# *LA VIDA PRIVADA Y EL PELIGRO ANTE EL DESARROLLO DE LA INFORMÁTICA*

**Juan Morales Godo**

*Abogado, magíster con mención en derecho civil por la Pontificia Universidad Católica del Perú. Profesor de Derecho Civil y Derecho Procesal Civil en las Universidades de San Marcos, Católica y de Lima. Exdecano del Colegio de Abogados del Callao. Autor de diversos ensayos de derecho civil y derecho procesal civil.*

## 1 GENERALIDADES

La lucha permanente del ser humano ha sido por la libertad, por lograr librarse de todo aquello que impide su libre desarrollo personal. Han existido y existen múltiples y variadas formas de provocar daño a las personas limitando su libertad. El desarrollo de la ciencia y el de la tecnología han producido efectos contradictorios: así como han traído progreso a la humanidad, siendo indudable que hoy en día el hombre vive más y mejor, también han provocado una serie de interrogantes de carácter ético, legal y político –de la misma forma como cuando se inventó la máquina, originando la revolución industrial en el siglo XVIII–, por los daños que pueden ocasionar al propio ser humano.

En efecto, así como la revolución industrial provocó una gran trasformación social en toda la humanidad, así también estamos viviendo en la actualidad una revolución que trae consigo una gran trasformación socioeconómica en todo el orbe. El gran invento que está provocando esta trasformación, al lado de otras, es la computadora. La máquina con "prótesis de inteligencia" ha revolucionado la información. Pero no podemos cegarnos, y así como reconocemos el gran valor para el avance de la informa-

ción, la informática trae consigo una serie de problemas de carácter ético, legal y político. De por medio está en debate la libertad del ser humano.

George Orwell, en su famosa obra *1984*, no avisoró el gran desarrollo de la informática, pero sí advirtió del peligro que representaba para la humanidad el control de la libertad de las personas a través de medios sofisticados, creados por la ciencia y la tecnología. La información ordenada por la prótesis de inteligencia constituye el elemento primario de la nueva sociedad tecnológica, y a través de ella se puede ejercer control sobre la libertad de los miembros de la comunidad[1].

John Diebold, a comienzos de la década del 70, presagiaba los problemas que podrían presentarse en el futuro. Decía el citado autor:

> "Cuando se disponga de medios para elaborar un registro de todos nuestros actos, y se tenga acceso a ese registro, ¿quién será capaz de autolimitarse en su uso y abuso? A medida que vayamos logrando el poder de control del comportamiento humano, ¿quién decidirá cómo utilizarlo?"[2].

Él mismo señalaba:

> "En el curso de las tres próximas décadas pueden surgir ante nosotros, en cualquier momento, amenazas contra la intimidad del individuo, el control del comportamiento humano y la capacidad para alterar el desarrollo genético. Las dos primeras se hallan ya muy próximas a nosotros, y, en cuanto a la tercera, es posible que no se nos plantee hasta finales de siglo. Pero, en gran medida, las tres pertenecen al mismo ámbito, a saber: el problema del individuo insuficientemente protegido por las instituciones sociales, las leyes y los preceptos formulados por sus predecesores, para enfrentarse a los distintos desafíos. Por todo ello, resulta conveniente añadir a este estudio preliminar un análisis del marco institucional de nuestra sociedad y de su capacidad de respuesta ante los cambios que se avecinan"[3].

Lo escrito por Diebold ya es una realidad inminente; por ello se exige una respuesta por parte del derecho a fin de proteger la vida privada y la identidad de las personas como garantía de un desarrollo libre de la personalidad con dignidad. El conflicto entre el derecho a la vida privada y la libertad de información cobra singulares características con el desarrollo de la informática. Ha permitido esta situación desarrollar aún más el derecho a la vida privada, con aspectos positivos como es el considerar este derecho como garantía de las demás libertades. Sin el respeto a la vida privada la libertad es una quimera, debiendo entendérsele no sólo como la defensa frente a la intrusión y la divulgación de hechos que reservamos para nosotros mismos, sino además como el derecho a obtener información a fin de poder tomar las decisiones más importantes de nuestra existencia.

¿Cómo es que a través de la informática el ser humano puede ser agredido en su vida privada? De muchas maneras y dependiendo de quién lo haga y para qué. En efecto, después de la primera y, fundamentalmente, después de la segunda guerra mundial, los Estados realizan un mayor control respecto de sus ciudadanos, exigiéndoles fidelidad al sistema. Con las computadoras es fácil recopilar y ordenar

1 FROSINI, Vittorio. *Informática y derecho*. Bogotá: Themis, pp. 27-28.

2 DIEBOLD, John. *El hombre y el ordenador*. Madrid: Península, 1976, p. 34.

3 Ibidem, p. 35.

una serie de datos que el ser humano va dejando en el trascurso de su existencia, los mismos que sistematizados permiten tener un perfil de comportamiento de la persona. Es lo que se denomina *inferential relational retrieval*. En efecto, distintos datos que el ser humano va dejando voluntariamente en distintas reparticiones públicas y privadas –como, por ejemplo: viajes realizados tanto al interior como al exterior; uso de tarjeta de crédito, cuentas corrientes o de ahorros en los bancos; declaraciones juradas ante la SUNAT; solicitudes de ingreso ante entidades privadas; fichas de libros solicitados a las bibliotecas, etc.–, pueden ser ordenados y sistematizados permitiendo obtener un perfil de comportamiento que restringe la libertad de la persona[4].

