

## **La protección de datos personales y el Internet Cifuentes (h.), Santos E.**

**SUMARIO: I. La ley 25.326 de protección de datos personales. — II. El habeas data. — III. El Internet.**

### I. La ley 25.326 de protección de datos personales

La protección de datos personales fue tarea del legislador que comenzó en 1970 en el ámbito europeo, cuando la evolución de la informática se expandió en la sociedad, con la elaboración de ficheros que podían amenazar la intimidad de las personas. La primera legislación fue la de Alemania en el Bundesland de Hesse, para la defensa de la intimidad frente al Estado. En 1973 Suecia dictó la primera ley nacional "Data Act", para proteger a las personas ante el almacenamiento de datos que usaba el Estado para control, vigilancia y prevención del delito. La ley federal alemana es de 1977.

Sin embargo, en España la primera creación provino del Tribunal Constitucional que, adelantándose al Parlamento y como derecho no expresamente reconocido en la Constitución, acogió la existencia de la garantía instrumental de la "autodeterminación informativa", para la tutela de la intimidad y el honor frente al uso de la informática (1). Este país y otros recibieron una carta de emplazamiento de la Comisión Europea, por no adoptar todas las medidas necesarias para adecuar su legislación sancionada en 1992, a la Directiva europea 95/46. Esta Directiva prohíbe la transferencia internacional de datos entre las naciones de la Comunidad Europea, y esa restricción fue extendida a otros países no europeos que no tengan nivel de protección adecuada. La Argentina quedó emplazada el 25 de octubre de 1998.

Nuestra ley del año 2000 tiene por objeto, según enuncia su art. 1º: "...la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el art. 43, párrafo tercero de la Constitución Nacional.

Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas".

El Decreto reglamentario n° 1558 del 29 de noviembre de 2001, delimitó el concepto del receptor de datos, en los siguientes términos: "A los efectos de esta reglamentación, quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito".

Se considera que son Bancos públicos los que operan en la organización estatal, y, según el texto transcripto, no se impone el requisito de que estén destinados a proveer informes. Luego, abarca la protección de la ley a los datos en una serie de archivos, registros y bancos de datos con informaciones sobre personas tengan o no ese destino. Se ha pensado inclusive, atendiendo a las funciones que desempeñan, que se deben considerar bancos públicos a ciertos organismos no estatales como los colegios profesionales y las obras sociales (2).

Los bancos privados deben estar destinados a "proveer informes" sean onerosos o gratuitos, por lo que solo quedan excluidos de la protección legal los que no tengan organización y funcionamiento para difundir o hacer conocer los datos que registran. Aunque, como bien se ha señalado, a través de la informática los exclusivamente personales, pueden transformarse en pocos segundos por simple conexión on line, en archivos que proveen informes. A partir de esa circunstancia quedan abarcados por las normas de la ley, empero los remedios pueden ser tardíos. En el concepto de "proveer informes", se incluye a las cesiones y transferencias de datos que es una forma de traspaso por comunicaciones.

He sostenido que la base de datos personales importa un derecho personalísimo nuevo e independiente, que deriva del valor dignidad de la persona, como derecho constitucional no enunciado (art. 33 de la Const. Nacional). La privacidad no es el único aspecto de la protección frente a la acción informática,

sino que hay que tener en cuenta también la identidad cuando, verbi gracia, se falsean o alteran los datos provistos con mentiras o errores que se deben corregir. También es posible con la informática lesionar la imagen de la persona en cuanto tal. La base de datos puede implicar no sólo referirse a un aspecto de la persona sino a su personalidad como un todo, íntegra, virtual. Basta el entrecruzamiento de datos para construir lo que la persona es, accediendo a sus negocios, familia, salud, proyecciones individuales y sociales, etc. De ahí que pueda sostenerse la existencia de una nueva figura jurídica que puede encontrar su protección a través del hábeas data, o de otras medidas protectoras y precautorias judiciales que no deben retacearse a la hora de tutelar la intimidad, la imagen, la identidad o el honor (3).

La ley ha definido los datos personales como toda "Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables" (art. 2º). Pero además ha reconocido la existencia de datos llamados "sensibles", que son los que "revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual". Ha sido criticada esta norma porque intenta definir por medio de supuestos y no de conceptos (4). Por lo mismo la enunciación es incompleta, dado que lo que realmente tiene interés, es que tales datos estén por su propia esencia vinculados a la intimidad. En definitiva no hay un concepto legal de "datos sensibles", aunque se previene que sólo pueden ser recolectados cuando medien razones de interés general autorizados por ley. De ahí algunas vacilaciones y elaboraciones complejas de la jurisprudencia y la doctrina.

En el art. 5º se estatuye que el tratamiento de datos es ilícito cuando el titular no ha prestado consentimiento valedero por escrito o por medio similar o que se le equipare.

