EDITORIAL ASTREA

*El consentimiento para el tratamiento de datos personales en el régimen de la ley 25.326**

Imposibilidad de usar el silencio del titular del dato personal a favor del responsable del tratamiento

Por Pablo A. Palazzi

1. Introducción: la plataforma fáctica

El caso que comentamos se origina cuando una entidad financiera decidió comunicar a sus clientes –mediante un folleto donde describía su política de privacidad– que compartiría con terceros los datos personales que tenía sobre ellos, a menos que éstos formularan una oposición expresa en un formulario que a tal efecto se acompañaba. Dicho formulario debía ser enviado por correo dentro de un plazo determinado unilateralmente por la entidad financiera. Vencido dicho plazo sin haber formulado oposición, el banco presumía el consentimiento del cliente para el tratamiento de datos personales.

2. La decisión judicial

El hábeas data fue iniciado por un cliente del banco que había recibido la referida comunicación (que el banco denominó "promesa de confidencialidad"). Mediante la promoción de dicha acción se solicitó acceso a los datos personales y confidencialidad de la información, esto es, que la demandada no compartiera los datos personales del cliente como se había informado que sucedería.

En este caso, el juzgado comercial de primera instancia hizo lugar al hábeas data ordenando "resguardar y conservar la confidencialidad de los datos que, respecto del actor, pudiere mantener en sus registros, que no podrán ser cedidos a terceros, salvo por imperativo legal, sin el previo consentimiento del demandante"[1]. Para ello, luego de recordar la política de privacidad informada por el banco al cliente sostuvo que "de todo lo analizado se desprende que el banco, sin la previa autorización de su cliente, proveyó o unilateralmente se facultó para dotar a compañías no individualizadas y según su criterio de selección de 'buena reputación', información crediticia y de riesgo (cláusula 8° del folleto), salvo que ese cliente pretenda su exclusión que, en ese caso, se hará efectiva en un lapso no mayor de noventa días". Consideró, en definitiva, que "tal y como fue pergeñado, el sistema implementado en el mencionado folleto violenta lo dispuesto por los arts. 5° y 11 de la ley 25.326".

Apelada la decisión, la Sala D de la Cámara Comercial la confirmó por los fundamentos del dictamen de la fiscalía y los suyos esbozados en la sentencia que seguidamente comentaremos[2].

---

* Bibliografía recomendada.

[1] JuzgCom n° 2, secretaria 3, 29/6/05, "Salvador, Claudio c/Citibank".

[2] CNCom, Sala D, 22/11/05, "Salvador, Claudio c/Citibank", *ED*, 218-353.

En su expresión de agravios la entidad financiera sostuvo que: *a*) no era una entidad destinada a proveer informes; *b*) que había sujeto a confidencialidad los datos personales y no los cedió a terceros; *c*) que las personas que recibirían los datos del banco serían sujetos entrenados en el manejo de datos personales y que si no cumplían con la promesa de confidencialidad serían sancionados, y por último *d*) que la ley autoriza a no recabar el consentimiento de los titulares con respecto a cierta clase de datos.

El dictamen de la fiscalía ante la Cámara Comercial[3], al que la Cámara se remitió, se encargó de refutar cada uno de estos agravios con fundada solvencia. Respecto a la falta de legitimación, se entendió que el banco demandado era legitimado pasivo en los términos del art. 35 de la ley 25.326. Añadió asimismo que la promesa de confidencialidad mencionaba la posibilidad de ceder los datos personales a terceros. En consecuencia, se consideró que la entidad bancaria era legitimada pasiva porque cedía datos a terceros.

La Cámara confirmó por similares fundamentos al sostener que "Por lo demás y referido a los agravios sostenidos por el demandado dirigidos a su falta de legitimación pasiva, destacase que si bien su finalidad no es la de proveer informes, distintas circulares del BCRA establecen que tales entidades deben suministrar determinada información, todo lo cual frente a la amplitud del carácter tuitivo con que la ley faculta demandar y en función de lo previsto en los arts. 22 y 33, determina el rechazo de la defensa articulada". Añadimos, por nuestra parte, que se trata de un tema que ya no admite discusión en doctrina ni en jurisprudencia[4].

Luego, el dictamen de la fiscal general evalúa si la política de privacidad del banco demandado cumplía con la ley 25.326 de protección de datos personales. La respuesta fue negativa por diversos motivos.

Primero, se señala que la política de privacidad pone a cargo del cliente del banco la realización de un trámite adicional para evitar la cesión de sus datos personales, lo cual violenta la ley 25.326 (como se dictaminó con anterioridad en el caso "Unión de Usuarios y Consumidores c/Citibank"), dado que se invierte la regla del "consentimiento expreso y por escrito" prevista en la ley. Se recuerda en este sentido el principio de lealtad y licitud y la exigencia del consentimiento requeridos por los arts. 5°, 6° y 11 de la ley 25.326.

Segundo, se recurre asimismo –como pilar de este razonamiento–, al principio de finalidad previsto en el art. 4.3 de la citada ley, que dispone que los datos no pueden ser usados para una finalidad distinta o incompatible con aquellos que motivaron su obtención, y se concluye que el uso para fines tales como marketing implica infracción a este principio, pues los clientes del banco no dieron su consentimiento para esta finalidad.

Tercero, se rechaza la defensa esgrimida por el banco demandado basada en el art. 5°, parr. 2°, inc. *c* de la ley 25.326 (que dispone que no es necesario el consentimiento cuando los datos se limiten a nombre, documento de identidad, identificación tributaria o provisional, ocupación, fecha de nacimiento y domicilio). Se dan

[3] Dictamen 108.590/05, expte. 90.107, "Salvador c/Citibank s/amparo".

[4] El tema lo tratamos en nuestra nota *Ámbito de aplicación de la ley de protección de datos personales*, *JA*, 2002-III-26.

dos motivos para esta conclusión. En primer lugar, que la mencionada política no limita su aplicación a estos datos solamente. En segundo lugar, se concluye que una cesión sólo de esos datos "importaría ceder implícitamente un dato que excede los previstos en el art. 5°, parr. 2°, inc. *c*, esto es, que el titular de los datos es cliente del banco".

Consideramos que el caso es un importante precedente para el derecho argentino de protección de datos personales y sobre todo para el principio del consentimiento en el tratamiento de datos personales –que es una de sus directrices fundamentales–[5] y otros principios de similar importancia, que las decisiones de ambas instancias y el dictamen fiscal supieron hacer valer, y que comentamos en esta nota.

3. Comentario

El tema central del litigio consistía en determinar si es posible considerar que ha existido consentimiento para el tratamiento de datos personales por el silencio del titular de los datos o por el mero transcurso del tiempo. La propuesta del banco, al asumir que el cliente daba su consentimiento si no se oponía en cierto plazo, intentaba equiparar el silencio al consentimiento.

Este tipo de ofertas reciben el nombre de "opciones negativas". Se denominan "opciones" porque engañosamente se le da al consumidor la falsa posibilidad de optar. Son negativas, porque en realidad la única opción que tiene el consumidor, dado que la oferta ya presupone que el consumidor contestó por el "si", es dar un "no" para rechazar el supuesto acuerdo.

