DERECHO PROCESAL CONSTITUCIONAL

Por OSVALDO ALFREDO GOZAÍNI

HÁBEAS DATA

Protección de datos personales

CAPÍTULO I. Fundamentos de la protección constitucional

1. Introducción

El hábeas data tiene una doble consideración. A veces se lo trata como derecho constitucional de las personas con raíces en el derecho a la intimidad; en otras, se atiende su función como garantía o proceso constitucional originado en la reforma de nuestra Ley Fundamental *.

En ambas cuestiones, el punto de partida puede ser correcto aunque debe tenerse en cuenta que es el producto de una serie de transformaciones y evoluciones que de soslayarse, produce inconsistencias claras en la explicación del fenómeno que reproduce el mentado proceso constitucional.

En efecto, observemos como punto de partida el objeto de esta garantía procesal o los contenidos de este nuevo derecho, según la tutela que se pretenda abordar, y de inmediato aparecen sucesivas alternativas. El hábeas data, dicen algunos, protege el derecho a la intimidad; pero al mismo tiempo, se afirma que la defensa es de la privacidad, o de la dignidad humana, o el derecho a la información, o bien, la tutela del honor, o de la propia imagen o perfil personal, o el derecho a la identidad, o simplemente acotado a la autodeterminación informativa. Como se ve, son multifacéticas y distintas las proyecciones en cada caso. De allí lo necesario de efectuar algunas consideraciones previas, antes de entrar a analizar puntualmente el texto legal sancionado.

> La preocupación, en los términos actuales, por la intimidad es el resultado de un largo proceso histórico de transformación de la conciencia que comienza con la contrarreforma, pasa por la desvalorización de la conciencia religiosa por los filósofos del siglo XVII (Hobbes, Locke, Descartes, Spinoza) y desemboca en la construcción de la conciencia moral, preparada por Thomasius y concluida por Kant. Con éste la libertad del hombre es la que permite enjuiciar por sí mismo sus acciones y determinar su voluntad a partir de una inclinación a la moralidad que le es innata. Sobre esta concepción del hombre –agrega Juan Manuel Fernández López- adquiere sentido la noción actual de intimidad como atributo necesario de su nuevo *status* de libertad-autonomía. La dualidad de la persona (interioridad y socialidad) se traslada a la intimidad que es bidireccional: *ad se* y *ad alteros*. La intimidad si bien hace referencia primariamente a un espacio propio, privativo del individuo, éste solo adquiere su pleno sentido frente a los otros, tanto para oponerlo a ellos como para compartirlo con los demás. Así, la intimidad es simultáneamente condición de la personalidad individual y de la personalidad social.

2. Diferencias previas a los fines de precisar los derechos contenidos

Si pretendemos determinar de qué se ocupa el proceso y esclarecer cuáles son sus contenidos mínimos y esenciales, es preciso tener en cuenta que existía antes de la reforma constitucional, cómo va

definiendo la jurisprudencia cada uno de los capítulos agregados, de qué manera influyen los tratados y normas de derechos humanos *, y cómo los ha regulado nuestra Constitución Nacional y la nueva ley de protección de datos personales.

Este encadenamiento permitirá resolver qué se puede hacer a través del hábeas data y dónde existirán límites; teniendo en cuenta que puede diferir la interpretación según se considere al instituto como proceso constitucional o como derecho fundamental de las personas.

> En efecto –dice Herrán Ortiz-, si se quiere delimitar el contenido esencial de éste o cualquier otro derecho fundamental, antes es preciso definir los intereses jurídicos o bienes que se encuentran en su ámbito de tutela. Así, por lo que respecta al derecho a la autodeterminación informativa, los instrumentos o medios directamente relacionados con la protección de la intimidad personal y familiar, el honor y el pleno ejercicio de los derechos, comprenden su contenido esencial. No cualquier aspecto o garantía o garantía de la protección de datos integra el contenido esencial del citado derecho,….[ ], aquél se circunscribe al conjunto de instrumentos o garantías indisponibles en una defensa de los intereses jurídicos propios o naturales de este derecho. ¿Con qué fin se garantizará el derecho a la protección de la persona frente a la informática si no se reconoce el derecho del afectado a estar informado de los datos que serán objeto de tratamiento automatizado?. Por ello, junto al derecho de información del afectado de los diversos aspectos relacionados con el tratamiento informático de los datos, otras facultades de obligado reconocimiento serán: la necesidad de contar con el consentimiento del afectado para el tratamiento de sus datos, la posibilidad de exigir la cancelación o rectificación de datos inexactos o incompletos o, el derecho a exigir que el tratamiento de la información se adecue a unos fines legítimos previamente determinados. Estas facultades constituyen las principales garantías que dan vida y sentido al derecho a la autodeterminación informativa, sin ellas no sería posible asegurar el respeto a los derechos individuales que se amparan bajo la protección de datos personales.

Asimismo, es de advertir que, tal como sucede en los sistemas para el control de constitucionalidad, también en esta materia las aguas se dividen en dos direcciones.

Mientras Europa persigue la defensa de la persona a través de normas que especifiquen los límites del Estado y de los particulares para el tratamiento de los datos; en Estados Unidos, principalmente, no hay políticas constitucionales sobre el tema, prefiriendo la revisión judicial de aquellos actos que agreden, eventualmente, el derecho a la privacidad (por eso lo de incluir el aborto dentro de la esfera íntima de la mujer) y que dieron lugar en el año 1974 a la *Privacy Act.**.

