La tutela jurídica del tratamiento de los datos personales frente a los avances de la información

Propuesta para un redimensionamiento del denominado derecho general de la personalidad y para una definición común del denominado *habeas data*(*)

Juan Espinoza Espinoza
Abogado. Profesor de derecho civil en la Pontificia Universidad Católica del Perú, en la Universidad Nacional Mayor de San Marcos y en la Universidad de Lima.

1 Premisa.

La tutela de los derechos de la persona ha sido una preocupación constante (aunque oscilante) de toda cultura jurídica. Ello se ha acentuado notoriamente después de la Primera Guerra Mundial. En efecto, si hacemos una mirada retrospectiva, constatamos que el jurista decimonónico regularizaba pormenorizadamente los derechos patrimoniales, dejando de lado aquellos denominados (debido a la carga ideológica imperante) extra-patrimoniales, por cuanto se pensaba que formaban parte del derecho natural y no requerían una tutela específica por parte del derecho positivo. Incluso, cuando comenzó a teorizarse sobre los derechos de la persona, se pretendía -erróneamente- explicar los mismos a través de esquemas propios de los derechos patrimoniales, principalmente, el derecho subjetivo de la propiedad. Es a partir de los aportes de la filosofía existencialista y de la corriente del personalismo ético que el jurista contemporáneo se **sensibiliza** y comienza a producir modelos jurídicos que se basan en la tutela de la persona, entendida come eje y centro del ordenamiento jurídico(1). Sin embargo, cada sistema jurídico ha asumido criterios propios en lo que se refiere al reconocimiento de los derechos de la persona y en los mecanismos de tutela de los mismos.

Así tenemos que en Alemania se reconoce un derecho general de la personalidad (*allgemeines Persönlichkeitsrecht*), el cual está dirigido a la conservación, inviolabilidad, dignidad y libre desenvolvimiento del individuo, y en el *common law* norteamericano insurge el *right of privacy*, entendido (no como equivocadamente se piensa: sinónimo del derecho a la privacidad, sino) como síntesis de las situaciones jurídicas existenciales de las personas. De estos derechos generales (o madres), surgen otros derechos especiales (o hijos).

Los ordenamientos jurídicos que no han adoptado el

(*) Este trabajo constituye la continuación del artículo publicado por el mismo autor, y bajo el mismo título, en la edición número 19 de nuestra revista.

(1) FERNÁNDEZ SESSAREGO, Carlos. *Un nuovo modo di fare diritto*. En: *Il diritto dei nuovi mondi*. A cura de Visintini. Padova: CEDAM, 1994. p.238.

modelo de un derecho general de la personalidad, reconocen legislativamente un elenco limitado de derechos de la persona: es el caso de todos los sistemas del *civil law* que siguen el modelo diseñado por el código civil francés.

Esta diferenciación que, producto de un enjuiciamiento apresurado, podría parecer de corte académico, resulta de suma incidencia práctica frente a la adopción de técnicas de tutela frente a posibles abusos que se puedan presentar. En efecto, si tomamos como ejemplo el tema de los abusos de la informática, ante una posible legislación que tenga como objetivo limitar los mismos, se presentan dos posibilidades: si estamos en un sistema como el francés: es imperativo **individualizar qué derechos** serían los que se desea proteger (sea intimidad, identidad, reputación, entre otros), asumiendo la contingencia que pueda quedar desprotegido alguno (imagen o voz, por ejemplo). En cambio, si nos encontramos frente a un sistema como el alemán o el estadounidense, el derecho general de la personalidad, o el *right of privacy* tutelaría **cualquier derecho** (o situación jurídica de ventaja) de la persona. Estas situaciones las vemos reflejadas, de alguna manera, en la Ley Federal de Alemania de 1977, en materia de *Datenschutz,* el *Privacy Act* de Estados Unidos de Norteamérica de 1974 y en la *Loi relative à linformatique, aux fichiers et aux libertés* francesa de 1978.

El propósito principal de este trabajo es comparar ambos sistemas y determinar cuál sería el más viable para enfrentar el vertiginoso avance de la informática, con el que se ha llegado a tal punto de invasión de los derechos de las personas, que ya podríamos hablar de una suerte de manipulación informática equiparable sólo a la manipulación genética. Si bien es cierto que las inquietudes del científico están siendo frenadas por la Bioética, no es nuestra intención sentar las bases de una suerte de **Infoética**; pero sí proponer un equilibrio entre los intereses y derechos de las personas (naturales o jurídicas) cuya información se registra, de las empresas (públicas o privadas) que almacenan, clasifican o difunden esa información y de los terceros interesados en obtener dicha información.

El trabajo estará dividido en tres partes y el método a emplearse es el comparativo: la primera parte estará dirigida a proponer una nueva concepción del denominado derecho general de la personalidad, estudiándose, para tal efecto, las experiencias jurídicas alemana y estadounidense(**). La segunda parte se centra en los modelos jurídicos de protección de los datos personales y se hace un recorrido a las experiencias estadounidense, alemana, francesa (que ya han devenido en clásicas en esta materia) y aquellas más recientes de la unión europea y la italiana. De ellas se extraerá un **común denominador** y se analizará su posible aplicación en realidades como la nuestra, lo cual será materia de la tercera parte de este trabajo.

2 Sobre la tutela específica en la experiencia jurídica comparada de la protección sobre los datos personales.

2.1 La Ley Federal alemana del 27 de enero de 1977 sobre protección de datos (*Bundesdatenschutzgesetz*).

Se ha observado que en la fase precedente a la entrada en vigor de esta Ley, la tutela del particular derecho de la personalidad que se denomina *Datenschutz* estaba basada de manera exclusiva en la referencia constitucional, estando argumentada bajo el fundamento del *allgemeines Persönlichkeitsrecht* de los artículos 1 y 2 de la Constitución(2). Incluso, a nivel del formante doctrinario, se realizaron importantes estudios sobre el *Datenschutz*(3).

(**) Ver: ESPINOZA ESPINOZA, Juan. *La tutela jurídica del tratamiento de los datos personales frente a los avances de la informática. Sobre el denominado derecho general de la personalidad.* En: *Ius et Veritas*. No.19. Año IX. pp.54-62.

(2) ROPPO. *I diritti della personalità.* En: *Banche dati telematica e diritti della persona.* A cura de Alpa y Bessone. Padova: CEDAM, 1984. p.71.

(3) SIMITIS. *Chancen und Gefahren der elektronichen Datenverarbeitung.* En: *Neue Juritische Wochensehrift*, 1971. pp.673-682. Citado por BESSONE. *Politica dellinformazione e strategie di Datenschutz.* En: *Banche dati telematica e diritti della persona*; el cual hace la siguiente glosa: la imagen de una absoluta objetividad de la información invariablemente garantizada por el recurso a instrumentos de elaboración completamente automatizados tiende a acreditar una mitología de la incorruptibilidad de la máquina (y de la eliminación de la intervención humana) que no encuentra respaldo en la realidad. Y Simitis tiene razón de escribir que nada sería (...) más errado que el asunto que un acceso ilimitado al banco de datos valga *per se* a asegurar informaciones exhaustivas y objetivas. Cualquier banco de datos opera, en efecto, siempre (y sólo) en aplicación de decisiones del hombre que tienden a degradar al *computer* al rol de un dúctil instrumento utilizado para obtener un sistema de datos conforme a los deseos (y a los planos de acción) del operador (p.267).

Los principios básicos del *Bundesdatenschutzgesetz* son los siguientes[4]:

a) Establece como misión de la protección de datos, prevenir todo perjuicio a intereses dignos de protección de los interesados, mediante la salvaguardia de datos de índole personal frente a cualesquiera abusos con ocasión del almacenamiento, transmisión, modificación y destrucción (tratamiento de datos) (artículo 1.1).

b) Se protege los datos de índole personal que fueren almacenados en ficheros, modificados, destruidos o transmitidos desde el fichero tanto por autoridades u otros entes públicos como por personas físicas o jurídicas de derecho privado (artículo 1.2).

c) Se excluye del ámbito de la Ley los datos de índole personal que se traten por empresas o, en su caso, por empresas auxiliares de la prensa, la radiodifusión y la cinematografía exclusivamente para sus propios fines publicitarios, siempre y cuando adopte las medidas técnicas y organizativas indispensables (artículo 1.3). Esta última obligación es común para todo tipo de personas que efectúe tratamiento de datos de tipo personal (artículo 6.1)

d) Se entiende por datos de índole personal a los datos individuales sobre circunstancias personales u objetivas de una persona física determinada o determinable (llamada interesado) (artículo 2.1). Nótese la exclusión que se hace de las personas jurídicas.

e) Se define como fichero de datos a una colección de estructura uniforme de datos que se pueda obtener y ordenar conforme a ciertos rasgos y cambiar de ordenación y evaluar conforme a otros rasgos determinados, con independencia del procedimiento empleado para ello, si bien no se incluyen en este concepto los documentos sueltos ni colecciones de documentos, a menos que se puedan ordenar y evaluar mediante procedimientos automatizados (artículo 2.3.3)

f) El tratamiento de los datos de índole personal será lícito únicamente cuando lo autorice esta Ley (BDSG) u otra norma legal o si lo hubiese consentido el interesado por escrito (artículo 3).

g) Se reconoce a los interesados los siguientes derechos (artículo 4):

- Recibir información sobre los datos almacenados acerca de ellos mismos.
- A la corrección de los datos almacenados sobre ellos mismos, cuando fueren inexactos.
- A que no sean accesibles los datos almacenados acerca de ellos mismos, cuando no se pudiere determinar si son exactos o inexactos, o bien en el caso de haber desaparecido los presupuestos de hecho existentes originariamente para el almacenamiento.
- Que se destruyan los datos almacenados acerca de ellos mismos, cuando el almacenamiento fuere ilícito o -como opción alternativa al derecho a la inaccesibilidad- cuando hayan desaparecido los supuestos de hecho originariamente existentes para el almacenamiento.

h) Se establece la obligación del secreto por parte de las personas que almacenen, modifiquen , destruyan o transmitan datos (artículo 5).

i) Se prevé el nombramiento de un Comisario Federal para Protección de Datos (artículo 17) el cual controlará la observancia de las normas de la presente Ley (BDSG) (artículo 19).

j) En el caso de entidades privadas que traten (para sí o por encargo) datos personales y tengan como mínimo cinco trabajadores a título personal, se deberá nombrar un encargado de la protección de datos (artículo 28). Asimismo, se prevé el nombramiento de una autoridad competente según el ordenamiento regional (artículo 30).

k) Se establece sanciones penales y pecuniarias por actos delictivos (artículo 41) así como multas en el caso de infracciones administrativas (artículo 42).