Pero no sólo el Estado puede realizar estas actividades en base a la informática; también pueden hacerlo los particulares, como por ejemplo las agencias de *credit report*, que son las encargadas de recopilar datos acerca de la solvencia económica y moral de las personas, llegando a informar respecto a los modos de vida y hábitos de quienes solicitan créditos. (Dicha información no siempre es de buena fuente, por lo que no sólo constituye un peligro por el ataque al derecho a la vida privada, sino que también puede distorsionar la identidad de la persona.) Otro ejemplo es la difusión de los tests psicológicos, de aptitud e inteligencia, para acceder a determinados cargos públicos o privados, donde debe responderse a preguntas en torno a la vida privada, hábitos sexuales, opciones religiosas o políticas, etc. Con estos datos se obtiene un perfil del comportamiento de la persona, como hemos señalado anteriormente.

Fue muy criticado el último censo realizado en el Perú, donde se solicitaban muchos datos concernientes a la vida privada de las personas y, lo que es más grave, se consignaba el nombre de las mismas. Estos datos computarizados y organizados con otros pueden ser mal utilizados con fines discriminatorios, políticos, económicos, sociales, etc.

## 2 INFORMÁTICA Y VIDA PRIVADA

La informática es el instrumento de la información; y así como hemos señalado que constituye toda una revolución cultural por los profundos cambios socioeconómicos que genera en la sociedad, así también constituye un peligro cuando su uso es atentatorio contra la libertad y la dignidad del ser humano. La comprensión de ello ha permitido que el derecho a la vida privada cobre singular importancia, a tal punto de convertirse en derecho-garantía[5], de tanta trascendencia como el derecho a la igualdad y a la libertad.

El elemento conceptual del derecho a la vida privada, denominado *autonomía*, cobra especial desarrollo. En efecto, si bien el derecho en comentario fue entendido fundamentalmente en sus aspectos negativos de impedir la intromisión y posteriormente la divulgación de hechos que la persona reserva para sí y su familia, hoy en día se analiza desde un punto de vista positivo como garantía de la libertad de la persona. Habíamos señalado que la autonomía significa la posibilidad de adoptar las decisiones más importantes de la exis-

4 PARELLADA, Carlos. *Daños en la actividad judicial e informática desde la responsabilidad profesional*. Buenos Aires: Astrea, 1999, pp. 178-179.

5 Ibídem, p. 191.

tencia de las personas. Ello implica una adecuada información, pero, a su vez, el ejercicio de una absoluta y plena libertad. No se cumple tal situación si la información es distorsionada, si no es divulgada con sentido de responsabilidad, y tampoco se cumple si la persona ve recortada su libertad en base a la invasión de su vida privada, la misma que es imperceptible y no requiere ser física, ya que con la recopilación y sistematización de los datos que uno deja a lo largo de su vida se está capturando su libertad.

Como se puede observar, existe una relación estrecha entre los aspectos de la vida privada y la información, relación que se hace evidente en términos positivos en el elemento conceptual denominado autonomía. Apreciamos dos aspectos: por un lado, el derecho a ser informados como garantía de una futura decisión libre y certera, y por otro lado, el control que debe ejercer la persona respecto de los datos proporcionados por ella misma a distintas instituciones o personas, en distintos lugares y en distintas etapas de su vida. Estas situaciones reales deben ser reguladas por la legislación a fin de proteger a la persona frente al uso irresponsable que efectúan algunos medios de comunicación masiva, tanto al brindar información como al recolectar información respecto de la vida privada de las personas –no existiendo de por medio ninguna situación que justifique la divulgación de hechos que corresponden a la vida privada–, así como frente al uso de datos existentes en las entidades públicas y privadas referentes a la existencia de las personas.

## 3 FUNDAMENTOS PARA LA REGULACIÓN JURÍDICA

Cuando hemos analizado los supuestos de la vida privada y la información, hemos concluido que son aspectos de la vida del ser humano que no son posibles de ser soslayados. Constituyen base de su existencia y desarrollo como ser humano, libre y creativo. Constituyen los cimientos del sistema democrático de gobierno y, por ende, deben ser protegidos por el derecho. Se requiere de un desarrollo doctrinario, pero fundamentalmente legislativo y jurisprudencial, porque, como hemos vislumbrado en los capítulos que anteceden, se producen con frecuencia conflictos entre ambos derechos.

El fundamento para regular los aspectos de la informática en relación al ser humano en cuanto se refiere a su vida privada, finalmente lo encontramos en el reconocimiento del derecho a la información como un derecho que corresponde a toda la sociedad, base de la democracia, y en el necesario equilibrio que debe existir frente a otro derecho fundamental como es la vida privada. Recordemos que ambos son derechos humanos proclamados por la Declaración Universal de los Derechos del Hombre –aprobada en París en 1948 por la Asamblea General de las Naciones Unidas– y en dos pactos internacionales complementarios celebrados en 1966, que contemplan por separado los derechos civiles y los derechos económicos, sociales y culturales.

Los primeros son denominados derechos individuales o derechos de la primera generación, y los segundos son denominados derechos sociales o derechos de la segunda generación, sobre lo cual ya hemos tratado en el capítulo anterior. En

ambos casos está de por medio el reconocimiento de aquello que enaltece al ser humano: su libertad y dignidad.

