Los ataques de la informática y la protección de datos personales en Nicaragua

Jovanka Ñancahuazú Durón Chow[1]

1 Egresada de la Licenciatura en Ciencias Jurídicas, Universidad Centroamericana (UCA).
e-mail: jduronchow@hotmail.com

Recibido: octubre 2004/ Aceptado: noviembre 2004

LA INFORMÁTICA OFRECE POSIBILIDADES DE ALMACENAMIENTO EN FICHEROS, registros o bases de datos, tratamiento de la documentación y recuperación de la información registrada en soportes magnéticos, virtuales y flexibles. Permite controlar esa información y puede llegar a convertirse en un instrumento de presión y control social sobre las personas y su derecho a la intimidad y privacidad. Las personas, sus identidades e intimidades han sido reducidas a números, códigos de barras, claves de acceso, por lo que es fácil saber sobre ellos y controlar lo que hacen en sus trabajos cuando marcan entradas o salidas; en sus vidas diarias cuando acuden a los bancos a realizar cualquier operación bancaria, cuando se compra y paga con tarjeta, al retirar dinero del cajero automático y al ser guardadas en ficheros de datos pertenecientes a entes públicos, privados o particulares.

Palabras clave: informática – protección de datos

1. Introducción

Actualmente, las empresas operan a partir de los datos que poseen. Por citar ejemplos, las entidades financieras trabajan con la información generada de sus actividades, de los créditos de sus deudores, las operaciones bancarias de sus depositantes, las instituciones públicas. Para realizar facultades y competencias conferidas solicitan datos personales y los compilan en ficheros. Nosotros, los ciudadanos, proveemos por nuestra parte mucha información personal todos los días sin enterarnos de su uso y sin creer que nos afecta. En Nicaragua, a raíz del Caso Infornet, en el que sin consentimiento de las personas, se obtenían datos sobre su solvencia económica y se comercializaban a empresas para que éstas ofreciesen sus productos, se decidió aunar esfuerzos y legislar sobre el tema de la protección de datos personales y se redactó un Anteproyecto de Ley de Protección de Datos Personales que, de ser aprobado, pondría al país a la cabeza de garantías en este ámbito, junto con Argentina a nivel latinoamericano.

Y es a partir del análisis de dicho Anteproyecto y la Ley 25326 de Protección de Datos Personales promulgada en Argentina el 30 de octubre del año 2000 -con su respectivo

Reglamento y la jurisprudencia generada a partir de su aplicación-, que construiré el estudio plasmado en el presente documento. Esto para comprender mejor la importancia de equilibrar el uso de la informática y el respeto a los derechos de las personas. A partir del artículo 26 inciso 4 de la Constitución Política, encontramos un precedente de protección a los ciudadanos otorgándoles el derecho a saber la información que sobre ellos se haya registrado y la finalidad conferida a dichos datos.

2. La protección de los datos personales

Con la ayuda de las telecomunicaciones se puede transferir datos entre computadoras permitiendo el cruce de ficheros con datos personales y registros informáticos con su correspondiente proceso y tratamiento automático de información a través de los programas adecuados. La persona titular de los datos puede perder así totalmente el control sobre la utilización de los mismos y el tratamiento al que se le puede someter. Estamos de esa forma expuestos a nuevos ataques a la intimidad y privacidad de las personas. Estos datos personales deben ser protegidos de manera que no sea posible el acceso, malintencionado o no, de quienes no estén autorizados a tenerlo. Éste debe ser solamente para aquellos fines y personas autorizadas a ello. Un dato en sí puede no ser agresivo al derecho a la intimidad, pero reunido con otros varios sí puede serlo.

Por ejemplo, el que un individuo consuma servicios en un restaurante y los pague con tarjeta de crédito parece ser inocuo en sí, lo está haciendo a vistas de los comensales del restaurante y de sus invitados, pero si se toman todos los estados de cuenta de la tarjeta de crédito de ese sujeto durante un año y se observa con qué frecuencia asiste a ese restaurante, a qué otros sitios va, dónde compra, cuánto gasta en promedio, etcétera, tomaremos conocimiento de otras realidades del sujeto, estaremos penetrando en la vida privada de él. Asimismo, no constituye ninguna agresión el que un juez penal investigue y recabe información sobre los antecedentes y vida pasada de un indiciado, pero si quien lo hace es una fuerza policíaca o un cuerpo de inteligencia, sin ninguna base o fundamento derivado de una sospecha o de un proceso legal abierto, estaremos en presencia de un atentado a la privacidad (Mejan, 1994:75-76).

Se encuentra difundida la idea de los datos personales como series de informaciones susceptibles de revelar la identidad de un ser humano, sus gustos, inclinaciones, preferencias, padecimientos y tendencias. Por esto, la persona posee el derecho a que se le respete su identidad y personalidad, su derecho a la intimidad y, por lo tanto, la facultad de excluir del conocimiento de terceros, informaciones propias que no desea que sean reveladas, aunque éstas se encuentren en manos de la administración pública o entes privados. En consecuencia, para evitar usos ilícitos de la información obtenida e intromisiones no autorizadas a la vida personal, se configura el derecho a la protección de datos personales. Puede definirse este concepto como un derecho autónomo de tercera generación que procura el amparo debido de los derechos fundamentales y libertades de los ciudadanos contra una singular forma de agresión: el almacenamiento de datos personales y su posterior cesión no autorizados.

> *Consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona a decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también*

> *permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso (Egusquiza, 2002:134).*

A través de la protección de datos personales, el derecho que se trata de proteger no es sólo el de la intimidad, sino algo con mayor profundidad que en el derecho anglosajón se denomina «privacy» y que se ha castellanizado como privacidad.[1] Lo que se busca es proteger aspectos de la personalidad que individualmente no tienen mayor trascendencia, pero que, al unirse con otros, pueden configurar un perfil determinado de las personas y la propensión a su divulgación sin su conocimiento las pueden afectar. Ante dicha posibilidad surge el derecho de sus titulares a exigir que los datos permanezcan en el ámbito de su privacidad. No sólo se protegen datos íntimos de la persona, sino cualquier tipo de dato personal cuyo conocimiento o empleo por terceros sea una amenaza para el individuo, pueda causarle un perjuicio, afectar a sus derechos, sean o no fundamentales, en su posición de ciudadano, consumidor o cliente, frente a los entes públicos, privados o particulares.

Se trata de proteger, como lo hemos indicado, la privacidad, pero también, de buscar equilibrio entre la libertad de expresión -que comprende la libertad de opinión y la libertad de recibir o comunicar informaciones-, ampliamente reconocida y expresamente recogida en las modernas recopilaciones de derechos suscritas por infinidad de países, y la protección a los individuos cuando se produce una intromisión en ella. En este caso, el tratamiento de datos en ejercicio del libre derecho de obtener y difundir libremente la información a la que hemos hecho referencia, no debe ser causa de perjuicio al honor y la imagen pública del individuo o la persona jurídica. Nace así la llamada privacidad y el reconocimiento de un derecho del ciudadano a proteger su ámbito personal ante la potencial agresividad del elemento informático

La protección de datos no solamente es una respuesta a la afectación del derecho a la intimidad sino de la identidad como seres humanos y ciudadanos. Sin embargo, es objeto de debate si la protección de datos debiese ser extensiva a las personas jurídicas. Existen dos posiciones: la positivista, apoyada por el Convenio Europeo de Derechos Humanos, permite la posibilidad de que se protejan y garanticen las informaciones relativas a grupos de personas, asociaciones, fundaciones, sociedades, corporaciones y cualquier otro organismo formado directa o indirectamente por personas físicas, tuvieren o no personalidad jurídica. Asimismo, afirma que las personas jurídicas poseen una identidad comercial que puede ser perjudicada. Por ejemplo: el aparecer en un listado de un banco como deudor, imposibilita tener relaciones mercantiles justas. También señala que se deben proteger datos de la persona jurídica cuando los datos sean referidos a las personas físicas que actúan como administradores o integrantes de las personas jurídicas. Por otro lado está la posición negativista, que esgrime lo exagerado de atribuir un derecho a la intimidad cuando ésta cuenta con el llamado secreto comercial.

Escobar Fornos (1999: 277) retoma este conflicto a favor de las garantías hacia las personas jurídicas aduciendo que en la práctica las personas jurídicas se ven afectadas en su prestigio y reputación:

...como cuando se les imputa un delito falso, una falsa insolvencia, una falsa adulteración de la calidad anunciada de sus productos, etcétera...

La posición adoptada por los legisladores nicaragüenses en el Anteproyecto de Ley de Protección de Datos Personales y la de los argentinos, es la de ampliar la protección de datos personales a las personas jurídicas.[2]

3. Consentimiento del interesado

En la vida diaria damos mucha información a terceros, por ejemplo, al realizar un trámite en una oficina pública, al solicitar la expedición de documentación, aperturar una cuenta bancaria, pagar bienes o servicios, etcétera. Cabe aclarar que el otorgamiento de esa información por parte de sus titulares no significa autorizar su uso para otros fines, aunque ello sí suceda en la práctica. El consentimiento constituye un elemento que, en principio, elimina el carácter ilícito de un ataque a un bien de la personalidad. En materia de protección de datos personales, el consentimiento del afectado constituye un elemento indispensable que justifica el tratamiento de datos personales por el responsable del fichero. Se erige, como señala Murillo de la Cueva, en la piedra angular a partir de la cual se construye el sistema de protección de datos personales frente al uso de la informática.