Después de la entrada en vigor del BDGS, surgió una etapa de autosuficiencia legislativa[5], la cual

(4) Los siguientes datos han sido extraídos del *Boletín de Legislación Extranjera*. Nos.90-91. Madrid, marzo-abril 1989. pp.21-45; en el cual se encuentran tanto la versión alemana como española del *Gestz zum Schutz von Missbrauch personenbezogenen Daten bei der Datenverarbeitung*, cuyo título abreviado es el *Bundesdatenschutzgesetz* (literalmente, Ley General de Protección de Datos-BDSC). La traducción es de Daranas Pelaez.

(5) ROPPO. Op.cit.; p.80.

pretendía excluir a la Constitución de la regulación del *Datenschutz*. Sin embargo, la doctrina criticó los límites, lagunas e inadecuaciones del BDGS, como es el caso del *Medienprivileg* regulado por el artículo 1.3, que favorecía peligrosamente a los medios de comunicación. Grandes problemas se suscitaron en torno al posible conflicto que representan los censos frente al *Datenschutz*. En efecto, un juez administrativo de Düsseldorf, con fecha 16 de mayo de 1978, había establecido qué leyes específicas relativas a la recolección de datos con finalidad estadística (*Hochschulstatistikgesetz*) prevalecían, en caso de contraste, sobre el BDGS. En 1983, las garantías establecidas por el BDGS sucumbieron frente al censo general que se hizo en ese año[6].

En vista de esta situación, se ha producido una fase de retorno a la Constitución, a la cual le está siguiendo otra de propuestas hacia reformas legislativas[7]. Esta ley prevé que también los *Länder* emanen normas sobre la protección de los datos. En 1980, todos los *Länder*, a excepción de Hamburgo, habían emanado disposiciones estatales de acuerdo a esta directiva federal[8].

Particular atención merece la ley bávara sobre la protección de datos individuales, *Bayerische Datenshutzgesetz* (BayDSG) del 28 de abril de 1978, que prevé el derecho a la indemnización frente a las entidades públicas bávaras[9].

2.2 El *Privacy Act* de 1974 y el *Freedom of Information Act* de 1966.

En materia de protección jurídica de los datos personales, el modelo jurídico alemán (así como el francés) puede ser definido como **uniforme**, casi monolítico, frente al modelo jurídico norteamericano, que es más bien **desagregado**, por cuanto está regulado en una articulada disciplina normativa[10], a través de distintas *sedes materiae*.

El *Privacy Act*, aprobado a finales de 1974, firmado en enero de 1975 y entrado en vigor el 25 de setiembre de 1975, disciplina la recolección, clasificación y el uso de las informaciones, producto de la actividad de gobierno federal y de todos los departamentos, las fuerzas armadas, las *agencies* independientes (entendidas en sentido genérico, como entes públicos), las sociedades de derecho público, las sociedades controladas por el gobierno, como el *Federal Reserve Banks* y la *Federal Home Loan Corporation*. No se aplica al Congreso, a los gobiernos estadounidenses en los territorios y posesiones no metropolitanas, en el Distrito de Columbia ni en las Cortes federales. Existen dudas si también puede ser aplicado a los procedimientos frente a las cortes marciales. En el caso que el sistema de clasificación de las informaciones de una *agency* esté organizado y dirigido por una sociedad privada, las reglas del

(6) Este censo, a pesar que fue varado inicialmente mediante ley de marzo de 1982, estableció una modalidad operativa alarmante: no sólo se establecía una multa de 10,000 marcos para los reticentes a dar información sino que, además, se establecía un premio en dinero para quien denunciase a algún reticente. ROPPO. Op.cit.; p.81.

(7) ROPPO. Op.cit.; p.80. Es necesario precisar además que el *Bund* ha integrado la ley para la protección de datos personales con tres ordenanzas que regulan respectivamente, las sumas a pagar por parte de quien solicita información sobre los propios datos memorizados (*Datenschutzgebührenordnung*, DSGebO, del 22 de diciembre de 1977), la formación del registro de los dancos de datos personales (*Datenschutzregisterordnung*, DSRegO, del 09 de febrero de 1978) y la publicación del tipo de datos personales memorizados por las entidades públicas (*Datenschutzveröffentlichungsordnung*, DSVeröffO, del 03 de agosto de 1977). Este complejo normativo vale para el *Bund* y en base al artículo 7 BDSG, también para los *Länder* que aún no hayan emanado sus propias disposiciones en materia. LOSANO. *La legislazione tedesca sulla protezione dei dati individuali*. En: *Banche dati telematica e diritti della persona*. Op.cit.; p.282.

(8) LOSANO. Op.cit.; p.281.

(9) Así, el artículo 13 establece lo siguiente: **Derecho a la indemnización**. (1) Si en el ejercicio de un cargo público se procede a la elaboración de datos en violación de las normas de esta ley, o de una particular norma sobre la protección de datos contenida en otra normativa, el responsable de la oficina que elabora los datos es responsable según las siguientes normas por los daños materiales provocados.
El daño material es indemnizado en dinero, hasta el monto máximo de DM 250.000 por sujeto y por evento dañino.
El daño patrimonial no es resarcible si no hubiera podido ser evitado incluso usando la diligencia necesaria. Sin embargo, ello no vale si el dañado por el ilícito ha sufrido un daño patrimonial relativo a una situación jurídica directamente tutelada por un derecho fundamental. Si no se puede aplicar la indemnización prevista por el punto (1), se puede establecer una indemnización equitativa.
Si al ocasionarse el daño patrimonial hay un concurso de culpa del dañado, se aplica el artículo 254 del BGB (relativo a la compensación de obligaciones).
El derecho a la indemnización es hecho valer frente a la magistratura ordinaria.
Toda pretensión ulterior queda a salvo.

(10) ALPA. *Privacy e statuto dellinformazione*. En: *Banche datti telematica* ... Op.cit.; p.209.

Act se aplican también a ésta[11].

El *Privacy Act* define como *record* a toda voz, colección, agrupación de informaciones sobre un individuo, depositadas en una *agency*, incluyendo noticias (pero no limitadas a éstas) relativas a su educación, operaciones económicas, historia clínica, cronohistoria penal y profesional que contienen su nombre o su número de identificación, un símbolo u otro signo particular que sea idóneo para identificarlo, como por ejemplo, la huella digital, el registro de voz o una fotografía. Se entiende por sistema de *records* a un grupo de datos de los cuales se puedan inferir informaciones idóneas a ser ubicadas usando el nombre u otro signo de identificación del sujeto. La expresión *statistical record*, indica un sistema de *records* usados con fines de investigación o de clasificación; pero no para obtener informaciones ni datos relativos de una determinada persona[12].

El *Privacy Act* no es entendido como una ley autónoma: constituye más bien un régimen de excepción al principio general puesto en 1966 por el *Freedom of Information Act* (FOIA), en el cual se reconocía el derecho de saber por parte de los ciudadanos frente a las entidades públicas. También, el FOIA estaba destinado a regular las relaciones entre ciudadanos y la administración pública, siendo su finalidad, justamente, la de asegurar a todo ciudadano el acceso a todas las informaciones sobre los entes públicos y depositadas en los entes públicos. Se entendía así regular formas de participación directa y al mismo tiempo, elevar a principio general la exigencia de una auténtica transparencia de las actividades administrativas. En este sentido el *Privacy Act* integra el FOIA bajo dos aspectos particulares: por un lado, pone una barrera a la circulación de las informaciones relativas a la *privacy* de los ciudadanos, y por el otro, facilita el ejercicio del derecho a saber por parte de los interesados, vale decir, de los investigados. Es por esto que se considera al *Privacy Act* un modelo **desagregado**, porque no se puede entender su significado normativo sin conocer las normas del FOIA, a la cual hacen referencia *per relationem*[13].

El *Freedom of Information Act* dispone la publicidad de una serie amplia de actos administrativos, obligando a las *agencies* a publicar en el *Federal Register* las informaciones que se refieren a cuatro categorías de actos:

a) La descripción del organigrama central y periférico de los entes, de los lugares y de las oficinas en los cuales los interesados pueden solicitar informaciones.

b) Las funciones, los modos y los métodos de actividad de la *agency*, los reglamentos relativos a los procedimientos y las informaciones necesarias para la participación a los procedimientos.

c) Las normas emanadas por delegación del legislativo y las enmiendas a tales disposiciones.

d) Se prevén otras formas de publicación de los actos que permiten a los ciudadanos, de manera individual o grupal, conocer las decisiones de la *agency* y las direcciones interpretativas elaboradas por la *agency* en materia de actividad administrativa, entre éstos, los códigos de comportamiento de la *agency*.

Como ya se adelantó, el FOIA introdujo el derecho a saber: hacer accesibles a los ciudadanos todos los documentos, archivos y datos recogidos por las *agencies*, salvo algunas excepciones. El derecho a saber no se aplica a nueve tipos[14] de información:

a) Cuando la información podría entrar en conflicto, si es difundida, con el interés público y la seguridad nacional.

b) Funcionamiento interno de la *agency*.

c) Actuación de otras leyes específicas.

d) Secretos comerciales.

e) *Memoranda* internos de las *agencies*.

f) Vinculaciones internas entre las *agencies*.

g) Fichas médicas y fichas del personal.

h) Investigaciones realizadas por las *agencies* para la tutela de la seguridad interna y la lucha contra el crimen.

i) Operaciones financieras, actividades de extracción, con particular referencia a las extracciones de petróleo.

Sin embargo, el FOIA no indica los métodos de

(11) Ibid.; pp.210-211.
(12) Ibid.; p.212.
(13) Ibid.; pp.215-216.
(14) Ibid.; p.216.

clasificación de las informaciones. Este *Act* contiene sólo algunas disposiciones de menor relieve, respecto a la disciplina general prevista por otros procedimientos (y por las mismas *agencies*, que tienen la prerrogativa de elaborar códigos internos de clasificación y archivo de datos). La disciplina general es organizada en gran parte por un *Executive Order* de 1972[15].

El sistema de clasificación de datos está organizado en forma de pirámide al revés: la punta, de la cual emanan los principios fundamentales, está constituída por el *National Security Council*, la base, en cambio, sólo por las *agencies* que están legitimadas para ello por el *Council*. No todas las *agencies* tienen el poder de proceder a la clasificación de los datos recogidos. Las *agencies* que no tienen esta prerrogativa deben transmitir los datos recogidos a las otras que están dotadas de tal competencia. En el desenvolvimiento de sus funciones, el *Council* está asistido por un Comité (*Interagency Classification Review Commitee*, ICRC), al cual todas las *agencies* envían sugerencias, pedidos e indicaciones. El público está invitado a hacer lo propio[16].