El problema no es novedoso, pues la discusión sobre los efectos del silencio como reemplazo del consentimiento ya se había planteado con anterioridad en el derecho de los contratos y en el derecho del consumidor. Las conclusiones y fundamentos que allí se elaboraron son plenamente aplicables al régimen de protección de datos personales, por lo que comenzamos nuestro análisis con una breve reseña sobre el silencio en la formación de los contratos.

a. El silencio en la formación de los contratos

En un artículo[6] escrito antes de que en nuestro país se aprobara la ley de defensa del consumidor, Leiva Fernández criticaba la práctica de enviar ofertas comerciales con una cláusula por la cual se le hace saber al destinatario que si no remitía un cupón dentro de cierto tiempo se juzgaría aceptada la oferta y prestado el consentimiento para la celebración del contrato recibiendo el bien en cuestión con una liquidación mensual. El autor concluía que en la formación de los contratos entre ausentes resultan ineficaces las ofertas en la que se provea que ante el silencio o falta de contestación del destinatario el oferente juzgará aceptada su propuesta.

[5] Palazzi, Pablo, *El hábeas data y el consentimiento para el tratamiento de datos personales*, *JA*, 1999-IV-399.

[6] Leiva Fernández, Luis F. P., *El silencio en la formación de los contratos (Si Ud. no manda este cupón)*, *LL*, 1991-A-987.

Leiva Fernández fundaba sus conclusiones en el art. 19 de la Const. nacional ("*ningún habitante de la Nación será obligado a hacer lo que la ley no manda*"), en el art. 919 del Cód. Civil[7], y en las interpretaciones doctrinarias y jurisprudenciales del silencio, que exigían una relación jurídica preexistente para darle valor positivo a la omisión de hacer o decir algo. La doctrina civilista fue unánime en esta posición, e incluso calificó estas prácticas con el término más grave de captación dolosa de la conclusión de un contrato[8].

En definitiva, como la ley no lo obliga, el recipiendario de una propuesta negativa no tiene porqué pronunciarse sobre la misma ni sentirse obligado a expresarse de tal o cual forma[9]. Las mismas conclusiones se adoptaron en jornadas y congresos de juristas. A modo de ejemplo, en el VII Encuentro de Abogados Civilistas realizado en la Ciudad de Rosario en junio de 1993 se concluyó en el punto III que el silencio tiene valor como manifestación de voluntad cuando existe un deber de explicarse por ley, o cuando dicho deber emerge de la relación entre el silencio actual y las declaraciones precedentes[10].

Toda esta argumentación no resultó más necesaria a partir de la vigencia de la ley 24.240 de defensa del consumidor, cuyo art. 35 –coincidiendo con pautas similares del derecho comparado[11]– dispone:

"*Queda prohibida la realización de propuesta al consumidor, por cualquier tipo de medio, sobre una cosa o servicio que no haya sido requerido previamente y que genere un cargo automático en cualquier sistema de débito, que obligue al consumidor a manifestarse por la negativa para que dicho cargo no se efectivice. Si con la oferta se envió una cosa, el receptor no está obligado a conservarla ni a restituirla al remitente aunque la restitución pueda ser realizada libre de gastos*".

---

[7] Que dispone "El silencio opuesto a actos, o a una interrogación, no es considerado como una manifestación de voluntad, conforme al acto o a la interrogación, sino en los casos en que haya una obligación de explicarse por la ley o por las relaciones de familia, o a causa de una relación entre el silencio actual y las declaraciones precedentes".

[8] Campoamor, Clara, *Del silencio como tácita manifestación de voluntad*, *JA*, 1947-I-7.

[9] La doctrina ha elaborado numerosos fundamentos para sostener la inadmisibilidad de una declaración unilateral de voluntad en la cual se impone a otro la carga de rechazarla para no quedar obligado. Puede consultarse el citado artículo de Leiva Fernández y también de Méndez Sierra, Eduardo C., *El silencio frente a la buena fe y los requerimientos privados*, *LL*, 1994-A-670 y autores citados en la nota al pie n° 38 del referido artículo.

[10] *LL*, 1994-A-685.

[11] Bajo la directiva 97/7/EC de la Unión Europea sobre contratos celebrados a distancia, cualquier intento de interpretar el silencio como consentimiento resulta ineficaz. A la misma conclusión se llegó en Estados Unidos prohibiéndose tales prácticas por la Postal Reorganization Act de 1970 (39 USC, 3009). Asimismo, bajo el *common law*, se considera que en estos casos no existe contrato. Ver Lamont, Dennis D., *Negative option offers in consumer service contracts: a principled reconciliation of commerce and consumer protection*, 42 UCLA L. Rev. 1315, 1995, quien sostiene "*The fundamental premise of silence as acceptance runs against the principles of common law. Common law imposes minimum procedural requirements to protect the integrity of a contract when a court is forced to resolve a disagreement between parties. Although the common law has exceptions related to a course of conduct to permit silence to act as acceptance, a unilateral negative option cannot fit within the ambit of those exceptions. Therefore, common law reduces a unilateral negative option to a legal nullity. If a court tested a unilateral negative option contract executed by a service provider, it would have no choice but to hold that there is no contract*". En igual sentido respecto a Canadá ver Bowal, Peter, *Reluctance to regulate: the case of negative option marketing*, 36 Am. Bus. L. J. 377, 1997.

La jurisprudencia que interpretó esta norma ha amparado a los consumidores contra este tipo de prácticas abusivas desde la óptica del derecho del consumidor[12], lo cual a nuestro entender, importó una variante en las prácticas bancarias donde el silencio –en general– se equipara al consentimiento[13]. No obstante ello, ya existían precedentes jurisprudenciales franceses que rechazaron el intento de otorgar efecto positivo al silencio en prácticas bancarias[14].

El autor ya citado señalaba una consecuencia lógica de su posición: de extenderse la práctica criticada, debería dedicarse una importante fracción de tiempo y esfuerzo en remitir cupones a cientos de oferentes so pena de resultar contratantes de múltiples bienes y servicios no buscados[15].

Podemos trasladar esta argumentación al caso de los datos personales y llegar a las mismas conclusiones. Los receptores de estas ofertas negativas en las cuales se les exige una acción positiva deberán dedicar gran parte de su tiempo a escribir estas cartas o notas solicitando que no se proceda al tratamiento de sus datos personales, cuando la regla vigente es justamente la opuesta: el *opt in* o el recaudo de obtener *el consentimiento expreso* del titular de los datos.

Cabe añadir que, si bien para cualquier abogado tal tarea puede resultar sumamente sencilla, el común de la gente (es decir, el consumidor o el titular de los datos: léase *Doña Rosa*) no saben cómo realizar estos menesteres o si los mismos requieren alguna clase de formalidad para que sean válidos y vinculantes jurídicamente. Dada la escasa entidad que se suele atribuir a los derechos que el titular tiene en materia de protección de datos personales[16], es probable que tampoco se mo-

[12] Ver entre otros los siguientes casos: CNContAdmFed, Sala I, 1/7/99, "Citibank c/Sec. de Comercio e Inversiones, Disp. DNCI 1273/98" (débitos automáticos ofrecidos por entidad financiera); íd., Sala II, 28/4/98, "Pegaso SA c/Sec. de Comercio e Inversiones, Disp. DNCI" (revista enviada en forma gratuita que incluía la carga de manifestarse por la negativa a fin de cancelar la recepción mensual de esa publicación); íd., Sala IV, 27/11/03, "Banco Francés SA c/ Disp. DNCI 135/02 (expte. 607-001450/98)" (entidad bancaria que procuró imperativamente imponerle la adopción de una tarjeta de crédito a un eventual cliente mediante el envío de un ejemplar a su nombre y la consiguiente apertura del crédito correspondiente viola el art. 35 de la ley 24.240); íd., Sala III, 23/9/99, "Citibank c/Sec. de Comercio" (el banco incurre en la sanción prevista en el art. 35 de la ley 24.240, al implementar compulsivamente un débito, en los resúmenes mensuales de las tarjetas de crédito, cuando el cliente no lo había autorizado a realizar); íd., Sala III, 15/8/00, "Banco de Galicia y Buenos Aires c/Sec. de Industria, Comercio y Minería, Disp. DNCI 126/00" y CNCom, Sala C, 4/10/05, "Unión de Usuarios y Consumidores c/Banco de la Provincia de Buenos Aires s/sumarísimo" (débito automático impuesto por entidad financiera con cargo a un seguro de robo en cajeros automáticos que nunca fue solicitado por los clientes).