En términos parecidos, la distinción que hacen los primeros entre derechos personalísimos (titular de los datos) y portadores o administradores de ellos (bancos de datos), busca ampliar el panorama de derechos de las personas y limitar el uso de los datos que tienen las empresas cuando está ausente el consentimiento del titular para la aplicación de ellos a un fin determinado.

En cambio, la jurisprudencia americana *, amplia y generosa en este capítulo de derechos fundamentales, perfila un cuadro sucesivo de protecciones que inician desde el famoso "*right to be alone*" (derecho de ser dejado a solas), atraviesa las relaciones con la prensa y los medios de comunicación y culmina con la tutela de los datos que se recopilan con medios informáticos.

> Es muy aconsejable el trabajo de Bianchi publicado en ED, 161-866 y ss., donde explica que en los Estados Unidos la protección del derecho a la privacidad (*right of privacy*) abarca numerosos casos, así como profusa doctrina. Aunque el problema siempre gira sobre el concepto que encierra la conocida cita del Juez Louis D. Brandeis según la cual privacidad significa el derecho "de ser dejado a solas". Ahora bien, agrega Bianchi, si queremos remontarnos a los orígenes del derecho a la privacidad advertiremos en primer lugar que se trata de una historia típicamente angloamericana. Asimismo y con fines metodológicos, es susceptible de ser dividida en cuatro períodos. El primero corre desde los orígenes del

> *common law* hasta el año 1890, fecha en que fue publicado un célebre artículo de Warren y Brandeis…, el segundo período que se extiende hasta un ensayo publicado en 1960 por William Prosser, está referido principalmente a los problemas suscitados entre la privacidad y la prensa. El tercer período –donde el eje de la *privacy* se traslada de los Estados Unidos a Inglaterra- comienza con el proyecto de ley elaborado por Lord Mancroft y enfoca los conflictos entre la privacidad y los medios masivos de comunicación (*mass media*). El cuarto período, finalmente, empieza en 1969 con el proyecto de ley de Walden, en el cual aparece por primera vez el problema de la tutela de los datos personales memorizados por ordenadores.

En la doctrina comparada se advierten también algunas polaridades. Mientras algunos fundamentan la necesidad de proteger al derecho desde la Constitución y con la creación de una garantía específica; otros sostienen que solamente se trata de problemas vinculados con la denominada "libertad informática" que pueden resolverse a través de leyes claras y precisas.

Nuestro país no se ubica en ninguno de los supuestos, pues el hábeas data se incorpora como herramienta destinada a controlar el uso de los datos que se tienen sobre las personas, sin tener específicamente contemplado el derecho, aunque pueda extraerse de otros similares (art. 19) o implícitos (art. 33). Inclusive, algunos autores argumentan que no es el párrafo agregado en el artículo 43 un derecho nuevo, sino una recreación de la defensa existente en el artículo 18 para la correspondencia epistolar y los papeles privados.

La Corte Suprema de Justicia de la Nación, en el caso "Urteaga"* al que referiremos más adelante, coloca un hito trascendente que modifica el entramado constitucional, pues proyecta la figura hacia otros destinos, avizorando, en consecuencia, la necesidad de tener una ley procesal reglamentaria del hábeas data; y otras normas que se ocupen del tratamiento de los datos y sus posibles interferencias en la vida de las personas.

> Para Gutierrez Castro, una apreciación global del instituto conduce a afirmar que tiene un radio de acción decididamente amplio, probablemente excesivo, después de este pronunciamiento del superior tribunal. La meta natural es proteger a las personas de los excesos del poder informático y no, en términos generales, por cualquier lesión que se infiera, por cualquier medio, a su honor, privacidad o propia imagen, o a la intimidad familiar o la voz.

3. Diferencias con el hábeas corpus

La figura del hábeas corpus tiene fuerte influencia en el hábeas data. No se trata, únicamente, de aplicar similitudes de nombre, sino de señalar que así como una persona tiene derecho a la plenitud de su libertad corporal, también se debe reconocer el derecho a disponer de sus propios datos, sea como atributos de la personalidad, o en su calidad de ciudadano que lo convierte en un ser social.

La libertad consecuente caracteriza ambos derechos, y en sí mismo, es un poder del hombre sobre la naturaleza y sobre la sociedad para oponerse a cualquier acción que posibilite un límite a su condición natural.

Por ello la libertad tiene una connotación que excede la libertad física, o de movimientos, o de defensa para evitar detenciones arbitrarias o prisiones sin causas, o en definitiva, de cualquier cercenamiento a los derechos humanos. La libertad también se ocupa de otras situaciones subjetivas de naturaleza defensiva, como son, la libertad de expresión, de información, de conciencia, de religión y culto, de asociación, etc., las que potencialmente persiguen anular las restricciones a través de acciones precisas como son los procesos constitucionales.

El hábeas data sirve a la defensa del hombre en la era informática, así como el hábeas corpus puso límites al Estado para consagrar la libertad física o de movimientos de las personas.

El paralelismo es evidente, por ejemplo, el derecho de acceso a los bancos de datos persiguiendo reconocer la información personal que se tiene archivada, se parece a la acción exhibitoria del hábeas corpus.

