

EL ENTRECRUZAMIENTO DE INFORMACIÓN RELATIVA A LOS CONSUMIDORES Y LA RESPONSABILIDAD DE LOS GRUPOS DE EMPRESAS

Alejandra M. Gils Carbó

PONENCIA

1. El manejo de la información recolectada sobre los consumidores, que usualmente intercambian las empresas vinculadas –ya sea para la realización de estudios de marketing, publicidad, evaluación del riesgo crediticio, etc.- va a abrir una nueva brecha en materia de responsabilidad (civil, administrativa y penal) ante la inminente sanción de una ley regulatoria del tratamiento de los datos personales.

2. La protección de la privacidad, el honor, la imagen y la identidad personal de los sujetos que puedan resultar afectados por el procesamiento de sus datos en bases automatizadas, requiere una regulación integral del tratamiento de los datos personales –mediante ley especial- que procure un equilibrio satisfactorio entre la tutela de aquellos derechos personalísimos y el aprovechamiento de las ventajas que proporciona el manejo de la información para un mejor desenvolvimiento de los sectores comercial, bancario y financiero, que también conciernen al interés general y –específicamente- a nuestra inserción en el mercado internacional.

DESARROLLO

1. Los nuevos retos de la tecnología en materia de informática.

Los avances tecnológicos han derivado en una nueva forma de interacción que se caracteriza por la convivencia en una sociedad de información. Las actividades más diversas, desde participar en un sorteo, usar la tarjeta de crédito o ingresar en un site de Internet, generan registros de datos sobre los consumidores que serán procesados con variados fines, de mercadeo, control, sondeo estadístico, etc.

Es usual el intercambio de listas entre empresas vinculadas, de distintos rubros, para entrecruzar información sobre datos personales. Cuando esta operación permite la combinación de datos, que aislados carecerían de relevancia, pero su tratamiento permite llegar a construir perfiles de los individuos, mostrando una radiografía de la persona al margen de su consentimiento, se está entrando en el campo de lo que se denomina información “sensible” y en un nuevo concepto de la violación de la intimidad.

La moderna tecnología en el área informática de que se valen los grupos de empresas para mejorar su actividad, ha generado nuevos peligros y lesiones, que se pueden manifestar ante la utilización indiscriminada de los datos personales para fines ilícitos o inmorales; la desprotección de los sujetos ante la posibilidad de ser objeto de decisiones adoptadas con base en el tratamiento de datos falsos o discriminatorios y la desnaturalización del fin para el cual fue recogida la información sobre las personas. También se han considerado situaciones más extremas, como la que derivaría de la digitalización de información genética que reve-

le los aspectos más íntimos de la salud física, constitución hereditaria y psicológica, para su utilización en el mercado laboral y de seguros, o con fines de control, vigilancia o discriminación.

Esto ha generado la correlativa reacción de las legislaciones en los países avanzados, que incorporaron un régimen especial de protección de los datos personales, que con más precisión debería calificarse como de regulación del tratamiento de los datos personales, ya que lo que se protegen no son los datos sino los derechos de las personas.

En nuestro país, la primera noticia de este estado de alerta tuvo lugar con la reforma constitucional de 1994 (art. 43 párrafo 3ro.), que amplió el elenco de derechos fundamentales del individuo, incorporando una acción de amparo especial cuyo objeto es que toda persona tome conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y que en caso de falsedad o discriminación pueda solicitar su rectificación, supresión, confidencialidad o actualización.

Pero esta acción constituye un aspecto parcial y mínimo dentro de un fenómeno más vasto, que es el del tratamiento automatizado de los datos personales. Este último abarcaría todas las operaciones que puedan realizarse mediante el uso de herramientas informáticas, o no, desde su recolección, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, hasta su comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los datos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

Ante la ausencia absoluta de previsiones legales sobre seguridad y confidencialidad de los datos, sobre los alcances del derecho de acceso y rectificación del afectado y acerca de los límites que impone el respeto al honor, intimidad, privacidad e identidad personal, resulta muy difícil que puedan alegarse con éxito lesiones por agresiones informáticas a los derechos fundamentales de las personas.