La fórmula en que debería redactarse el requisito del consentimiento previo es la que a continuación menciono: "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado consienta el tratamiento de datos personales que le conciernan, así como los procedimientos de cesión y transferencia internacional de datos una vez que se le indiquen las finalidades de dichos procedimientos y se le aseguren la legitimidad de los fines y del cifrado para la transferencia a otro país que tenga idénticas o mayores garantías de protección de datos en su legislación".

Se trata de incluir la autorización para los principales procesos a los cuales se someten los datos de carácter personal, los cuales representan las mayores lesiones a los derechos del ciudadano, en caso de realizarse sin el conocimiento y la autorización del interesado.

Se habla de un consentimiento *libre* en cuanto es otorgado al margen de cualquier presión o coacción física o psíquica; *informado*, para que sea inequívoco, que el interesado pueda sopesar los riesgos y ventajas del tratamiento de sus datos y ejercer los derechos que le asisten al interesado. Deberá ser *expreso y específico*, es decir, debe ser referido al tratamiento de los datos referentes a su persona por el responsable del fichero y para una determinada finalidad. Además deberá precisarse qué tipo de datos, formas del tratamiento y, en su caso, qué transferencias o cesiones de datos a terceros se autorizan. No caben, en conclusión, autorizaciones generales, sino pronunciamientos caso por caso en los cuales el control pueda ejercerse de manera efectiva (Murillo de la Cueva, 1993:59).

El interesado debe tener también la posibilidad de revocar en cualquier momento su consentimiento cuando exista causa justificada. Ahora bien, la revocación no puede tener efectos retroactivos, ya que de lo contrario resulta ilegal de manera sobrevenida un tratamiento de datos personales previamente lícito.

Para algunos doctrinarios, entre ellos Sánchez Bravo, se discute sobre la practicidad de prestar el consentimiento mediante su formalización por escrito. Por razones prácticas no debe imponerse por escrito, prefiero adoptar una postura más garante y menos pragmática, resulta de mayor respaldo informar en un documento acerca de la finalidad de los datos y en base a ello, solicitar el consentimiento, mencionar la inclusión en un fichero, los procesos a los cuales serán sometidos los datos, la identificación del responsable del fichero y el derecho que le asiste al interesado, de esa manera se busca una mayor formalidad y obligación, por parte del responsable del fichero, en cumplir las finalidades del tratamiento de datos.

Será preciso el consentimiento expreso y escrito por anticipado cuando del tratamiento de "datos sensibles" – como los relativos a la salud, ideología, religión, raza, preferencia sexual, etcétera – estemos hablando; así como de aquellos supuestos en los que de la prestación del consentimiento se deriven para el afectado cualquier género de carga o de gravamen.

Si analizamos la posición tomada sobre el consentimiento en la regulación nacional (Artículo 6 inciso a) Anteproyecto de Ley de Protección de Datos Personales de Nicaragua), se aduce que se otorga licitud al tratamiento de datos al ser inequívoco. Y continua diciendo: *o por otro medio que permita que se le equipare.* Al respecto señalo que la mejor forma de brindar el consentimiento expreso es de forma verbal e induciría error permitir expresarlo por otro medio equiparable in dejarlo definido en la ley. En mi opinión, será inequívoco cuando el interesado esté informado expresando claramente su voluntad y por lo tanto no pueda deducirse por otro medio cuál hubiese sido la intención del interesado si no fuese expreso, se sigue la postura doctrinaria de que será expreso al respecto de otras declaraciones y prestado caso por caso.

En Argentina, aparte de ser expreso como en Nicaragua, el consentimiento debe ser libre e informado y deberá constar por escrito o por otro medio que se le equipare, demarcando una redacción mas depurada y apropiada del articulado. Es claro que la redacción de la partícula *o por otro medio que se le equipare* hace referencia a otro medio comparable al escrito tradicional; puede ser una aceptación, vía Internet, de un procedimiento disponible en línea, como los sitios de consulta bancaria *on line* que solicitan datos para permitir el acceso, que solamente puede proveer el cliente interesado.

Excepciones al consentimiento

Como regla general, las legislaciones de protección de datos exigen el consentimiento previo del interesado para recopilar datos, someterlos a tratamiento automatizado y cederlos, salvo excepciones expresamente tasadas en su articulado. Los casos tasados que preveen las legislaciones de Nicaragua y Argentina coinciden al regular la excepción de brindar el consentimiento3 cuando:

1. *los datos se obtengan de fuentes de acceso público irrestricto*[4]*;*
2. *se recaben para el ejercicio de funciones propias de los poderes del Estado en el ámbito de competencia* (esta fracción es de reconocida importancia en Nicaragua, para delimitar la legalidad como garantía de legitimidad, o en virtud de una obligación legal);
3. *se derive una relación contractual, comercial, laboral, científica o profesional y*

resulten necesario para su desarrollo o cumplimiento (es necesario designar para el cumplimiento de una relación contractual las generales de ley de las partes y demás requisitos de validez según la figura jurídica que se consigna en el contrato, los cuales serán por excelencia los limites de legalidad a la proporcionalidad de los datos);

4. *se trate de listados cuyos datos se limiten a nombre, cédula de identidad, profesión u oficio, fecha de nacimiento y domicilio* (se delimitan taxativamente qué datos generales son los necesarios para identificar a los miembros de gremios profesionales, porque al publico en general le interesa tener datos de contacto),
5. *se trate de operaciones que realicen las entidades financieras y de las informaciones que reciben de sus clientes conforme a las disposiciones de la materia* (o sea, los requerimientos fijados por la Superintendencia de Bancos (SIB) como necesarios para cumplir con las actividades propias de las entidades financieras, siempre que no sean excesivas, que se le informe al cliente sobre las finalidades, su derecho al acceso y rectificación, sobre lo obligatorio o facultativo de dar la información);
6. *la prestación de servicios de información crediticia no requiera el previo consentimiento del titular de los datos a los efectos de su cesión*[1] (aquí, la cesión de datos es vista como una extensión del giro comercial de la empresa, como lo es brindar servicios de información acerca de la solvencia fiscal y económica de las personas. Asimismo, cuentan con el consentimiento inicial para colectar datos facilitados por el interesado o de fuentes accesibles al público, por lo que no requiere el consentimiento del afectado para ceder sus datos a terceros que estén relacionados entre sí con el giro de las actividades comerciales o crediticias. Aunque siempre subsiste la obligación del responsable del fichero de comunicar, a solicitud del titular de los datos, el tratamiento al cual ha sometido los datos, producto de lo cual se hayan generado informaciones, evaluaciones y apreciaciones sobre el mismo y hayan sido comunicadas a terceros durante los últimos seis meses. A diferencia de Argentina, en Nicaragua el plazo es de los últimos tres meses -además comunicar el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión). (Cfr. Artículo 25 inciso e) Anteproyecto Ley de Protección de Datos Personales de Nicaragua y Artículo 26 inciso 5) Ley 25326 de Protección de Datos Personales de Argentina)
7. *el tratamiento de datos personales sea con fines de defensa o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia* (Cfr. Artículo 23 inciso 2) Ley 25326 de Protección de Datos personales de Argentina). (Aquí no es necesario el consentimiento del afectado para el tratamiento de datos. Se justifica, porque son entes especializados de seguridad para los casos, supuestos y categorías, que resulten necesarios en el estricto cumplimiento de las misiones legalmente asignadas para la defensa nacional, la seguridad pública o la represión de los delitos. Aunque en Nicaragua se exime el consentimiento del afectado tanto para la colecta como para el tratamiento de datos). (Cfr. Artículo 22 inciso b) Anteproyecto de Ley de Protección de Datos Personales de Nicaragua)

4. Derechos del interesado

Es indiscutible la necesidad de establecer legalmente unos derechos que puedan ser ejercidos por los ciudadanos como garantía frente a las intromisiones que constituyen una vulneración a la intimidad, al honor y a otros derechos fundamentales, todo ello provocado por el uso de

la informática. No solo se trata de evitar lo que Davara (2003: 83) bautiza como dictadura tecnológica, sino que, a través de estas garantías, el afectado se proteja de una manera eficaz frente a posibles lesiones de sus derechos, sancionando a todos aquellos infractores que los vulneren buscando, de forma concreta, un equilibrio entre los fichadores y los fichados.

Los derechos que posee el interesado revisten obligaciones para el responsable del fichero de datos. A continuación haré una breve enunciación de los principales derechos del interesado según lo mencionado por la doctrina y lo que consta en las legislaciones a partir del derecho comparado:

Derecho de información

Se conoce también como el principio de transparencia. Puede ser considerado como la condición previa para el ejercicio de los demás derechos reconocidos a los ciudadanos y el control sobre la información tratada por terceros. Para que se pueda aplicar eficazmente se requiere que en la práctica se posibilite adquirir información sobre la recogida,
 almacenamiento, finalidad, cesión o transferencia internacional de datos personales; la existencia de un fichero, identidad y dirección de su responsable, destinatarios de la información, carácter obligatorio o facultativo de la respuesta; consecuencias de la obtención de datos o de la negativa a facilitarlos (Murillo de la Cueva, 1990: 187).