Sobre la base de las directivas emanadas por el *Council*, las *agencies* que tienen legitimación elaboran códigos internos de clasificación de datos. Generalmente, los datos son clasificados en tres categorías, según su relevancia a efectos de seguridad interna y externa. Se distinguen, en escala jerárquica, los datos *top secret*, cuya revelación puede provocar un daño excepcional a la seguridad nacional, los datos simplemente *secret*, cuya revelación puede causar un daño grave y los datos *confidential*, cuya difusión puede ocasionar un daño razonablemente relevante[17].

Se prevé un sistema de reglas para definir la vida de la información, que permita, por un lado, el uso eficiente de los elaboradores y la sustitución de las informaciones y por el otro, la eliminación de datos que, con el tiempo, pueden haber perdido su valor originario. Se procede a la clasificación de modo mecánico, desde el momento que se debe conservar sólo el mínimo de informaciones útiles para la seguridad nacional[18].

En la práctica, el sistema funciona de manera menos lineal y orgánica de cuanto se podría pensar. En efecto, los comentadores evidencian que a menudo, por razones de seguridad, se falsifican los datos conservados y se difunden notician alteradas intencionalmente, se recogen informaciones que trascienden las finalidades propias de las *agencies*, se conservan noticias por un período mucho más largo que el previsto, incluso, las tareas de clasificación no obedecen a criterios nacionales, sino asumen -como es comprensible- tintes políticos, desde el momento que el 95% de datos está custodiado por la *Central Intelligence Agency* y por los Ministerios de Defensa y de Justicia[19].

El imperfecto funcionamiento del sistema de clasificación es documentado por un alto contencioso en esta materia. Existen algunos casos en los cuales las *agencies* son renuentes a proporcionar las informaciones solicitadas, por otro lado, hay una orientación cauta de las cortes que, para no entrar en conflicto con los criterios de oportunidad seguidos por el gobierno de turno, tienden a alinearse a las decisiones de las *agencies*, en vez de reconocer las pretensiones de los particulares[20]. Ello nos evidencia un sistema de leyes y procedimientos basado en los principios de acceso a la información (con numerosos límites) y de objetividad (relativa) de los criterios de clasificación[21].

El *Privacy Act*, en lo que se refiere a la recolección de la información, se preocupa de indicar dos criterios fundamentales, que sirven para seleccionar los datos: el primero se refiere al nexo entre tipo de información y finalidad de la *agency* (criterio funcional) y el segundo, de naturaleza objetiva, se refiere al contenido de la información, estando prohibida la recolección de informaciones personales de los administrados. Se trata, como resulta evidente,

(15) Ibid..
(16) Ibid.; pp.216-217.
(17) Ibid.; p.217.
(18) Ibid..
(19) Ibid.; pp.217-218.
(20) Ibid.; p.218.
(21) Ibid.; p.219.

de criterios muy elásticos, que confían a las *agencies* poderes de investigación amplios: cualquier información puede ser adquirida, si puede calificarse como relevante a los fines perseguidos por la *agency*. Ejemplos numerosos de recolección de datos, no siempre pertinentes a las finalidades institucionales del ente, demuestran que la elasticidad del criterio se transforma en una débil tutela de los interesados[22].

Sin embargo, estas formas de protección se refuerzan por el segundo criterio de selección. En otras palabras: las *agencies* no pueden recoger informaciones (y si son recogidas, no pueden conservarlas), cuando éstas se refieran al modo en el cual cada individuo ejercita los derechos derivados de la Primera Enmienda, a menos que no haya una autorización explícita del interesado. Por consiguiente, la selección de datos de naturaleza personal es, más bien, contenida: si no se pueden archivar datos sobre las orientaciones religiosas, sobre las adhesiones a grupos y asociaciones, sobre la manera del ejercicio de la libertad de información, si se puede adquirir información sobre las orientaciones sexuales, sobre la vida matrimonial y familiar, en general, así como las relaciones de consanguinidad: un amplio espectro de sectores en los cuales la *privacy* puede ser sacrificada[23].

También existen otras normas de tutela: por ejemplo, aquellas que prescriben que la *agency*, al recoger los datos, indique al interesado las normas sobre la base de las cuales está legitimada a adquirirlos; pero se subraya que esta forma de control es muy débil: se puede eludir fácilmente porque otras leyes subordinan la erogación de servicios (por ejemplo, servicios asistenciales), a la verificación de determinados requisitos para ser destinatario de los mismos, siendo obligatoria la comunicación de los datos personales, frente a lo cual, el individuo no puede desentenderse, a menos que quiera renunciar a los servicios ofrecidos. Otro motivo de evasión es la natural confianza inspirada por los órganos públicos, por lo cual los individuos son proclives a comunicar a la *agency* el más amplio número de informaciones personales. Al mismo tiempo, el *Privacy Act* no prevé la obligación, por parte de las *agencies*, de comunicar a los investigados la identidad de los terceros que hayan suministrado información sobre aquellos, ni la identidad de los terceros que hayan solicitado informaciones sobre los administrados. Resulta fácil ocultar las fuentes de información y los *dossiers* preparados con el aporte de terceros[24].

> La tutela de la persona frente al tratamiento de los datos informáticos (...) no sólo debe limitarse al sujeto individualmente considerado, sino también en su dimensión de coexistencialidad, vale decir, como integrante de alguna formación social (...)

En efecto, no obstante se indique que las *agencies* deben dirigirse directamente al interesado para adquirir las informaciones, y sólo cuando razones logísticas y financieras lo sugieran, están autorizadas a dirigirse a terceros, es práctica común recurrir a la vía excepcional. La amplia discrecionalidad de las *agencies* en la recolección y en la clasificación de los datos está temperada por la configuración de algunas posiciones subjetivas que corresponden a los administrados. Al poder de la *agency* se contrapone el derecho de conocimiento y de acceso a los datos, por parte del interesado[25].

Como se ha observado, derecho de conocimiento no significa derecho de ser informado de oficio por la *agency* sobre la existencia de los datos o *dossiers* sobre el interesado. En un sistema que se preocupa de tutelar al individuo; pero, sobre todo, de limitar cuanto sea posible los costos de actuación del *Act*, informar *ex officio* al interesado hubiera importado un dispendio de tiempo y de energía; pero también una

(22) Ibid.; pp.219-220.
(23) Ibid.; p.220.
(24) Ibid.; pp.220-221.
(25) Ibid.; p.221.

carga financiera considerable. Este derecho es garantizado de manera indirecta: cada año se publica en el *Federal Register* el aviso de la existencia de procedimientos de investigación, con indicación de su naturaleza y sobre los sistemas de *records* conservados, con esta finalidad, por las *agencies*. Es una prescripción que la *agency* no puede eludir. Pudiendo tomar conocimiento de iniciativas en curso dirigidas a la recolección de datos, el individuo es colocado en grado de dirigir a la *agency* competente, la solicitud de saber si han sido recogidos datos sobre su persona y la petición, en caso positivo, de tener el contenido[26].

Sin embargo, existen hipótesis de excepción, en las cuales las *agencies* están exoneradas de las obligaciones correspondientes a estos derechos, como es el caso de informaciones con finalidad estadística o científica, los datos de los candidatos a cargos públicos o de los dependientes del orgánico federal[27].

Al lado del derecho de conocimiento, están el derecho de control y de rectificación (*right to challange*) que se ejercen sobre todas las informaciones a las cuales el interesado tiene acceso. Tienen la misma amplitud que el derecho de conocimiento y el derecho de acceso: es el interesado quien debe suministrar a la *agency* todo material, indicación, sugerencia, para poder operar una modificación de los datos almacenados[28]. Si la *agency* ha acogido la solicitud, o en el caso de mandato judicial (ante la denegatoria de la *agency*), se prevé que la corrección realizada sobre los datos conservados, sea difundida a todas las *agencies* y a los particulares que hubiesen adquirido informaciones erróneas, para evitar ulteriores daños al interesado. Sin embargo, el *Act* no prevé que, una vez recibida la comunicación, las *agencies* que precedentemente eran depositarias de la información errada, estén obligadas a corregirla, ni se establecen plazos para el inicio del proceso de difusión de la comunicación de la corrección[29].

No se reconoce, de manera explícita, un derecho al olvido de los interesados, vale decir, la supresión de datos pasados, eventualmente perjudiciales para su honor o reputación[30]. El modelo jurídico norteamericano se preocupa más de controlar el fenómeno de la circulación de las noticias, en vez de la exigencia de reservar al individuo un espacio libre en el cual desenvolver su intimidad, tratándose, por consiguiente de una ley que recurre a la regulación de procesos, en vez de la elaboración de derechos sustanciales[31].

En lo que se refiere al uso y difusión de las informaciones, el *Privacy Act* prohíbe que las *agencies* diseminen informaciones que no sean objeto de uso rutinario, el cual es definido como el uso (...) para un propósito compatible con aquel por el cual la información ha sido recogida. Sin embargo, la *praxis* administrativa norteamericana está plagada de intrusiones indebidas, abusos de poder y ausencia de controles eficaces, así como una serie de derogaciones a este principio[32].

En cuanto a los remedios, éstos pueden ser de naturaleza civil, penal y administrativa. Los remedios consisten en el resarcimiento del daño, o en la inhibición del uso de la información (*injunctive relief*), según el tipo de violación perpetuado por la *agency*. No obstante ello, se establecen límites consistentes a la imposición de sanciones: se solicita que la violación haya sido realizada voluntaria o intencionalmente y que la *agency* haya actuado de manera gravemente negligente (*gross negligence*). El resarcimiento del daño es pagado por el gobierno federal y no por la *agency*, a la cual le corresponde corregir (cumpliendo el mandato judicial) los datos erróneos[33].

En materia de sanciones, el *Act*, prevé multas frente a los dependientes de la *agency* que hayan cometido materialmente le violación, sanciones análogas son previstas para los terceros que, con

(26) Ibid.; pp.221-222.
(27) Ibid.; p.223.
(28) Ibid.
(29) Ibid.; pp.223-224.
(30) Ibid.; p.224.
(31) Ibid.; p.225.
(32) Ibid.; pp.225-226; quien menciona como excepciones las informaciones relativas a la identificación de los criminales y aquellas recogidas en el curso de procedimientos dirigidos a la represión de delitos (p.226).
(33) Ibid.; p.227.

pretensiones falsas, hayan obtenido informaciones de otras personas[34]. Considerado en su conjunto, el sistema de sanciones es articulado; pero débil: se disponen sanciones casi exclusivamente por violaciones cometidas en la fase de conservación de los datos, en vez que en la fase de adquisición o difusión. Las sanciones son tenues y fácilmente pagables, logrando con ello que los particulares que quiera disfrutar económicamente las informaciones ilícitamente adquiridas, encuentren un incentivo, en vez de un impedimento, en las penas previstas[35].