2. Hacia una regulación del tratamiento de los datos personales:

El panorama actual en nuestro derecho es de descontrol. La instrumentación de una acción especial con jerarquía constitucional, ha sido insuficiente para proporcionar un marco regulatorio adecuado.

Esta acción, que ha sido denominada “habeas data” (“que tengas los datos”) a partir de la Constitución Brasileña de 1988 es, de acuerdo a su ubicación constitucional, una sub-especie de amparo. Esta asimilación que estuvo dirigida a imprimirle el carácter de una acción expedita y rápida -como dice el art. 43 CN 1er.párrafo al referirse al amparo común- tuvo en la práctica un efecto no deseado. Y es que muchos jueces hayan asignado al habeas data el carácter restrictivo y excepcional que caracteriza al amparo -por su calidad de remedio extraordinario y residual¹ - cuando, lejos de ello, debía constituir un instrumento sencillo y ágil a

¹ Ver Gozafni Osvaldo “El Derecho de Amparo” pag. 3, Depalma.

favor de los sujetos perjudicados por el creciente manejo de datos personales en bases automatizadas, permitiéndoles, por esa vía, alguna intervención para hacer valer sus derechos.

Los repertorios de jurisprudencia registran numerosos casos en que se ha rechazado liminarmente la acción porque el actor no había justificado la existencia de “arbitrariedad o ilegalidad manifiesta” e, incluso, el agotamiento de instancias administrativas, ambos recaudos exigidos por la ley 16.986:arts.1 y 2. Esos presupuestos de admisibilidad no tienen “nada que ver” con el habeas data, cuyo objeto es permitir el acceso a la información para que el afectado tome conocimiento de los datos a él referidos.

La sanción de una ley reglamentaria debería subsanar este conflicto a fin de establecer un procedimiento adecuado a la tutela de los intereses –de jerarquía constitucional- que se busca proteger.

Por otra parte, la protección de los sujetos que puedan resultar afectados por el procesamiento de sus datos, requiere una regulación integral que procure un equilibrio satisfactorio entre la tutela de sus derechos personalísimos y el aprovechamiento de las ventajas que proporciona el manejo de la información para un mejor desenvolvimiento de los sectores comercial, bancario y financiero, que también conciernen al interés general y –específicamente- a nuestra inserción en el mercado internacional.

Los proyectos de ley presentados hasta ahora en la legislatura por los senadores Branda, Fernández Meijide, Arias y Eduardo Menem, e incluso la vetada ley 24.745, siguen el temperamento de no limitarse a una regulación meramente procesal de la acción de amparo especial (como lo hace el proyecto del diputado Alasino), sino a establecer un régimen global del tratamiento de datos, recogiendo principios básicos aceptados por otras legislaciones, para bien y para mal.

En el derecho comparado se distinguen dos sistemas básicos de regulación, amén de un espectro de variantes: el del derecho americano y el europeo. El primero ha seguido una orientación liberal relativa a la transmisión de datos, salvo determinadas materias que fueron sucesivamente reguladas. Así, en el año 1966 se dictó la Freedom of Information Act que estableció y garantizó el libre acceso a los datos de los registros públicos; la Fair Reporting Act en 1970 relativa a los informes comerciales y la Privacy Act en 1974 referida a los registros del gobierno federal sobre los particulares, limitando su almacenamiento de acuerdo a la competencia del ente estatal.

En el derecho europeo predominan las legislaciones que establecen una severa restricción para la transmisión de datos personales, exigiendo el consentimiento del titular para su recolección y transferencia, creando un poderoso organismo de control que rige la actividad (especialmente Alemania, España, Bélgica e Italia).