Igualmente debe informarse de los derechos que le asisten en materia de protección de datos de carácter personal, así como las formas y modalidades de su ejercicio. Estas facultades reconocidas a los particulares incorporan como contrapartida la obligación, para los responsables de los ficheros de datos, de darle un estatus de publicidad a sus registros, los cuales serán de consulta pública y gratuita (Cfr. Artículo 14 Anteproyecto de Ley de Protección de Datos Personales de Nicaragua y 13 Ley 25326 de Protección de Datos personales de Argentina); esto se concreta en la inscripción del responsable del fichero en un registro público (Cfr. Artículo 20 y Artículo 21 Op. Cit.).

La mayoría de las leyes de protección de datos incorpora entre sus previsiones la creación de un registro a cargo del órgano de control, donde deberán inscribirse todos aquellos ficheros que traten datos personales, con descripción de las actividades relativas al tratamiento, tanto subjetivas como materiales, estableciendo de esa forma un modelo unitario del contenido de la inscripción. La publicidad se completa a través de la publicación en el Diario Oficial, por parte del órgano de control, de una relación de los ficheros inscritos y notificados.

En frecuentes ocasiones, y de forma dispersa en las legislaciones nicaragüense y argentina, se destacan las obligaciones de los responsables de ficheros de datos:

1. *Cuando se recaben datos personales se deberá informar a los titulares* (Cfr. Artículo 7 y Artículo 6 Op. Cit.).
2. *El responsable de los ficheros de datos debe proporcionar información solicitada por el titular de los datos...*(Cfr. Artículo 15 inciso 2) y Artículo 14 inciso 2 Op. Cit.)
3. *En la prestación de servicios de información crediticia, el responsable deberá, a solicitud del titular de los datos, comunicarle las informaciones, evaluaciones, apreciaciones que sobre el mismo hayan sido comunicadas.*

Derecho de acceso

Es la facultad personalísima, que se le concede al afectado, de comprobar si se dispone de información sobre él mismo y conocer el origen de la existencia de los datos, así como la finalidad con que se conserva, las cesiones que se han hecho de los datos del afectado a terceros, la identidad de los cesionarios y la finalidad que éstos persiguen. Todo a través de la solicitud, al responsable del fichero, de la rendición de un informe con los datos arriba señalados.

Al ser un derecho personalísimo no puede ser ejercitado más que por el titular y, en el caso que fallezca, por sus sucesores universales. No se podrá acceder a informaciones referentes a terceros y los informes que se brinden no deberán contener informaciones de otras personas. Este derecho de acceso debe de ser de fácil ejercicio y los datos deben ser comunicados en un plazo razonable. La fórmula seguida por Argentina es que el titular, previa identificación, tiene derecho a solicitar información (Cfr. Artículo 14 inciso 1) Ley 25326 de Protección de Datos Personales de Argentina). Se trata de un requisito no mencionado en el anteproyecto nacional, lo cual debería retomarse para acreditar la legitimidad en el ejercicio de dicho derecho.

La información debe ser proporcionada por el responsable del fichero dentro de diez días posteriores a la recepción de la solicitud que, en caso de la legislación argentina, habilita a solicitarse por medio escrito, electrónico, telefónico u otro medio idóneo (Cfr. Artículo 14 párrafo primero del Decreto 1558/2001 Reglamento a la Ley 25326), facilitándole al interesado, medios diversos para ejercer su derecho.

La información proveída debe ser clara, sencilla, exenta de codificaciones o con su explicación según lo exigido. En Argentina debe ser en lenguaje accesible del conocimiento medio de la población (Cfr. Artículo 15 inciso 1) Ley 25326 de Protección de Datos Personales de Argentina); amplia aun cuando lo solicitado sólo comprenda un aspecto de los datos personales; debe versar sobre la totalidad del registro perteneciente al titular. Ambas legislaciones prohíben la revelación de datos de terceros aunque estén vinculados con el interesado. Los datos podrán ser suministrados en diferentes medios, sean electrónicos, telefónicos, de imagen u otro que determine el interesado según la capacidad técnica del responsable de archivo (Cfr. Artículo 16 incisos a-c) Anteproyecto de Ley de Protección de Datos personales de Nicaragua y Artículo 15 inciso 1-3) Ley 25326 de Protección de Datos personales de Argentina).

En caso de no proveerse la información o de ser estimada por el particular como insuficiente, como se agrega en el caso argentino, ambas leyes legitiman al afectado a interponer la acción de protección de datos, o *habeas data* (Cfr. Artículo 15 inciso b) párrafo segundo Op. cit y Artículo 14 inciso 2) párrafo segundo Op. Cit), ante la autoridad competente para restituir su derecho, dicha acción y su implementación procedimental serán abordados en lo sucesivo.

Existe un límite al ejercicio gratuito de este derecho y sólo se puede ejercer sin costo alguno al efectuarse por intervalos delimitados no inferiores a cuatro meses en el caso de Nicaragua; y para Argentina es de seis meses, salvo acreditarse un interés legitimo (Cfr. Artículo 15

inciso c) Op. Cit. y Artículo 14 inciso 3) Op. Cit.) en cuyo caso podrá ejercitarse antes. Por regla general y en la práctica, se ha entendido el interés especial legitimador en que se acredite por el interesado la existencia de indicios que le hacen sospechar que los datos que se someten a tratamiento son más que los que se conocen en virtud del acceso ejercido, el interés por saber si no se han incluido más datos de los consentidos inicialmente, se han agregado datos sensibles o se ha operado un uso diferente a la finalidad para la cual fueron recabados. Sin embargo, de no acreditarse dicho interés legítimo, el responsable del tratamiento puede negarse a brindar el informe o exigir el pago de algún tipo de compensación económica (Téllez Aguilera, 2001:162).

Derecho de rectificación, actualización y cancelación

Si conocidos los datos que le afectan, el individuo constata que aquellos contienen errores, puede solicitar la rectificación. Este derecho se dirige a obtener la corrección, adición o actualización de aquellos datos que figuren de manera inexacta, incompleta o desfasada. Acerca de lo anteriormente dicho, ambas legislaciones sometidas a comparación reconocen el derecho del interesado a que sus datos personales sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad (Cfr. Artículo 17 inciso 1) Anteproyecto de Ley de Protección de Datos Personales de Nicaragua y 16 inciso 1) Ley 25326 de Protección de Datos Personales).

Cuando se constata que los datos no son pertinentes o adecuados, en relación con la finalidad para la cual fueron registrados, o pertenecen a una categoría tal que impide su registro, o se ha procedido a su registro de forma ilegal o contraviniendo el consentimiento del interesado, éste podrá ejercitar su derecho de cancelación para eliminar del fichero aquellos datos personales.

La polémica en este derecho estriba en determinar qué debe entenderse por cancelación; si debe equivaler a destrucción de material o borrado de datos, o debe limitarse simplemente al apartamiento de tales datos de los canales de uso señalando que no pueden ser utilizados, pero conservándolos en el propio fichero. En atención a la naturaleza y objetivos de este derecho, esto nos lleva a asumir la primera de las variables; ante el uso ilegítimo de datos personales, sólo pueden salvaguardarse los derechos ciudadanos eliminándolos totalmente para evitar eventuales perjuicios. Además, ¿qué sentido tendría conservar unos datos incorrectos? ¿No podría darse lugar a una tentación futura y utilizar los datos incorrectos con fines ilegítimos? (Sánchez Bravo, 1998:97).

El hecho que un dato sea incorrecto deberá ser probado por la persona interesada. Este derecho debe ser escrupulosamente respetado por los responsables del fichero y le impone a éstos velar por la exactitud, actualidad y veracidad de los datos para que no conste en ellos una imagen distorsionada de la verdad. Sustituidos los datos incorrectos, éstos deben ser borrados para evitar que esa dualidad en el registro ocasione perjuicios a terceros. Se obliga al responsable del fichero a hacer efectivo este derecho en un plazo razonable, que coincidentemente en Nicaragua y Argentina es de cinco días hábiles desde que se recibió la solicitud de rectificación y sin coste al ciudadano (Cfr. Artículo 17 inciso b) párrafo segundo Anteproyecto de Ley de Protección de Datos Personales de Nicaragua y artículo 16 inciso 2)

Ley 25326 de Protección de Datos Personales). Durante el proceso de verificación y rectificación del error o falsedad de los datos, el responsable del fichero debe bloquear los datos materia de la solicitud o consignar una nota al proveer información relativa que se tramita en un procedimiento con determinado objeto (Cfr. Artículo 17 inciso f) Op. cit y Artículo 16 inciso 6) Op. cit). Cuando los datos hayan sido cedidos a terceros, para proteger los intereses del afectado, el responsable del fichero está obligado a comunicar al cesionario la rectificación, actualización y cancelación de los datos, para que éste lo haga a su vez con los datos que le fueron cedidos.