> Sostiene Perez Luño que el hábeas corpus surge como réplica frente a los fenómenos abusivos de privación de la libertad física de la persona, que había conturbado a la antigüedad y el medioevo proyectándose a través del absolutismo hasta las diversas manifestaciones totalitarias de nuestros días. El hábeas corpus aparece como un recurso procesal por el que se solicita del Juez que se dirija al funcionario que tiene una persona detenida y la presente ante él. Se trata, por tanto, de una garantía judicial específica para la tutela de la libertad personal. Al cotejar el hábeas corpus y el hábeas data se comprueba una inicial coincidencia en lo referente a su naturaleza jurídica. En ambos casos no se trata de derechos fundamentales, *stricto sensu*, sino de instrumentos o garantías procesales de defensa de los derechos a la libertad personal, en el caso del hábeas corpus, y de la libertad informática en lo concerniente al hábeas data. El hábeas corpus y el hábeas data representan, además, dos garantías procesales de aspectos diferentes de la libertad. Así, mientras el primero se circunscribe a la dimensión física y externa de la libertad; el segundo tiende a proteger prioritariamente aspectos internos de la libertad: la identidad de la persona, su autodeterminación, su intimidad…Si bien no debe soslayarse que, en las sociedades informatizadas actuales, también la libre actuación pública de los ciudadanos se halla condicionada por sus posibilidades de acceso a la información.

La proximidad también se advierte en algunas legislaciones de provincia, como es el caso de Mendoza que regula el hábeas data dentro del código procesal penal, aplicando la reglamentación del hábeas corpus para el trámite dispuesto (lo que origina algunas controversias en punto a la competencia judicial, bilateralidad eventual o mínima contradicción, legitimación para actuar, etc.).

> La corte mendocina ha sostenido lo siguiente: ”Esta fuera de discusión la similitud terminológica de ambas figuras, aunque debe recordarse que la expresión hábeas data no fue usada por el constituyente argentino, pero sí por el brasileño. Además de esa semejanza, la doctrina marca las siguientes: así como a través del hábeas corpus se reclama que se traiga el cuerpo (que se lo exhiba, que se lo presente) en el hábeas data lo que se impetra es que se traigan los datos. Mientras la finalidad del hábeas corpus es indagar los motivos de la privación de la libertad, la del hábeas data reside en la posibilidad de verificar la exactitud, actualidad y pertinencia de los datos. La ilegalidad de la detención debe cesar de inmediato; también debe cesar de inmediato el dato inexacto, desactualizado, etc….” (Suprema Corte de Justicia de Mendoza, en pleno, noviembre 17/997, in re “Costa Esquivel, Oscar c/ CO.DE.ME”, publicado por Jurisprudencia Argentina, semanario del 8 de Julio de 1998, pág. 31 y ss.).

Inclusive, nuestros diputados en la convención constituyente expusieron que el hábeas data era un complemento del hábeas corpus, o bien, “un desprendimiento acorde con los tiempos que vivimos del ya secular y universal hábeas corpus” (Diputado Cafiero). *

> No obstante, debemos recordar que el “Pacto de Olivos” no había previsto el tratamiento de las garantías personales contra los avances de la informática, de forma tal que el instrumento que propicia el “hábeas data” era un tema no habilitado. Razón por la cual, como lo sostiene buena parte de la doctrina y, especialmente el trabajo de Alvarez Larrondo, los convencionales se vieron compelidos a presentar la figura bajo análisis, como desprendimiento de las otras figuras cuyo planteamiento se encontraba habilitado.

De todos modos, existen severas críticas a la utilización de parecidos entre figuras que, por su origen y naturaleza, son absolutamente diferentes.

No debemos olvidar que el clásico instituto del derecho a la locomoción surge en 1215 con la *Carta Magna* como una clara manifestación en pro de la libertad corporal, ratificada en 1679 con el hábeas corpus. Traer el cuerpo, tenía un significado para el Juez y también para quien lo requería. En ambos casos, se puede encontrar funciones similares en el hábeas data, pero tiene más sentido privilegiar la pretensión de quien

reclama antes que asegurar el conocimiento judicial, de forma tal que los objetivos de ambas garantías serían diferentes.

En efecto, la libertad física es producto de un tiempo muy distinto de la era informática; son diversas las agresiones recibidas en la esfera de los derechos personales y hasta se podría afirmar que en el hábeas data no es preciso tener lesión constitucional alguna, en la medida que uno de los aspectos tutelados en la dimensión protectora es el derecho a conocer los datos que se tienen sobre uno mismo.

> En tal sentido, afirma Othon Sidou que el hábeas corpus persigue la exhibición de la persona encarcelada para que el Juez tome contacto con ella y conozca los motivos de la prisión; mientras que el hábeas data, no es una propiamente una exhibición de los datos ante un Juez y mucho menos para que él pueda apreciarlos. La valoración de esas informaciones, registro de datos por el órgano juzgador, en el caso, se torna absolutamente secundario respecto a la fase inicial que ordena traer (hábeas); pues lo que trasciende es asegurar el conocimiento a las personas, y sólo excepcionalmente se requiere la actuación jurisdiccional. Por ello -agrega el autor-, se trata de un barbarismo gramatical, antes que un neologismo.

A pesar de todo, la Corte Suprema reconoce que el hábeas data es una garantía que, si bien no sustituye al hábeas corpus, cuya función para la defensa de la libertad física sigue siendo plenamente vigente, está presente para proteger las distintas agresiones que pueden sufrir otras facetas de la libertad (caso Urteaga).