[13] Nos refirimos específicamente a los casos donde, transcurrido el plazo para impugnar un resumen de cuenta bancaria remitido al cliente, éste se considera aprobado si el consumidor no formula objeciones. Un claro ejemplo es el art. 793 del Cód. de Comercio.

[14] Ver los fallos citados en nota al pie n° 23 del trabajo de Leiva Fernández, *El silencio en la formación de los contratos (Si Ud. no manda este cupón)*, *LL*, 1991-A-987 y los casos citados por Halperin, Isaac, *El silencio en la formación de los contratos*, *LL*, 3-33.

[15] Leiva Fernández, *El silencio en la formación de los contratos (Si Ud. no manda este cupón)*, *LL*, 1991-A-987.

[16] Ver Froomkin, Michael, *The death of privacy?*, 52 Stan. L. Rev. 1502, 2000 quien señala que en los Estados Unidos los consumidores sobreestiman el valor marginal de sus datos personales puesto que no llegan a tomar conciencia del valor agregado que su perfil personal tiene para el comercio. Cabe agregar, además que actualmente no se valora ni se piensa en función de la privacidad las acciones cotidianas, que pueden tener un alto costo para el amparo de la intimidad y de la seguridad individual. Piénsese en los casos en los que los consumidores dejan datos en Internet, el *phis-*

lesten en averiguarlo con un profesional y dejarán transcurrir el plazo. Por ende, a la ilicitud del procedimiento se le suma la consideración empresarial de que gran parte de la gente obrará como se espera que obren: no harán nada y se generará en la clientela una supuesta presunción legítima sobre la conducta del responsable del tratamiento[17].

b. La importancia del consentimiento en el tratamiento de datos personales

El consentimiento es la regla más importante en el sistema de protección de datos. Por ello Puccinelli ha dicho que es el "principio cardinal del tratamiento de datos de carácter personal y fundamento de la autodeterminación informativa"[18]. En la doctrina española, destacamos la opinión de Murillo de la Cueva, quien señala que el consentimiento del afectado es la expresión quintaesenciada de la autodeterminación o autodisposición sobre la información que le atañe[19]. La importancia del consentimiento reside en que –según Gils Carbó–, éste constituye el medio o modalidad a través del cual el interesado tiene la oportunidad de elegir el nivel de protección que le dará a la información sobre su persona. Por eso debe tratarse de una expresión de voluntad consciente e informada[20].

Existen dos modelos claramente diferenciados de leyes de protección de datos personales. Los que siguen la regla del *opt in* por el cual se parte de la base que todo tratamiento de datos personales (salvo excepciones expresamente previstas) requiere el consentimiento del titular de los datos. Esto es, el sujeto tiene la capacidad de decidir que información sobre su persona podrá ser tratada y almacenada en bancos de datos personales.

Por otra parte, en ciertos países o en ciertas áreas se adopta por norma el *opt out*, por el cual, por regla, pueden tratarse datos de individuos, a menos que estos en forma expresa comuniquen su oposición. Como por defecto siempre se tratan estos datos, son contados los casos en los cuales el consumidor puede manifestar su oposición, sin contar además con que la forma en que a veces se posibilita ejercer esta opción está específicamente diseñada para desincentivar el intento de obtener la remoción de sus datos personales de la base de datos.

---

hing, el robo de identidad, y las estafas bancarias, por citar algunos ejemplos cada vez más frecuentes de apropiación de datos personales.

[17] Un estudio realizado por la FCC en Estados Unidos demostró que se recurre frecuentemente a este tipo de ofertas mediante opciones negativas por el alto grado de aceptación que genera en los consumidores. Si se realiza una oferta simple, sólo el 15% de los consumidores responderá positivamente. Si se plantea la misma oferta de bienes o servicios a través de una opción negativa, cerca de un 80% de los consumidores serán "reclutados" por su falta de respuesta. Cfr. Lamont, Dennis D., *Negative option offers in consumer service contracts: a principled reconciliation of commerce and consumer protection*, 42 UCLA L. Rev. 1315.

[18] Puccinelli, Oscar R., *Protección de datos de carácter personal*, Bs. As., Astrea, 2004, p. 202.

[19] Murillo de la Cueva, Pablo L., *Informática y protección de datos personales*, p. 56. Ver también P. Grimalt Servera, *La responsabilidad civil en el tratamiento de datos personales*, p. 7 y ss; Herrán Ortiz, Ana I., *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales*, p. 220.

[20] Gils Carbó, Alejandra M., *Régimen legal de las bases de datos y hábeas data*, Bs. As., La Ley, 2001, p. 78 y siguientes.

En el derecho comparado ninguno de los dos sistemas es puramente adoptado cien por ciento por una legislación ya que siempre existen excepciones. En la Unión Europea la regla general en materia de protección de datos personales suele ser el *opt in*, y en Estados Unidos de América la regla es la opuesta, esto es el *opt out*[21].

La adopción de uno u otro modelo tiene consecuencias para ciertas industrias, por ejemplo el marketing en Estados Unidos se alimenta de la recopilación de datos de las más diversas fuentes, y es el consumidor el que muchas veces debe sufrir una invasión de anuncios telefónicos, por correspondencia y más modernamente por *email* (conocido como *spam*), y solicitar expresamente la remoción de su información personal de la base de datos.

El *opt out* puede ser objeto entonces de una crítica simple: descuida al consumidor y usuario, pues establece como "regla por defecto" que todo dato puede ser recopilado y sólo cuando el consumidor objeta la comunicación, la ley le presta atención y establece que el dueño de la base de datos debe eliminarlo.

Naturalmente esto obliga al consumidor a realizar incesantes pedidos de no ser molestado, o en la mayoría de los casos, a no ejercer sus derechos por el costo y molestia que ello significa. En segundo lugar, esta libre circulación de datos personales hace que cuando el titular de los datos solicita la eliminación de sus datos personales, el pedido llegará tarde. A lo sumo el consumidor logrará erradicar sus datos personales de uno o dos bancos de datos, pero puede haber cientos más que tengan sus correos electrónicos, teléfonos y direcciones (sin contar además otros datos mucho más jugosos)[22].

Asimismo la obligación de adoptar en forma afirmativa una acción, enviar una carta, un llamado telefónico, un *email* o cualquier otra actividad generalmente hará que las personas renuncien tácitamente a sus derechos, por lo difícil y complicado que es ejercer su cumplimiento[23]. Si al lector le queda alguna duda, sugiero que intente la remoción de su correo electrónico de una base de datos cada vez que recibe un *spam*.

Esto es lo que ocurre en Internet con el *spam*, por la facilidad y frecuencia con que se recopilan datos personales. En cambio el *opt in* comienza respetando al titular, y le permite controlar en forma amplia y más realista la información que otros tendrán sobre su persona, como una derivación del derecho constitucional de hábeas data (art. 43, Const. nacional) y la ley de protección de datos personales[24].