Un caso que se ha discutido, dentro del orden político, es si la afiliación partidaria es un dato protegido. Esta cuestión había sido plenamente discutida ante el decreto 1397/2002 (Adla, LXII-D, 4072), que disponía que el padrón provisorio a utilizar en las elecciones abiertas se publicaría (art.3º) y la CNac. Electoral dispuso la publicación de las listas respectivas, y ordenó la instalación de esas bases de datos en un sitio de Internet (5). Esta cuestión reapareció en 2005 con el decreto 2923/2005, y el tribunal sostuvo que no puede equipararse al conocimiento de las opiniones políticas de los interesados. Descartó que tal afiliación fuera un "dato sensible" como lo son dichas opiniones políticas, agregando que la misma ley en su art. 27 establece el carácter público de los registros partidarios (6). De ahí que nada impediría la publicidad de esos registros. Si la persona es famosa y de alto nivel de exposición, a lo que se suma la trascendencia social de los hechos, parece poco admisible sostener que los datos correspondientes fueran sensibles y que se deban mantener en secreto. Sin embargo, ha dicho Gozaíni, se debe distinguir el secreto de la reserva y confidencialidad, ya que no todo secreto es íntimo y si no lo fuera de todas maneras está protegido, en tanto son inviolables la correspondencia, los papeles privados (art. 18 de la Constitución), quedando incluidas, como ya se ha visto, las comunicaciones por teléfono y por ello las interceptaciones telefónicas y de los despachos telegráficos son también ilegítimos. El autor mencionado ha dicho que la presencia informática en la vida de las personas es cotidiana y el hombre encuentra que su vida está archivada (desde el nacimiento y primeros pasos por el mundo) prolijamente en un banco de información. Otros autores, como Puccinelli, estiman que esa publicación de los padrones es inconstitucional, pues si bien como había opinado Bidart Campos no es auspiciosa la cultura del ocultamiento y debe cultivarse una política madura (7), muchas veces quien decide afiliarse a un partido no lo hace voluntariamente ni porque tenga intenciones de participar en la política y en el gobierno del partido, sobre todo en nuestros países y especialmente en las provincias, en las que esa afiliación se erige como una exigencia para obtener ciertos bienes. Porque tampoco es dable confundir afiliación con militancia, ni tal afiliación se hace para ponerla en conocimiento general. Por lo demás la "ficha" que debe llenarse para la afiliación, contiene una serie de datos que entran en aspectos de reserva, para los que no se daría consentimiento expreso a la luz de la ley 25.326. Luego, en realidad, sólo deberían poder acceder a esos datos los legalmente interesados y no, a través del Internet, el público en general. También se dice que no es condición el carácter íntimo para considerar que un dato es o no sensible, pues bastaría que ese dato pueda producir discriminación aunque no fuere íntimo. Además, si el individuo pertenece a un partido político ello revela directa o indirectamente cuál es su opinión política, tal como surge del art. 2 de la ley de datos personales.

La ley de datos personales ha creado tipos penales incorporando los arts. 117bis y 157 bis al Código

Penal, de tal manera establece penas de prisión y según el caso de inhabilitación para la persona que insertara a sabiendas datos falsos en un archivo, proporcionara información falsa, o ilegítimamente o violando sistemas de la confidencialidad, accediere a un banco de datos personales o revelare secretos que debiera guardar. En tal supuesto, por ejemplo, está el secreto fiscal, establecido en el art. 101 de la ley 11.683 (t.o. 1998) (Adla, LVIII-C, 2969) para las declaraciones juradas, manifestaciones e informes a la Administración Federal de Ingresos Públicos (AFIP), cuya divulgación por parte de terceros importa la comisión del delito que regla el art. 157 del citado Código.

Hay desde ya excepciones a este secreto que sólo nacen especialmente de las normas aplicables, ya que no es exigible el consentimiento del titular cuando los datos se recaben en el ejercicio de funciones del Estado o por una obligación legal. Una aplicación de estas excepciones es la expuesta de la AFIP, a efectos de obtener datos para fiscalizar el cumplimiento de las leyes tributarias (art. 35 de la ley 11.683), organismo exento del recaudo del consentimiento para brindar información a la Secretaría pertinente. O sea que los datos propios y de terceros que surgen de las declaraciones juradas impositivas, es decir, entre otros, las actividades, los ingresos, bienes que le pertenecen y su valuación, familiares a cargo, etc. deben ser confiados al organismo recaudador que, a la vez debe prestar la información de esos datos cuando le sea requerida, tal como regula el art. 14 de la ley de datos personales. En caso de denegatoria puede reclamar por medio de la acción de hábeas data, así como exigir su rectificación si son erróneos, la supresión si no corresponde registrarlos o la actualización cuando han perdido actualidad (8).