La ley 24.745 –vetada totalmente por decreto 1616/96² - siguió muy de cerca la

² En sus considerandos el decreto observó el art. 5º que creaba una Comisión Bicameral de Seguimiento de Protección Legislativa de Datos, que al no especificarse ni delimitarse las facultades otorgadas por dicha norma, resultaban de tal amplitud que vulneraban la distribución constitucional de incumbencias estatales, dado que en nuestro sistema el único poder con atribuciones para resolver sobre la protección de los derechos de los individuos es el Poder Judicial de la Nación. Que en su art. 16 prohibía la cesión o transmisión internacional de datos entre la República Argentina y otros Estados o con organismos internacionales que no aseguren una protección equivalente de datos de carácter personal. Consideró el PE que esa disposición omitía la previsión de supuestos de excepción en aras de la cooperación

línea rígida de la ley española, lo que motivó la reacción de las corporaciones bancarias, financieras y publicitarias, porque esa normativa conducía a suprimir llanamente la utilización de registros automatizados para proveer informes sobre la solvencia, y la publicidad por marketing directo.

Habiéndose reiniciado el tratamiento parlamentario de varios proyectos, entre los cuales el del senador Eduardo Menem lleva la delantera, la situación aun es bastante incierta.

No está claro todavía cuál va a ser la solución transaccional entre los reclamos del sector bancario y financiero, y los derechos de los sujetos perjudicados por la difusión de la información relativa a su solvencia.

Los primeros alegan que el acceso a la información crediticia les permite a las entidades que otorgan créditos seleccionar en forma más eficiente y objetiva sus clientes y realizar el *prizing* de los préstamos en forma más precisa al delimitar categorías de riesgo. De otro modo, sin información, los bancos cargarían una tasa activa uniforme que les permita cubrir sus pérdidas producidas por el incumplimiento de algunos clientes, con la ganancia extra de los que cumplen, encareciendo el crédito. Además, sostienen que un sistema de información con amplia cobertura incentiva el cumplimiento y la disposición a invertir en reputación.

Los sujetos afectados –en especial la pequeña y mediana empresa– manifiestan que un informe negativo sobre la solvencia implica una *capitis diminutio* que, en un medio donde el crédito les resulta escaso, los relega a las redes del circuito parabancario. Además, un comerciante en dificultades ve cerrado el camino para superarlas –no sólo en virtud de la información que tienen las entidades financieras– sino porque cualquier particular puede acceder a los informes que suministran empresas especializadas (que aunque sea demandan algún trámite o erogación), y aun mejor, al registro de deudores del sector financiero que el Banco Central difunde masivamente por Internet, lo cual amplía el espectro de sujetos que no querrán operar con un deudor en dificultades. Esta situación –sostienen– los conduce inexorablemente a la cesación de pagos.

Verdaderamente, resulta difícil congeniar los intereses en conflicto. Pero más difícil resultará si no se advierte que debe hallarse un equilibrio acorde con nuestra realidad y nuestras necesidades. La solución no se encontrará imitando llanamente el modelo de países anglosajones con otro nivel de desarrollo económico y otra conducta comercial. Ni tampoco copiando soluciones de naciones europeas, algunas precedidas por décadas dictaduras y regímenes totalitarios, que tal vez las tornan proclives a regular excesivamente el avance del poder –informático, en el caso–.

3. Los grupos de empresas y la responsabilidad derivada del tratamiento de datos personales.

El avanzado trámite parlamentario indica que es inminente la instauración de un régimen de control y de reglas específicas para el tratamiento de datos perso-

internacional y obligaciones asumidas por el Estado ante otros organismos. También objetó que la ley confería al Defensor del Pueblo el ejercicio de funciones jurisdiccionales y que la acción de *habeas data* regulada era insuficiente para una adecuada tutela del justiciable porque no era de aplicación contra los

nales, cuya inobservancia comprometerá la responsabilidad civil, administrativa y aun penal, del infractor.