A nivel jurisprudencial, se presentó un caso en 1971, en el cual dos profesores de derecho laboral, que estaban desarrollando una investigación, solicitaron una lista de nombres y direcciones a la *agency* del trabajo (NLRB). La finalidad de la investigación se refería al estudio de las técnicas de control seguidas por la *agency* en las elecciones de los representantes de fábrica y tenía el propósito de demostrar la inutilidad de algunas técnicas de control, que generaban muchos gastos y eran de poco provecho. Obtenido el rechazo por parte de la *agency*, que había invocado las excepciones contenidas en las normas sobre la protección de la *privacy*, los estudiosos se quejaron ante la corte distrital. Los jueces acogieron el pedido de los autores, recurriendo al principio del balance de los intereses y argumentando la utilidad pública de la investigación. La decisión fue criticada por quienes observaron que no es posible resolver el conflicto de intereses, teniendo en cuenta la finalidad de quien requiere la información, sin preocuparse del posible daño que se puede ocasionar al investigado, por la difusión de las noticias[36].

El mosaico legislativo estadounidense se acrecienta con otras leyes, como es el caso del *Fair Credit Reporting Act*, de 1970, el cual disciplina la actividad de información crediticia y da al consumidor el derecho de verificar las informaciones aunque sea de manera parcial e indirecta[37]. Por todo ello, nos adherimos a la opinión que el *Freedon of Information Act* no es la panacea universal para el logro del Gobierno abierto, pero su práctica aplicativa representa ya, sin lugar a dudas, un referente importantísimo emplazable en el haber de los sistemas democráticos[38].

2.3 La *Loi relative à l'informatique, aux fichiers et aux libertés* francesa No.78-17 del 06 de enero de 1978.

En la experiencia jurídica francesa, una intervención legislativa en materia de tutela de la persona no es un hecho insólito: la ley del 17de julio de 1990 dirigida a regular la garantía de los derechos individuales de los ciudadanos, ya había modificado al viejo *Code civil* (artículo 9), así como algunas reglas del código penal, de manera tal de asegurar a los ciudadanos el respeto de la vida privada y un verdadero y propio derecho al secreto y a la intimidad[39]. La *Loi relative à l'informatique, aux fichiers et aux libertés* francesa de 1978 tiene influencia del modelo sueco de 1973; pero contiene algunas directivas tomadas del *Privacy Act* de 1974 y de la ley federal alemana[40].

Los principios de esta ley son los siguientes[41]:

a) Se establece que la informática deberá estar al servicio de cada ciudadano y su desarrollo se realizará en el marco de la cooperación internacional. No podrá atentar ni a la identidad humana, ni a los derechos humanos, ni a la vida privada, ni a las libertades individuales o públicas (artículo 1).

b) Ninguna decisión judicial, administrativa o privada que implique apreciación sobre la conducta humana podrá estar fundada en un tratamiento informatizado de

(34) Ibid.
(35) Ibid.; p.228.
(36) Ibid.; pp.230-231
(37) PAGANO. *Aspetti economici e giuridici delle banche dati*. En: *Bache dati telematica* ... Op.cit.; p.111.
(38) REVENGA SÁNCHEZ. *El acceso a información reservada por motivos de seguridad nacional en los Estados Unidos. Un balance de la aplicación de la Freedon of Information Act*. En: *Derecho*. No.51. PUCP: Lima, diciembre 1997. p.94. Para tener una idea del movimiento que genera esta ley, basta mencionar que en 1978, a los cuatro años de su sanción, se recibieron más de 700,000 demandas anuales para acceder a información personal (CORREA, NAZAR ESPECHE, CZAR DE ZALDUENDO y BATTO. *Derecho Informático*. Buenos Aires: Depalma, 1987 p.242.
(39) ALPA. Op.cit.; p.243.
(40) Ibid.; p.246.
(41) Los siguientes datos han sido extraídos del *Boletín de Legislación Extranjera*. Nos.88-89. Madrid, enero-febrero 1989. pp.3-16; en el cual se encuentran tanto la versión francesa como española de esta ley. La traducción es de Daranas Pelaez.

informaciones que suministren una definición del perfil o de la personalidad del interesado (artículo 2).

c) Toda persona tendrá derecho a conocer e impugnar las informaciones y los razonamientos utilizados en los tratamientos automatizados cuyos resultados se aleguen en contra de ella (artículo 3).

d) Se consideran nominativas las informaciones que permitan de cualquier modo, directamente o no, la identificación de las personas físicas a que se apliquen, tanto si el tratamiento fuere efectuado por una persona física como por una persona jurídica (artículo 4).

e) Se denomina tratamiento automatizado de informaciones nominativas, a todo conjunto de operaciones de la misma naturaleza referentes a la explotación de ficheros o bases de datos, y en particular las interconexiones o cotejos, consultas o comunicación de informaciones nominativas (artículo 5).

f) Se crea una Comisión Nacional de Informática y de las Libertades, encargada de velar por el respeto de los preceptos de esta ley (artículo 6). También tiene como función la de elevar cada año al Presidente de la República y al Parlamento una memoria en la que rendirá cuentas del cumplimiento de su misión, la cual será publicada (artículo 23).

g) Los miembros y agentes de la Comisión están sujetos al deber del secreto profesional por los hechos, actos o informaciones que pudieran tener conocimiento, con motivo de sus funciones, bajo responsabilidad penal (artículo 12).

h) Salvo en los casos que deban ser autorizados por la ley, los tratamientos de informaciones nominativas efectuados por cuenta del Estado, o de un organismo público o de una autoridad territorial, o de alguna persona jurídica de derecho privado que esté gestionando un servicio público, serán acordados por acto reglamentario, previo dictamen motivado de la Comisión (artículo 15).

i) Serán objeto de una declaración ante la Comisión, los tratamientos automatizados de informaciones nominativas efectuados por cuenta de personas distintas de las sometidas en el artículo 15, previamente a toda puesta en práctica de los mismos (artículo 16)[42].

j) La Comisión pondrá a disposición del público la lista de los tratamientos, que especifique, en relación con cada uno (artículo 22):

- la ley o el acto reglamentario por el que se haya acordado su creación o la fecha de su declaración;
- su denominación y su finalidad;
- el servicio ante el cual se ejercerá en derecho de acceso[43];
- las categorías de informaciones nominativas registradas, así como los destinatarios o categorías de destinatarios autorizados para recibir copia de esas informaciones.

k) Se prohibe el recojo de datos efectuado por medios fraudulentos, desleales o ilícitos (artículo 25). Asimismo, toda persona física tendrá derecho a oponerse, por razones legítimas, a que información alguna, en relación a ella, sea objeto de tratamiento. Salvo lo dispuesto en el artículo 15 (artículo 26).

l) Las personas de quienes se recojan informaciones de carácter nominativo deberán ser informadas de lo siguiente (artículo 27):

- del carácter obligatorio o facultativo de las respuestas;
- de las consecuencias para ellas de una falta de respuesta;
- de quiénes son las personas físicas o jurídicas destinatarias de esas informaciones;
- de la existencia de un derecho de acceso y rectificación.

m) Salvo precepto legislativo en contrario, las informaciones no deberán conservarse en forma nominativa más allá de la duración prevista en la solicitud del dictamen o en la declaración, a menos que la Comisión autorice su conservación (artículo 28).

n) Toda persona que ordene o efectúe un

(42) Sin embargo, el artículo 24 prevé que a propuesta o previo dictamen de la Comisión, la transmisión entre el territorio francés y el extranjero, en todas sus formas, de informaciones nominativas, que fueren objeto de tratamientos automatizados regidos por el artículo 16, podrá ser sometida a previa autorización o reglamentada según modalidades fijadas por decreto acordado en el Consejo de Estado, con el fin de asegurar el respeto de los principios establecidos en esta ley.

(43) En atención a ello, el artículo 34 establece que toda persona que justifique su identidad tendrá derecho de consultar a los servicios u organismos encargados de poner en práctica los tratamientos automatizados cuya lista fuere accesible al público, con el fin de saber si esos tratamientos versan sobre informaciones nominativas relativas al solicitante y, en su caso, de que se les dé traslado.

tratamiento de informaciones nominativas se obliga por este hecho, ante las personas afectadas, a tomar toda clase de precauciones convenientes para preservar la seguridad de las informaciones y en especial, para impedir que sean deformadas, dañadas o transmitidas a terceros no autorizados (artículo 29).

o) Queda prohibido insertar o conservar dentro de una memoria informatizada, salvo conformidad expresa del interesado, datos nominativos que, directa o indirectamente, den a conocer los orígenes raciales u opiniones públicas, filosóficas o religiosas o la adscripción sindical de las personas (artículo 30)[44].

p) Se establece un régimen de excepción para el caso de las informaciones nominativas tratadas por los organismos de la prensa escrita o audiovisual, en el marco de las leyes que las regulen, en los casos en que su aplicación tuviere como efecto limitar el ejercicio de la libertad de expresión (artículo 33).

q) Podrá el titular del derecho de acceso exigir que se rectifiquen, completen, aclaren, pongan al día o borren las informaciones que, versando sobre él, fueren inexactas, incompletas, equívocas o atrasadas y cuyo recojo, utilización, comunicación o conservación, esté prohibido (artículo 36)[45].

r) Los ficheros nominativos deberán ser completados o corregidos, incluso de oficio, cuando los organismos que los lleven tuvieren conocimiento de la inexactitud o del carácter incompleto de informaciones nominativas contenidas en ellos (artículo 37). Si se hubiere transmitido una información a un tercero, se notificará igualmente a éste toda rectificación o anulación, salvo dispensa otorgada por la Comisión (artículo 38).

s) En lo relativo a los tratamientos que afecten a la seguridad del Estado, la defensa y la seguridad pública, la petición se dirigirá a la Comisión, la cual designará a uno de sus miembros que pertenezca o haya pertenecido al Consejo de Estado, al Tribunal de Casación o al Tribunal de Cuentas, para que lleve a cabo todas las investigaciones convenientes y hacer que se proceda a las modificaciones necesarias. Dicho miembro podrá recabar la ayuda de un agente de la Comisión. Se notificará al peticionario que se ha procedido a las comprobaciones (artículo 39).

t) Cuando se aplique el ejercicio del derecho de acceso a informaciones de carácter médico, éstas sólo podrán ser comunicadas al interesado por mediación de un médico designado para este fin (artículo 40).

u) Las disposiciones de los artículos 25, 27, 29, 30, 31 y 33 se aplican también en materia de recojo, registro y conservación de las informaciones nominativas a los ficheros no automatizados o mecanográficos, distintos de aquellos cuyo uso constituya ejercicio estricto del derecho a la vida privada (artículo 45).

v) Se establecen sanciones penales y multas frente a una serie de incumplimientos.