Las combinaciones y peligros que las bases de datos informáticos pueden ocasionar a las personas, han sido puestas de relieve en diversos trabajos, mostrando que en forma instantánea y en muchos lugares a la vez, puede reproducirse el pasado, el fugaz presente y el posible futuro de las personas. La creación de la realidad virtual de los hombres y de los grupos, atendiendo a sus gastos, dolencias, inclinaciones, hábitos, puede ser peligrosa y hasta devastadora, cierta, mendaz y errónea, como si fuera un instrumento para sojuzgar y esclavizar (9).

Las defensas que se pueden blandir para evitar esas intromisiones es dable enunciarlas no taxativamente. Así la facultad que tiene la persona frente a la apropiación y manejo de sus datos de exigir que se le dé conocimiento de la información guardada por la entidad colectora; se la corrija si ese archivo tiene errores; se la actualice si figura con antecedentes históricos que no se corresponden con la personalidad presente del interesado; se la suprima y haga cesar si ya no tiene sentido preservarla en la base de datos; se impida su publicación y se la mantenga en reserva, salvo en ciertos archivos que por intereses públicos y de terceros tiene que subsistir con los resguardos del caso (exigencia, por ejemplo, de un interés jurídico actual para conocerlos); que haya un verdadero interés social para la recolección; tratándose de datos confidenciales y sensibles, limitar al mínimo indispensable la incorporación a los registros; reclamar y hacer cesar la obtención por medios ilícitos o ilegítimos; que se disponga la cancelación oportuna de los transitorios; exigir el anonimato, cuando los fines son exclusivamente estadísticos o de índole similar; que esos fines están justificados en la ley; que se pueda identificar al que colecciona los datos, se establezcan sus propósitos y los métodos y prácticas a realizar; y, desde ya, que cese toda infracción, se suprima toda amenaza y se paguen los daños y perjuicios que las acciones antijurídicas con los datos han ocasionado (10).

El conjunto de estas medidas que en algunos casos superan la tutela del derecho a la intimidad, tienen bases constitucionales iberoamericanas en Portugal en 1976 (reformas de 1982 y 1991); en España en 1978 y la ley de 1992, luego modificada en 1999 (llamada Lortad); en la Argentina desde 1994 (art. 43 de la Constitución Nacional); en Brasil desde 1988 que reguló por primera vez una garantía específica designada como habeas data; en Colombia desde 1991; en Paraguay desde 1992; en Perú desde 1984 y 1993; Guatemala desde 1985; Nicaragua desde 1987; Ecuador desde 1996 y 1998; desde Venezuela en 1999; en Bolivia desde 2004 (11).

## **II. El hábeas data**

A partir del art. 43, tercer párrafo, de la Constitución Nacional de 1994, entró en vigencia un recurso de protección de los datos personales, que fue considerado como una especie del recurso de amparo allí estatuido. La norma establece: "Toda persona podrá interponer esta acción (referida a la de amparo) para tomar 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 en caso de falsedad o discriminación, para

exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística". La reglamentación no ha sido posible, pese a haberse llegado a la sanción de un proyecto que tuvo aceptación parlamentaria, pero fue vetado por el Poder Ejecutivo (12).

Por su lado la Constitución de la Ciudad Autónoma de Buenos Aires, en el art. 16 expresamente reconoce el derecho de toda persona, mediante acción de amparo, al libre acceso a los registros públicos o privados, para conocer cualquier asiento sobre su persona, su fuente, origen, finalidad o uso que del mismo se haga. También se puede pedir la actualización, rectificación, confidencialidad, o supresión cuando tal información lesione o restrinja un derecho. En general en las provincias se coincide en este sentido y han dictado sus propias normas (13). Atendiendo a todas esas normas así como a las de la mayoría de los países de América del Sur, se ha clasificado del siguiente modo: A) Hábeas data informativo, que representa solo el derecho a obtener informes de los datos registrados y que puede ser: a1) localizador, destinado a indagar la existencia y ubicación; a2) finalista, para determinar cuál es el fin del registro; a3) Exhibitorio, para enterarse sobre los datos personales almacenados; a4) Autoral: establecer la persona que dio los datos al registro. B) Hábeas data aditivo, para agregar los datos no asentados, del que puede ser: b1) actualizador, o poner al día los datos viejos ciertos; b2) aclaratorio, aclarar situaciones ciertas pero que pueden ser incorrectamente interpretadas; b3) inclusorio, para llenar las omisiones que pueden perjudicar. C) Hábeas data cancelatorio, para eliminar datos falsos. D) Hábeas data reservador, para que un dato cierto mantenga su confidencialidad y sólo se comunique a quienes estén autorizados y en los supuestos para los que fueron habilitados (14). E) Hábeas data disociador, o sea utilizar los datos de una persona haciendo valoraciones, sin que el que los aprovecha conozca la identidad de esa persona, caso contrario se puede entablar la acción. F) Hábeas data encriptador, acudiendo a técnicas de encriptación para ocultar el dato en general y sólo darlo a conocer a quienes pueden tener la clave. G) Hábeas data bloqueador, para trabar el tratamiento de datos en un registro. Puede ser bloqueo transitorio ordenado judicialmente, o bien más allá de una medida cautelar, una sentencia con un bloqueo definitivo por haber expirado el plazo de comunicación. H) Hábeas data asegurador, pidiéndose la constatación judicial para que el sistema de información presente condiciones mínimas de seguridad que eviten fugas o alteraciones. I) Hábeas data impugnativo, es decir para cuestionar las valoraciones que realiza sobre los datos el informador. J) Hábeas data resarcitorio, o reparador, lográndose la indemnización cuando hay derecho a la exclusión o rectificación de los datos. K) Hábeas data impropio, para obtener información pública negada a quien tiene legitimación o bien para replicar información personal difundida por los medios. También, acceder a la información pública (15).