Las empresas vinculadas ya no tendrán absoluta libertad de intercambiar su información relativa a los consumidores, sino que deberán atenerse a los límites que imponga la protección de un nuevo concepto de intimidad. Ello no implica que vaya a proscribirse el tratamiento electrónico de datos, que es actualmente una condición para el progreso económico y técnico, se trata mas bien de procurar que ese procesamiento se realice respetando los derechos y garantías de los individuos, asegurándoles el control de la información relativa a su persona.

Esta tutela tendrá lugar a través de la creación de un organismo de control, que desempeñará –cuanto menos– funciones de asesoramiento, registro, y sancionatorias.

Las empresas privadas que administren bancos de datos destinados a proveer informes a terceros deberán inscribirse en un registro. Si la transmisión de datos opera entre empresas vinculadas, no está previsto un régimen especial, de modo que depende cuáles sean las limitaciones que se establezcan para la transmisión de datos a terceros, deberán o no requerir el consentimiento del interesado para ceder información sobre datos personales.

Es que una ley reglamentaria no se inmiscuirá en la regulación de archivos de uso personal o privados, pero si los registros, bases o bancos de datos son comercializados o transmitidos a terceros, en forma total o parcial, por vía de interconexión o consulta, quedarán sometidos al ámbito de aplicación del nuevo régimen de protección de datos.

A la fecha, la orientación del proyecto presentado por el senador Eduardo Menem establece como regla general, la exigencia del consentimiento del titular de los datos para su tratamiento y transmisión, salvo que provengan de archivos públicos de acceso irrestricto; se limiten a ciertos aspectos y tengan fines publicitarios; que se trate de informes relacionados con la solvencia y el riesgo crediticio; o que se preserve la identidad del sujeto desdoblado o bloqueando la identificación.³ También está previsto que el organismo de control desarrolle una función preventiva, lo que conduciría a atribuirle facultades de inspección y supervisión técnica del tratamiento de datos y de los medios de recolección y sistemas de seguridad.

entes públicos.

³ El proyecto de Senador Eduardo Menem, dice en lo pertinente:

“Artículo 5.- Consentimiento. El tratamiento de datos de carácter personal es ilícito cuando el titular no hubiere prestado su consentimiento expreso, el que deberá constar por escrito o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, juntamente con las advertencias previstas en el art. 6 de la presente ley.

No será necesario el consentimiento cuando:

los datos se obtengan de fuentes de acceso público irrestricto; se recaben para el ejercicio de funciones propias de los poderes del Estado; se trate de listados cuyos datos se limiten a nombre, ocupación, fecha de nacimiento y domicilio; deriven de una relación contractual y resulten necesarios para su cumplimiento; se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la ley 21.526.

Artículo 7.- Categoría de datos. Ninguna persona puede ser obligada a proporcionar datos sensibles.

Los datos indicados en el apartado anterior sólo pueden ser recabados y objeto de tratamiento cuando median razones de interés general autorizadas por ley, o con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares;

Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o

Las empresas que hasta el presente entrecruzaban sus registros de datos personales sobre consumidores o terceros, deberán adecuar esa actividad observando reglas de seguridad, de transparencia y de información a los titulares de los datos, que les serán impuestas con el fin de evitar su utilización ilegítima.

indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes en el marco de las leyes y reglamentaciones respectivas.

Artículo 26.- Prestación de servicios de información crediticia. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial o pertinentes para la evaluación de la solvencia económica y el riesgo crediticio (en lugar de: crédito), obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

Pueden tratarse igualmente datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.

Sólo se podrán archivar, registrar o ceder los datos de carácter personal que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos diez años.

La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

Artículo 27.- Archivos, registros o bancos de datos con fines de publicidad. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso, que comprenderá también los datos que hubieren sido dados de baja y la fuente de donde han sido obtenidos, sin cargo alguno.

El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo.

Artículo 28.- Archivos, registros o bancos de datos relativos a encuestas. Las normas de la presente ley no se aplicarán a las encuestas de opinión, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable.

Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna en particular.