El modelo francés, inspirado en el principio que la informática debe estar al servicio de todo ciudadano, atribuye valor normativo a un propósito importante, que está dirigido a tutelar al individuo en su vida privada, incluso en el sector de las informaciones y proteger al ciudadano de posibles abusos de otros particulares o de la misma Administración; la informática, en otros términos, adquiere la dimensión de un verdadero y propio servicio público y su utilización presupone un control de naturaleza pública[46]. Sin embargo, se advierte que, frente a una compleja legislación sobre control de datos, se presenta, a diferencia del modelo estadounidense y alemán, una escasa jurisprudencia constitucional[47].

(44) Este artículo establece además que podrán, sin embargo, las iglesias y las agrupaciones de carácter religioso, filosófico, político o sindical, llevar un registro de sus miembros o de sus corresponsales en forma automatizada. No se podrá ejercer sobre ellas control alguno por este concepto. Asimismo, por razones de interés público se podrán establecer excepciones a la prohibición anterior a propuesta o previo parecer favorable de la Comisión, mediante decreto acordado en Consejo de Estado.

(45) El mismo numeral prevé que, cuando lo pida el interesado, el servicio u organismo interesado deberá expedir sin gasto alguno, copia del registro modificado. En caso de impugnación, la carga de la prueba corresponderá al servicio ante el cual se ejerza el derecho de acceso, salvo cuando se haya probado que las informaciones impugnadas han sido proporcionadas por el propio interesado o con su consentimiento.

(46) ALPA. Op.cit.; p.247.

(47) ZÚÑIGA URBINA. *Derecho a la intimidad y Hábeas Data (del recurso de protección al Hábeas Data).* En: *Derecho.* Op.cit.; pp.205-206; quien afirma que a partir de la jurisprudencia del Tribunal Europeo de los Derechos Humanos y de una legislación modélica se ha reconstruido un derecho a la vida privada con múltiples facetas (p.219).

2.4 La Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

Esta directiva, que contiene setenta y dos considerandos, tiene como objeto la protección de las libertades y de los derechos fundamentales de las personas físicas y, en particular, el derecho a la intimidad, en lo que respecta al tratamiento de los datos personales (artículo 1.1). Establece como principios básicos los siguientes[48]:

a) Se define como datos personales a toda información sobre una persona física identificada o identificable (el interesado)[49] (artículo 2, inciso a).

b) Se entiende como tratamiento de datos personales (tratamiento) a cualquier operación o conjunto de operaciones, efectuadas o no, mediante procedimientos automatizados y aplicadas a datos personales, como el recojo, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso de los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción (artículo 2, inciso b).

c) Se distingue el responsable del tratamiento (artículo 2, inciso d)[50], del encargado del tratamiento (artículo 2, inciso e)[51].

d) El ámbito de aplicación de la Directiva es el tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero (artículo 3.1)[52].

e) Se establece que los Estados miembros dispondrán que los datos personales sean (artículo 6):

- tratados de manera leal y lícita;
- recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines[53];
- adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
- exactos y, cuando sea necesario, actualizarlos[54];

conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines que se traten ulteriormente[55].

f) Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

- el interesado haya dado su consentimiento de forma inequívoca, o
- es necesario para ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o
- es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
- es necesario para proteger el interés vital

(48) Los datos han sido tomados del *Diario Oficial de las Comunidades Europeas*. Libro 281. Año 38. Del 23 de noviembre de 1995. Edición en lengua española. pp.31-50.

(49) El mismo numeral establece que se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

(50) El cual es definido como: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el derecho nacional o comunitario

(51) Descrito como la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

(52) El mismo artículo prevé que la Directiva no se aplica, entre otros casos, en el tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal. También está fuera de esta Directiva el tratamiento es efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas (artículo 3.2).

(53) Se establece que no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas.

(54) Se prescribe que deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron tratados posteriormente, sean suprimidos o rectificados.

(55) Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

del interesado, o

- es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o

- es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección.

g) Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de datos relativos a la salud o a la sexualidad (artículo 8.1)[56]. Una excepción a este principio, también se constituye cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional, sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente al secreto (artículo 8.3)

h) El tratamiento de datos relativos a las infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro, basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos (artículo 8.5).

i) Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento (artículo 8.7).

j) En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión (artículo 9).

En el caso de la información producto de la obtención de datos recabados del propio interesado, se sigue al modelo francés[57].

(56) Lo dispuesto en este apartado no se aplicará cuando (artículo 8.2):
a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado; o
b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de derecho laboral en la medida que esté autorizado por la legislación y ésta prevea garantías adecuadas; o
c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento; o
d) el tratamiento sea efectuado en el curso de sus actividades legítimas y las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a su miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal que los datos no se comuniquen a terceros sin el consentimiento de los interesados; o
e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

(57) En efecto, el artículo 10 establece que los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:
a) la identidad del responsable del tratamiento y, en su caso, de su representante;
b) los fines del tratamiento de que van a ser objeto los datos;
c) cualquier otra información tal como:
- los destinatarios o las categorías de destinatarios de los datos,
- el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder,
- la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.
Rige una disposición análoga para el caso que la información provenga de datos que no han sido recabados por los interesados (artículo 11.1), estableciéndose un régimen de excepción para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas (artículo 11.2)

k) Al regular el derecho de acceso del interesado a los datos, se establece que los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento (artículo 12):

- libremente y sin restricciones y con una periodicidad razonable y si retrasos ni gastos excesivos:

i) la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;

ii) la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos;

iii) el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones individuales automatizadas a que se refiere el artículo 15;

- en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de esta Directiva, en particular a causa del carácter incompleto o inexacto de los datos;

- la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con el punto anterior, si no resulta imposible o supone un esfuerzo desproporcionado.

l) Se establece como régimen de excepción, frente al principio de la calidad de los datos (artículo 6.1), a las obligaciones en el caso de información obtenida de datos recabados del propio interesado (artículo 10) o que no han sido recabados por el mismo (artículo 11.1), al derecho de acceso (artículo 12) y al principio de publicidad (artículo 21), la salvaguardia de (artículo 13.1)[58]:

- la seguridad del Estado;
- la defensa;
- la seguridad pública;
- la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de deontología en las profesiones reglamentarias;
- un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;
- una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);
- la protección del interesado o de los derechos y libertades de otras personas.

m) Se le reconoce a los interesados el derecho de oposición[59].

n) Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

(58) Asimismo, sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12, cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un periodo que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de elaboración de estadísticas (artículo 13.2).

(59) El artículo 14 establece que los Estados miembros reconocerán al interesado el derecho a:
a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7 (interés público e interés legítimo del responsable del tratamiento de datos, respectivamente), en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos; y
b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho a oponerse, sin gastos, a dicha comunicación o utilización.

(artículo 15.1)[60].

o) Se regula el principio de confidencialidad, al establecer que las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal (artículo 16).

p) En materia de seguridad del tratamiento, los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de datos personales contra la destrucción, accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red y contra cualquier otro tratamiento ilícito de datos personales (artículo 17.1)[61].

q) Los Estados miembros dispondrán que el responsable del tratamiento o, en su caso, su representante, efectúe una notificación a la autoridad de control[62], con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos, total o parcialmente automatizados, destinados a la consecución de un fin o de varios fines conexos (artículo 18.1)[63]. Se establece como posible régimen de excepción, aquellos tratamientos cuya única finalidad sea la de llevar un registro que, en virtud de disposiciones legales o reglamentarias, esté destinado a facilitar información al público y estén abiertos a la consulta por el público en general o por toda persona que pueda demostrar un interés legítimo (artículo 18.3).

r) En materia de controles previos, se prevé que los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados y velarán porque sean examinados antes del comienzo del tratamiento (artículo 20).

s) Los Estados miembros adoptarán las medidas necesarias para garantizar la publicidad de los tratamientos (artículo 21.1).

t) Se establece que sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control instituida en esta Directiva, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garantice las disposiciones del derecho nacional aplicables al tratamiento del que se trate (artículo 22).

u) Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación por el perjuicio sufrido. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputa

(60) Sin embargo, el artículo 15.2, prescribe que los Estados miembros permitirán, sin perjuicio de lo dispuesto en los artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el artículo 15.1, cuando dicha decisión:
a) se haya adoptado en el marco de celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; o
b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

(61) El mismo numeral establece que:
a) En caso de tratamiento por cuenta del responsable del mismo, éste deberá elegir un encargado del tratamiento que reuna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas (artículo 17.2).
b) En caso de tratamiento realizado por encargo, éste deberá estar regulado por contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento y que disponga, en particular (artículo 17.3):
- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento; y
- que las obligaciones del artículo 17.1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

(62) La autoridad de control está prevista en el artículo 28, al establecerse que todos los Estado miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia. La autoridad de control tiene poders de investigación, de intervención y capacidad procesal. Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

(63) Caben excepciones, en las cuales los Estados miembros podrán disponer la simplificación o la omisión de la notificación (artículo 18.2).

el hecho que ha provocado el daño (artículo 23).

v) Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva (artículo 24).

w) Se establece que los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado (artículo 25).

x) Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva (artículo 27).

y) Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, el cual tendrá carácter consultivo e independiente (artículo 29), el cual elaborará, además, un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión. Dicho informe será publicado (artículo 30.6).

z) La Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión (artículo 31).

2.5 La Ley No.675, del 31 de diciembre de 1996, *Tutela delle persone e di altri sogetti rispetto al trattamemto dei dati personali,* de Italia.

La ley de tutela de las personas y de otros sujetos respecto al tratamiento de datos personales, es el producto de una intensa iniciativa por parte de la comunidad jurídica italiana y de ciertos precedentes legislativos. Dentro de las primeras regulación normativas relativas a la tutela de la persona y a la recolección de los datos personales se encuentra el Estatuto de los trabajadores (Ley No.300 de 1970)[64], que prohibe toda forma de control a distancia del trabajador[65]. También la Ley No.382, de fecha 17 de julio de 1978, en materia de prestaciones de servicio militar, establece en su artículo 17, que está prohibido el uso de los archivos de información a efectos de discriminación política de los militares[66]. La Ley No.121, del 01 de abril de 1981, de reforma de la Seguridad Pública, fija una competencia del Ministerio del Interior sobre los bancos de datos personales, en cuanto impone a los entes públicos y privados notificar a este Ministerio la existencia de sus propios bancos de datos[67]. Las normas de carácter reglamentario que disciplinan el uso de las informaciones recogidas por los consejos tributarios (instituidos a efectos de la verificación de la base imponible de las personas naturales, de acuerdo al artículo 10, segundo párrafo, de la ley delegada del 09 de octubre de 1971, No.825 y del artículo 44 del d.p.r. No.600 del 29 de setiembre de 1973) tratan de temperar la exigencia de verificar con la máxima precisión y transparencia posible, la posición fiscal de los contribuyentes, con la finalidad de reprimir la evasión de la obligación tributaria con la exigencia de no lesionar la reserva de los contribuyentes investigados[68].