Los responsables de ficheros deben proceder de oficio a la cancelación de aquellos datos que consten indebidamente en su fichero. En lo concerniente al plazo en que debe operarse la cancelación, es necesario considerar el cumplimiento del plazo que contemplaba la autorización del afectado o la disposición normativa que habilitaba su recogida (Murillo de la Cueva, 1993:80) o el tiempo en que hubiesen dejado de ser necesarios, como es el caso retomado en las legislaciones nicaragüense y argentina, que mandan cancelar los datos personales registrados con fines policiales cuando ya no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Además, reconocen el caso de proveedores de servicios de datos personales, regulando el hecho que, una vez cumplida la prestación contractual, los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de quien ha solicitado el servicio cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrán almacenar con las debidas condiciones de seguridad por un periodo de hasta dos años (Cfr. Artículo 24 inciso b) Anteproyecto de Ley de Protección de Datos Personales de Nicaragua y artículo 25 inciso 2) Ley 25326 de Protección de Datos Personales de Argentina).

Sin embargo, nos topamos con otra excepción al ejercicio de los derechos reconocidos a favor del ciudadano y es que la cancelación de los datos no procede por razones de interés social, de seguridad nacional, de salud pública, o por afectarse derechos de terceros (Cfr. Artículo 17 inciso e) Anteproyecto Ley de Protección de Datos Personales de Nicaragua) y, por si fuera poco, además, se excepciona la obligación de rectificar, actualizar, complementar, cancelar, incluir o reservar los datos, mediante resolución debidamente fundada y motivada en la ley (Cfr. Artículo 18 inciso a) Op. Cit.), según lo enunciado en la legislación nacional. En cambio, en el caso de Argentina se alega que no procede la supresión cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros o cuando existiera una obligación legal de conservar los datos (Cfr. Artículo 16 inciso 5) Ley 25326 de Protección de Datos Personales de Argentina); para complementar, también se les permite a los responsables de ficheros:

1. denegar el acceso, rectificación o supresión en función de la defensa de la nación, del orden y la seguridad públicos o la protección a los derechos o intereses de terceros,

2. además se podrá denegar la información por los responsables de ficheros públicos cuando ello pudiera constituir un obstáculo a las actuaciones judiciales o administrativas en curso, vinculadas a la investigación del cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de salud y del medio ambiente, la

investigación de delitos y la verificación de infracciones administrativas (Cfr. Artículo 17 inciso 1) y 2) Op. Cit.).

A diferencia de Argentina, que presenta excepciones más limitadas como el derecho de terceros, una obligación patente a través de una ley, y para evitar obstaculizar averiguaciones legales, tributarias o administrativas en Nicaragua, los motivos por los cuales no procede la cancelación de los datos no preveen explicación ni la debida garantía a favor del interesado en que se especifique cuáles son taxativamente los casos en que se habla de interés social, de seguridad nacional, etcétera. Por lo tanto, estamos ante un enorme escudo que puede ser esgrimido por los responsables de ficheros para negarse a cumplir con lo impuesto por la ley. Y es que la mayoría de las causales de excepción se configuran para proteger a los ficheros en propiedad de la Administración Pública. Lo que dicta la lógica es preguntarse a quién le es útil conservar datos inexactos y desactualizados sin causar un perjuicio por ello al ciudadano.

A pesar de dichas excepciones, ante la negativa del responsable del fichero a cancelar los
40 datos, siempre se encuentra legitimado el ciudadano para acudir ante la vía judicial ejerciendo la acción de protección de datos personales (Cfr. Artículo 17 inciso c) Op. Cit y Artículo 16 inciso 3) Op.cit.).

Derecho de oposición

En los casos que no sea necesario el consentimiento del afectado para el tratamiento y cesión de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a dichos procesos cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado. Conjuntamente subsiste la obligación de comunicar al afectado la fuente por medio de la cual se obtuvo la información (Cfr. Artículo22 inciso b) 25 inciso c) Op. cit y Artículo23 inciso 2) 26 inciso 3) y 5) Op. Cit.). Entre los motivos legítimos de oposición puede citarse la falta de justificación legal de un tratamiento determinado de datos personales. Sin embargo, la mayoría de las legislaciones establecen la imposibilidad de oponerse cuando sea objeto de un tratamiento lícito y necesario para el cumplimiento de determinadas tareas públicas o privadas.

Se trata de una confrontación entre el reconocimiento a las personas, de un derecho sobre las informaciones que le conciernen, y el poder, generalmente de la autoridad pública para registrar y tratar estas informaciones con bases diversas como el interés y seguridad pública, la defensa nacional, salud pública, etcétera. A pesar de tratar de establecer límites, la Administración Pública es la que menos se sujeta a controles.

Este derecho está disperso y no se agrega como un solo artículo junto a los otros relativos a los derechos del interesado. Además, a diferencia de los derechos de acceso y rectificación, no cuenta con un plazo para que el responsable del fichero lo haga efectivo, por lo que es necesario suplirlo a través de la reglamentación. Este derecho consiste en la negativa de los afectados a cualquier posible tratamiento de datos. Mientras, la Administración Pública excepciona de buena gana el consentimiento del interesado y limita su derecho de oposición

y se permite a sí misma tratar datos personales. En consecuencia reprime por una parte y admite por otra, estableciendo la posibilidad de los interesados a oponerse, previa petición y sin costo, al tratamiento de datos obtenidos de fuentes accesibles al público con fines de publicidad y prospección comercial, a partir de la presunción general que ningún ciudadano desea recibir informaciones, comunicaciones o servicios no solicitados ni deseados.

Concerniente a lo anteriormente apuntado difieren la legislación de Nicaragua y Argentina, al permitir únicamente el derecho a la oposición, en el caso de registros con fines de publicidad en donde se manda al responsable de dicho registro a retirar o bloquear los datos a solicitud del interesado (Cfr. Artículo 26 inciso c) Op. cit y Artículo 27 inciso 3) Op. Cit.); y no así cuando se traten de registros de prospección o solvencia económica. En el caso que la oposición del interesado se manifestara, el responsable del tratamiento deberá suspender de inmediato el tratamiento de los datos personales. Si pese a esta oposición, el tratamiento tuviera lugar, deberá reconocerse al interesado la posibilidad de plantear una acción tendente a la reparación de las consecuencias que dicho tratamiento ilícito le hubiera acarreado. Si el tratamiento estuviera en trámite de ejecución, o existiera el riesgo de que un tratamiento tal pudiera verificarse, el interesado podrá ejercitar una acción tendente a la paralización y/o cesación del tratamiento abusivo que le perturba (Sánchez Bravo, 1998:99). En estos supuestos propongo legitimar como otro supuesto que, de no proveerse el derecho de oposición, facultaría al afectado a ejercer la acción de protección de datos o *habeas data* con los efectos antes mencionados.

Derecho a indemnización

Los interesados, que como consecuencia del incumplimiento de lo dispuesto en la Ley, sufran daño en sus bienes o lesión en sus derechos deberían tener derecho a ser indemnizados ampliando los efectos de la sentencia que resuelva la acción de protección de datos o habeas data y aparte de restablecer lo derechos que se han violado o de detener la amenaza inminente de lesión, dar lugar a que se indemnice al ciudadano por los daños causados, para constituirse en una sanción ejemplar tendente a evitar que se sigan violentando derechos. Tres serían los requisitos que justificarían la solicitud de indemnización:

1. La persona está sometida a una decisión perjudicial.
2. Una supuesta conducta negligente por parte del responsable o encargado del tratamiento de los datos derivada de actos u omisiones.
3. Un daño o lesión no sólo en los bienes del afectado, sino también en sus intereses.

En lo relativo a los ficheros de titularidad pública, el artículo 132 párrafo segundo de la Constitución Política de Nicaragua es claro al reconocer la responsabilidad patrimonial del Estado por las lesiones a los derechos, bienes e intereses de los particulares, y el régimen de responsabilidad aplicable es el de la jurisdicción de lo Contencioso Administrativo (Cfr. Artículo 1, 15 inciso 2), 50, 94 inciso 3) Ley 350 de Regulación de la Jurisdicción de lo Contencioso Administrativo de Nicaragua); y cuando sean ficheros privados será la jurisdicción ordinaria, a través de un procedimiento civil, la que determinará cualquier responsabilidad y el derecho a una indemnización por daños. Esto es lo que se aplicaría de no incluirse dentro de la ley de protección de datos el derecho a la indemnización y permitirse como uno de los efectos de la sentencia de acción de protección de datos o *habeas data*.

Porque este derecho aún no se encuentra ni previsto ni regulado en el Anteproyecto de Ley de Protección de Datos Personales de Nicaragua ni en la Ley 25326 de Protección de Datos Personales de Argentina o su reglamento y debido a la importancia que he venido explicando en este apartado, debería reconocerse y regularse el derecho a ser indemnizado como una opción del afectado para que se respeten sus derechos.

Derecho de impugnación de decisiones automatizadas

Fue de repercusión general la decisión de la Dirección General de Ingresos (DGI), en el 2002, de ampliar de oficio la base de contribuyentes del Impuesto Sobre la Renta con los particulares que ofertaban sus servicios profesionales en las páginas amarillas de la guía telefónica de PUBLICAR S.A[5]. Era obvio que su tratamiento automatizado de datos incluyó de ipso, como contribuyentes, a los anunciantes en las páginas amarillas y por lo tanto dio por sentado que sus ingresos anuales eran los suficientes para contribuir.