Estas diferentes clases de hábeas data tienen asiento legal en la Constitución y en la ley de datos. Vienen a ser una importante disquisición doctrinal, que permite clarificar el campo de aplicación del recurso destinado a resguardar los datos.

Sin embargo, de la falta de reglamentación, en general la jurisprudencia consideró que el recurso en el orden nacional estaba vigente, tratándolo como una especie de amparo, de ahí que iniciado el procedimiento quedó sin efecto el rechazo judicial in límite (16). La principal cuestión y que ha dado serias dificultades a la doctrina y a la jurisprudencia tiene su base en la información crediticia, especialmente frente a entidades particulares destinadas a dar informes, como la ya conocida Veraz S.A. o bien los bancos privados y públicos. Así en varios casos se ha rechazado la acción dirigida al suministro de información por el Banco Central si no se prueba la falsedad de la información, desvirtuando los elementos aportados que confirman la existencia de la deuda (17). Sostenido en el art. 26 de la ley 25.326, el tribunal comercial legitimó los "informes comerciales" no obstante la falta de consentimiento del interesado, lo cual no basta para suprimir los datos que lo califican de deudor "irrecuperable", basándose en que esos informes permiten evaluar la solvencia y el riesgo crediticio cuando se recaban informes patrimoniales de fuentes accesibles al público. Al efecto debe demostrarse la falsedad del dato o facilitadas por el interesado o con su consentimiento y además se autorizan datos sobre morosidad facilitados por el acreedor o por quien actúe por su cuenta a interés (18).

Se va abriendo otra corriente positiva y ponderable que exige que las empresas que suministran datos extremen los medios de seguridad en el flujo de la información evitando la que es falsa. Si el informador procedió a rectificar debe comunicarlo a quien le transmitió la información falsa y hacerse cargo de las

costas del habeas data (19). Si bien la empresa Veraz S.A. no puede ser responsabilizada por difundir datos erróneos de fuentes accesibles —en el caso del Banco Central—, es dable condenarla a reparar los daños por la persistencia de incluir en sus registros los datos que habían sido considerados erróneos con anterioridad y eliminados de su base de datos, al tratarse de una idéntica calificación a la eliminada, dado que a esa informadora le incumbía asegurarse de que se trataba de un nuevo incumplimiento y no de un error de la institución bancaria (20). Asimismo, la Corte Suprema estimó viable el Hábeas data para que rectifique la información de deudor moroso y se la complete para que no dé una imagen parcializada del mismo (21). Este tribunal superior ya había dispuesto por mayoría que la ausencia de normas regulatorias no impedía el ejercicio del Hábeas data, incumbiendo a la jurisdicción determinar las características con que el derecho habrá de desarrollarse (en el caso el hermano demandó para obtener informes de su hermano) (22). Dijo también que si el suministro de la información se pretende o alega que afecta a la seguridad nacional o a una investigación criminal, tales excusas debían ser invocadas por el titular de la respectiva institución administrativa (23). Por otra parte y a través del habeas data se ha ordenado al Gobierno de la Ciudad de Buenos Aires a que dé cumplimiento a la obligación de informar qué medidas se adoptaron en relación con diversas irregularidades puestas de manifiesto en las instalaciones y prestaciones brindadas por el hospital (24).

Como puede observarse, la jurisprudencia ha dado un vuelco positivo al Hábeas data, que en los primeros tiempos se redujo y cercó de exigencias, particularmente limitándolo a la información falsa. Hoy es mucho más abierta y sobre todo ante los datos crediticios hay mayor acogimiento, sobre todo porque las entidades privadas como Veraz S.A., actúan como verdaderas empresas de negocio, que cobran por cada información que proporcionan, de donde deben actuar con toda responsabilidad en la medida en que no benefician a otros altruistamente. Es así que la jurisprudencia ha abierto un camino hacia la responsabilidad de los informadores, sosteniendo que no es suficiente que el Banco Central distribuidor del dato falso y por consiguiente del daño ocasionado a la persona, se limite a suprimir de su base de datos la información errónea y a no volver a repetirla, puesto que en un lapso de tiempo la dio a conocer, por lo que corresponde que indique en sus registros que el damnificado estuvo inhabilitado desde julio de 1997 a febrero de 1998 por causa de una información errónea proporcionada por el Banco y que nunca debió ser inhabilitado. En ese caso se dispuso que las costas debe pagarlas la entidad responsable pese a que se haya allanado al hábeas data, pues no le había dado oportunidad al actor de demostrar la verdad (25).