A nivel de propuestas legislativas, se cuenta con la propuesta de ley de 1981 (proyecto Accame), la propuesta de ley de 1982 (proyecto Picano) y la

(64) Cuyo artículo 8 prohibe las investigaciones sobre las opiniones políticas, religiosas o sindicales del trabajador, así como los hechos que no son relevantes a los efectos de la evaluación de la actitud profesional del trabajador. ICHINO. Citado en la *Introduzione.* En: *Banche dati telematica* ... Op.cit.; p.5.

(65) LOSANO. *I progetti di legge italiani sulla riservatezza dei dati personali.* En: *Banche dati telematica* ... Op.cit.; p.151.

(66) *Introduzione.* Op.cit.; p.7.

(67) LOSANO. Op.cit.

(68) *Introduzione.* Op.cit.; p.8.

propuesta de ley de 1983 (proyecto Mirabelli)[69].

Se puede decir que la Ley No.675, del 31 de diciembre de 1996 es hija, producto de la necesidad impuesta por la Directiva Comunitaria 95/46/CE (por tanto, basada principalmente en sus principios) y del proyecto Mirabelli[70]. Se ha observado que esta ley, no obstante su sectorial terreno de intervención, no indica ninguna fórmula general en materia de violación del derecho a la vida privada, queriendo regular, verdaderamente, controlar, los *data bases*[71].

Sus notas características son las siguientes:

a) En cuanto a su finalidad, se establece que, además de la garantía del tratamiento de los datos personales dentro del respeto de las libertades, los derechos fundamentales de la persona y, en particular, el derecho a la intimidad (como se regula en la Directiva), se protege la dignidad de la persona física y su derecho a la identidad personal. Se amplía el ámbito de protección a las personas jurídicas y otro ente o asociación (artículo 1.1).

b) Se excluye del ámbito de aplicación el tratamiento de datos personales efectuados por personas físicas para fines exclusivamente personales, siempre y cuando los datos no estén destinados a una comunicación sistemática o a la difusión (artículo 3.1).

c) El tratamiento de los datos personales realizado sin el auxilio de medios electrónicos o automatizados está sujeto a la misma disciplina prevista para el tratamiento efectuado con el auxilio de tales medios (artículo 5).

d) El titular[72] que desea realizar un tratamiento de datos personales, sujeto al campo de aplicación de esta ley, está obligado a darle notificación al Garante (artículo 7). En dicha notificación, entre otros requisitos, se deberá indicar el nombre, denominación o razón social, así como el domicilio, la residencia o la sede del responsable[73]; a falta de tal notificación, se considera responsable al notificante (artículo 7.4.h).

e) En materia de calidad de los datos, se siguen los mismos criterios del artículo 6 de la Directiva (lealtad, compatibilidad, pertinencia, exactitud, actualización y conservación) (artículo 9). Si del incumplimiento de esta disposición se deriva un daño al interesado, se establece que también es resarcible el daño no patrimonial (artículo 29.2)[74].

f) No se requiere el consentimiento del interesado cuando el tratamiento se refiere a datos relativos al desenvolvimiento de la actividad económica, recogidos incluso para los fines indicados en el artículo 13, apartado 1, inciso e)[75], dentro del respeto de la normativa vigente en materia de secreto financiero e industrial (artículo 12.1.f).

g) Se le reconocen al interesado los siguientes derechos (artículo 13):

- de conocimiento, mediante acceso gratuito al registro del Garante, de a existencia de tratamientos de datos que se refieran a él;
- de ser informado de las generales de ley del titular y del responsable, así como de las finalidades y modalidades del tratamiento;
- de obtener a cargo del titular o del responsable, sin retardo, la confirmación de los datos que se refieren a él, la lógica o finalidad del tratamiento, la cancelación y la actualización de los datos (de acuerdo a lo establecido por el artículo 12 de la Directiva).

(69) LOSANO. Op.cit.; pp.152-154.

(70) Este proyecto, puede ser definido como una propuesta de modelo jurídico de segunda generación, por cuanto se basa en el sistema de notificación, seguido por un control y se construye la figura del responsable del banco de datos. Se diferencia de los modelos jurídicos de primera generación, que son tendencialmente muy restrictivos, sometiendo a una autorización previa la creación de toda banca de datos y que limitan drásticamente la recolección de los datos sensibles. MIRABELLI. *Banche dati e contemperamento degli interessi.* En: *Banche dati telematica* ... Op.cit.; p.160.

(71) COSSU. *Il diritto alla riservatezza nel nuovo diritto delle banche dati.* En: *Giurisprudenza Italiana.* Año 149. Torino: Dispensa, UTET, diciembre 1997. p.363.

(72) Que es el equivalente al responsable del tratamiento de la Directiva.

(73) Que es el equivalente al encargado del tratamiento de la Directiva.

(74) Recordemos que en el código civil italiano, el artículo 2059 establece que: El daño patrimonial debe ser resarcido sólo en los casos determinados por ley:

(75) En el que se regula el derecho de oposición (por parte del interesado), en todo o en parte, al tratamiento de datos personales que se refieren al mismo, previsto con fines de información comercial o de envío de material publicitario o de venta directa o para el cumplimiento de investigaciones de mercado o comunicación comercial interactiva y de ser informado por el titular, no más allá del momento en el cual los datos son comunicados o difundidos, de la posibilidad de ejercitar gratuitamente tal derecho.

Si estos derechos se refieren a personas muertas, pueden ser ejercitados por quien tenga interés.

h) En caso de cese, por cualquier causa, de tratamiento de datos, el titular debe notificar preventivamente al Garante su destino (artículo 16.1). Los datos pueden ser (16.2):

- destruidos;
- cedidos a otro titular, siempre que estén destinados a un tratamiento para finalidades análogas a las finalidades para las cuales los datos son recolectados;
- conservados para fines exclusivamente personales y no destinados a una comunicación sistemática o a la difusión.

i) Ningún acto o procedimiento judicial o administrativo que implique una valoración del comportamiento humano puede ser fundado únicamente sobre un tratamiento automatizado de datos personales dirigido a definir el perfil o la personalidad del interesado (artículo 17).

j) Quien ocasione daño a otro debido al tratamiento de daños personales está obligado al resarcimiento a los efectos del artículo 2050 del Código Civil Italiano[76].

k) La comunicación y difusión de los datos personales por parte de los privados y de entes públicos económicos son admitidas (fuera de los casos establecidos en el artículo 26 de la Directiva), entre otros supuestos, por los siguientes (artículo 20):

- en el ejercicio de una profesión de periodista o para la exclusiva persecución de finalidades relativas, en los límites del derecho de crónica puestos a tutela de la reserva y en particular de la esencialidad de la información con respecto a los hechos de interés público y en el respeto del código de deontología[77] (inc. d);
- si los datos se refieren al desenvolvimiento de actividades económicas, dentro del respeto de la normatividad vigente en materia de secreto financiero e industrial (inc. e).

l) La comunicación y la difusión de datos está permitida (artículo 21):

- cuando sean necesarias para fines de investigación científica o estadística y se trate de datos anónimos;
- cuando sean solicitadas por determinados entes públicos para fines de defensa o de seguridad del Estado o de prevención, verificación o represión de los delitos, con la observación de normas de la materia.

m) Los datos sensibles pueden ser objeto de tratamiento sólo con el consentimiento escrito del interesado y previa autorización del Garante (artículo 22).

n) Los datos personales idóneos a revelar el estado de salud pueden ser dados a conocer al interesado sólo a través de un médico designado por el interesado o el titular (artículo 23.2). La difusión de estos datos está prohibida, salvo en el caso en el cual

(76) Este artículo establece que: Quien ocasione daño a otro en el desenvolvimiento de una actividad peligrosa, por su naturaleza o por la naturaleza de los medios utilizados, está obligado al resarcimiento, si no prueba haber adoptado todas las medidas idóneas a evitar el daño.

(77) El artículo 25.2 establece que el Garante debe promover, por parte del Consejo nacional de la orden de los periodistas, un código de deontología, respecto de los datos que éstos traten, que prevea medidas dirigidas a la garantía de los interesados, que el Consejo estará obligado a respetar. El artículo 25.2 prescribe que si dentro de seis meses no se ha adoptado el código de deontología por parte del Consejo, se adoptará en sustitución uno elaborado por el Garante, hasta que no se adopte otro diverso.

sea necesaria por finalidades de prevención, verificación o represión de delitos, con la observación de normas de la materia (artículo23.4).

o) Salvo para los datos idóneos a revelar el estado de salud y la vida sexual, no se requiere el consentimiento del interesado cuando el tratamiento de los datos sensibles (artículo 22) es efectuado en el ejercicio de la profesión de periodista y para el logro exclusivo de finalidades relativas, dentro de los límites del derecho de crónica y en particular de la esencialidad de la información con respecto a los hechos de interés público (artículo 25.1)[78].

p) El tratamiento de los datos personales por parte de los sujetos públicos, salvo los entes públicos económicos, está permitido sólo para el desarrollo de las funciones institucionales, en los límites establecidos por la ley y por los reglamentos (artículo 27).

q) La transferencia, incluso temporal fuera del territorio nacional, con cualquier forma o medio, de datos personales objeto de tratamiento debe ser previamente notificado al Garante, cuando esté dirigido a un país que no pertenece a la Unión Europea y se refiere a los datos sensibles y a los relativos a aspectos penales (artículo 28.1). La transferencia está prohibida cuando el ordenamiento del Estado de destino o de tránsito de los datos no asegure un nivel de tutela de las personas adecuado o, si se tratan de datos sensibles o relativos a aspectos penales, de igual grado a aquel asegurado por el ordenamiento italiano. Se evalúan además las modalidades de transferencia y de los tratamientos previstos, las finalidades, la naturaleza de los datos y las medidas de seguridad (artículo 28.4).

r) El tratamiento, así como la cesación del tratamiento de los datos referentes a las personas jurídicas, entes o asociaciones no están sujetas a notificación (artículo 26.1). Tampoco se aplican a los mismos la normatividad establecida para la transferencia de datos al extranjero (artículo 26.2).

s) Los derechos del interesado (regulados en el artículo 13) se pueden hacer valer frente a la autoridad judicial o con recurso al garante. No procede el recurso ante el Garante cuando, por el mismo objeto y entre las mismas partes, se haya recurrido ante la autoridad judicial (artículo 29.1). Asimismo, la presentación del recurso ante el Garante, hace improponible una demanda ulterior frente a la autoridad judicial entre las misma partes y por el mismo objeto (artículo 29.2).

t) Se instituye como autoridad al Garante para la protección de los datos personales, el cual es un órgano colegiado conformado por cuatro miembros, los cuales eligen entre sí un presidente (artículo 30).

u) Se establece un régimen de sanciones penales de prisión y sanciones administrativas. Se prescribe, además, que la condena por uno de los delitos previstos por esta ley importa la publicación de la sentencia (artículo 38).