En consecuencia, si, como estamos apreciando a lo largo de este trabajo, la informática puede poner en peligro la libertad del hombre reduciéndolo a una mera expresión de datos recolectados, rebajando su dignidad, limitándolo como ser libre y constructor de su propio destino, es indudable que deben establecerse los límites en el uso de esta técnica e impedir que se convierta en un instrumento que perjudique el desarrollo integral del ser humano. El ser humano es y debe ser un fin en sí mismo; jamás medio para nada, conforme al imperativo categórico kantiano.

Este fundamento jurídicofilosófico constituye hoy en día la base de la mayoría de los códigos civiles en el mundo. El ser humano como fin supremo de la sociedad y del Estado fue recogido por la Constitución Política del Estado peruano de 1979; en la actualidad, la Constitución Política recientemente consultada en referéndum establece que "la defensa de la persona humana y el respeto a su dignidad son el fin supremo de la sociedad y del Estado". Por su parte, el Código Civil peruano de 1984 tiene un desarrollo integral de los derechos fundamentales de la persona como no lo tiene ningún otro código, inspirado en la concepción humanista que coloca al ser humano como centro de preocupación y protección.

El conflicto es cada vez más clamoroso.

> "Los riesgos de violación de derechos y libertades fundamentales mediante el uso de las nuevas técnicas informáticas se hacen más evidentes en el caso de las llamadas informaciones sensibles (datos sobre creencias o convicciones religiosas, opiniones políticas, origen racial, hábitos sexuales, circunstancias penales y pertenencia a sindicatos o partidos políticos, etc.), que pueden dar lugar a conductas discriminatorias por parte de quienes tienen monopolios de información."[6].

El avance de la informática ha hecho tomar conciencia de la necesidad de legislar protegiendo los datos que pueda proporcionar una persona libremente o que pudieran existir –sin su consentimiento– en alguna dependencia pública o privada; especialmente aquellos datos denominados *sensibles*, como los mencionados en el párrafo anterior. Sin embargo, algunos autores consideran que no hay que hacer distingos entre información sensible y la que no lo es, porque toda la información es relevante según el contexto y finalidad con que sea usada[7]. Estos últimos son más radicales en la protección de los derechos fundamentales del ser humano.

Esto ha motivado un cambio en la concepción del derecho a la vida privada, la misma que no puede ser entendida sólo como el derecho a ser dejado solo, en paz, concepción que coincide con una época caracterizada por un acentuado individualismo, sino que fundamentalmente debe ser entendida como la libertad positiva de supervisar el uso de la información[8].

## 4 PROTECCIÓN DE DATOS

El problema ha sido encarado a través de leyes que protegen los datos referentes a la persona, y en algunos países se ha logrado incorporarlos con rango constitucional, como en Brasil, Colombia, Paraguay y –recientemente– el Perú.

6 CORREA, Carlos, Nazar ESPECHE, Cruz de ZALDUENDO Y RATTO. *Derecho informático*. Argentina: Depalma, 1987, p. 248.

7 Ibídem, p. 250.

8 Ibídem, p. 250.

Según Rodotá[9], para una regulación eficaz debería contarse con los siguientes elementos:

a) Una ley básica que contenga principios generales.
b) Normas específicas destinadas a regular los conflictos que se plantean en determinados sectores.
c) Un órgano independiente con funciones de supervisión.
d) Sistema de intervención del Poder Judicial.

Se debe tener en consideración que existen una serie de intereses que deben ser protegidos:

a) *Interés en la confidencialidad.* Las personas tienen derecho a exigir que determinada información no sea revelada, evidentemente con especial interés respecto de las informaciones denominadas sensibles. Este derecho no puede tener un sentido absoluto, por lo que deberá determinarse en qué circunstancias no será amparable la oposición del interesado.
b) *Interés en que los datos sean completos y actualizados.* Existen una serie de dependencias que pueden no tener al día los datos relativos a una persona, por el mismo hecho de que el ser humano es libre y por ello cambia, de tal suerte que no puede manejarse una información que no esté actualizada y que puede estar distorsionando la identidad de la persona.
c) *Interés de estar informado acerca de lo que se pretende hacer con los datos.* Los datos forman parte de la identidad personal, de tal suerte que es menester que la persona esté informada respecto a cuál será el uso que se dará a dicha información.
d) *Interés en contar con una administración eficiente.* Indudablemente que resulta de especial interés para la persona que los datos sean administrados con eficiencia, significando ello un gran sentido de responsabilidad en el manejo, en el acopio y en el uso en general que se dará a las informaciones contenidas.
e) *Interés en que los datos no sean utilizados de manera ilícita.* El peligro del uso de los datos correspondientes a una persona lo hemos señalado anteriormente. Las computadoras permiten un acopio y sistematización de la información, que pueden provocar gravísimos daños eventuales y permanentes si es que los datos van a ser usados ilícitamente. Aquí encontramos el interés primario para regular el poder informático frente al ser humano.