El art. 5° de la ley 25.326 dispone que: "*1*) El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e in-

---

[21] Cabe aclarar que en los Estados Unidos esta regla no está expresada en una norma de carácter general sino que es consecuencia de la inexistencia a nivel federal de una ley de protección de datos personales como las vigentes en Europa o en América latina. Para un análisis comparativo de los regimenes de protección de datos en Europa y Estados Unidos (ver Reidenberg, Joel - Schwartz, Paul, *Data privacy law: A study of United States data protection*, Charlottesville, Michie, 1996).

[22] Palazzi, Pablo, *Aspectos legales del correo electrónico no solicitado (derecho a enviar, derecho a no recibir y a no distribuir correo electrónico)*, *JA*, 2004-I-920.

[23] Solove, Daniel J., *Privacy and power: Computer databases and metaphors for information privacy*, Stanford Law Review, vol. 53, 2001, p. 1458.

[24] Palazzi, *Aspectos legales del correo electrónico no solicitado (derecho a enviar, derecho a no recibir y a no distribuir correo electrónico)*, *JA*, 2004-I-920.

formado, 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, previa notificación al requerido de datos, de la información descripta en el art. 6° de la presente ley".

Como es dable observar, se parte de la base que la regla es el *opt in*, no siendo necesario el consentimiento en contados supuestos que, como son excepciones a la regla general, deben ser de interpretación restrictiva[25].

c. El silencio en el tratamiento de datos personales

La ley 25.326 requiere que el consentimiento del titular de los datos esté presente para la licitud del tratamiento. No se trata de cualquier consentimiento. En concreto, como vimos antes, la norma dice "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".

Al establecer el consentimiento como requisito legal para la validez del tratamiento de datos personales, la ley adopta el modelo del *opt in*, sin perjuicio de las excepciones previstas en el art. 5° de la ley 25.326. Por eso la propuesta del banco en el caso que comentamos transformó el derecho del cliente en una carga.

En otra oportunidad[26] explicamos que la ley requiere un consentimiento expreso, el que deberá constar por escrito (o por medios similares[27]). Este consentimiento no puede ser inferido ni por el mero transcurso del tiempo ni por el silencio del titular de los datos. Se requiere por lo tanto de alguna aserción o acción positiva sobre los datos a ser recopilados y los efectos del mismo. Resultan aplicables a este supuesto los arts. 917 a 919 del Cód. Civil.

De conformidad con lo dispuesto en los arts. 917 a 919 –y su interpretación unánime en la doctrina[28]–, no es posible inferir que el silencio constituye un consen-

---

[25] El art. 5.2. dispone que "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.
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".

[26] Palazzi, Pablo, *La protección de los datos personales en la Argentina*, Bs. As., Errepar, p. 42.

[27] Por ejemplo, un documento digital firmado digitalmente, conforme la equiparación que dispone el art. 6° de la ley argentina de firma digital.

[28] Ver la siguiente doctrina y los fallos allí citados: Bueres, Alberto J. (dir.) - Highton, Elena I. (coord.), *Código Civil y normas complementarias*, t. 2B, Bs. As., Hammurabi, 1998, p. 475; Rivera, Julio C. - Medina, Graciela, *Código Civil anotado. Hechos y actos jurídicos*, Santa Fe, Rubinzal Culzoni, 2005, p. 157, arts. 896 a 1067; Llambías, Jorge J., *Código Civil anotado*, t. II-B, Bs. As., Abeledo-Perrot, p. 43; Salas, Acdeel E. - Trigo Represas, Félix A. - López Mesa, Marcelo J., *Código Civil anotado*, t. 4A, Bs. As., Depalma, 1999, p. 392 y ss; Ghersi, Carlos A. - Weingarten, Celia (dirs.), *Código Civil. Análisis jurisprudencial*, t. II, Nova Tesis, 2005, p. 37; Cifuentes, Santos, *Código Civil anotado*, t. I, Bs. As., La Ley, p. 642; Leiva Fernández, *El silencio en la formación de los contratos (Si Ud.*

timiento válido –en el caso para la adquisición, tratamiento o cesión de datos personales–, y menos aun cuando la ley 25.326 expresamente dispone lo contrario[29].

Como bien señala Cifuentes "a diferencia del adagio del derecho canónico 'el que calla otorga', en nuestro derecho el silencio no importa ni sí ni no: no es aceptación o consentimiento pero tampoco rechazo o negación. Nuestro Código Civil sigue esa línea y establece el principio de que el silencio no puede valer como consentimiento"[30]. Quiroga Lavié, al comentar esta norma señala que, más allá de su pésima redacción, es evidente que el legislador ha querido prohibir en forma terminante las autorizaciones implícitas y las encubiertas en autorizaciones de otro tipo[31].

Al banco, por ende, no le quedaba otra opción que solicitar el consentimiento expreso a sus clientes, cosa que, como surge del caso, no se hizo. La lógica consecuencia de la ausencia de consentimiento para el tratamiento de datos personales es su ilicitud (arg. art. 5°, ley 25.326), conclusión compartida en ambas instancias.

Como la ley argentina se inspiró en el modelo europeo de protección de datos, y en especial en la ley española, nos parece útil una exposición de esta cuestión en la Unión Europea. Ello servirá para confirmar que la decisión anotada comparte criterios jurídicos desarrollados en otras jurisdicciones. En Europa, la mayor parte de las leyes de protección de datos personales establecen el requisito de consentimiento expreso para el tratamiento de datos personales, siguiendo para ello el texto de la directiva europea en materia de protección de datos personales.

Esta norma define en el art. 2°, inc. *h* al "consentimiento del interesado" como "toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan". Por su parte, el art. 7° de la referida directiva señala que "Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: *a*) el interesado ha dado su consentimiento de forma *inequívoca*"[32].

Al interpretar esta norma la doctrina se encargó de señalar que el consentimiento debe ser una clara indicación, en otras palabras, el titular de los datos debe significar su acuerdo con alguna clase de *acción positiva*. Puede ser oral o escrita pero debe ser una acción positiva. Se reconoce que no queda claro qué sucede bajo la directiva cuando se presume el consentimiento implícito en los casos donde ese consentimiento del titular de los datos es interpretado como acuerdo. Pero como la directiva usa la palabra "manifestación", ello parece indicar alguna suerte de *acción positiva* por parte del titular de los datos[33].

La transposición de la directiva 95/46/EC en las diversas leyes nacionales no alteró este resultado. Varios países definieron el consentimiento como lo hace la di-

---

no manda este cupón), *LL*, 1991-A-987; Méndez Sierra, *El silencio frente a la buena fe y los requerimientos privados*, *LL*, 1994-A-670; Halperin, *El silencio en la formación de los contratos*, *LL*, 3-33 y Spota, Alberto G., *El silencio como manifestación del consentimiento en los contratos*, *LL*, 24-715.

[29] Palazzi, *La protección de los datos personales en la Argentina*, p. 42.

[30] Cifuentes, *Código Civil anotado*, t. I, p. 642.

[31] Quiroga Lavié, Humberto, *Hábeas data*, Bs. As., Zavalía, 2001, p. 80.

[32] El texto de la directiva, en castellano, se puede consultar en Palazzi, Pablo (dir.), "Derecho y Nuevas Tecnologías", n° 0, año 1, p. 159 y siguientes.