Otro ejemplo que no puede dejar de citarse para ilustrar este derecho es el acaecido durante el primer semestre del año 2004: la Empresa Nacional de Telecomunicaciones (ENITEL) realizó de oficio un cambio en las categorías de usuarios del servicio de telefonía, pasando de un cargo básico de consumo residencial de US $5.94 (cinco dólares de los Estados Unidos de Norteamérica con noventa y cuatro centavos) al no residencial con un cargo de US $15.85 (quince dólares de los Estados Unidos de Norteamérica con ochenta y cinco centavos) a las personas que aparecían ofreciendo sus servicios profesionales en las páginas amarrillas de PUBLICAR S.A. Todo ello sin consultarlos o permitirles intervenir antes de tomar la decisión, si es que realmente poseían una empresa, un taller, un bufete, restaurante, etcétera... con entregas a domicilio o con forma de operar básicamente vía telefónica. Si bien hacían uso del teléfono para generar riqueza, de ninguna forma esto justifica o legitima hacer un cobro tan exorbitante en una moneda extranjera, cuando el Córdoba es la moneda de curso legal y además, se cobra Impuesto al Valor Agregado, por lo que el cargo básico de consumo constituye una doble carga tributaria, sobre todo cuando ENITEL no está facultada para hacerlo si el servicio telefónico está incluido como un servicio primario y básico, al igual que la energía eléctrica y el agua.

No se puede afectar a los usuarios suponiendo de ipso, en detrimento de sus derechos, cuando es la empresa la que ha fabricado una imagen del ciudadano a partir de datos que no le han sido proporcionados directamente por los afectados. En ambos casos, la DGI y ENITEL carecían de criterios específicos y concretos para tomar dichas decisiones lesivas que imponen arbitrariamente una carga monetaria sin dar debida intervención al afectado para que aclare su verdadera situación. Ambas instituciones actuaron de oficio y tomaron decisiones basadas en los resultados de un tratamiento automatizado de los datos de más de diez mil profesionales que aparecían en la guía telefónica. Únicamente se encargaban de enviar los formatos de notificación en los que ni siquiera se incluían los elementos concretos para emitir tal resolución.

La utilización abusiva de la informática en la toma de decisiones constituye uno de los riesgos esenciales que se plantean en el futuro, ya que el resultado que proporciona la "máquina" que usa cada día programas más refinados e incluso sistemas expertos, tiene un

carácter aparentemente objetivo e indubitable al que el responsable de tomar las decisiones puede conceder una importancia decisiva. El afectado tiene derecho a impugnar dichos actos y decisiones, pues no debe verse sometido a una decisión judicial, administrativa o privada, que le resulte arbitraria o perjudicial. Debe preservarse un cierto nivel de humanidad en la adopción de decisiones y asegurar una motivación suficiente a los actos administrativos y privados, para que no resulten en una agresión al ciudadano como resultado de fabricar una personalidad sustituyendo su identidad por otra que no se corresponde con la verdadera (Murillo de la Cueva, 1993: 83-93).

En este caso, el afectado tendrá derecho ineludible de obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizado en el tratamiento que sirvió para adoptar la decisión en que consistió el acto. Se permite la oposición e impugnación del afectado en las circunstancias siguientes:

1. Es una decisión basada exclusivamente en un tratamiento automatizado y no han concurrido otros elementos de indicios, dejando fuera la posibilidad de apreciación humana.
2. El tratamiento atribuye a los datos relativos al interesado, variables absolutas que determinan un perfil de personalidad tipo, considerado bueno o malo, apto o no apto, contribuyente o no contribuyente, usuario residencial o no residencial, etcétera.
3. Se trata de un perfil erróneo del ciudadano y sus consecuentes resultados negativos para el sujeto.

Al respecto de este derecho, únicamente Argentina lo ha reconocido en su Ley de Protección de Datos Personales y enuncia que las decisiones judiciales o actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministran una definición del perfil o personalidad del interesado, advirtiendo que de ser así, son insanablemente nulos (Cfr. Artículo 20 incisos 1) y 2) Ley 25326 de Protección de Datos Personales de Argentina). Hago un comentario a este precepto y señalo que se ha olvidado incluir las decisiones de entes privados, que son igual de dañinas que las judiciales o administrativas, y que la regulación nacional sobre la materia lo ha omitido debiéndose incluir un artículo al respecto.

5. Entidad reguladora

Al respecto se debe mencionar que en el Anteproyecto de Ley de Protección de Datos de Nicaragua se prevee la creación de una entidad reguladora, que es la Dirección de Protección de Datos Personales adscrita al Consejo Nacional de Ciencia y Tecnología, ente a su vez dependiente de la Vicepresidencia de la República.

Entre sus facultades está la de imponer sanciones administrativas en caso de incumplimiento de la Ley, llevar un registro de la creación y modificación de los ficheros de datos personales, asesorar a las personas sobre la Ley, dictar sus propias normas, solicitar a la autoridad judicial competente autorización para inspeccionar los inmuebles, equipos y programas de captura de datos, características generales de los campos, recopilación, finalidad, uso, tratamiento y generales de los titulares de ficheros de datos tanto privados como públicos

(Cfr. Artículo 28-32 Anteproyecto de Ley de Protección de Datos Personales de Nicaragua).

Pero a diferencia de Nicaragua, el órgano competente en Argentina está adscrito al Ministerio de Justicia y Derechos Humanos. Su director es designado por el Poder Ejecutivo con acuerdo del Senado. A mi parecer, el Ejecutivo debería escoger de una lista propuesta y consensuada por el Senado, lográndose equilibrio en el reparto del poder, lo cual debería ser retomado para elegir al director del órgano rector en el caso de Nicaragua. Aparte de las mismas facultades antes mencionadas, puede constituirse como querellante en las acciones penales que se promovieren por la violación a la presente ley, dada la naturaleza de órgano adscrito al Poder Judicial. Puede solicitar información a los responsables de los ficheros, pero no prevee, a diferencia de Nicaragua, la realización de inspecciones sobre los medios técnicos de tratamiento de datos o el inmueble en que se lleva a cabo.

Ambos están facultados a imponer sanciones administrativas en caso de incumplimiento de la presente ley, pero lo novedoso de la legislación argentina es que prevee la adición, en el Código Penal, de tipos penales que reprimen la inserción de datos falsos, por proporcionar información falsa a quien viole las medidas de seguridad y confidencialidad logrando acceder a ficheros de datos, la revelación de información y, como agravante, el hecho que el autor sea funcionario publico, inhabilitándolo de su cargo (Cfr. Artículo 29-32 Ley 25326 de Protección de Datos Personales de Argentina). Este último tipo penal sería por el cual debieron haber juzgar a los responsables de la Empresa Infornet, puesto que trabajaban a partir de bases de datos propiedad del Consejo Supremo Electoral, por lo que propongo que se adicionen nuevos tipos penales que sancionen el fraude en la obtención, finalidad y manejo de los datos personales que son una extensión de la identidad humana, amparados bajo la propia intimidad.

6. Acción de protección de datos personales o habeas data

Ante tales situaciones de indefensión enunciadas anteriormente, el Anteproyecto de Ley de Protección de Datos de Nicaragua, legitima al ciudadano afectado permitiéndole ejercer la acción de Protección de datos personales, o *habeas data*, que protege contra la vulneración de los secretos informáticos y los atentados contra la intimidad personal. Más técnicamente, para nosotros, la acción de *habeas data* es el derecho que asiste a toda persona, identificada o identificable, sobre la base de los supuestos siguientes:

1. En caso de negarse el responsable del fichero a revelar la información solicitada por el ciudadano, éste está legitimado a interponer la acción dirigida a la exhibición de los registros, públicos o privados, en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud.
2 De oponerse el titular del fichero a suprimir, rectificar o actualizar los datos personales, la acción va encaminada a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación, por ejemplo, afiliación a partido político, creencia religiosa, etcétera.
3. Cuando el responsable del fichero de datos se niegue a proveer al ciudadano el derecho de oponerse a figurar en ficheros de datos, aun cuando los datos hayan sido recabados de fuentes accesibles al público.

Naturaleza jurídica

1) Es una garantía
El *habeas data* es una garantía de tercera generación, un instrumento procesal para la protección de determinados derechos humanos.

2) Es una acción
A su vez es, de principio y sin perjuicio de alguna posibilidad diversa que dependerá de la casuística y del derecho positivo, una acción, porque no es un medio impugnativo o incidente dentro de un proceso determinado.

Una similitud fundamental radica en que, en ambos institutos, los recursos y las acciones proceden de acuerdo al reconocimiento expreso en la legislación pertinente. De no existir tal, la garantía genérica de los derechos humanos es la acción de amparo. Así es como hasta ahora se han venido tramitando las violaciones al Artículo 26 inciso 4) de la Constitución Política[6] en Nicaragua, por la falta de promulgación del Anteproyecto de Ley de Protección de Datos Personales.