Inclusive, el derecho comparado reconoce supletoriamente el trámite del hábeas corpus, tal como ocurre en Perú (art. 3º de la ley 26.301 de Hábeas Data y Acción de Cumplimiento), entre otros tantos países.

4. Diferencias entre los derechos posiblemente referidos por el hábeas data

Encontrar la tutela específica que concreta el proceso constitucional de hábeas data parece sencillo cuando el análisis se circunscribe a las posibilidades de acción que tiene un individuo frente a quien aplica en su provecho los datos que aquél le conciernen.

Desde esta perspectiva, bastaría con sostener que la función básica a cumplir es asegurar el acceso a las bases de datos y demás registros que se tengan sobre una persona, determinando con ello la posibilidad de suprimir, rectificar, modificar o actualizar la información que allí se contenga.

> Oportunamente agregamos que, el hábeas data, era 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).

Sin embargo, esta es una visión acotada al perímetro de la garantía procesal. Sería el estudio del proceso, sus dimensiones y alcances, y en definitiva, un capítulo más dentro de los procesos constitucionales.

Pero el hábeas data se proyecta hacia otros fines inconmensurables que se expone en el pórtico inmediato de la nueva ley de hábeas data. Allí se indica que la tutela no es sólo para el cuadro de posibilidades que específicamente consigna el artículo 43 para el hábeas data, sino además, garantizar el ejercicio pleno de los derechos que tiene la persona sobre sus datos personales.

En efecto, después de un largo despliegue de proyectos reglamentarios* del tercer párrafo del artículo 43 de la Constitución Nacional, se sanciona una norma que pretende superar la dificultad existente en el razonamiento del proceso, pues no se reglamenta precisamente la garantía procesal, exclusivamente, sino también, se abarcan otras cuestiones como son la creación y administración de bancos de datos, la autorización de las personas para aplicar y utilizar los registros, los derechos de las personas jurídicas, etc., etc.

Estas situaciones de incertidumbre debieran ser superadas, para evitar la dispersión de criterios en la jurisprudencia emitida al presente:

- No existe operatividad directa del artículo 43 párrafo 3º de la Constitución Nacional. Por ello, los jueces en lugar de preferir la garantía creada y permitir el acceso expedito para esta modalidad instrumental, optan por asignar el trámite del juicio de amparo y anular así la vía. Por ejemplo, la Cámara Nacional en lo Comercial * es común que rechace el hábeas data por sostener que no existe arbitrariedad o ilegalidad manifiesta, y la parte actora no acredita la inexistencia de procedimientos idóneos que puedan remediar sus agravios.
- Un relevamiento poco preciso sobre las acciones presentadas ante la justicia comercial (buena parte de ellas contra la Organización Veraz S.A.) advierte el proteccionismo hacia la circulación de los datos. Suele indicarse que las disposiciones constitucionales requieren como presupuesto de admisibilidad que se configure un caso de falsedad o desactualización en cierta información, cuando el dato se divulga sin afectar la confidencialidad propia de este tipo de información.
- En la mayoría de los proyectos legislativos se observó la preocupación del legislador para definir correctamente cada una de las voces que pueden originar temperamentos disímiles. Por el caso: dato personal, dato sensible, dato automatizado, tratamiento de datos, base de datos, banco o archivo, etc.

4.1 Intimidad: derechos tutelados en el Código Civil

El derecho a la intimidad es amplio y omnicomprensivo. Ocupa sencillas manifestaciones del derecho a la soledad y a no ser perturbado en la vida privada, como también otras situaciones, por ejemplo, la reserva y confidencialidad de ciertos actos, la intimidad familiar, la defensa del honor, el derecho a la propia imagen, o la protección de la identidad. Inclusive, la categoría principal no se precisa, de forma que para algunos es la dignidad humana y para otros el derecho a la privacidad; pero si únicamente se focaliza el tema procesal, la mayoría sostiene que se trata de un límite al derecho a la información, o bien, un derecho a la autodeterminación informativa.

Evidentemente, tamaña extensión y perfiles impide sostener que el hábeas data sea el proceso de defensa para todos ellos, y por eso, pareciera más importante, antes que definir la vía procesal, establecer el alcance del derecho fundamental agregado en el capítulo nuevo de derechos y garantías de la Constitución Nacional.

> En el artículo de Warren y Brandeis encontramos –dice García San Miguel– una definición ya clásica que hizo fortuna: la intimidad es *the right to be alone*, el derecho a estar solo, el derecho a la soledad. Sin embargo, esta definición no parece cubrir todo lo que actualmente consideramos incluido en el ámbito de aquél derecho. Pensamos que nuestra intimidad viene agredida por escuchas telefónicas, fotos tomadas a distancia con teleobjetivo y uso indebido de datos informáticos, pese a que nada de ello comporta la presencia física de otras personas. Es decir que, aunque en muchos casos estemos literalmente solos, nuestra intimidad puede resultar dañada por manejos que se emprenden a distancia y, a menudo, sin que el interesado se entere de los mismos.
>
> Por ello, algunos autores propusieron definiciones diferentes. Fried, en un trabajo de 1979 que lleva por título *An anatomy of values* define la intimidad como "control sobre la información que nos concierne", y Parker, en otro trabajo de 1974, con el título *A definition of privacy*, la define como "control sobre cuándo y quién puede percibir diferentes aspectos de nuestra persona"….
>
> La intimidad es, por tanto, el derecho a no ser conocidos, en ciertos aspectos, por los demás. Es un derecho al secreto, a que los demás no sepan lo que somos o lo que hacemos.