[33] Ver Cullen International, *A business guide to changes in European data protection legislation*, Kluwer Law International, 1999, p. 35.

rectiva, pero Suecia y España agregaron el término "inequívoco" y "no ambiguo" en sus legislaciones, y la ley de Luxemburgo exige que el consentimiento sea explícito e inequívoco. La ley griega, por su parte, requiere que ciertas informaciones sean provistas al titular de los datos para que el consentimiento sea válido. Alemania e Italia establecen que el consentimiento debe ser obtenido por escrito. La conclusión es que existe un acuerdo generalizado entre las agencias de protección de datos de los países miembros que la directiva, al requerir una manifestación de voluntad, libre, específica e informada del interesado, impide equiparar dicho consentimiento al silencio[34].

La doctrina italiana[35], por ejemplo, considera que en el ámbito de la protección de datos el consentimiento no puede ser tácitamente manifestado ni deducido del comportamiento del titular de los datos, por lo que no tiene ninguna relevancia el silencio, ni la inercia del interesado, ni la tolerancia a un tratamiento de sus propios datos. La doctrina española llega a las mismas conclusiones[36]. Al analizar la ley de privacidad de la provincia canadiense de Québec, norma que se inspiró en el modelo europeo de protección de datos personales se ha llegado a las mismas conclusiones[37].

La jurisprudencia europea, tanto administrativa como judicial, ha seguido la misma línea. Cuando una práctica similar a la que comentamos se intentó en Inglaterra, el comisionado de protección de datos de aquel país, en base a la *Data Protection Act de 1998* consideró que el silencio nunca podía equipararse al consentimiento para tratar datos personales[38].

Este criterio ya había sido fijado en el caso "British Gas"[39], donde se discutió la diferencia entre *opt in* y *opt out* bajo la *Data Protection Act* inglesa de 1984. La empresa British Gas poseía dos bases de datos, una de aranceles de gas y otra de marketing. A comienzos de 1997 incluyó en la correspondencia mensual un folleto titulado "Sus derechos de protección de datos" con cada factura que envió a sus clientes. Este folleto establecía que British Gas comunicaría a sus clientes todos sus productos y servicios, y les haría saber asimismo de la existencia de productos de otras empresas avisando la posibilidad de ceder información sobre sus clientes a otras empresas en el grupo de British Gas de modo que los clientes pudieran recibir nuevas ofertas de bienes o servicios. Si los clientes no querían recibir esa información, podían excluirse devolviendo un formulario a British Gas.

---

[34] Carey, Peter comentando el documento de la Comisión Europea *Analysis and impact study on the implementation of directive EC 95/46 in member States*, y sus reflexiones publicadas en el vol. 3, Issue 6 de Privacy & Data Protection, 2003, p. 2. Ver también Douwe Korff, *Study on implementation of data protection directive. Comparative summary of national laws*, Human Rights Centre, University of Essex.

[35] Manes, Paola, *Il consenso al trattamento dei dati personali*, Cedam, Padova, 2001, p. 98 y doctrina allí citada.

[36] Grimalt Servera, Pedro, *La responsabilidad civil en el tratamiento automatizado de datos personales*, Comares, p. 178.

[37] Scassa, Teresa, *Text and context: Making sense of Canada's new personal information protection legislation*, 32 Ottawa L. Rev. 1, 2001.

[38] Ver *Citibank. Breach of data protection law?*, en vol. 3, Issue 6 of Privacy & Data Protection, 2003, p. 1 y 14.

[39] British Gas Trading Ltd. v. Data Protection Registrar, Info T.L.R. 393, 1998, disponible en 1999 WL 276828 (Data Protection Trib., mar. 24, 1998) (traducción del autor).

La autoridad inglesa de protección de datos entendió que esta práctica era contraria a la ley de protección de datos pues requería a los clientes recurrir a un procedimiento de *opt in* en vez de uno de *opt out*, en especial pues estadísticamente era más probable que sólo unos pocos clientes estarían al tanto de haber recibido la noticia o conocer las consecuencias de no responder.

El tribunal de protección de datos, al analizar la licitud de este procedimiento tuvo en cuenta que la demandada era una empresa monopólica (en aquel entonces) y que el procesamiento de los datos para cederlos a terceros con fines de "marketing directo" era ilegítimo a menos que se realizara con el consentimiento del titular de los datos.

En un caso muy similar, "Midlands Electricity Plc v. Data Protection Registrar" (1999), la autoridad inglesa había emitido una orden ante una queja de una persona que había recibido material de publicidad de la demandada cuyo envío no había consentido. En el caso, la empresa había comenzado una campaña de marketing directo donde se incluía un folleto y una revista (Homebright Magazine) al remitir la factura a sus clientes. El folleto no sólo incluía ofertas de Midlands Electricity sino también de terceras empresas como Boots y Midland Gas. Un usuario formuló una queja y la autoridad sancionó a la empresa. Apelada la decisión, el tribunal entendió que este tipo de procesamiento de datos personales era ilegal y que violaba el primer principio de protección de datos de la ley. Agregó que los clientes recibían la revista en forma general, sin haber tenido la oportunidad de consentir el uso de sus datos personales para esta finalidad.

Respecto a la forma de obtener el consentimiento en el área de marketing directo, el tribunal sostuvo en este caso que: "tanto con clientes existentes como con nuevos clientes …no consideramos que sea suficiente el envío al cliente de un folleto dándole una oportunidad de objetar el procesamiento de sus datos personales para finalidades distintas a aquellas relacionadas con la electricidad, tales como la preservación de energía …que hemos identificado como disponible para procesar datos sin consentimiento y sin ser ilegítimo… Sería suficiente para prevenir un procesamiento ilegal que los clientes sean informados que la demandada desea continuar enviándoles la revista conteniendo publicidad de terceras personas que Midlands seleccionará o cualquier otra promoción que Midlands desee realizar, siempre que se les brinde la oportunidad de consentir o no o que no objeten que sus datos personales sea utilizados para dichos fines… Alternativamente, antes de que ese procesamiento tenga lugar, el cliente devuelve a Midlands un documento u otro medio de comunicación que reciba Midlands donde indica su consentimiento, o por ejemplo, por no tildar un casillero de *opt out*, u otro medio indicando que no objeta el procesamiento de sus datos personales para esos fines de marketing directo o promocionales"[40].

La agencia española de protección de datos ha tenido opiniones diversas. Si bien en un comienzo esta práctica ha sido vista desfavorablemente, un informe de memoria de 1995 pareció aceptarla como válida.

[40] Carey, Peter, *Data protection. A practical guide to UK and EU law*, Oxford, p. 43 y 44.

Pero más recientemente estas prácticas fueron consideradas ilegales bajo la actual conducción, lo que fue confirmado por un fallo de la audiencia nacional sobre el mismo tema.

Según da cuenta una noticia reciente, la Agencia Española de Protección de Datos sancionó a una filial del Grupo Gas Natural por usar datos de la empresa matriz[41]. La noticia explica que "La Audiencia Nacional desestimó el recurso contencioso administrativo presentado por Gas Natural Servicios, contra la resolución de la Agencia Española de Protección de Datos de 28 de febrero de 2002. En esta resolución, la Agencia había impuesto a Gas Natural SDG, y a Gas Natural Servicios SDG, sendas sanciones por haber infringido, respectivamente, los arts. 11 y 6.1 de la ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD)"[42].