Frente a este modelo jurídico, se afirma que la situación de absoluta libertad ahora se invierte: tendencialmente las informaciones, incluso las de los registros administrativos, entregadas por una persona en una determinada situación, ya no pueden ser utilizadas con fines diversos, si no es con el consentimiento del interesado. En particular las instituciones bancarias y de seguros, depositarias de amplia información, deberán modificar profundamente sus comportamientos, aunque sea fácil prever obstinadas resistencias y tentativas de evasión de la nueva normatividad, trámite la predisposición de cláusulas de estilo que se harán suscribir al cliente[79].

3 El Sistema jurídico latinoamericano: ¿Tratamiento de datos personales o *habeas data*?

3.1 Sobre los momentos fisiológico y patológico del tratamiento de datos personales.

Cuando nace un niño, los padres (orgullosos de su **obra maestra**), se dedican a la complicada tarea

(78) Los límites de este derecho de los periodistas deben ser interpretados sistemáticamente con los artículos 25.2 y 25.3, detallados en la nota anterior.

(79) COSSU. Op.cit.; p.375. Hipótesis semejante, en la cual se pretenda, mediante una cláusula predispuesta unilateralmente eludir o limitar responsabilidad por los daños derivados a los derechos de la persona, configura lo que se denomina una cláusula vejatoria, la cual sería atacada de nulidad. Sobre el particular, permítaseme remitir a ESPINOZA ESPINOZA, Juan. *Las cláusulas vejatorias en los contratos estipulados unilateralmente.* En: *Thémis.* Segunda Epoca. No.38. Lima, 1998. pp.141-162.

de ponerle un nombre y en esta decisión, que para muchos puede pasar inadvertida, se revela su manera de ser. En efecto, aparte de los aquellos que -tradicionalmente- le ponen al niño o niña, el nombre del padre o de la madre, hay quienes prefieren poner un nombre de moda, otros un nombre extranjero, algunos optan por un nombre totalmente oriundo y no pocos se esfuerzan en escoger un nombre original, llegando algunos a inventar un nombre: tengo la sensación que esto ha ocurrido con el denominado *habeas data* en el sistema jurídico latinoamericano.

Sin embargo, en este caso, el orgullo del doctrinario o del legislador, no ha tenido medida: al crear (o reconocer) a este nuevo hijo (que, en todos los ordenamientos precedentes que hemos visto, tiene en común una tutela pormenorizada y no este nombre), no sólo se le ha pretendido perennizar con esta identificación (que llamaríamos, original), sino que cada padre le ha dado un contenido, o percepción, diversos: así tenemos que para algunos es un derecho[80] para otros es una garantía[81], cuando no una acción[82] o un proceso constitucional[83].

Esto, como sistema jurídico, nos crea no pocos problemas; porque, aparte de protagonizar un pasaje de *Cien años de soledad*, en el cual los pobladores de Macondo, por extrañas circunstancias, tenían objetos cuidadosamente etiquetados; pero no recordaban para qué servían, genera un serio obstáculo para un fluido intercambio de datos personales más allá de las fronteras de cada país. En efecto, es un principio básico el de no autorizar la transmisión de datos fuera del país, si en el país destinatario no se garantizan las mismas seguridades en el tratamiento, difusión y conservación de esos datos.

No es mi propósito criticar el nombre escogido para este niño[84], sino el de establecer una suerte de mínimo conceptual común entre los países de nuestro sistema, el cual (ya contando con la ventaja de tener -casi- un idioma común) resultaría imperativo, para pasar de una etapa de **regulación nacional** hacia otra de **regulación comunitaria**, en materia de protección jurídica al tratamiento de datos personales.

La regulación pormenorizada a nivel legislativo de los países que nos llevan por delante una gran

(80) Pareciera percibirse este concepto, cuando se lee que: la libertad informática encierra así un derecho de autotutela de la propia identidad informática, cuya primera exigencia es la protección de los datos informáticos personales frente a aquellas personas no autorizadas para conocerlos, procesarlos, modificarlos o difundirlos, razón por la que, como una vez más señala Frosini, el primero de los contenidos cuya normación viene exigida por la efectividad de la nueva libertad es el del acceso al banco de datos, con el fin de, por un lado, poder disponer de toda la información almacenada en un archivo electrónico sobre la propia personalidad y, por otro, poder rectificar ciertos datos concernientes a la misma. Nace así el Hábeas Data. FERNÁNDEZ SEGADO. *El régimen jurídico del tratameinto autorizado de los datos de carácter personal en España.* En: *Derecho.* No.51. Lima: PUCP, diciembre de 1997. p.9.

(81) Así, cuando se sostiene que es una de las garantías constitucionales más modernas, definiéndola como el derecho que asiste a toda persona -identificada o identificable- a solicitar judicialmente 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; a requerir la rectificación, la supresión de datos inexactos u obsoletos que impliquen discriminación (por ejemplo, la confesión religiosa, si el registro no tiene por objeto constatar tal situación). Esta herramienta tiende a proteger a la persona contra **calificaciones sospechosas** incluídas en registros (especialmente estatales, aunque también pueden serlo privados) que, -sin darle derecho e contradecirlas- pueden llegar a perjudicarle de cualquier modo. EKMEKDJIAN y PIZZOLO. *Hábeas data. El derecho a la intimidad frente a la revolución informática.* Buenos Aires: Depalma, 1996. pp.1-2. En este mismo sentido, MORALES GODO. *El derecho a la vida privada y el conflicto con la libertad de información.* Lima: Grijley, 1995. p.241.

(82) La Constitución del Perú de 1993, en su artículo 200, inciso 3, regula la Acción de Hábeas Data. Sobre su origen, ver TORRES Y TORRES LARA. *Derechos Humanos e Informática. La Constitución de 1993, la Informática y el hábeas data.* En: *Ius et Praxis.* No.26. Lima: Universidad de Lima, enero-diciembre, 1996, quien afirma que la denominación podría no ser la más apropiada (p.23).

(83) SAGÜES. *El hábeas data: alcances y problemática.* En: *El Derecho Público Actual.* Homenaje al profesor Dr. Pablo A. Ramella. Buenos Aires: Depalma, 1994. p.179. Se alinea también en esta posición Gozaíni, quien opina que la función básica del hábeas data es asegurar el acceso a las bases de datos y demás registraciones que se tengan de una persona, determinando con ello la posibilidad de suprimir, rectificar, modificar o actualizar la información que allí se contenga.
Es, en suma un derecho de entrada a los bancos de información en vías de obstruir la afectación de los derechos de la personalidad del hombre, en cuyo caso corresponde acceder al control de exactitud como un dato que debe ser puesto al día para su conocimiento (cuando se autoriza su difusión), o impedido para su publicidad (en el caso del derecho al secreto para los datos sensibles). GOZAÍNI. *El Derecho de Amparo. Los nuevos derechos y garantías del artículo 43 de la Constitución Nacional.* 2a.ed. Buenos Aires: Depalma, 1998. p.224.
García Belaunde, quien parte de la premisa del problema de terminología que encierra el *habeas data*, establece que el mismo no es acción sino proceso constitucional, porque la acción es algo abstracto, que sirve para iniciar algo, pues la acción en sí misma no es nada. GARCIA BELAUNDE. *Sobre el Hábeas Data y su tutela.* En: *Derecho.* Op.cit.; p.51.

(84) Así, se afirma que la locución *habeas data* es un préstamo poco ceremonioso a la historia. FALCON. *Habeas data. Concepto y procedimiento.* Buenos Aires: Abeledo-Perrot, 1996. p.23.

experiencia en tutela del tratamiento de los datos personales, fue recogida a nivel constitucional por primera vez, aparentemente, en el artículo 35 de la Constitución de Portugal de 1976, después en los artículos 18.4 y 105, b, de la Constitución de España de 1978 (no utilizándose el nombre de *habeas data*). Recién en el artículo 5, inciso LXXII, de la Constitución de Brasil de 1988, se le pone el nombre propio al niño. De aquí se generó la confusión (tanto legislativa, doctrinaria como judicial). Los esfuerzos por parte de la doctrina en clasificar el denominado *habeas data* han sido notables. Así tenemos un sector[85] que lo clasifica, en función de lo que se pretende respecto de los propios datos personales que se encuentren en un registro, de la siguiente manera:

a) Habeas data informativo (que comprende el habeas data exhibitorio, el habeas data finalista y el habeas data autoral).

b) Habeas data aditivo.

c) Habeas data rectificador.

d) Habeas data reservador.

e) Habeas data cancelatorio.

Otro sector[86] distingue habeas data propio o tradicional, entendido como la garantía que tiende a operar sobre los datos personales, del habeas data impropio, que pretende constituirse en medio para la obtención de información pública.

En materia de tutela de los datos personales es imperativo distinguir el momento fisiológico (reconocimiento de los derechos materiales que se tienen sobre los datos personales), del momento patológico (mecanismos procesales de tutela frente a la (o amenaza de) lesión de estos derechos). El ámbito del *habeas data* (si queremos denominarlo así), debe estar reservado para este último momento, debiéndolo entender como el cauce procesal para salvaguardar la libertad de la persona en la esfera informática[87].

Es necesario delimitar el ámbito de ambos momentos. Para el caso del momento fisiológico, se debe responder a la pregunta ¿Qué derecho (o derechos) se debe (o se deben) proteger? No hay respuesta unívoca: algunos hablan del derecho a la intimidad, otros de la identidad, o de ambos[88], no faltan quienes le añaden el adjetivo de informáticas[89] y hay quienes proponen configurar el derecho a la autodeterminación informativa[90]. Asimismo, se presenta la disyuntiva si se trata de un derecho individual o de un derecho constitucional[91].

En mi opinión, partiendo de la premisa de la unicidad del fundamento de los derechos de la persona, el cual, como ya lo señalamos, reside en la realización del proyecto vital de existencia del ser humano, en materia de protección jurídica de los datos personales, debido a la vasta complejidad de la informática, la cual puede comprometer derechos insospechados (como la imagen y la voz), debemos conferir una tutela amplia a todos los derechos de la persona, lo cual no impide que se le dé particular atención a uno (o algunos) de ellos. El reconocimiento del principio de tutela de (todos los) derechos de la persona frente a la informática podría

(85) SAGÜES. El *Habeas data en Argentina (Orden nacional)*. En: *Gaceta Jurídica*. Tomo 57. Lima, agosto de 1998. pp.58-A y 59-A.