En la legislación argentina, la intimidad se encuentra en el artículo 19 de la Constitución Nacional *:

"Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohibe".

También, los artículos 31 y correlativos de la ley 11.723 * (Propiedad Intelectual) y el artículo 21 de la ley 18.248 * (Ley del nombre) refieren a ella. Específicamente, la intimidad se incorpora al Código Civil, con la sanción de la ley 21.173. El artículo 1071 bis dice:

"El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otro en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación".

Este conjunto normativo no se vincula en caso alguno al impacto informático, por ello recién con la reforma constitucional de 1994 comienza alguna cobertura específica.

No obstante, es preciso armonizar el ámbito de derechos protegidos por cada uno, pues existen en todos los casos, posibilidades que son alternativas para la eficacia de la defensa judicial de la intimidad.

La perturbación que menciona el código de fondo se refiere a la publicación de retratos (derecho a la imagen); difusión de correspondencia (derecho al secreto; confidencialidad y reserva); mortificación de costumbres o sentimientos (posible vulneración de datos sensibles); o cualquier otro modo de perturbación que afecta la vida privada (dar a publicidad situaciones de crisis conyugal; cesaciones de pago; publicar una declaración elogiando un producto o suscribiendo una petición política que nunca firmó; revelar arbitrariamente el carácter adoptivo o matrimonial de un hijo sin el consentimiento de los padres; no entregar el cadáver de un niño nacido muerto a sus padres dándole horrible destino, etcétera. En cada supuesto el actor puede reclamar: 1) el cese o la suspensión de la perturbación; 2) el reclamo indemnizatorio.

En el primer caso, la acción de abstención que se propone puede ser adecuada si con ello se consigue paralizar los efectos perniciosos de la invasión a la intimidad; pero no resulta efectiva para resolver la afectación de otros supuestos como la lesión a la imagen, la difusión de un secreto, la exposición pública de costumbres o comportamientos que inciden en la personalidad del damnificado. Para estos supuestos, se puede escoger entre la acción indemnizatoria, o la acción penal correspondiente (si ella está prevista), o ambas simultáneamente.

Ahora bien, ¿dónde coincide la tutela civil de la intimidad con la previsión constitucional que trae el artículo 43 constitucional?.

El artículo 1071 bis establece como presupuestos del acto lesivo los siguientes:

- *Entrometimiento arbitrario,* que supone sancionar a quien sin derecho viola la esfera de intimidad personal, afectando con ello, la vida privada. Es una acción positiva, que se manifiesta en el hacer.

  Aquí hay coincidencia con el hábeas data.

- *Perturbación de cualquier modo,* siempre que no constituya un delito penal.

  También tiene su correlato con el hábeas data.

- *Publicación de retratos sin consentimiento, difusión de correspondencia, mortificación en costumbres o sentimientos*, conceptuando las modalidades de lesión al derecho de las personas.

  Sin coincidencia con el hábeas data.

El paralelo pretende significar que los derechos proyectados desde la tutela de la intimidad en el campo sustantivo, difiere del amparo constitucional previsto, debiendo el Juez en cada supuesto establecer el tipo de procedimiento adecuado a la pretensión que se promueva.

Asimismo, en el terreno de la intimidad anidan otras cuestiones que se vinculan como derechos personalísimos, tales como el honor, la imagen, la dignidad, el perfil frente al público o la opinión personal que de uno se tiene, etc., los que por su variedad llevan a trazar un conjunto de situaciones que merecen tanto respeto como los ya observados. Y, en consecuencia, ¿cuál es la respuesta procesal para ellos? ¿Es el hábeas data?.

> Se ha simplificado el problema de limitar los derechos que ocupan el espacio de la intimidad con el fin de precisar las vías procesales específicas. En este sentido Herrán Ortiz sostiene que resulta un claro desacierto considerar que cuanto menos se conozca de la vida de las personas se goza de mayor intimidad, ya que ésta no consiste simplemente en la ausencia de información personal. En efecto, la intimidad se refiere a una esfera tan interior del individuo que en principio solo él puede revelar. Así, el carácter confidencial de los datos no es, a diferencia del derecho a la intimidad, un instrumento cuya utilización dependerá de los fines y del modo en que se haga uso de la misma.
>
> En definitiva, si "íntimo" es lo que cada persona reserva para sí y a los demás no es lícito invadir, confidencial es aquello que se revela a alguien con la intención o ánimo de que no sea revelado a los demás sin el consentimiento del interesado. De igual manera, no puede desconocerse que si bien en un primer acercamiento al derecho a la intimidad éste se puede relacionar estrechamente al "secreto", debe admitirse que la intimidad no implica exclusivamente la ausencia de información sobre la vida de la persona; representa, por el contrario, una necesidad de "vida interior", o relación intra-personal, de reflexión de los propios sentimientos y pensamientos.

La respuesta requiere desgranar cada uno de estos derechos.

4.2 El derecho al honor

Reconoce una larga prosapia el derecho al honor. Aparece en las XII Tablas –*carmen famosum*-, se encuentra en el derecho romano, en la Grecia antigua y fue motivo central de buena parte de la historia del mundo, confiar en las personas honorables.