En el caso, Gas Natural envió a sus clientes una carta en la que se les informaba de que, en el caso de que no manifestaran su oposición a que Gas Natural SDG, cediera sus datos a empresas del grupo Gas Natural, Gas Natural SDG, entendería concedido dicho consentimiento y procedería a comunicar sus datos a sus empresas filiales. No obstante, y de manera previa al envío de las cartas, Gas Natural SDG, solicitó a la entonces Agencia de Protección de Datos un pronunciamiento sobre la licitud de este procedimiento de recogida del consentimiento, que ésta entendió conforme con la derogada ley orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de los datos de carácter personal (LORTAD). Tras recibir numerosas denuncias de particulares que entendieron que sus datos habían sido cedidos de manera ilegítima, y que sostenían no haber recibido dichas cartas, la Agencia entendió que el consentimiento así obtenido no reunía los requisitos previstos en la vigente LOPD y sancionó a dichas empresas.

En este contexto, la Audiencia Nacional "resolvió el recurso planteado por Gas Natural Servicios, frente a la resolución de la Agencia afirmando que el cesionario de los datos tiene la obligación de verificar 'de forma razonable y diligente' que los titulares de los datos cedidos hayan prestado válidamente su consentimiento a la cesión". Además sostuvo la Audiencia Nacional que "el pronunciamiento solicitado de la Agencia carece de valor vinculante y que, en cualquier caso, se dictó al amparo de la derogada LORTAD"[43].

Pero este principio de *opt in* no parece ser unánime en todo el mundo. A diferencia del régimen europeo, la ley de privacidad financiera de Estados Unidos[44] (Gramm-Leach-Bliley Act-GLBA) permite el uso de datos para marketing siempre que exista una notificación previa de la política de privacidad y se de oportunidad al cliente bancario de pedir el retiro de la base de datos (lo que se conoce en la ley como *disclosure* y *opt out*). Si bien no existen casos judiciales, la presunción que establece la GLBA es que las entidades financieras pueden usar estos datos hasta

[41] Ver "Boletín Noticias de Competencia y Mercado", n° 3, Perez Llorca Abogados, 2005, p. 10.

[42] En estos artículos se regula la comunicación de los datos de carácter personal a terceros y los requisitos que debe reunir el consentimiento prestado por el titular de los datos para su tratamiento.

[43] Sentencia de la audiencia nacional del 30 de junio de 2004, España.

[44] Gramm-Leach-Bliley Act, Pub. L. n° 106-102, 133 Stat. 1338, 1999, conocida con ese nombre por los legisladores que la impulsaron.

que el cliente diga lo contrario. Esto ha generado críticas de la doctrina[45], por lo extenso de las políticas de privacidad, por lo complejo de su redacción, lo que hace difícil entenderlas al común de la gente[46], y porque en la práctica con esto muy pocos clientes ejercitan su derecho de *opt out* o cambian las políticas de privacidad que por defecto ya están establecidas de cierta forma[47].

La ley GLBA derogó la ley denominada "Glass-Steagal Act". Esta última norma, aprobada a raíz de la crisis financiera de la gran depresión, prohibía las fusiones de bancos y compañías financieras y de bolsa[48]. La GLBA también modificó la Bank Holding Company Act, que restringía las asociaciones o fusiones entre bancos y compañías de seguros, creando así la posibilidad de formar verdaderos "supermercados financieros"[49]. Para contrarrestar estas libertades otorgadas se establecieron ciertos resguardos sobre los datos personales. Entre otras cuestiones, el Título V de la GLBA requiere que los bancos envíen a sus clientes anualmente su política de privacidad, y que les informen que pueden ejercer su derecho de *opt out*, pero salvo estos recaudos, los bancos pueden compartir libremente la información en su poder.

Pero la ley GLBA podía entrar en conflicto con normas del resto de los Estados que desean brindar mayor privacidad a los clientes de bancos. El Estado de California, por ejemplo, aprobó una ley[50] –pionera en materia de privacidad financiera– que establecía como regla el *opt in* del cliente cuando la institución financiera quería compartir información de sus clientes con empresas no afiliadas (en caso de ser afiliadas o del mismo grupo económico se implementaba la regla del *opt out*).

Tanto una reforma de la FCRA del año 1996 como la ley GLBA se basan exclusivamente en el *opt out*. Como la ley de California resultaba más protectora y exigía más requisitos a los bancos para compartir datos personales de sus clientes que estas leyes federales, la ley local fue suspendida por una cautelar en una acción declarativa iniciada por la asociación de bancos contra dicho Estado[51].

---

[45] Reidenebrg, Joel R., su opinión en *Symposium The Future Of Law And Financial Services*, Panel Ii: The Policy Aspect, Consumer Data Privacy, 6 Fordham J. Corp. & Fin. L. 69, 2001. El autor, un conocido profesor estadounidense de derecho especializado en protección de datos personales, sostiene, irónicamente, que si tuviera que calificar la ley bancaria norteamericana GLB, la aprobaría sólo con un "C menos".

[46] Puede verse el interesante estudio de Hockhauser, Mark, *Lost in the fine print: Readability of financial privacy notices*, publicado en http://www.privacyrights.org/ar/GLB-Reading.htm, donde se analizan cerca de 60 políticas de privacidad de entidades financieras norteamericanas, y donde se concluye que la mayoría se encuentran redactadas de una forma que hacen difícil su comprensión.

[47] Bellman, Steven - Johnson, Eric J. - Lohse, Gerald, *To opt in or opt out? It depends on the question*, 44 Communication of the ACH 25, 2001.

[48] La separación tuvo como finalidad el evitar los conflictos de interés que tienen lugar cuando actúan conjuntamente. Para una explicación ver Silva (h.), Roberto E., *Separación entre la banca comercial y la banca de inversión en los Estados Unidos. La Glass-Steagall Act. Pasado, presente y futuro*, en Rev. D. B y la A. F. año 1, n° 4, p. 727.

[49] Jange, Edward J. - Schwartz, Paul M., *The Gramm-Leach-Bliley Act, Information Privacy, and the limits of default rules*, 86 Minn. L. Rev. 1219, 2002. Los autores critican la GLB explicando que al establecerse como regla por defecto la posibilidad de compartir datos personales, no se ampara la privacidad de los usuarios bancarios y se impide que éstos controlen adecuadamente su información personal.

[50] Conocida como SB-1, "California's Financial Information Privacy Act" (Fin. Code § 4050).

[51] "American Bankers Association v. Gould", 412 F.3d 1081 (9th Cir. 2005).

Por supuesto, en Estados Unidos las críticas al régimen general de *opt out* por parte de especialistas en derecho a la privacidad son constantes y muy lógicas. Al respecto Hoofnagle[52] señala que el principio de *opt in* equivale al consentimiento, donde el consumidor aprueba el tratamiento de sus datos personales, en cambio la industria denomina "elección" (*choice*) al *opt out* cuando en realidad ellos optan por el consumidor y éste en definitiva nada decide. Explica que el *opt out* o las opciones negativas son métodos extraños para asegurar el cumplimiento de un derecho y los compara con el consentimiento informado en las lesiones o en la cirugía. De la misma forma que sería absurdo adoptar el sistema de *opt out* en estos casos, la recopilación de datos personales debería tener las mismas reglas. Antes que cualquiera pueda usar datos personales, se debería contar con el consentimiento del titular de los datos. Propone finalmente que se adopten en Estados Unidos las reglas de la OCDE en materia de protección de datos, sobre todo en lo relativo al consentimiento y en forma general, ya que la existencia de normas sectoriales (por ejemplo, el *opt in* sólo para alquiler de videos dispuesto en la ley Video Privacy Protection Act) produce resultados absurdos. A tal fin comenta que si un consumidor "va al videoclub y alquila un video, si quieren vender la información sobre las películas que alquilan, deberán solicitarle permiso[53]. Lo que es interesante es que en los Estados Unidos, los clientes de videoclubes tienen, de hecho, más privacidad en los registros de alquiler de videos que la privacidad que en sus cuentas bancarias[54]. El cliente tiene más privacidad en el hecho de que alquila un video de Bambi, que en sus registros médicos[55]. El enfoque sectorial, por oposición a una ley general, produce estos resultados absurdos".