## 5 PRINCIPIOS BÁSICOS PARA UNA LEGISLACIÓN DE PROTECCIÓN DE DATOS

En la década del 70 se sancionaron en distintos países leyes basadas en los eventos internacionales que se realizaron y en las experiencias acumuladas. Hilda Batto[10], en un análisis comparativo de las diversas legislaciones, resumió los siguientes principios que las estructuran y que pueden servir de pauta para futuras legislaciones:

### *5.1 Principio de la justificación social*

La recolección de datos deberá tener un propósito general y usos específicos socialmente aceptables. El artículo 1 de la ley francesa señala:

9 Ibídem, p. 252.

10 Bátkan, p. 257.

"La informática deberá estar al servicio de cada ciudadano. Su desarrollo deberá tener lugar dentro del marco de cooperación internacional. No deberá atentar a la dignidad humana ni a los derechos del hombre ni a la vida privada ni a las libertades individuales o públicas".

Este artículo se explica por sí solo y traduce el principio en comentario que permite el uso equilibrado y razonable de la informática en razón a los intereses del propio ser humano, nunca en contra de él.

### 5.2 *Principio de limitación de la recolección*

Existen una serie de datos cuya recolección debe prohibirse –salvo excepciones justificadas–, como, por ejemplo, datos referentes a la raza, religión, salud, costumbres sexuales, opiniones políticas, uso de estupefacientes, etc.

Fuera de estos datos sensibles, la recolección de otros datos debe ser con autorización, conocimiento y consentimiento del interesado y deberán limitarse al mínimo necesario para alcanzar el fin perseguido con la recolección. La ley francesa y la austriaca exigen una habilitación legal para la recolección de cualquier tipo de datos personales.

### 5.3 *Principio de la calidad o fidelidad de la información*

Conforme a este principio, los datos recolectados deben ser verdaderos, de tal suerte que no produzcan una falsa imagen de la persona. Por ello es que las legislaciones deben permitir el acceso para una verificación, pudiendo rectificarse, anularse o actualizarse cualquier dato que no corresponda a la realidad.

### 5.4 *Principio de la especificación del propósito o la finalidad*

Al recolectarse los datos debe especificarse la razón o finalidad de aquélla, no pudiendo usarse los datos para fines distintos a los señalados como razón para la recolección.

### 5.5 *Principio de confidencialidad*

El acceso a la información por parte de terceros sólo será posible si lo consiente el propio sujeto de la información o por mandato judicial. Indudablemente, debe distinguirse cuando los datos se proporcionen sin especificar ni identificar al sujeto, y ello puede ocurrir cuando se realiza un estudio de carácter estadístico, en cuyo caso no acarreará sanción alguna.

### 5.6 *Principio de salvaguarda de seguridad*

A través de este principio se establece la obligación, por parte del responsable del registro, de adoptar las seguridades adecuadas para proteger la información contra posibles pérdidas, destrucciones o acceso no autorizado. Incluso puede disponerse la posibilidad de destruir la información en circunstancias especiales, como en los casos de guerra, por ejemplo.

### 5.7 *Principio de la política de apertura*

Se garantiza a través de este principio la trasparencia de la acción de la administración pública o privada respecto de los procedimientos y prácticas concernientes al procesamiento de datos personales. Por ello, debe ser de conocimiento público la existencia, fines, usos y métodos de operación de los registros de datos personales.

### *5.8 Principio de la limitación en el tiempo*

Los datos deben conservarse sólo hasta el cumplimiento de la finalidad para la cual fueron recolectados. Cumplida la finalidad, la información debe ser cancelada, salvo casos excepcionales.

### *5.9 Principio de control*

Se debe prever un organismo de control, responsable de la efectividad de los principios enunciados. Tanto la ley danesa como la ley francesa prevén organismos especiales. La primera crea una Inspección de Registros y la segunda la Comisión Nacional de la Informática y las Libertades.

### *5.10 Principio de la participación individual*

Consagra el derecho de acceso de las personas al registro de datos en donde se hayan recolectado los referidos a su vida personal o familiar.

"Este derecho de acceso comprende el derecho a:

a) Obtener información de la entidad responsable de los datos, acerca de la existencia de datos que le conciernan.
b) Ser informado dentro de un tiempo razonable y de manera comprensible.
c) Oponerse a cualquier dato que le concierna y a que esa oposición quede registrada.
d) Obtener que los datos relativos a su persona, en caso de prosperar su oposición, sean suprimidos, rectificados o completados.
e) Ser informado de las razones por las cuales se deniega su derecho de acceso o éste no se le conceda en lugar, tiempo y forma razonables.
f) Oponerse a toda negativa a darles las razones mencionadas precedentemente."[11].

11 Ibidem, p. 261.

## 6 BANCO DE DATOS

La información se ha incrementado a tales niveles y es tanta su importancia, que a través de la informática se ha ido desarrollando una industria de la información por medio de la creación de bancos de datos. Hoy en día la información es una mercancía y por un precio se puede tener acceso a los bancos con los más diferentes contenidos, tanto a nivel nacional como a nivel internacional.

"Esta nueva industria –paradigmática, para algunos, de la era de la información– pone en movimiento diversos protagonistas: los productores de bases de datos: instituciones científicas, universitarias, profesionales o empresas que estructuran y actualizan datos concernientes a su área de actuación; los distribuidores: empresas que disponen de gran capacidad de cómputo orientada a la prestación de servicios de consulta; los operadores de redes de trasmisión, sean telefónicas o redes especiales de trasmisión de datos..."[12].

Indudablemente ello ha originado una serie de problemas de orden jurídico: por un lado, lo relativo a los derechos de los productores, y por otro, al derecho de los autores; pero, además, al derecho que tiene toda persona cuyos datos relativos a su vida, especialmente aquellos denominados "sensibles", aparecen registrados en estos bancos, que están al alcance de cualquier persona o entidad pública o privada, nacional o internacional.