Objeto

Permite:
- Que un individuo pueda acceder a la información que sobre él exista en un banco de datos.
- Que el sujeto, legitimado activo, exija que se actualicen esos datos.
- Que se rectifique los que son inexactos.
- Que se asegure la confidencialidad y no divulgación de cierta información evitando su conocimiento por terceros.
- Exigir la supresión de la información sensible que exista sobre sí en los bancos de datos de que se trate, y que se le indemnice por los daños causados.

Diferencias con el *habeas* corpus

Las diferencias fundamentales respecto del habeas corpus son las siguientes:
1) El *habeas corpus* es una garantía respecto de la libertad física, en sentido amplio, inclusivo, de las condiciones de detención. *El habeas data* protege el derecho de intimidad, privacidad, honor y verdad del hombre, así como le exhibición, no de la persona como en el caso del *habeas corpus*, sino de los datos personales.
2) Generalmente, la legitimación activa en el supuesto del *habeas data* requiere, y con posibles excepciones de acuerdo a esa situación jurídica subjetiva, un interés legítimo y personalísimo. Sin embargo, en general y con algunas excepciones (por ej. ley española), la legitimación activa en el supuesto de *habeas corpus* es universal.

Diferencias con el recurso de amparo

La diferencia principal entre ambos institutos surge del objeto específico de protección de cada una de las garantías. El amparo protege todas las garantías constitucionales, mientras

que el *habeas data* se presenta como la instrumentalización de la protección al derecho a la intimidad, la protección de datos y la libertad informática.

Por otra parte, debe recordarse que el amparo es la garantía de principio. Por ello, las normas que regulan esta acción siempre serán, en mayor o menor medida y en lo pertinente, aplicables al proceso de *habeas data*.

1. El amparo se dirige para restituir una garantía constitucional ya violentada y su efecto es suspender los actos u omisiones de funcionarios públicos en ejercicio de sus funciones.
2. El *habeas data*, a diferencia del amparo, se dirige en contra de funcionarios públicos o particulares que posean bases de datos personales y que se nieguen a revelar la información que solicita el ciudadano o a rectificar sus datos, evitando que se violente un derecho, de tal manera que su efecto va encaminado a proveer lo solicitado.

Al respecto cito la jurisprudencia de los tribunales argentinos[7] en los cuales se deja de manifiesto que para la procedencia del habeas data no es necesaria la lesión actual e irreversible de los derechos.

Órgano Jurisdiccional Competente: forma de Resolución y Efectos

En este marco jurídico, y para hacer efectivos los derechos de información, acceso, actualización, rectificación, confidencialidad, oposición y cancelación de datos personales, se plantea la actuación del Estado en dos etapas: la administrativa y la judicial.

En la vía administrativa, el titular del derecho o su representante con poder notarial, el Fiscal o la Defensa Pública, peticionarán ante el responsable o encargado de los ficheros públicos o privados, un informe para saber si sus datos personales figuran en algún fichero de su propiedad y de qué datos se tratan. La autoridad o representante legal deberá revolver la solicitud en el plazo de diez días hábiles de la recepción del reclamo, la que hará conocer al interesado en forma escrita.

Una vez que el ciudadano sepa cuáles datos suyos figuran en el fichero de datos público o privado, sabrá si estos datos son erróneos o no están acordes con la realidad. De ser así, el ciudadano puede solicitar su actualización, supresión o corrección, a realizarse dentro del plazo de cinco días de recibida la solicitud. En caso de desestimación o negativa en alguno de los supuestos arriba mencionados se legitima al afectado a recurrir ante la autoridad judicial competente.

Por su parte, la vía judicial se activa, no a partir del previo agotamiento de la esfera administrativa, sino en situaciones en que se nieguen los derechos de información, acceso, actualización, rectificación, confidencialidad, oposición y cancelación de datos, por parte de los responsables o encargados de los ficheros. Sin embargo, es criterio jurisprudencial hasta ahora de la Corte Suprema de Justicia, cuando se interpone Recurso de Amparo en contra de la Administración pública y sus funcionarios por violación del derecho a la intimidad, que es como hasta ahora se ha venido tramitando lo que debería ser la acción de protección de datos o *habeas data*: mandar al interesado a agotar la vía administrativa dispuesta en cada ente público.

En la vía judicial, la acción del *habeas data* se interpondrá con motivación razonada por el titular del derecho o su representante. No se habla de si pueden accionar el Fiscal o la Defensa Pública. A mi criterio creo que debería habilitárseles a accionar. No se menciona la materia del Juez Competente en el Anteproyecto Nacional, pero a través de entrevista en la Sala Constitucional de la Corte Suprema de Justicia se deduce, y coincido en el criterio, la analogía con el trámite del Recurso de Amparo que se admite en la Sala Civil del Tribunal de Apelaciones. En consecuencia, la admisión y trámite de la acción de protección de datos deberá hacerse ante el Juez Civil de Distrito del domicilio del actor, el del demandado, del lugar en que el hecho o acto se exteriorice o pudiera tener efecto a elección del actor.

En lo que respecta al cuerpo de la demanda ésta deberá expresar (Cfr. Artículo 37 incisos del a) al j) Anteproyecto de Ley de Protección de Datos Personales de Nicaragua):

1. Mención del Juzgado ante el que se promueve.
2. El nombre del actor y del demandado.
3. Objeto de la Acción.
4. Con la mayor precisión posible, el nombre y domicilio del archivo, registro o base de datos y, en su caso, el nombre y responsable del mismo.
5. En el caso de bases de datos públicos se procurará establecer la institución estatal de la cual dependen.
6. Los hechos en que el actor funda su petición, narrando sucintamente los motivos en que apoya su acción y considera que los registros o bases de datos son omisos o incompletos, falsos o inexactos, o por los cuales considera que los datos deben reservarse, suspenderse o cancelarse y destruirse.
7. Existe la posibilidad de solicitar que se asiente, mientras dure el proceso en que la información cuestionada se encuentra sujeta a un proceso judicial.
8. El fundamento de derecho.
9. Lo que se pida designándolo con toda exactitud, por mi parte agrego que debería establecerse la posibilidad de solicitar una indemnización en caso de causarse daños al actor, puesto que se reforzaría la protección al derecho.

Con la demanda, el actor debe presentar los documentos en que funde su acción o señalar el archivo. Si no los tiene a su disposición, con dicha designación el Juez mandará expedir, a costa del actor, copia de los documentos correspondientes. Considero que esto constituiría ser un impedimento para intentar la acción, puesto que la acción se intenta ante la negativa injustificada y perjudicial del responsable del registro de expedir informe sobre los datos personales. Es gravoso fijar una costa para el actor cuando éste quiera probar su derecho, además de ser contradictorio, porque en el texto legal se fija la obligación del titular del fichero a brindar el acceso a los registros en el momento que el afectado tenga que ejercer su derecho de defensa (Cfr. Artículo 18 inciso b) Op. Cit.).

El juez está facultado para disponer de oficio, por causa fundada y motivada, la suspensión o reserva de los datos personales. A mi parecer deben fijarse parámetros para proceder conforme a ellos sin provocar perjuicio a ninguna de las partes. Además, en todo momento, y antes de dictar sentencia, se puede recabar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte

conducente a la resolución de la causa (Cfr. Artículo 40 Op. Cit.). Admitida la demanda se da traslado al demandado para que conteste dentro de los tres días siguientes. Las cuestiones de competencia, jurisdicción y personalidad deberán promoverse en la contestación de la demanda y se resolverán en el auto que se provea sobre ellas. En este tipo de procesos, no procede la contrademanda ni la ampliación de la contestación. Contestada la demanda, de oficio el juez abrirá el proceso a pruebas por un plazo único e improrrogable de seis días comunes a las partes. Vencido el plazo de pruebas se dictara sentencia dentro de los tres días siguientes. La sentencia a saber puede dictarse en varios sentidos, procedencia estimatoria o improcedencia desestimatoria:

1. Resolviendo como fundada la acción, el juez mandará al responsable de los ficheros a rendir informe sobre sus datos personales al ciudadano titular o si se trata de la acción de corrección, cancelación o actualización de datos, el juez determinará los datos que deben ser incluidos, complementados, actualizados, reservados, suspendidos o cancelados y destruidos, estableciendo un plazo no superior de quince días para su cumplimiento y acreditación y, en su caso, la forma de hacerlo.

   Aquí mismo es en donde el juez procedería a fijar los daños y perjuicios, si es que hubiere motivos justificados para ello. En caso de no ser posible la calificación en la misma audiencia, se tramitarán los daños por separado, abriendo un plazo probatorio de cinco días comunes a las partes. El monto que se fije será ejecutado inmediatamente por el obligado.
2. Improcedencia de la acción. No se presume responsabilidad alguna en la cual pueda incurrir el demandante.

Si se presenta este supuesto, es obvio que se vulneraría el derecho del interesado puesto que en el Anteproyecto de Ley de Protección de Datos Personales no se fija un ulterior proceso de revisión. Por lo tanto, propongo y coincido con lo expresado, en la sala Constitucional de la Corte Suprema de Justicia, que debería proveerse un procedimiento de revisión posterior de Apelación.