Honradez y dignidad personal son premisas del Fuero Juzgo, y las Leyes de Partidas las establecen como principios generales del derecho.

> En las grandes universidades del Renacimiento (París, Pavia, Salamanca, Coimbra) se comentaron las frases de la "Summa" de Santo Tomás sobre la vida, la integridad corporal, la tranquilidad espiritual, el honor y la fama. Las lecciones de Vitoria –dice Concepción Rodríguez-, llenas de vida y de sentimiento humano, despiertan el interés general. Soto expondrá con su habitual concisión y exactitud sistemática, la nueva doctrina de los bienes intrínsecos de la persona. Dice que el hombre tiene tres géneros de bienes: 1. La vida; 2. Honor y fama, y 3. Los bienes temporales.
>
> El hombre tiene el dominio de su honor y fama, pero no puede usarlos como el dinero, porque su valor es superior; aquellos bienes son más nuestros. Honor y fama a los que, por eso, colocará no en el orden de la vida, sino en el de los bienes externos.

Tiempo después, los códigos civiles desatienden la esencia de este derecho personalísimo, quizás influidos por la condición de derecho fundamental que le otorgó la Declaración de los Derechos del Hombre.

En suma, podemos afirmar que las normas sustanciales no se han detenido cuidadosamente en la reglamentación de los derechos de la personalidad hasta bien avanzado el presente siglo, que coincide con su caracterización como derecho constitucional.

Ahora bien, ¿puede ampararse al honor desde el hábeas data?

En principio la respuesta sería negativa, pero no absoluta. Por varios motivos. Uno de ellos proviene de la misma ley cuyo artículo 1º establece que *"el hábeas data garantiza el derecho al honor"*, otra razón es la naturaleza del proceso que sólo se ocupa de la invasión a la persona tomando datos que se recopilan y transfieren provocando una crisis en el derecho a la identidad. No obstante, la identidad es una parte del honor, pero no es el honor en sí mismo.

> La identidad se distingue también de la intimidad: aquella asegura la fiel representación de la propia proyección social; ésta, la no representación al exterior de las propias vicisitudes personales, cuando un tercero no posee un interés socialmente apreciable, tal como lo sostiene Herrero Tejedor.

Es verdad que definir al honor arrastra complejas disquisiciones y opiniones dispares. Por un lado, de manera general, se hallarían implicados valores como la intimidad, la buena fama, la reputación, el respeto propio y ajeno, la consideración familiar y social, y en definitiva, es propiamente un sentimiento propio sobre nuestra persona y una estima de los demás hacia nosotros.

Desde esta perspectiva, se trata de observar qué es lo intolerable cuando el honor se afecta, y qué puede admitirse aun existiendo un perjuicio contra el derecho de la personalidad.

> Este es el criterio predominante: la doble conceptuación que distingue el honor como resultado del juicio de valor que los demás hombres hacen de nuestras cualidades (honor objetivo), y como el sentimiento y la conciencia del propio honor: las representaciones que el sujeto tiene de sí mismo –conciencia del honor- y la voluntad de afirmar su propio valor –sentimiento del honor-
>
> Resumiendo ambas nociones, De Cupis define el honor como el íntimo valor moral del hombre, la estima de los terceros, o bien la consideración social, el buen nombre o buena fama, así como el sentimiento y conciencia de la propia dignidad.

Otra visión llega de su significado etimológico. La Real Academia dice que el honor es una *cualidad moral que nos lleva al más severo cumplimiento de nuestros deberes*, mientras que la honra se la define como la *estima y respeto de la propia dignidad.*

De esta lectura surge un honor subjetivo, propio, que se vincula con la autoestima o propia consideración (dignidad personal); y otro aspecto objetivo que es el respeto que de nosotros tienen los demás: la reputación, en definitiva.

> La concepción jurídica actual, de acuerdo con las enseñanzas cristianas –apunta Concepción Rodríguez-, considera que el honor es inherente al hombre; es un reflejo de la personalidad y uno de los derechos esenciales que le dan contenido. A toda persona corresponde un mínimo de responsabilidad y honorabilidad, que debe ser protegida por el orden jurídico.
>
> Nadie, indica Alfredo Orgaz, está *a priori* excluido de esa tutela, ni siquiera las personas deshonestas o de mala reputación; también éstas pueden ser sujeto pasivo de un delito contra el honor, siempre que de acuerdo con las circunstancias, el ataque debe ser considerado como ilegítimo esto es, como no justificado por un interés superior. La inviolabilidad de la integridad moral, como la protección de los demás derechos naturales, no es absoluta e ilimitada.

La defensa del honor esta mejor diseñada en el derecho penal *. En este, el análisis recae sobre cuestiones fácticas que conducen a tipificar un delito preestablecido (v.gr.: calumnia, injuria). El derecho a ser respetado, se afinca asimismo en la Constitución, pero siempre calificando la ofensa como un hecho a comprobar, y al honor como un derecho subjetivo (individual).

> Algunos autores –dice Cifuentes- han negado la existencia de un derecho subjetivo al honor. En particular aquellos que no reconocen los derechos personalísimos. Ennecerus, por ejemplo, dice que el honor es el reconocimiento del valor de una persona por sus contemporáneos, pero que ese concepto no pertenece al derecho y, en cambio, tiene una significación, moral y jurídica el

> honor civil, o grado de estimación y reconocimiento del valor que corresponde a todo hombre intachable.