En cuanto al problema del conocimiento de las "historias clínicas" que están reservadas en los Hospitales y Sanatorios, se trata de instrumentos muy particulares donde no sólo está ausente la firma de partes sino que tienen una vida interior y están confeccionadas por profesionales (médicos y enfermeras) que les dan un matiz documental muy específico. Es así que se ha dispuesto que no corresponde hacer lugar a la acción de hábeas data para tomar conocimiento de su contenido ni que al efecto se proporcionen fotocopias. Pero dado el interés del paciente, el que naturalmente surge a simple vista, se ha dispuesto que puede pedirse su secuestro, que se expida dicha fotocopia por el Juzgado y que se devuelva al nosocomio, aplicándose el art. 323, inc. 2 del Código Procesal Civil y Comercial de la Nación (26).

### **III. El Internet**

La informática, vocablo que tiene su origen en Francia al reflejar la síntesis de las palabras "información" y "automática", tiene una expansión incalculable a partir del uso de las computadoras y de los equipos de computadoras, de los que nace la llamada "telemática" que combina la "telecomunicación" y la "informática" (27).

En la etapa inicial los ordenadores electrónicos (años 1952 a 1958), presentaban limitaciones pues eran modelos "no comerciales" que se empleaban para las aplicaciones matemáticas, cálculos, operaciones de entradas y salidas, no abiertos al mercado genérico de usuarios, sino dentro del espacio puramente laboral. El invento fue diseñado en 1946 por los ingenieros de la Universidad de Pensylvania: J. P. Eckert y J. W. Mandley. Era el "Electronic Numerical Integrator and Computer" —ENIAC— prototipo de modelos posteriores más elaborados, tales como el EDAUC de J. V. Newman, o el UNIVAC-I de Sperry Rand y, más tarde, las series 600 y 700 de IBM-, no escapaban a esas limitaciones usuarias.

La segunda generación de 1958 hasta 1964 importó una paulatina comercialización "a pequeña escala", aunque sin sobrepasar el mercado empresarial aún no abierto a los particulares. Así la marca

NCR 304 y la serie 1400 de IBM. A partir de ese año 1964, la tercera generación recae en los ordenadores 360 y 370 de IBM, comenzando la comercialización en gran escala.

Todavía hasta 1970 las consecuencias sociales de la informática no excedían a las relaciones de trabajo en la organización interna de las empresas privadas y de la Administración pública. Por entonces, por causa de la guerra fría entre las dos potencias mundiales (EE. UU. y Rusia), se volcaban recursos de todo tipo para la defensa y, concentrar los sistemas de comunicación en puntos específicos, podía derivar en que el enemigo destruyera un puesto estratégico o lo incomunicara. De ahí que los EE. UU. hayan iniciado un programa sobre técnicas de redes de distintas clases y que las computadoras pudieran quedar enlazadas, con el sistema llamado "internetting", que después llegó a ser el "Internet". En 1986, la "Fundación Nacional de Ciencias de Estados Unidos (NSF) inició la red de la Fundación Nacional de Ciencia de Estados Unidos (NSFNET) que sirve de base del transporte de cerca de 12 billones de paquetes por mes entre las redes y quienes están enlazados en estas redes. Pero con la terminación de la guerra fría, se fue extendiendo la influencia a los campos educativo, comercial y a la sociedad global. Microsoft ha sido uno de los principales motores de difusión de las computadoras por medio de ventanas, o sea el Sistema Operativo Windows (28).

Se advierte en particular el empleo de los "ficheros administrativos", mostrando cómo todo ciudadano es afectado por la tecnología, lo que pone en peligro la intimidad y la libertad. Las posibilidades cada vez más ciertas y extendidas sobre almacenamiento de datos y su tratamiento, revelan la peligrosidad del empleo de esas herramientas por la Administración, ya que un ordenador central o por el entrecruzamiento de ficheros, permite reagrupar todas las informaciones dispersas personales de un individuo. Los riesgos y amenazas para los derechos de la esfera de intimidad dieron pie al eslogan de finales de 1970 "Informatique et Libertés" ("Informática versus Libertades"), que a partir de la ley francesa de 1978, sobre regulación de ficheros nominativos y consiguiente protección de las libertades, fue cita recurrente.