d. Consentimiento e información al titular de los datos: el cambio de finalidad requiere un nuevo consentimiento

En este punto vamos a analizar las relaciones entre el principio de finalidad y el consentimiento en la recolección de datos personales. Como otro pilar de su razonamiento, la fiscal ante la Cámara Comercial acudió al principio de finalidad previsto en el art. 4.3 de la ley de protección de datos personales, que dispone que los datos no pueden ser usados para una finalidad distinta o incompatible con aquellos que motivaron su obtención. En su dictamen compartido por el tribunal se concluye que el uso para fines tales como marketing implica infracción a este principio, pues los clientes del banco no dieron su consentimiento para esta finalidad.

En todo caso, el responsable del tratamiento debió obtener un consentimiento específico, haciendo saber la nueva finalidad que se le daría a la información, no explicitada inicialmente en la recogida original de los datos personales. Lo mismo

[52] Hoofnagle, Chris, *Colloquium on privacy & security*, 50 Buffalo L. Rev. 703, 2002.

[53] The Video Privacy Protection Act, 18 U.S.C. 2710, 1994.

[54] La ley Gramm-Leach-Bliley Act, como vimos, permite a las instituciones financieras compartir información personal de sus clientes, incluyendo hasta el *bank account balances*, con terceros, siempre que exista la posibilidad de *opt out*. Ver 15 U. S. C. 6801, 2001.

[55] La ley federal conocida con el nombre de Health Insurance Portability y la Accountability Act Privacy Rule permiten el marketing basado en registros médicos. Algunos tipos de información médica son considerados registros con fines de educación y en esos casos el individuo no tiene derecho de *opt out*, cfr. 45 C. F. R. 164.501. Cfr. Hoofnagle, *Colloquium on privacy & security*.

sucedería si el cliente bancario había dado un consentimiento general, ya que éste se entiende dado en el contexto de las operaciones bancarias[56].

Por ello, a nuestro juicio, tampoco se aplicaría la excepción del ap. *e* del párr. 2°, del art. 5° de la ley 25.326 prevista expresamente para las entidades financieras, pues ceder los datos personales (presumiblemente con fines de marketing) no es una operación de las allí mencionadas. Más bien, dicha norma apunta a las operaciones bancarias que ocurren a diario entre el banco y el cliente. Además, tal excepción debe ser interpretada estrictamente y constituye una dispensa para el consentimiento pero no para la finalidad.

Tal vez la relación entre el consentimiento dado y la finalidad del uso de los datos no es tan clara en nuestra ley como en otras[57], pero surge de la integración de los arts. 4° y 5° de la norma.

Por otra parte, esta no es la única situación que puede plantearse con el consentimiento y la finalidad. Como éste debe ser expreso e informado, suele suceder que se informe una finalidad distinta a la real o no se informe ninguna. Así, los datos se obtienen en forma engañosa o fraudulenta, metodología expresamente prohibida por el art. 4° de la ley 25.326.

En tales supuestos, tampoco existen consentimiento válido para ese tratamiento pues la persona dio un consentimiento teniendo en miras una expresa situación, o una determinada finalidad, y no otra (existiría, para usar otra vez terminología contractual, una diferencia entre la voluntad real y la voluntad declarada del recopilador del dato personal).

Un clásico ejemplo de obtención fraudulenta de datos es lo que ocurrió con el "regalo" que en el año 2001 realizó la revista de tecnología Wired a todos sus suscriptores: un lector de código de barras que permitía leer los códigos de barras de las publicidades contenidas en su revista. Con este dispositivo conectado al ordenador, y sin tener que tipear, el usuario era "llevado" directamente al sitio de Internet de la respectiva publicidad. Lo que no se aclaraba en ningún momento era que cada dispositivo lector tenía un código único que permitía saber los gustos o intereses de

[56] En tal sentido, Schvartz, Liliana, *La cláusula contractual de consentimiento del titular al tratamiento o cesión de sus datos personales en el marco de un contrato de consumo. Reflexiones sobre su abusividad*, *JA*, 2004-III-868. La autora señala que resulta indispensable determinar la vinculación que el consentimiento para el tratamiento de los datos personales tiene con el objeto del contrato en cuestión, visto el mismo desde el fin perseguido por el consumidor al contratar. Ejemplifica que "si se firmó el contrato para adherirse a un sistema de alquiler de videos, tener cobertura médica o irse de vacaciones, resulta claro que el consentimiento para que se traten y cedan los datos personales resulta absolutamente ajeno al fin del cliente al contratar". En igual sentido Mario Masciotra señala que "puede darse el caso que al momento de suscribir la solicitud de apertura de una caja de ahorro o cuenta corriente bancaria, aportemos una serie de datos personales imprescindibles para el funcionamiento de dichas operatorias; y luego esos mismos datos sean utilizados por la institución bancaria con otros fines, tales como marketing para la comercialización de otros productos, con lo que se estaría violando el principio de la finalidad que consagra el art. 4°" (*El hábeas data. La garantía polifuncional*, La Plata, LEP, 2002, p. 286).

[57] La Quebec Privacy Act por ejemplo, dispone que "14. *Consent to the communication or use of personal information must be manifest, free and enlightened, and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested*".

cada desprevenido suscriptor. Las críticas generalizadas de los consumidores impactaron en la difusión de este producto[58].

Otro caso similar fue el de General Electric. Esta empresa, envió una supuesta encuesta anónima a todos sus accionistas en las cuales les solicitaba que calificaran diversos aspectos de la empresa y su *management*. El pedido incluía un sobre con el franqueo postal previamente pagado para facilitar el envío de la respuesta. Sin embargo, los accionistas no fueron informados que cada sobre también contenía un código de barras único destinado a poder ser cruzado con la base de datos de los accionistas de la empresa y conocer así la opinión personal de cada uno, que en un principio, debía resultar anónima[59].

Estos son casos de obtención fraudulenta del consentimiento por falta de adecuada información, no de intentos de imponer una opción negativa al consumidor. Pero ambos supuestos apuntan a lo mismo, a tratar de obtener datos personales bajo un manto de legalidad.

La jurisprudencia inglesa ha aplicado este principio bajo la vigencia de la ley de protección de datos del año 1984. En numerosos casos, el tribunal recordó la importancia de obtener los datos personales de una manera leal, y recordó que la obtención y tratamiento por medios leales requiere que el titular de los datos debe conocer los usos "no obvios" de sus datos personales al momento en que sus datos son obtenidos y no antes. Por ello el individuo debe tener el derecho de objetar esos usos "no obvios". En general, estos casos se relacionaban con el uso de datos personales con fines de marketing directo, cuando los datos del titular eran cedidos a terceros para esos fines[60].

Es decir que –y esto vale para Argentina– la obtención de datos sabiendo que serán usados para otra finalidad es una violación del principio de finalidad, y también del art. 6° de la ley 25.326.