El juez elevará la sentencia de improcedencia ante el Tribunal de Apelaciones en grado de revisión. El Tribunal admitirá la misma en el plazo de cinco días y pronunciará sentencia en el plazo de treinta días, sin perjuicio de solicitar a las partes cuanta prueba sea necesaria para formar convicción. La sentencia que dicte el Tribunal podrá ser estimatoria cuando esté conforme con la interpretación del inferior y revocatoria en caso contrario (Gareca Perales, 2004:97).

En el desarrollo del proceso por su naturaleza expedita de 3-6-3 no se aceptarán cuestiones previas o prejudiciales u otras que tiendan a retardar la decisión. Se aplicarán las disposiciones comunes del Código de Procedimiento Civil.

7. Casuística

En Nicaragua se duda de su existencia como un recurso autónomo a partir de la falta de instrumentalización de un proceso independiente. Existen casos en que la intimidad de las personas se ha visto amenazada por la tenencia de terceros, de datos acerca de sus vidas

privadas, como ejemplo cito la denuncia ante el Centro Nicaragüense de Derechos Humanos (CENIDH) solicitando la realización de gestiones de protección y prevención frente a amenazas, interpuesta por Mirna Velásquez, redactora del Diario LA PRENSA, quien dijo sentirse intimidada, coaccionada, vigilada y violentada en su privacidad, seguridad e integridad por el Juez Suplente del Juzgado Quinto del Distrito del Crimen Carlos Mario Peña, al poseer este último, datos minuciosos sobre la vida privada de la denunciante e imputar injuriosas acusaciones sobre la base de informaciones personales obtenidas ilícitamente: *"el Juez Peña le dijo* (a Velásquez) *que tiene correos electrónicos de una persona que le informa sobre su vida y que se los daría según el contenido de las noticias que sobre él siga publicando* [8] *.... Además de darle detalles de su vida privada con tal certeza que la hacen sospechar que lleva a cabo una investigación sobre ella al margen de la ley".* Velásquez interpuso, además, Recurso de Exhibición Personal para protegerse contra cualquier intento de arresto, así como una queja en la Comisión de Régimen Disciplinario de la Corte Suprema de Justicia, reservándose la presentación de una acusación por los delitos de injurias y abuso de autoridad.

Esta situación se originaó a partir de una serie de artículos publicados en el diario La Prensa redactados por Mirna Velásquez, en que se develan procesos criminales abiertos en contra del juez suplente Carlos Mario Peña al momento de su nombramiento, por tráfico ilegal de inmigrantes (Artículo del diario La Prensa del domingo 22 de agosto de 2004, edición No. 23549, sección Nacionales, página 4).

En este caso cabría la presentación de un recurso de *habeas data* por tratarse de la tenencia ilícita de datos personales que deriva en la comisión de los delitos de amenazas, extorsión, chantaje, injurias, calumnias etc., que dañan la intimidad, el derecho al honor y otros atributos más de la identidad del ciudadano. Exigiría que se acceda a la información que se tiene del afectado, a pesar de ser un juez quien posee la información, a la periodista no se le ha abierto causa alguna que fundamente la posesión de información por parte del juez Peña. Cito como fundamento, el hecho que no es necesario que se trate de un fichero o una persona o ente dedicado a brindar informes para enderezar contra este una Acción de Protección de Datos Personales o Habeas Data según lo que consta en la Jurisprudencia Argentina:

> *La garantía del hábeas data alcanza aún aquellos supuestos en los que no interviene una entidad destinada estrictamente a proveer informes («Halabi, Ernesto c/ Citibank N.A.». C.N.Com., Sala C, 26/03/02. JA, 2002-III-18. ED, 197-327).*

En lo que respecta al abordaje más amplio de la posibilidad de solicitar indemnización por daños junto con la presentación del *habeas data*, o demandar por separado daños y perjuicios, teniendo como referente causante la no corrección de datos personales erróneos, el pronunciamiento argentino es que se da a lugar tal petición, pues, en el caso citado se trata de una información errónea, una negativa injustificada del responsable del fichero de datos y que además produce daños morales al demandante de la acción de protección de datos personales. Véase al respecto lo proveído por los tribunales argentinos en demandas contra los responsables de ficheros con fines de brindar informes sobre solvencia económica:

La existencia y publicidad de datos desactualizados y erróneos relacionados con el actor deben haber repercutido en su espíritu, sentimientos o afecciones más íntimas, ya que implicaron un ataque a su honor, a su imagen y reputación; máxime si se tiene en cuenta la extensa labor profesional y académica del actor. Tales circunstancias, justifican sin hesitación la procedencia del daño moral. («Ravina, Arturo Octavio c/ Organización Veraz S.A.». CNCiv., Sala F, 06/02/02 - ED, 197-265).

Corresponde admitir la indemnización por daño moral solicitada por los gerentes de una empresa contra la entidad bancaria con la que ésta operaba, por cierre de una cuenta corriente que provocó que el Banco Central dispusiera la inclusión de sus datos -tanto de la empresa como de los gerentes- en un boletín periódico de personas inhabilitadas para operar como cuentacorrentistas dirigido a bancos. («Coccia, Carlos Antonio c/ Veritas DGC Land Inc. Sucursal y otro s/ Daños y Perjuicios» - CNCiv., Sala C - 26-09-00. Revista El Derecho, 16/03/ 2001).

Un dato falso o inexacto registrado en el Banco de Datos «Organización Veraz S.A.» con respecto al actor y como consecuencia de una errónea información suministrada por el B.C.R.A. por el Banco codemandado pudo y debió causar al actor una profunda lesión en su persona porque toca a su prestigio profesional y a su innegable derecho a requerir la protección de su intimidad (arts. 19, Constitución Nacional y 1.071 bis, Código Civil en su redacción posterior a la ley 17.711) («Gutiérrez, Vicente Juan Carlos Demetrio c/ Banco de la Provincia de Buenos Aires y otro». CNCiv., Sala K, 22/10/02).

Con relación al agravio esta última, diré que la apelante parece olvidar tener en cuenta que el daño moral no requiere prueba específica alguna, en cuanto ha de tenérselo por demostrado por el solo hecho de la acción antijurídica - prueba in re ipsa-, que, en el caso, consistió en colocar al actor públicamente en condición de deudor irrecuperable (grado 5). Es claro que la publicación de aquellos datos erróneos -atribuibles a la demandada- y, además, por tan prolongado tiempo tienen que haber repercutido en el espíritu y en los sentimientos o afecciones más íntimas del actor ya que implicaron un ataque a su honor, a su imagen y reputación. («Fallone, Eugenio Donato c/ HSBC Banco Roberts S.A. s/ daños y perjuicios». CNCivil, Sala F, 06/11/03. Expte. N° 368.998).

8. Conclusiones

Es obvio que la informática y sus avances como el Internet, videoconferencias, comunicaciones satelitales, sistemas de posicionamiento global, rastreo de datos, *sniffers*, troyanos y demás, han hecho posible la recopilación de información de las personas, pero que se corresponde con otros intereses, no el de proteger a las personas sino comercializar lo que se sabe de ellas. No es malo que circulen los datos, pero que eso se convierta en factor de discriminación a las personas al antojo de quienes poseen la información sobre los demás, sí es repudiable.

Esta facilidad de compilación de datos se deriva de la deshumanización y reducción de las personas, sus identidades e intimidades, a números, códigos de barras, claves de acceso, por lo que es fácil saber sobre ellos y controlar lo que hacen, transferir sus datos y contrastarlos entre sí para crear un perfil de la persona y llegar a saber más de lo que el propio ciudadano conoce de sí mismo.

El problema con la informática no es que convierta las tareas más difíciles en accesibles y realizables, como analizar grandes cantidades de información en busca de patrones, proporcionar facilidades para un comercio igualitario, accesible a todos a nivel mundial y a precios menores, sino el usar la informática como un instrumento de agresiones más depuradas y olvidar que se trata de personas; separarles el componente de humanidad con sus complejidades para reducirlos a números. Ello no debe significar la desaparición del sujeto. Al contrario, esos números y los datos, que se deriven de las actividades diarias son una extensión e interpretación de la personalidad de los sujetos en un mundo digital y virtual.

Ahora se configuran mayores vejaciones al derecho a la intimidad, privacidad, imagen y honor de las personas. Ya no sólo se trata de evitar que los demás se enteren de facetas propias pertenecientes a nuestra esfera más personal, sino que estamos ante nuevos ataques y la configuración de nuevas protecciones jurídicas encaminadas a conferir la facultad y el derecho de controlar la información que sobre las personas circula, a saber quién la posee y con qué finalidad, a oponerse al uso de dichos datos, que se corrijan o cancelen los que no se corresponden con la verdadera situación de las personas y demás facultades abarcadas dentro del derecho a la protección de datos personales explicado en este humilde esbozo.

Con el auge de valorar monetariamente cada bien que constituye la esfera de desenvolvimiento del sujeto, con el fin de protegerlo, venderle más y mejores productos, prolifera un nuevo mercado: el de los datos personales, porque para las empresas y proveedores de servicios es necesario saber más de las personas que serán futuros clientes. Pero es necesario un saber con límites en la dignidad de la persona, no hacerle daño ni cometer infracciones en su honor e imagen.