En los años ochenta con los microprocesadores, grandes redes, servicios de comunicación y las PC8, la protección fue desbordada y aparece la llamada informatización de la sociedad, que considera a la informática asociada a las telecomunicaciones como factor de cambio social y económico, para llegar a ser como una especie de "socialización de la información". O sea una herramienta que modela a la sociedad vía informática, y, más tarde, vía Internet. No sólo el desarrollo de los micro-procesadores, orientados al empleo doméstico, con reducción de costos y precios, sino la posibilidad de unificar servicios, sea los telefónicos, de telecopia y tráfico de datos informáticos que se avizora en esta etapa, constituyendo la "telemática" o "teleinformática". Estas llevan a la posibilidad de una información no limitada y la apertura a una comunicación global o lo que también fue llamado la "aldea global". Es fácil concebir un sistema integrado y unificado de informaciones, o sea un network único y multifuncional, como la reunificación del teléfono, el telex y el tratamiento informático de datos, si son sometidos a un sistema numérico, dado que el teléfono, el telex y las imágenes fijas y móviles son representadas bajo la forma de "octets". La incorporación de la fibra óptica para la comunicación por cable expande las capacidades de transmisión y da posibilidades a la comunicación interactiva. La fibra óptica impide la pérdida de electricidad y luz y juega un papel sustancial en los sistemas de giga bits.

Internet es la "Red de Redes", como red mundial con interconexión sin limitaciones espacio-temporales, las unidades de actividad de cada uno de los individuos que se encuentren conectados, en el llamado "ciberespacio". La vida está invadida por la informática, pudiendo con la utilización abusiva perjudicar la vida privada y las libertades personales, en tanto se dice que podemos estar fichados, observados, "diseccionados, desnudados, con el empleo malintencionado e ilegítimo de información personal recopilada por bases de datos de titularidad pública y privada (como el caso de las empresas bancarias que poseen toda la información de cada individuo: estado civil, parentesco, situación familiar, estado de salud, capacidad adquisitiva, vivienda habitual y residencias secundarias, patrimonio familiar, situación profesional, perspectivas salariales....) (29).

La red de redes, o gran red integrada por infinidad de redes de computación, se pone a la par de las comunicaciones por el correo tradicional (30), e importa una suerte de biblioteca virtual, como una especie de poderoso instrumento para expandir el conocimiento y favorecer la comunicación entre personas y grupos. Antes de toda regla positiva, la jurisprudencia ha establecido que el Internet es un

nuevo medio de comunicación por el que se expresan actividades de todo orden (científicas, comerciales, periodísticas, personales) que está al amparo de la Constitución. Por ello el haber usado el espacio cibernético para difundir ideas sobre el consumo de estupefacientes y su prohibición legal, ha importado valerse de un medio de prensa para criticar, dar y recibir información por lo que de ello no deriva conducta delictiva; "...el derecho de los ciudadanos a expresarse en dirección contraria a la política criminal del Estado debe prevalecer sobre el interés estatal expresado en la norma contenida en el art. 12 ley 23.737 (Adla, XLIX-D, 3692) (31).

Nada impide considerar que a los actos ilícitos cometidos a través de este medio, como pueden ser las injurias o calumnias, se les aplique el conjunto de normas que fueron creadas cuando ni siquiera imaginaba el legislador la existencia de este tipo de comunicaciones, es decir, los arts. 512, 1109, 1113, 1114, 1122 y concordantes del código civil. Por de contado que asimismo se aplicará a los actos realizados a través de la electrónica y telemática, las disposiciones que resguardan la intimidad, como el art. 1071 bis. del Código. Queda equiparado el medio para aplicar la responsabilidad refleja o indirecta, como cuando son los dependientes o incapaces los que utilizan la red informática del empleador o representante, para lesionar el honor, la imagen, la intimidad o la identidad de terceros. Pienso que inclusive es también el Internet un medio que posibilita la comisión de otros delitos, como pueden ser el plagio, la piratería que atañe a los derechos de autor, pudiendo aplicarse la respectiva ley que protege la propiedad intelectual (n° 11.723 , Adla, 1920-1940, 443).

En los Estados Unidos la Corte Suprema declaró contraria a la primera enmienda sobre libertad de prensa la ley del 26 de junio de 1997 sobre "Decencia de las Comunicaciones", aplicándola a la red telemática. Alguno de los artículos de esa ley, dijo el tribunal por siete votos contra dos, vulneran el derecho a la libre expresión al imponer restricciones a Internet por sus materiales sexuales explícitos difundidos a menores de 18 años. Se consideró que el gobierno no podía discriminar a los adultos con materiales no aptos para niños (32).

Luego, violentar el E´mail mediante el acoso indebido al correo electrónico ajeno, como dar a conocer el contenido de sus datos, afecta la intimidad del emisor del mensaje. Ello puede ocurrir cuando el empleado utiliza para su propio beneficio los correos electrónicos de los empleadores, tanto los que emiten como los que reciben comunicaciones desde el lugar de trabajo donde están las computadoras. Pero también con el spam, o correo basura, o con los llamados cookies. El spam es la utilización del e´mails para mandar publicidad no solicitada (33).