En cambio, no se repara la autoestima, es decir, la consideración que uno tiene sobre sí mismo y que entiende afectada por actos de otros.

La ley penal califica como "injuria", en la tipicidad requerida, la lesión al derecho subjetivo del honor; mientras que es "calumnia" la forma objetiva de agraviar la honra.

Las normas constitucionales no definen el derecho a defender el honor, sólo asignan una garantía procesal contra toda acción o amenaza que lesione la fama, el prestigio, la consideración, la dignidad, la reputación, el crédito, o el sentimiento de estima, por enumerar algunas de las probables alegaciones del interés dañado.

> Doctrina local sostiene que la norma constitucional argentina adopta una fórmula amplia, ya que no enuncia cuál es el bien jurídico protegido, tan sólo se limita a señalar que actúa frente a supuestos de "falsedad" o "discriminación", dejando abierta la posibilidad de inferirlo en cada caso concreto. Quizá por apresuramiento –dice Sagüés- el nuevo texto constitucional contempla el hábeas data para supuestos de "falsedad" o "discriminación", en custodia de los valores verdad e igualdad; y no para otras hipótesis clásicas de esta figura como la protección del honor o privacidad.

Como regla, la protección llega después de los hechos tornándose inevitablemente en un derecho indemnizatorio. A veces, la reparación se consigue con la publicación de la sentencia que condena al difamador, pero es evidente que la tacha ya se produjo. En pocas palabras, no hay sentido preventivo en nuestra legislación positiva.

En la jurisprudencia generada desde el hábeas data, a pesar de lo expresado, se ha hecho lugar a la defensa del honor aun cuando no se lo diga abiertamente.

En efecto, en la causa *"Gutierrez, Héctor R. c/ Casino Militar del Personal Superior de la Base Naval Puerto Belgrano"* (C.Fed. de Bahía Blanca, Sala 1, diciembre 30/994) se sostuvo que la acción no procedía si no estaba demostrado "prima facie" el motivo descalificante o discriminatorio que le impedía a un oficial de la Marina argentina ingresar al Casino Naval de su puerto de destino. Sin embargo, se advirtió que "*la denegatoria de la admisión como socio en un club en el caso, Casino Militar- no esta incluida dentro de los presupuestos de procedencia de la acción de hábeas data, salvo que para tal negativa se haya tenido en cuenta algún dato descalificante o discriminatorio que conste en sus propios archivos, categoría que no alcanzan ni el listado de socios ni el registro de pago de cuotas"*.

En otra sentencia, se alegó que *"la información que brinda la demandada (empresa de transmisión de datos con fines comerciales) no puede incursionar en el terreno del honor e intimidad de los actores y con ello resultar discriminatoria en su vida de relación por orientarse a actividades de índole estrictamente comercial y crediticia"* (CNCiv., Sala A, setiembre 8/997, *in re*: Pochini, Oscar y otro c/ Organización Veraz S.A.). Con ello dio a entender que la simple información registrada y difundida a quien le adquiere el dato, si ella no es incorrecta ni desactualizada, no provoca discriminación ni afectación a las personas referidas, toda vez que la información transmitida es cierta.

La Corte Suprema de Justicia de la Nación sostiene que "*artículo 43, párrafo tercero de la Constitución Nacional, ha incorporado un nuevo derecho a la protección de los datos personales frente a cualquier intromisión arbitraria o abusiva que pudiera implicar una violación a la intimidad y a los demás derechos constitucionales, hallándose en íntima relación con el derecho a la integridad, a la dignidad humana, a la identidad, al honor, a la propia imagen, a la seguridad, al de peticionar, a la igualdad, a la libertad de conciencia, a la libertad de expresión, a la libertad de reunión, de asociación, de comerciar y con cualquier otro que pudiera resultar afectado"* (Voto del Dr. Boggiano, en "Suárez Mason, Carlos G., del 13 de agosto de 1998).

Posteriormente, se dijo: "*el hábeas data -en tanto garantía de un derecho individual, personalísimo-, sólo puede ser ejercida por el titular del derecho a interponer la acción, en defensa de aspectos de su personalidad, vinculados con su intimidad, que no pueden encontrarse a disposición del público ni ser utilizados sin derecho" (*del voto del Dr. Fayt en la causa "Urteaga, Facundo R. c/ Estado Mayor Conjunto de

las Fuerzas Armadas, del 15 de octubre de 1998). También agregó que "*la garantía del hábeas data –dirigida a que el particular tenga la posibilidad de controlar la veracidad de la información y el uso que de ella se haga-, forma parte de la vida privada y se trata, como el honor y la propia imagen, de uno de los bienes que integran la personalidad*".

Observemos ahora como juega el conjunto normativo que tenemos.

En primer lugar, el *Pacto de San José de Costa Rica* * en su artículo 11 determina:

> *"Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; 2) Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; 3) Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques"*

De esta convención surge el derecho al honor como una expresión natural de los derechos humanos; pero de poco sirve si no cuenta con la herramienta precisa que le otorgue una particular fisonomía.

La Declaración Universal de Derechos Humanos * establece:

> *Artículo 12: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".*

Es similar la redacción del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos *.

En conjunto, todas estas normas llevan a sostener que, sea considerado el derecho al honor y a la honra como un derecho del hombre o como un derecho subjetivo público, en ambos casos es un límite a la actuación de otros sobre nuestra persona y una obligación del Estado aportar la garantía procesal.