### *6.1 Flujo internacional de datos y la vida privada*

La Declaración Universal de Derechos Humanos, aprobada por la Asamblea Ge-

12 Ibidem, p. 289.

neral de las Naciones Unidas el 10 de diciembre de 1948, consagró en el artículo 19 la libertad de opinión, de expresión y la libertad de información. En dicho artículo se estableció no sólo la posibilidad de ejercer estas libertades a través de cualquier medio de trasmisión de información, sino que se precisó que no existía limitación de fronteras.

En este concepto se ha desarrollado el nuevo derecho a la trasmisión internacional de datos, lo que ha revolucionado el campo de la información, pues esta trasmisión internacional opera a través de las redes de datos de las computadoras. Este hecho ha motivado, a su vez, preocupación, a tal punto que la propia Asamblea General de las Naciones Unidas, en su resolución 2450 del 19 de diciembre de 1968,

> "Invita al secretario general a realizar, con la ayuda del Comité Consultivo sobre la Aplicación de la Ciencia y de la Técnica al Desarrollo, y en cooperación con los jefes de los secretariados de las instituciones especializadas competentes, el estudio de los problemas planteados desde el punto de vista de los derechos del hombre por los logros de la ciencia y de la tecnología, en particular en lo que se refiere a: a) El respeto a la vida privada de los individuos y de la integridad y la soberanía de las naciones ante el progreso de las técnicas de grabación y otras."[13].

La preocupación de las Naciones Unidas por el tema, demuestra la impoetancia del mismo y la urgencia de adoptar acuerdos internacionales y fijar reglas para la trasmisión de los datos en relación a los cuales la ciencia y la tecnología permiten una libre difusión poniendo en peligro la vida privada de las personas y la soberanía de las naciones.

Sin perjuicio de las diferencias ostensibles que existen entre las naciones respecto de su desarrollo científico y tecnológico –que las colocan en una situación de desigualdad, convirtiendo a unas naciones en trasmisoras, otras en meras receptoras y otras que no pueden estar en ninguna de las dos situaciones–, es preciso trabajar en aras de una democratización internacional en la trasmisión de datos, estableciendo como limitación el respeto de la dignidad del ser humano, y específicamente a su vida privada, y la preservación del orden social y económico de las naciones.

## 7 El HÁBEAS DATA

Es la garantía constitucional que protege la libertad de las personas cuando ésta se ve amenazada o vulnerada como consecuencia de datos recogidos, almacenados, sistematizados o trasmitidos por medios automáticos o no, públicos o privados. Así como el hábeas corpus protege la libertad física de la persona, el hábeas data protege la libertad de la persona cuando existen datos que la perjudiquen, en algún banco de datos o archivo. Protege, además, en el caso peruano, el derecho a la información de asuntos públicos. Esta protección es el nuevo contenido del derecho a la vida privada, y como lo señala Frosini[14],

> "ésta no es ya la libertad de rechazar información pública sobre los propios hechos privados o datos personales, pretensión que hoy no podrá encontrar adecuada pro-

13 FERNÁNDEZ DE ZUBIRÍA, Jaime. *Derecho de prensa, calidad, derecho internacional y derechos humanos*. Colombia: Facultad de Ciencias Jurídicas y Socioeconómicas de la Pontificia Universidad Javeriana, pp. 7-8.

14 FROSINI, Vittorio. Op. cit., pp. 164-165.

> tección en muchos casos, sino que es la libertad de controlar el uso que se haga de los propios datos personales incluidos en un programa informativo; es el hábeas data, correspondiente al antiguo hábeas corpus del respeto debido a la integridad y libertad de la persona. Por consiguiente, derecho de acceso a los bancos de datos, derecho de control sobre la exactitud de ellos, derecho de actualización y de rectificación, derecho de secreto para los datos sensibles, derecho de autorización para la difusión de ellos; este conjunto de derechos es el que hoy constituye el nuevo *right to privacy*".

La concepción del hábeas data radica en el reconocimiento de que es la persona la que debe gobernar los datos que se recolecten respecto de ella, ya que los mismos constituyen una proyección de su personalidad. Es la garantía procesal-constitucional que tiene todo sujeto de derecho para conocer los datos o registros respecto de él que obren en bancos de datos, computarizados o no, públicos o privados y con posibilidades de difusión. Éste es el primer objetivo histórico del hábeas data.

Un segundo objetivo es la posibilidad de que la persona pueda actualizar los datos que figuran en los bancos o registros. Por ejemplo, si figura como procesado por algún delito o comprendido en un proceso de carácter administrativo, cuando ya fue absuelto penal o administrativamente, en estos casos la persona tiene derecho a actualizar los datos a fin de que se tenga una información completa y no parcial que lo perjudique.

Un tercer objetivo es la rectificación de datos incorrectos, falsos o inexactos que obren en un banco o registro de datos, público o privado. Sería el caso de la persona que figura como que ha sido condenada a una pena determinada por un delito del cual fue acusado, y que, sin embargo, constituye un dato falso porque ya había sido absuelta por sentencia ejecutoriada.

Un cuarto objetivo, importantísimo, es el derecho de suprimir datos referentes a lo que la doctrina denomina "información sensible", los que están referidos a aspectos de la vida privada, al honor y a la identidad de la persona, como, por ejemplo, la religión que profesa, raza, ideas políticas, conducta sexual, etc., y que pueden provocar discriminación de cualquier índole.