(86) PUCCINELLI. *El habeas data en el constitucionalismo indoiberoamericano finisecular*. En. *El amparo constitucional. Perspectivas y modalidades (artículo 43 de la Constitución Nacional)*. Buenos Aires: Depalma, 1999. p.189.

(87) FALCON. Op.cit.; p.29. Dentro de esta óptica se sostiene que: cae por su propio peso que el Hábeas Data es una figura procesal para la defensa de determinados derechos, que es propia de la disciplina que algunos conoce, estudian, divulgan, etc., como Derecho Procesal Constitucional. Lo que pasa es que su manejo, su ejercicio es procesal, pero sus fundamentos constitucionales. Lo cual no impide, que los constitucionalistas lo estudien y practiquen. GARCÍA BELAUNDE. Op.cit.; p.52.

(88) PARELLADA. *El derecho de la persona y la informática*. En: *Derecho Civil*. Ponencias presentadas en el Congreso Internacional celebrado en Lima del 16 al 18 de noviembre de 1989, organizado por la Facultad de Derecho y Ciencias Políticas de la Universidad de Lima, 1992, quien sostiene que una legislación específica protectora de los derechos a la identidad personal y a la intimidad que asuma el fenómeno informático debe partir del reconocimiento de que la dignidad de la persona humana exige que ésta no pueda ser reducida a un conjunto de datos. De tal premisa deben extraerse los derechos que le corresponden y establecerse los mecanismos garantistas de vigencia de los mismos (p.225).

(89) Vega Mere, cuando habla de identidad informática. VEGA MERE. *Intimidad, identidad e informática. A propósito de la Constitución peruana de 1993*. En: *Ius et Praxis*. Op.cit.; p.57.

(90) LUCAS MURILLO DE LA CUEVA. *La protección de los datos personales ante el uso de la informática*. En: *Diez años de desarrollo constitucional. Estudios en homenaje al Profesor Don Luis Sánchez Agesta*. En: *Revista de la Facultad de Derecho de la Universidad Complutense*. No.15. Monográfico. Madrid, 1989. p.614, quien sigue el *decisum* de la sentencia del Tribunal Constitucional Federal Alemán, de fecha 15 de diciembre de 1983.

(91) Como observan CORREA, NAZAR ESPECHE, CZAR DE ZALDUENDO y BATTO. Op.cit.; p.246.

tener una *sedes materiae* constitucional, civil o especial. Creo que se ha dado un paso importante con el reconocimiento constitucional, por parte de algunos países (aunque con muchos matices) de este principio[92]: es hora de elevarlo a nivel de legislación uniforme en todo el sistema.

A nivel del momento patológico, debemos responder a la pregunta de ¿Cómo defiendo mis derechos? Es aquí en donde irrumpen todos los mecanismos que permiten que la tutela frente al tratamiento de los datos personales sea efectiva y no se convierta en retórica inútil, entre los cuales tenemos, a título ejemplificativo[93]:

a) el derecho de acceso a la información;

b) el derecho a la rectificación o cancelación de datos inexactos o caducos;

c) el derecho de exigir que los datos sean utilizados conforme con el fin para el cual fueron recogidos;

d) el derecho de inserción de la información personal, de bancos de datos, si es presupuesto para la obtención de alguna prestación;

e) el derecho a que no se emita un juicio de valor judicial, administrativo o privado fundado en un tratamiento informatizado de informaciones que suministren una definición del perfil o de la personalidad del interesado[94].

Como bien sabemos, estos derechos -como todos los demás- pueden ser entendidos bajo la perspectiva de una relación jurídica sustancial como de una relación jurídica procesal[95]: este último ámbito es el que -a mi entender- correspondería al denominado *habeas data*.

3.2 Algunos principios a tenerse en cuenta.

Basándonos en la Convención del Consejo de Europa del 28 de enero de 1991, para la protección de las personas en relación a la elaboración automática de datos de carácter personal y la Recomendación de la Organización de Cooperación y Desarrollo Económico (OCDE), del 23 de setiembre de 1980, que se refiere a las líneas directivas sobre la protección de la vida privada y la circulación transnacional de los datos de carácter personal[96]:

a) el principio de corrección, en la recolección y en el tratamiento de las informaciones;

b) el principio de la exactitud en los datos recogidos, a los cuales se acompaña la obligación de su actualización;

c) el principio de la finalidad de la recolección de datos, que debe ser conocida antes que la recolección

(92) Así, Argentina, Brasil, Colombia, Guatemala, Paraguay y Perú. PUCCINELLI. *Tipos y subtipos de Hábeas Data en el Derecho Constitucional Latinoamericano, con especial referencia al caso peruano*. En: *Diálogo con la Jurisprudencia*. No.5. Año III. Lima, 1997. pp.29-30.

(93) Los incisos comprendidos entre los puntos a) y d), han sido tomados de las conclusiones del Primer Congreso Internacional de Derecho de Daños, en homenaje al Prof. Dr. Jorge Mosset Iturraspe, realizado en 1989, en *El Derecho Privado en la Argentina. Conclusiones de Congresos y Jornadas de los últimos treinta años*. Buenos Aires: Universidad Notarial Argentina, 1991. p.287.

(94) Tomado de la legislación francesa.

(95) Así, se explica que: La existencia de un caso justiciable, es decir, de una cuestión jurídica, supone la presencia de dos o más sujetos de derecho que participan entre sí de un conflicto de intereses con relevancia jurídica. Esa relación existente entre los futuros litigantes, base material para la existencia de un proceso judicial, recibe el nombre de **relación jurídica sustancial**. Es precisamente esta relación la que permite a uno de sus conformantes tener una pretensión material respecto del otro. Pues bien, esta relación jurídica sustancial, llamada también **material**, y caracterizada por ser conflictiva, es el antecedente directo del proceso. Precisamente, este no es otra cosa que una rama de relaciones en donde se reproducen los argumentos y medios probatorios de los sujetos en conflicto.
Este nuevo ambiente en donde la relación jurídica sustancial es discutida, hecho que ocurre ante la presencia y dirección de un tercero y en condiciones civilizadas, se denomina comúnmente **proceso o relación jurídica procesal**.
Atendiendo a los conceptos antes expresados, el tránsito de la relación jurídica sustancial a la relación jurídica procesal o proceso ocurre como consecuencia del ejercicio del derecho de acción por parte de uno de los litigantes, en mérito del cual este solicita al Estado tutela jurídica.
Finalmente, es necesario precisar que la existencia de una relación jurídica procesal no elimina o desaparece la relación jurídica sustancial. Esta -en tanto expresión de la realidad concreta- se mantiene como tal. Inclusive es perfectamente posible que las partes, a pesar de tener un proceso iniciado -una relación jurídica procesal establecida- puedan llegar a un acuerdo prescindiendo de este,o , de otro lado, es factible también que uno de los sujetos de la relación sustancial pueda, después de iniciado el proceso, transmitir su derecho o posición en la relación material a otro, quien procederá a actuar en este. Esta última institución se denomina **sucesión procesal**. MONROY GÁLVEZ *Introducción al Proceso Civil*. Tomo I. Santa Fe de Bogotá: Temis-De Belaúnde & Monroy, 1996. pp.121-122.

(96) Tomados de RODOTÀ. *Tecnologie e diritti*. Bologna: Il Mulino, 1995 pp.62-63.

sea hecha y que se especifica en lo siguiente:

- la relación entre los datos recolectados y finalidad perseguida (principio de pertinencia);
- la relación entre la finalidad de la recolección y utilización de los datos (principio de la utilización no abusiva);
- la eliminación o la transformación de datos anónimos, de las informaciones que ya no son necesarias (principio del derecho al olvido);

d) principio de la publicidad de los bancos de datos que tratan de informaciones personales, las cuales deben estar reguladas bajo el régimen público;

e) principio de acceso individual, a efectos de conocer las informaciones personales que hayan sido recogidas, obtener copia, solicitar la corrección de aquellas erradas, la integración de los datos incompletos, la eliminación de aquellas obtenidas ilegítimamente;

f) principio de seguridad física y lógica de la recolección de datos.

4 A manera de conclusión.

Se ha observado con certeza que la importancia adquirida por la elaboración electrónica de los datos informativos es tal, que hoy la sociedad tecnológica es definida como sociedad informática(97). Es por ello que, quienes de una u otra manera, estamos vinculados con el quehacer jurídico debemos asumir una conciencia informática y promover que ésta se extienda a la población(98).

La tutela de la persona frente al tratamiento de los datos informáticos (y también mecanizados, cuando no sean de uso personal) no sólo debe limitarse al sujeto individualmente considerado, sino también en su dimensión de coexistencialidad, vale decir, como integrante de alguna formación social: es por ello que se debe ampliar la tutela de datos personales también a las personas jurídicas y demás sujetos de derecho colectivos, obviamente, en lo que le fuera aplicable(99).

Un aspecto que no puede pasar desapercibido es el del **costo** de la protección de los datos. En efecto, sería extremadamente peligroso evaluar en abstracto la tutela acordada por la ley a las personas. Se correría el riesgo de crear una ley perfecta; pero ineficaz, por cuanto la complejidad de los controles (y, por consiguiente, su costo) acabaría por empujar a las empresas a violar las normas, sujetándose a una eventual condena. Tarea asaz ardua y difícil es la de balancear la economía de la gestión de las empresas que traten datos personales y la tutela que merecen los derechos de las personas(100).

Frente a esta situación, el jurista debe estar atento, meditar sobre las nuevas necesidades que demanda la sociedad y diseñar modelos jurídicos producto de una seria y no apresurada evaluación de los intereses en conflicto. Es por ello que concluyo con el siguiente llamado de atención: muchos tienen prisa, invocando respuestas definitivas y tal vez, tratan de imponerlas. Pero la realidad no es sólo mutable y como tal escapa continuamente de los esquemas en los cuales se desearía encerrarla: es además extraordinariamente rica, y no puede quedar comprendida dentro de las viejas categorías. Por ello se requieren análisis pacientes, reconocimientos puntuales de las nuevas cuestiones, antes de correr hacia soluciones apresuradas e ineficientes(101).

(97) FROSINI. *Diritto alla riservatezza e calcolatori elettronici*. En: *Banche dati telematica* ... Op.cit.; p.31.
(98) LOSANO. *La legislazione tedesca sulla protezione dei dati individuali*. Op.cit.; p.288.
(99) Así, aunque de manera limitada, cuando se afirma que: la tutela de la reserva no se puede limitarse a las personas individualmente consideradas, excluyéndolas de las formaciones sociales de las cuales forman parte y en las cuales realizan plenamente su personalidad, aunque en forma colectiva y anónima. FROSINI. *Linformatica e la Pubblica Amministrazion*. En: *Banche dati telematica* ... Op.cit.; pp.141-142.
(100) LOSANO. Op.cit.; p.291.
(101) RODOTÀ. Op.cit.; p.9.