Especial para La Ley. Derechos reservados (ley 11.723)

(1) STC 292/2000, de 30 de diciembre, ver: Canosa Usera, Raúl, "El viaje del Derecho Constitucional hacia su efectividad", Estudio Preliminar en la obra de Beatriz Sbdar, Claudia, "El amparo de derechos fundamentales", ed. Ciudad Argentina, Buenos Aires 2003, p. 15.

(2) Indudablemente son bancos públicos el Registro Nacional de las Personas, la Cámara Nacional Electoral, el Registro Nacional de Reincidencia, la Dirección Nacional de Migraciones, la Anses, la Policía Federal Argentina y las policías de provincia, el Banco Central de la República Argentina, el Instituto Nacional de Estadística y Censos -INDEC-, el Registro del Estado y Capacidad de las Personas, los Registros Nacional y Provinciales de Propiedad Automotor, Registros Nacional y Provinciales de Propiedad Inmueble, el Registro Público de Comercio, etcétera. Ver Peyrano, Guillermo F., Régimen Legal de los datos Personales y Habeas Data, Comentario a la Ley 25326 y a la Reglamentación Aprobada por Dec. 1558/2001, Depalma, Bs. As. 2002, p. 19; Puccinelli, Oscar., R., "Protección de Datos de Carácter Personal", Astrea, Bs. As. 2004, p. 151.

(3) Cifuentes, Santos, "Los datos personales informáticos, un derecho autónomo personalísimo (consecuencias de su reconocimiento y características)", "J. A." 1999- IV, p. 835; "La Responsabilidad frente al Derecho personalísimo de los Datos Personales", Revista de Lecciones y Ensayos, nrs. 72/73/74, ps. 111 y sigts.

(4) Puccinelli, Oscar R., "Protección de datos de carácter personal", op. cit. p.170.

(5) CNElectoral, 9 de septiembre de 2002, "L. L.", 2002 - F, p. 1437. Ver sobre la discusión consiguiente en doctrina, Puccinelli, Oscar R., "Los datos de afiliación partidaria son sensibles en los términos de la ley 25.326 y no deben ser puestos a disposición del público en general. A propósito de su inclusión en padrones electorales y en bases de datos disponibles en Internet "J. A." 12 de abril de 2006,

p. 3.

(6) CNElectoral, 14/04/2005, LA LEY, 2005-C, 278, n° 108.893, con nota del Gozáni, Osvaldo Alfredo, "La afiliación partidaria no es un dato sensible".

(7) Bidart Campos, Germán J., "¿Ser afiliado a un partido político configura un dato sensible?", LA LEY, 2003-A, 1299.

(8) Ver Vanoli, Francisco, "El habeas data y su aplicación en materia tributaria", LA LEY Actualidad, 13/04/2006.

(9) Parellada, Carlos A., "Daños en la actividad judicial e informática desde la responsabilidad profesional", Astrea 1990, p. 257; Borda, Alejandro, "Responsabilidad extracontractual por ilícitos informáticos en las jornadas en homenaje a Jorge Bustamante Alsina", E.D., t. 139, p. 936; Lloveras de Resk, María E., "La intrusión a la intimidad a través de la informática", J.A., 1989 - II, p. 916; Arson de Glinberg, Gloria, H., "Intrusión a la intimidad través de la informática y los medios masivos de comunicación", LA LEY Actualidad, 23/11/1989; Rabinovich Berkman, Ricardo "Cuestiones actuales en derechos personalísimos", Dunken 1997, ps.135, 163 y sgts.; Cifuentes, Santos, "J. A." 1999 IV, p. 835; "Derecho personalísimo a los datos personales, LA LEY, 1997-D, 1323.

(10) Campanella de Rizzi, Elena y Stodart de Sasim, Ana María, "Derecho a la intimidad e informática", LA LEY, 1984-B, 667; Parellada, Carlos A., "Daños en la actividad judicial e informática desde la responsabilidad profesional", p. 198; Rivera, Julio C., "Instituciones de Derecho Civil", t. II, p. 102, n° 775; Rabinovich - Berkman, "Cuestiones actuales en Derechos Personalísimos", Dunken 1997, p. 164 y ss.

(11) Ver estos antecedentes estudiados y transcritos por Puccinelli, Oscar R. "Protección de datos de carácter personal", ps. 22, 25 a 29.

(12) Puede consultarse entre otros, la transcripción del proyecto de ley 24.745 de octubre de 1996 y el decreto 1616/96 que lo observó y vetó en su totalidad, en la obra Pierini, Alicia, Lorences, Valentín y Tornabese, María Inés, "Hábeas data. Derecho a la intimidad", Ed. Universidad, Bs. As., 1999, p. 95 y sigts.

(13) Pierini, Lorences y Tornabese, op.cit., p. 115; Ver la transcripción de los regímenes provinciales en Puccinelli, Oscar R., "Versiones, tipos, subtipos y subespecies de hábeas data en el derecho latinoamericano (Un intento clasificador con fines didácticos)", J. A. 2004 -III, p. 731.

