece el artículo 6º de la ley reglamentaria.

Por otro lado el tratamiento que los demandados hacían de los datos tenía un propósito distinto de su finalidad originaria, por lo que incumplían también con el principio de finalidad establecido en el artículo 4º de la ley 25.326.

---

[22] JCivyCom Nº 3, Sec.6, *"Tanús Gustavo Daniel y otro c/ Cosa Carlos Alberto y otro s/ habeas data (art. 43 c.n.)"*, del 7/4/2006

[23] MINOTTI, Sebastian E, "La justicia ordenó cesar en el envío de SPAM por violar la Ley de Protección de Datos Personales". Comentario al Fallo: JCivyCom Nº 3, Sec.6, *"Tanús Gustavo Daniel y otro c/ Cosa Carlos Alberto y otro s/ habeas data (art. 43 c.n.)"*, del 7/4/2006. Publicado en El Dial, www.eldial.com, elDial - DC8D8.

Si bien no hubo condena por daños, la sentencia reconoció e que la recepción de *spam* ocasiona un costo económico a cargo del receptor, por el tiempo que lleva descargarlos, identificarlos, seleccionarlos y borrarlos, así como también el incremento del costo de recepción y procesamiento de correo electrónico.

Además, genera la necesidad de implementar sistemas para bloquear y, aún, lograr la protección de los virus que pueden dispersar, así como también el perjuicio que se crea en los equipos informáticos por la fragmentación que tiene lugar durante el almacenamiento y la eliminación de los archivos.

Por último, y en lo que hace al bien tutelado por la garantía del habeas data, la sentencia resolvió que la actividad de los demandados comportaba una invasión a la intimidad y a la tranquilidad de los actores.

Siguiendo este lineamiento, según surge de los fundamentos de la disposición de la Dirección Nacional de Datos Personales, el derecho de solicitar el retiro o bloqueo que el legislador le otorga a los titulares de los datos, es conocido comúnmente a través de la voz inglesa *opt out*, que alude a la opción de ser excluido de una lista de distribución.

En consecuencia, todas las comunicaciones publicitarias, sin importar el medio por el cual se realicen deben indicar al titular, de forma expresa y destacaba, la posibilidad de solicitar el retiro o bloqueo, sea total o parcial, de su nombre de la base de datos.

Es que, al no existir una ley que establezca la obligación de los bancos de datos emisores de publicidades no solicitadas de permitir al titular del dato la remoción de su nombre de la base de datos respectiva, es lógica la previsión del órgano de control de exigir que la misma sea citada expresamente en las comunicaciones remitidas con fines publicitarios.

De este modo, los titulares pueden fácilmente tomar conocimiento de que esa opción es un derecho que les corresponde, debido a que no siempre existe una solicitud previa del titular del dato y deben saber que se trata de una publicidad.

6. Conclusiones.

A los fines de permitir un mejor ejercicio de los derechos del titular del dato en las actividades de publicidad directa, resulta conveniente instrumentar mecanismos que permitan identificar con facilidad las comunicaciones no requeridas.

Sin perjuicio del gran avance que implica hoy en día acceder a internet, no se puede afirmar que la red sea una fuente de acceso público irrestricto en los términos de la ley

de protección de datos personales.[24] En efecto, gran parte de los datos personales que se encuentran en internet son publicados sin el consentimiento de su titular.

No obstante, la mayoría de los datos personales que circulan en la red fueron dados por los titulares en virtud de un interés propio que consiente la publicidad de los mismos para fines específicos preestablecidos. Justamente, la licitud de estos datos suministrados por internet, está dada porque los mismos solo pueden utilizarse para el fin específico para el cual fueron publicados, y no para otros.

Es que, si nuestra intimidad se ve menoscabada y perturbada cuando alguien se intromete sin nuestro consentimiento en algún aspecto de nuestra vida privada, sin duda, esa intromisión constituye una lesión al derecho a la intimidad.

[24] FRENE, Lisandro. "El 'Spam' a la luz de la Ley de Protección de Datos Personales". Publicado en El Dial, www.eldial.com DC890