Un quinto objetivo del hábeas data, también, es el derecho a exigir confidencialidad respecto de datos que figuran en determinados registros, es decir, derecho a que no se divulguen determinados datos. Sería el caso aquel en que no podemos exigir la supresión de dichos datos. Ejemplo de ello lo tenemos en los datos que tiene registrados la SUNAT. Éste es el objetivo que ha resaltado la Constitución Peruana de 1993, aun cuando no se descarta, vía interpretación, el cumplimiento de los demás objetivos mencionados anteriormente.

### *7.1 Origen del hábeas data*

El hábeas data surge como respuesta al exceso del poder informático, el mismo que se ha agudizado por su gran desarrollo. Las computadoras, por la enorme cantidad de datos que pueden almacenar, son capaces de desnudar la vida privada de cualquier persona. Como se trata de un fenómeno nuevo, la respuesta también es novísima. El tratamiento doctrinario data de la década del 70.

La primera ley sobre protección de datos fue dictada el 7 de octubre de 1970 por el Parlamento del Land de Hesse, en la República Federal Alemana, donde se designó un magistrado especial para la vigilancia en la aplicación de dicha ley. Posteriormente, en 1973, Suecia aprobó una ley que fue considerada modelo para una legisla-

ción sobre informática, donde se consagró el deber de registrar, en un registro público, los archivos electrónicos, incluso aquellos procesados por las empresas privadas[15].

Años después, estas leyes fueron diseñando un nuevo principio de la libertad informática que fue proclamado en dos Constituciones: la de Portugal en 1977 (arts. 33 y 35) y la española de 1978 (art. 18). Esta libertad informática implica el principio de la reserva de los datos personales en los bancos o archivos de datos, y la facultad de control reconocida al ciudadano sobre el uso y la circulación de la información registrada. En ambos casos, no se le conoce con la denominación de hábeas data.

En América latina adquiere rango constitucional hace aproximadamente seis años (1988), con la Constitución brasileña, donde ya se usa la expresión *hábeas data*; luego es incorporada en la Constitución colombiana; posteriormente, en 1992, se incorpora a la Constitución paraguaya y en 1993 a la Constitución peruana.

En la Constitución brasileña (LXXII) el hábeas data es la garantía para poder rectificar los datos que sobre la persona se tengan en registros de datos públicos o privados. La Constitución paraguaya (art. 135) ha ido más lejos, considerando que no sólo existe el derecho a rectificar la información registrada, sino también a actualizarla o destruirla, así como el derecho a conocer el uso y finalidad de la información que se acumula.

Como se puede observar, su origen y desarrollo está centrado en la protección del ser humano en tanto que datos de su vida privada pueden ser capturados por un registro informático poniendo en peligro su libre desarrollo y su libertad.

### *7.2 El hábeas data en el Perú*

La Constitución peruana de 1993, consultada en referéndum y actualmente en vigencia, acoge la figura del hábeas data –en el inciso 3 del artículo 200– como una garantía constitucional, a la par que el hábeas corpus, la acción de amparo, la acción popular y la acción de cumplimiento. Señala el indicado dispositivo constitucional que la acción de hábeas data "procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5, 6 y 7, de la Constitución".

Los incisos 5, 6 y 7 del artículo 2 de la Constitución antes referida, señalan lo siguiente:

> "Artículo 2. Toda persona tiene derecho:
> (...)
> 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. El secreto bancario y la reserva tributaria pueden levantarse a pedido del juez, del fiscal de la nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado.
> 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.
> 7. Al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias.
> Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en for-

15 PROSINO, Vittorio. Op. cit., pp. 76-77.

ma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley".

Debe destacarse la incorporación de esta garantía constitucional de defensa de los derechos fundamentales de la persona. Ésta es, sin embargo, una regulación peculiar, por cuanto en los otros países anteriormente mencionados la protección del hábeas data sólo cubre el derecho a que se brinde información por parte de las dependencias públicas y al control y confidencialidad que deben dar los bancos y/o archivos de datos, computarizados o no, públicos o privados.

El derecho a ser informado resulta de trascendental importancia para una sociedad democrática, especialmente cuando se refiere a los asuntos públicos. En este sentido, el inciso 5 reconoce el derecho de todo ciudadano a solicitar información a cualquier entidad pública, sin expresión de causa, y con la limitación de los casos en que la información pueda afectar la vida privada de las personas, se excluyan expresamente por ley o por razones de seguridad nacional.

Con relación a que la información pueda afectar la vida privada de las personas, es perfectamente explicable esta limitación, aun cuando las circunstancias que comprende la vida privada no están precisadas por ley, por lo que quedará sujeta a la jurisprudencia aquella delimitación. Por otro lado, respecto a las razones de seguridad nacional, si bien son perfectamente valederas en países como los nuestros, el peligro es que se use de aquel argumento para justificar verdaderas faltas al derecho a la información.

El secreto bancario y la reserva tributaria pueden levantarse, pero sólo por mandato de un juez, del fiscal de la nación o de una comisión investigadora del Congreso. Las informaciones contenidas en las referidas entidades son reservadas, y para brindar información debe mediar mandato judicial.