(14) En contra Palazzi, Pablo A. "El hábeas data en la Constitución Nacional (la protección de la privacidad en la era de la información)", LA LEY, 20/12/94.

(15) Ver sobre estos tipos y subtipos, Puccinelli, op. cit., "J.A" 2004 - III, p. 731.

(16) CNCiv, Sala I, 29/4/1999, "J. A." 1999 -IV, p. 88, causa: "Acedo, Gustavo v/. Organización Veraz S.A."; id, Sala "B", 30/1/1998, "J. A." 2000- IV, p. 88, causa: "Basigaluz Saez c/ Organización Veraz S.A."

(17) CNCom, Sala "B": 6/12/2000, LA LEY, 2001-B, 208; CNCiv, Sala "G", 14/5/2003, "J. A." 2003-III, p. 87; CNCiv, Sala "C", 3/6/2004, "J. A." 2004 - IV, p. 75; CNCiv, Sala "M", 27/2/2000, "E. D." T. 191 - p. 415.

(18) CNCom., Sala "E", 23/5/2003, "J.A." 2003 - IV, p. 64.

(19) CNCiv, Sala "A", 26/2/2001, "E. D." T. 193, p. 21.

(20) CNCiv, Sala "E", 2/1/2004, LA LEY, 2005-A, 780.

(21) CSJN, 5/4/2005, LA LEY, 2005-B, 743, con nota de Marcela I. Basterra "Aspectos procesales y sustanciales del habeas data en un fallo de la Corte Suprema de Justicia de la Nación", y "J. A." 2005 - III, p. 31, con nota de Peyrano Guillermo F., "La determinación de ciertos lineamientos del hábeas data en un fallo de la Corte Suprema de Justicia de la Nación. Carácter del instituto. Requisito de la ilegalidad y arbitrariedad manifiestas. Falsedad e inexactitud de los datos para su procedencia. La legitimación pasiva".

(22) CSJN, 15/10/1998, LA LEY, 1998-F, 297, con nota de Bianchi, Alberto B., "El hábeas data, como medio de protección del derecho a la información objetiva en un valioso fallo de la Corte Suprema" (ver fallo in extenso en p. 236).

(23) CSJN, 16/9/1999, LA LEY, 2000-A, 348, con nota de Sagüés, Néstor Pedro, "El hábeas data



contra organismos estatales de seguridad".

(24) C.Cont.Ad. y Trib. Ciudad Bs.As., sala 2ª, 30/4/2002, "J. A." 2003 - IV, p. 65, con nota de Carranza, Luis R. y Palazzi, Pablo A. "Derecho de acceso a la información pública y derecho de acceso a la información privada (hábeas data): Semejanzas y diferencias".

(25) C.Civ. y Com. Federal, Sala II, 12/12/1998, "E. D." T. 188, p. 599.

(26) CNCiv, Sala "F", 6/7/1995, "J.A." 1996 - II, p. 397 y LA LEY, 1996-C, 473, con nota de Claudia E. Baigorria, "Algunas precisiones sobre la procedencia del habeas data".

(27) Guibourg, Ricardo A., "Informática jurídica decisoria, introducción. Sobre la técnica en el derecho", Bs. As. 1993, p. 19.

(28) Gamboa Bernate, Rafael Hernando, "Soberanía estatal en Internet; análisis desde la perspectiva de conflictos de jurisdicción y competencia en el plano nacional a internacional", Comercio Electrónico, GECTI, Legis, Los Andes, 2005.

(29) En este estudio descriptivo e historiográfico de la informática y sus peligros, he seguido las enseñanzas de García, Teresa y Hernández, Berrio, "Informática y Libertades. La protección de datos personales y su regulación en Francia y España", Universidad de Murcia, 2003, ps. 25 a 43.

(30) Equiparación en la causa "Lanata, Jorge s/ desestimación", Sala 6º C.C.y C. de Capital Federal de 1999. E. Martollo vio publicados varios E.Mails que había enviado o recibido en una revista que dirigía Lanata y que no podía difundir por falta de consentimiento de los remitentes o destinatarios. Dijo el tribunal que el sistema de e-mails "posee características de protección a la privacidad más acentuada que la inveterada vía postal a la que estamos acostumbrados, ya que para su funcionamiento se requieren varias condiciones que impiden el acceso de terceros extraños a la información". Ver Hugo A. Vaninetti: "Derecho a la intimidad e Internet", "J. A." 2005 - I, p. 992.

(31) CNCrim. y Correc. Fed., sala 1a. 13/3/2002, causa 33628; íd. Sala 2a, 29/8/2003, causa 20336, cit. por Molina Quiroga, Eduardo "Internet y libertad de expresión. A propósito de la ley 26032", "J. A." 2005 - III, p. 865.

(32) Molina Quiroga, op. cit. p. 55.

(33) Ver Hugo A. Vaninetti, Derecho a la intimidad e internet", "J. A." 2005 - I, p. 992.

© Thomson Reuters