En el caso inglés "Innovations (Mail Order) v. Data Protection Registrar" una compañía de venta directa vendía y obtenía datos a través de dos canales: las ventas por catálogos y las ventas realizadas a través de avisos de publicidad en diarios y revistas. Los clientes eran informados acerca de la posibilidad de la utilización de sus datos para otras finalidades, pero sólo luego que la información fuera obtenida. La empresa decidió alquilar los datos obtenidos a través de ambas categorías.

La autoridad de protección de datos inglesa alegó que los clientes debían ser informados de todos los fines con que se pensaba usar sus datos personales al momento que la orden era hecha, esto es cuando el cliente proveía los datos a la compañía. La empresa se defendió argumentando la imposibilidad práctica de cumplir con dicho recaudo y alegó que la industria consideraba esa práctica inaceptable. El tribunal de protección de datos inglés concluyó "que la ausencia de una advertencia en la publicidad en los diarios llevaba a concluir a los clientes que su información personal no sería vendida. Esto también significaba que la demandada había enga-

[58] La historia del CueCat puede consultarse en http://en.wikipedia.org/wiki/Cuecat.

[59] Solove, Daniel J., *The digital persona. Technology and privacy in the information age*, 2004, New York University, p. 51.

[60] Bainbridge, David, *Data protection law*, Welwyn: Emis Professional Publishing, 2000, capítulo relativo al consentimiento.

ñado al público consumidor y por ende la obtención de los datos personales fue ilegal"[61].

Similares redacciones encontramos en las diversas leyes de protección de datos europeas, con lo que la interpretación de estos principios sirve como guía de nuestra ley pues estas normas, y sobre todo la española, han sido su fuente.

Así, Troncoso Reigada[62] señala en una reciente publicación que entre las "facultades positivas que conforman el derecho fundamental a la protección de datos personales, hay que destacar el consentimiento del afectado para el tratamiento de sus datos personales" y agrega que "lógicamente, para que este consentimiento sea realmente libre y consciente, ha de ser un *consentimiento 'informado', información que debe alcanzar los posibles destinatarios de sus datos personales*. Así, muchas vulneraciones de este derecho fundamental se producen por una falta o por una deficiente información en el momento de la recogida de los datos. La información es también núcleo de este derecho fundamental, a la vez que una exigencia del propio consentimiento"[63].

La jurisprudencia española sostuvo "la garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona; la llamada 'libertad informática' es así derecho a controlar el uso de los mismos datos insertos en un programa informático (hábeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para *fines distintos* de aquel legítimo que justificó su obtención"[64].

Otro conocido fallo del Tribunal Constitucional español[65] estimó un recurso de amparo interpuesto por un trabajador de RENFE contra la sentencia de la Sala de lo Social del TSJ Madrid que revocó la sentencia de instancia y absolvió a la empresa de su conducta de descuento de retribuciones del trabajador por entender que había participado en una huelga, basándose exclusivamente en el dato de afiliación sindical que poseía. Entendió la Sala que el trabajador había proporcionado el dato de la afiliación sindical a efectos de reducción de la cuota sindical, *pero no con la finalidad de que la empresa, tratándolo automatizadamente, hiciese otro uso diferente*.

---

[61] Opinión de Carey, *Data protection. A practical guide to UK and EU law*.

[62] Troncoso Reigada, Antonio, *La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional*, "Derecho y Nuevas Tecnologías", n° 6/7, 2006.

[63] El autor cita un fallo del TC español que sostuvo "es evidente que el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de éstos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales. Para lo que no basta que conozca que tal cesión es posible según la disposición que ha creado o modificado el fichero, sino también las circunstancias de cada cesión concreta. Pues en otro caso sería fácil al responsable del fichero soslayar el consentimiento del interesado mediante la genérica información de que sus datos pueden ser cedidos. De suerte que, sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5°, LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia –F. J. 13–".

[64] SSTC 254/1993, fundamento jurídico 7°; 11/1998, fundamento jurídico 4°; 11/1998, fundamento jurídico 4° y 94/1998, fundamento jurídico 4°.

[65] TC Sala 1ª, sentencia 77/1998 de 31 marzo, ponente D. Cruz Villalón.

De todo lo expuesto, resulta que el cambio de finalidad (esté previamente informado o no al cliente) es accionable por la vía de hábeas data, pues fue otro de los fundamentos usados por el tribunal para declarar que la política de privacidad del Citibank violaba la ley 25.326.

e. Las cesiones implícitas en la ley de protección de datos personales

El dictamen de la fiscalía de Cámara trata por primera vez un tema que se plantea en la práctica profesional a diario, pero que no se había decidido judicialmente: una base de datos simplemente nominativos pero donde se conoce el origen, lo que importa asumir que se refieren a clientes de determinado banco, ¿puede cederse libremente?

En el mencionado dictamen, y en este punto compartido por el tribunal, se rechaza la defensa esgrimida por el banco demandado basada en el art. 5°, párr. 2°, inc. *c* de la ley 25.326 (que dispone que no es necesario el consentimiento cuando los datos se limiten a nombre, documento de identidad, identificación tributario o provisional, ocupación, fecha de nacimiento y domicilio). Se dan dos motivos para esta conclusión. En primer lugar, que la mencionada política de privacidad del banco no limita su aplicación a estos datos solamente. En segundo lugar, se concluye que una cesión solamente de esos datos "importaría ceder implícitamente un dato que excede los previstos en el art. 5°, párr. 2°, inc. *c*, esto es, que el titular de los datos es cliente del banco".

Esto último es lo que se conoce como cesiones implícitas, y hasta donde sabemos, es el primer fallo en Argentina en tratar la cuestión. Compartimos la regla que elabora el tribunal pues implica superar la interpretación literal para ir al espíritu de la ley, que de otra forma se vería fácilmente burlado cediendo listados de nombres y direcciones. Obviamente, para la ilegalidad de este accionar se requiere la cesión de los datos y el conocimiento de su origen.

Piénsese que si se sostuviera lo contrario, podrían cederse libremente bases de datos conteniendo datos sensibles formados sólo por listados de nombres y direcciones de miembros de sindicatos, partidos políticos, iglesias o religiones o cualquier otra clase de datos sensibles. Si el receptor o cesionario de estas bases de datos sabe que esa base de datos proviene, por ejemplo, de cierto sindicato, o de un partido político[66], existe un dato extra que se cede en forma implícita sin que exista el "campo" extra en la base de datos que denota el origen de la misma. Sería una forma muy sencilla de burlar las nobles finalidades de la ley.

[66] La afiliación a un partido político es un dato sensible. Aunque existen opiniones encontradas en materia de datos sobre afiliaciones partidarias, la mayoría de la doctrina lo considera un dato sensible. Ver nuestra nota *La protección de los datos sensibles y la publicación de la afiliación partidaria*, *JA*, 2002-IV-496 y Puccinelli, Oscar R., *Los datos de afiliación partidaria son datos sensibles y no deben ser puestos a disposición del público en general (A propósito de su inclusión en padrones electorales y en bases de datos disponibles en la Internet)*, artículo en prensa. En contra ver Basterra, Marcela I., *La "opinión política" o la "idea política" es un dato sensible. La "afiliación partidaria" no*, *LL*, columna de opinión, 4/5/05. A nuestro juicio, la distinción entre opinión política y la "afiliación partidaria" es *naive* e impracticable y tiene como efecto derogar la protección que la ley 25.326 otorga a los datos sensibles.

4. Conclusiones

El fallo que comentamos nos parece acertado porque reafirma una serie de conceptos que, si bien son claros en la ley argentina de protección de datos personales, por ahora no habían tenido pronunciamientos judiciales.