Como podemos observar, el legislador peruano ha puesto el acento en el derecho a solicitar información –que es la otra columna del derecho a la información, que fue entendido en nuestro medio sólo como el de brindar información–. Específicamente, se refiere a las dependencias públicas, de tal manera que no sólo constituye un derecho de los ciudadanos, sino de los medios de comunicación masiva –en especial–, el acudir en busca de información a las dependencias públicas con el fundamento de que se trata de asuntos públicos y, por ende, sujetos a la fiscalización de los ciudadanos.

El inciso 6 se refiere al control que debe ejercer la persona sobre los registros, públicos o privados, donde consten datos relativos a su vida privada. Puede impedir que se suministre información sobre datos que corresponden a su intimidad personal o familiar. Es una función preventiva que protege el hábeas data.

Es necesario precisar que la extensión de este inciso está en concordancia con el inciso 4 del mismo artículo 2 de la Constitución, en cuanto protege la libertad de información, opinión, expresión y difusión del pensamiento mediante la palabra oral, escrita o la imagen, por cualquier medio de comunicación social, *sin previa autorización, ni censura ni impedimento algunos, bajo las responsabilidades de ley*. Esto significa que los medios de comunicación masiva no están sujetos a prevención alguna respecto de informaciones que puedan verter. Cuando el inciso 6 se refiere a servicios informáticos, computarizados o no, públicos o privados, éstos son comprensivos de los existentes en los medios de comunicación; sin embargo, ello no puede impedir que la información se divulgue,

por cuanto constituiría una limitación a la libertad de expresión e implicaría una censura previa. Una interpretación sistemática garantiza la libertad de prensa, la misma que está sujeta a responsabilidad *ex post*, pero no sujeta a limitaciones ni impedimentos ni censura previos. Sin embargo, tratándose de la vida privada merece una interpretación específica, conforme lo haremos líneas adelante.

Este aspecto, consideramos, merece una precisión normativa, por cuanto la extensión del inciso 6 comprende todos los servicios informáticos existentes, incluidos los de los medios de comunicación masiva. Ayuda a comprender la extensión del mismo no sólo el inciso 4 antes mencionado, sino también el propio inciso 7 cuando señala que toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley. La responsabilidad es *ex post* y el agraviado no sólo puede recurrir al derecho de rectificación, sino, de considerarlo pertinente, proceder a denunciar penalmente el hecho por delito contra el honor (querella) o por delito contra la intimidad, o, de lo contrario, optar por demandar en la vía civil por daños y perjuicios (responsabilidad civil).

Líneas arriba hemos mencionado todas las posibilidades que brinda el hábeas data respeto al control de los datos; sin embargo, el legislador peruano sólo ha privilegiado la confidencialidad de los servicios informáticos respecto de los datos almacenados. Si bien ésta es una garantía, ello no significa que el ciudadano no pueda acceder a la información, solicitar su corrección, o la supresión, de ser falso el dato. Se reconoce que tener acceso a todos los servicios informáticos es poco más que imposible, y quizá por ello se han limitado a proteger la confidencialidad, pero, tomado conocimiento de la existencia de datos equivocados, desactualizados o falsos en algún archivo informático, no se puede negar el derecho a la rectificación o a la supresión de los mismos, de ser el caso.

En relación al inciso 7, si bien él se refiere al derecho a la rectificación cuando la persona es agraviada a través de algún medio de comunicación social, no se descartan las responsabilidades penales y civiles comentadas en el párrafo anterior. La interrogante es si a través del hábeas data se puede exigir la rectificación inmediata y proporcional de una información divulgada por un medio de comunicación masiva y que es atentatoria de alguno de los derechos fundamentales que protege, o si debe solicitarse previamente la rectificación correspondiente, y sólo si se le niega este derecho o el mismo no se produce en los términos que señala la ley, es decir, de manera inmediata y proporcional, el agraviado puede hacer uso del hábeas data.

Nuestro punto de vista es que a través del hábeas data se puede exigir la rectificación inmediata y proporcional. Esperar el incumplimiento del derecho de rectificación es dilatar la posibilidad de una rectificación inmediata, que muchas veces puede constituir una buena forma de mitigar el daño ya ocasionado. El hábeas data perdería eficacia, su razón de ser, si se convierte en un instrumento procesal que sólo puede ejercerse después de haberse hecho uso del derecho de rectificación. Por ello es que expresamos nuestra discrepancia con la resolución emitida por la Sala Penal de la Corte Superior de Lima que conoció el primer caso de hábeas data interpuesto –cuyo comentario lo haremos más adelante–, en cuanto considera que el hábeas data no puede sustituir el ejercicio del derecho de rectificación y, por ende,

sólo puede hacerse uso de él ante una denegatoria o mal cumplimiento de tal derecho. Sin embargo, cuando concluimos el presente trabajo se promulgó la ley 26301 (de 3 de mayo de 1994), que señala expresamente que constituye vía previa para el ejercicio de la acción de hábeas data, además de lo señalado en el artículo 27 de la ley 23506, el requerimiento, por conducto notarial, con una antelación no menor de cinco días calendario, de la publicación de la correspondiente rectificación, con lo que precisa los alcances de la garantía constitucional coincidiendo con el pronunciamiento de la Sala Penal de la Corte Superior de Lima.