Es evidente que ya no se violenta solamente la intimidad a los ciudadanos, porque ésta se basa en conocimientos que sobre sí mismo posee y controla -para decidir si los revela o no a la sociedad, siendo consciente que estos datos condicionarán o no su interacción social libre-, sino que se trata del hecho que ahora el ciudadano desconoce información sobre sí mismo y por lo tanto no puede controlarla y muchas veces es producto de los avances tecnológicos. Estos datos, al encontrarse en posesión de desconocidos, que en la mayoría de los casos no cuentan con el consentimiento del afectado, son utilizados a su antojo.

Sin embargo, no todo el panorama es un sombrío túnel. Existe la configuración del derecho a la protección de datos personales, que ha instrumentalizado y configurado un equilibrio a favor del ciudadano frente a los propietarios de los ficheros de datos. Existe una nueva configuración procesal en la acción de protección de datos personales, o *habeas data*, que protege más efectivamente el ejercicio de los derechos. Es así que propugno, a partir de lo antes expuesto, por la aprobación, mejoras y reglamentación del Anteproyecto de Protección

de Datos Personales Nicaragüense. Cada día que pasa sin aprobarse, son mayores las transgresiones a los derechos de las personas, las cuales son permitidas por vacíos regulatorios y falta de sensibilización al respecto sobre el tema.

No obstante es válido mencionar que Nicaragua es miembro de la Red Iberoamericana de Protección de Datos Personales. Se trata de un foro cuyo fin es potenciar las iniciativas de intercambio de experiencias y promover las soluciones armonizadas. Se ha constituido a partir de la Agencia Española de Protección de Datos en cumplimiento de su objetivo prioritario de cooperación mutua y colaboración con los responsables de protección de datos de los diferentes Estados de la región. Con este precedente nace la Red Iberoamericana de Protección de Datos Personales, que promueve reuniones anuales. La primera de ellas fue en Antigua, Guatemala, en el año 2003. Entre sus sus conclusiones cabe exponer:

> *... la consideración de la protección de datos personales como un auténtico derecho fundamental de las personas, sobre todo en orden al respeto a su intimidad y de su facultad de control y disposición sobre los mismos.*
>
> *El derecho a la protección de datos personales fortalece el Estado de Derecho y ayuda a reforzar la democracia en los países iberoamericanos, así como su prestigio y credibilidad en un mundo globalizado.*

Notas

1 La intimidad y el honor ya están regulados. Se habla de limitar el uso de la informática. Es, sin duda, un nuevo concepto (....) una nueva dimensión que corresponde a unos nuevos medios tecnológicos y un nivel de desarrollo que con el paso de los años empiezan a demostrar su verdadera dimensión, también su peligro auténtico (...) el uso frecuente de medios informáticos amenaza con hacer que el perfil de cada cual pueda ser reconocido por cualquier persona, en cualquier sitio y en cualquier momento, afectando por eso una dimensión nueva (Cfr. Intervención del Ministro de Justicia Español ante el Congreso de Diputados, Diario de Sesiones del Congreso de los Diputados número 151. IV Legislatura. Año 1991. r. 7572).

2 Artículo 2 Ámbito de Aplicación, Anteproyecto de Ley de Protección de Datos Personales y Artículo 1 de la Ley 25.236 de Protección de Datos Personales de Argentina.

3 Artículo 6 inciso b) numeral 1-5, Anteproyecto de Ley de Protección de Datos Personales de Nicaragua y Artículo 5 inciso 2) numeral a-b Ley 25.326 de Protección de Datos Personales de Argentina.

4 Amplios sectores doctrinarios coinciden en designar como fuentes accesibles al público aquéllas en que se dispongan datos al público en general, no impedida por cualquier norma limitativa y que estén recogidas en medios tales como censos, anuarios, repertorios de jurisprudencia, boletines oficiales, diarios, archivos de prensa, guías telefónicas, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados profesionales, dirección e indicación de su pertenencia al grupo. Cfr. A. Téllez Aguilera, Nuevas Tecnologías, Intimidad y Protección de Datos, 121-122.

5 Es una empresa privada que ganó, por medio de licitación pública, la concesión para editar una guía telefónica con el repertorio de los abonados al servicio de telefonía pública, facultad perteneciente anteriormente a TELCOR.

6 Es de notar que en la reforma, de 1995, a la Constitución Política Nicaragüense se agregó, al Artículo 26, el inciso 4) a la redacción de este precepto constitucional. Y es a partir de ahí donde se encuentra de forma implícita la protección de los datos personales de los ciudadanos nicaragüenses, asimismo plantea un limite legal a la Administración Pública, en cuanto ésta se encuentra en el deber de informar, a petición del ciudadano, qué datos personales tiene registrados, el porqué y la finalidad de ello. Este precepto tiene como circunstancia motivadora las facultades de investigar a las personas por parte de la Fiscalia General de la República, pues era necesario dotar de un instrumento equilibrante y una facultad legitimadota, para evitar investigaciones, para reprimir delitos y recoger elementos incriminatorios sin fundamento en la ley y límite de tiempo.

7 Para la procedencia del habeas data no se requiere, en principio, arbitrariedad o ilegalidad manifiesta dado que procede ante la mera falsedad en el contenido de los datos o la discriminación que de ellos pudiere resultar. Y aun sólo para conocer dichos datos, sin que sea necesario que ellos vulneren inmediatamente derechos o garantías constitucionales (CNCont. Adm. Fed., Sala IV, "Gaziglia, Carlos Raimundo y otro c/ B.C.R.A. y otro s/ Amparo Ley 16.986". 04-10-1995).

8 Una diferencia importante entre la lesión del derecho al honor (que da facultad para iniciar un proceso criminal por injurias y calumnias) y la lesión de la intimidad (que sustenta la interposición de un recurso de habeas data para restituir la esfera de la intimidad, resultado de una intromisión ilegitima) es la falsedad o veracidad de la información. Si los hechos son falsos se habrá atacado al honor. Si los hechos son reales, la intromisión se habrá hecho en la intimidad de la persona. Así, en la Sentencia 197/91 (caso Sara Montiel) se dice: "El requisito de veracidad merece distinto tratamiento según se trate del derecho al honor o del derecho a la intimidad, ya que mientras que la veracidad funciona, en principio, como causa legitimadora de las intromisiones en el en el honor, si se trata del derecho a la intimidad esa veracidad es presupuesto necesario para que la intromisión se produzca, dado que la realidad de éste requiere que sean veraces los hechos de la vida privada que se divulgan" Cfr. M.L Fernández Esteban, Nuevas Tecnologías, Internet y Derechos Fundamentales, 118.

Referencias bibliográficas

-ASAMBLEA NACIONAL DE NICARAGUA, Constitución Política de la República de Nicaragua, 2000.

-ASAMBLEA NACIONAL DE NICARAGUA, Ley 350 de Regulación de la Jurisdicción de lo Contencioso Administrativo publicado en la Gaceta No. 140 y 141 del 25 y 26 de julio del 2000 respectivamente

-CONGRESO NACIONAL DE DIPUTADOS DE LA REPÚBLICA DE ARGENTINA, Ley 25.236 de Protección de Datos Personales de Argentina promulgada el 30 de octubre del 2000.

-DAVARA RODRÍGUEZ, M. A. (2003) *Manual de Derecho Informático*. Madrid, Editorial Thomson-Civitas 5ta edición.

-EGUSQUIZA BALMACEDA, M.A (2002). *"Intimidad del Consumidor y Protección de Datos"* en Internet y Comercio Electrónico I y II Jornada sobre Derecho e Informática, Ediciones Universidad de Salamanca, España.

-ESCOBAR FORNOS, I. (1999). *Derecho Procesal Constitucional. La Constitución y su Defensa*. Managua, Hispamer.

-GARECA, PERALES, P (2004). *El Habeas Data en la Constitución de Bolivia*, Bolivia.

-MEJAN, L. M. (1994) *El Derecho a la Intimidad y la informática*. México, Editorial Porrúa.

-MURILLO DE LA CUEVA, P. L. (1990), *El Derecho a la Autodeterminación Informativa: la Protección de los Datos personales frente al uso de la Informática*. Madrid, Editorial Tecnos.

-MURILLO DE LA CUEVA, P.L. (1993). *"Informática y Protección de Datos Personales. Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal.*Madrid, Centro de Estudios Constitucionales.

-PRESIDENCIA DE ARGENTINA, Decreto 1558/2001 Reglamento a la Ley 25.326. promulgada el 29 de Noviembre del 2001.

-SÁNCHEZ BRAVO, A. A. (1998). *La Protección del Derecho a la Informática en la Unión Europea*. Sevilla, Universidad de Sevilla, Secretariado de Publicaciones.

-TÉLLEZ AGUILERA, A. (2001). *Nuevas Tecnologías. Intimidad y Protección de Datos. Estudio Sistemático de la Ley Orgánica 15/1999*. Madrid, Editorial EDISOFER S.L.

-VICEPRESIDENCIA DE LA REPÚBLICA DE NICARAGUA, Secretaria Ejecutiva del Consejo Nacional de Ciencia y Tecnología (CONYCIT) Anteproyecto de Ley de Protección de Datos Personales, Julio del 2004.