¿Esta acción procede también cuando los datos se encuentran recolectados en algún medio de comunicación masiva y, por ende, es posible evitar la propalación masiva de dicha información? Éste es un tema sumamente discutible, ya que el inciso 4 del mismo artículo 2 que comentamos establece el derecho a la libertad de información sin previa autorización ni censura ni impedimento algunos. En buena cuenta, primero se difunde la información y luego se sanciona si es que ha existido un agravio a los derechos fundamentales. Puede solicitarse la rectificación y/o formularse la denuncia penal correspondiente y/o la responsabilidad civil, pero lo que no se acepta es que se impida la difusión de la información. Los periodistas y los propietarios de los medios de comunicación masiva señalan las conveniencias de no poner cortapisas a la libertad de expresión.

Algunos consideran que existen razones más que suficientes para repensar que la información tiene limitaciones y éstas están dadas por el derecho a la vida privada; por ello es conveniente que se establezca la posibilidad de ejercer un derecho en forma preventiva. Sin embargo, la tendencia universal, así como constitucional peruana, es confiar en la responsabilidad del medio de comunicación social; es preferible el ejercicio de la libertad responsable, porque establecer mecanismos que impliquen censura previa pudiera constituir la válvula de escape por la cual se restrinja la libertad de expresión que también es garantía de una sociedad democrática. En todo caso, se señala, existen las responsabilidades establecidas por ley en caso se haga uso extralimitado de aquella libertad.

Sin embargo, como hemos señalado en el capítulo anterior, hay que distinguir el derecho a la vida privada de los demás derechos de la personalidad y, específicamente, del derecho al honor. En efecto, teniendo en consideración que tanto el derecho a la información como el derecho a la vida privada son derechos básicos y fundamentales para la vigencia y desarrollo de una sociedad democrática, no puede sostenerse racionalmente un derecho cuya agresión no pueda prevenirse. Ahora bien, en el caso del derecho a la vida privada, la verdad del hecho a divulgarse no es determinante para la responsabilidad o no del autor de la divulgación. Aun siendo verdad el hecho divulgado, la agresión se ha cometido y hay responsabilidad, siempre que no exista alguna causa o interés mayor (general) que justifique la divulgación. Distinto es el caso del derecho al honor, en el que la verdad de la divulgación constituye eximente de responsabilidad en el autor. Por ello se afirma que, tratándose del derecho a la vida privada, la acción preventiva –que, dicho sea de paso, la considera el artículo 686 del Código Procesal Civil al permitir la admisión de medidas cautelares innovativas para el reconocimiento del derecho a la vida privada– no constituye una censura previa, sino más bien una limitación del derecho a la información, máxime cuando quien trata de divulgar lo hace porque ya se entrometió

en la vida privada de la persona. El actuar de esta forma, cuando se considera que está en peligro el derecho al honor, sí puede convertirse en una censura previa y entraña en conflicto con la norma constitucional señalada en el inciso 4 del artículo 2.

En resumen, el hábeas data que plantea la Constitución peruana de 1993 tiene tres objetivos concretos: a) Obtener información de las dependencias públicas (inc. 5, art. 2); b) Asegurar la reserva de los servicios informáticos respecto de informaciones que afecten la vida privada personal y familiar (inc. 6, art. 2), y c) Lograr la rectificación de informaciones inexactas propaladas a través de los medios de comunicación social (inc. 7, art. 2).

Mucho se ha cuestionado la extensión que hace nuestra Constitución Política de los alcances del hábeas data. No nos vamos a referir a los que sostienen que debe derogarse íntegramente dicha garantía. Más bien coincidimos con quienes sostienen que ni en el origen del hábeas data ni en su desarrollo legislativo, tanto en Estados Unidos como en Europa y América latina, se vinculó al derecho de libertad de expresión, de opinión y al derecho de rectificación reconocido en las normas internacionales y en la propia Constitución peruana de 1993. Este sector plantea la derogatoria del hábeas data en cuanto se refiere a la protección de los derechos mencionados en el inciso 7 del artículo 2 de la Constitución Política del Estado, por cuanto la misma entraña peligro de ser atentatoria del derecho a la libertad de información, de expresión, opinión y difusión del pensamiento.

Si de lo que se trata es de purificar el contenido de una institución, podemos convenir con esta posición a efectos de que el hábeas data se limite para la protección de los derechos contenidos en los incisos 5 y 6 del artículo 2 de la Constitución peruana de 1993, pero ello no soluciona el problema latente en la sociedad, cual es el conflicto entre el derecho a la vida privada y la libertad de información y, específicamente, con la libertad de prensa. Consideramos, más bien, la necesidad de una regulación teniendo en consideración que hay necesidad de proteger la vida privada de las personas con remedios procesales rápidos y efectivos.

Recientemente el Congreso del Perú ha aprobado en una primera legislatura la derogatoria del inciso 3 del artículo 200, en lo que se refiere al ámbito de aplicación del hábeas data, restringiéndolo a los incisos 5 y 6 del artículo 2 de la Constitución Política del Estado de 1993; es decir, la derogatoria se refiere al ámbito de protección del inciso 7 del indicado artículo constitucional. Para que dicho ámbito quede totalmente derogado se requiere de la aprobación de una segunda legislatura, que necesariamente sólo podrá llevarse a cabo en 1995.

Sin embargo, el problema sigue latente; esto es, el conflicto entre la libertad de información y la vida privada de las personas, conflicto que, en vista de la previsible total derogación que se llevará a cabo el próximo año, tendrá que ser dilucidado por la otra garantía constitucional que es la acción de amparo.