Cabe agregar que ni de los pactos ni de las convenciones incorporadas por el artículo 75 inciso 22 a nuestra Constitución Nacional surge que sea el hábeas data la vía reglamentaria que se espera para la tutela del honor.

Por su parte el Código Penal introduce como "Delitos contra el honor":

> *Art. 109: "La calumnia o falsa imputación…"; art. 110: "El que deshonrare o desacreditare a otro…"; art. 111: "El acusado de injuria sólo podrá probar la verdad de la imputación en los casos siguientes: 1. Si la imputación hubiere tenido por objeto defender o garantizar un interés público actual; 2. Si el hecho atribuido a la persona ofendida hubiere dado lugar a un proceso penal; 3. Si el querellante pidiere la prueba de la imputación dirigida contra él. En estos casos, si se probare la verdad de las imputaciones el acusado quedará exento de pena.*
>
> *Los artículos 112 y 113 se refieren a las calumnias o injurias encubiertas y publicadas, respectivamente. En su caso, el artículo 114 permite requerir la publicación de la sentencia condenatoria en el mismo diario donde se emitió la ofensa o descalificación.*
>
> *Los artículos 115 a 117 reglamentan las penas establecidas cuando el delito provenga del apoderado o defensor, o sean recíprocas, o hubiese retractación.*

Las normas, sumariamente presentadas, exigen el "*animus injuriandi*" para tipificar al delito, pero al individuo le otorga un derecho subjetivo y una vía de reparación.

El Código Civil contiene varias disposiciones:

Art. 1089: "Si el delito fuere de calumnia o de injuria de cualquier especie, el ofendido sólo tendrá derecho a exigir una indemnización pecuniaria, si probase que por la calumnia o injuria le resultó un daño efectivo o cesación de ganancia apreciable en dinero, siempre que el delincuente no probare la verdad de la imputación"

De esta amplia manifestación ("…*injuria de cualquier especie*…) se podría interpretar que anida allí el "hábeas data". ¿Es ello correcto?.

Pareciera que no. La previsión legal se sostiene en el delito (art. 1072) y una vez lograda la sentencia condenatoria, la obligación se desenvuelve como indemnización y no como un deber de realizar tal o cual acto, como correspondería al hábeas data.

La *exceptio veritatis* le agrega un elemento más al fundamento, pues si la garantía procesal que se tiene para evitar la manipulación de nuestros datos lleva implícita la idea de proteger la intimidad personal, es probable que permitiendo que el delincuente (¿es delincuente quien registra datos o los transfiere aun a sabiendas del error informativo?) pruebe la verdad de sus dichos (o registros, por el caso), se deje expuesto al honor a una expoliación mayor.

> Sostiene Cifuentes que hay que defender hoy como nunca a la persona. Se extienden a diario, introduciéndose en el hogar mismo, los sistemas difusivos con nuevas formas de ataque, con una extraordinaria perfección en las comunicaciones, las noticias, los entretenimientos visuales y radiales. Se pretende, en no pocas ocasiones, halagar al público e interesarlo moviendo bajos instintos, haciendo fáciles y desdorosas apologías, destruyendo honras y respetabilidades, o sacando gavetas de la historia de anécdotas risueñas, trágicas y mortificantes. Bastaría probar la realidad celosamente guardada para conservar la impunidad. De ahí que al intérprete de una norma como el artículo 1089 le corresponda restringir el ámbito de la *exceptio veritatis.*

El artículo 1090 agrega:

"Si el delito fuere de acusación calumniosa, el delincuente, además de la indemnización del artículo anterior, pagará al ofendido todo lo que hubiese gastado en su defensa, y todas las ganancias que dejó de tener por motivo de la acusación calumniosa, sin perjuicio de las multas o penas que el derecho criminal estableciere, tanto sobre el delito de este artículo como sobre los demás de este capítulo".

¿Se aplica el precepto al hábeas data?. Una vez más el mismo interrogante. ¿Puede considerarse calumniosa la difusión de datos equivocados, parciales o desactualizados?. En principio, parece que no, porque la norma refiere a la acción realizada a sabiendas y con intención de dañar, sin tener relación con la actitud imprudente, ligera o precipitada de quien transmite un dato sin haberlo confirmado. No obstante, esta actitud culpable podría repararse por el artículo 1109 del Código Civil.

Resulta así que la acción de hábeas data se afinca en un preciso punto de referencia, que de por sí es acotado (conocer el dato, y requerir su actualidad, supresión o rectificación) y no podría transferirse hacia otros que cuentan ya con una vía procesal de protección.

De todos modos, el honor se puede afectar con la transmisión de datos sensibles o que impliquen alguna forma de discriminación (por ejemplo: la raza o el origen étnico), en cuyo caso la garantía constitucional es procedente para lo que al dato concierne; como también lo es el proceso civil reparatorio del perjuicio emergente. Serían las denominadas vías concurrentes que no pueden impedir el progreso del hábeas data.

En suma, lo que queremos significar es que aun cuando la protección del honor y la reputación pueda tener respuestas en el ordenamiento positivo actual, es bien sabido que la actuación es posterior al hecho y obra como sanción al ofensor y como reparación para el ofendido.

En cambio el hábeas data reglamentado puede servir indirectamente para estos derechos personalísimos, en la medida que la afectación puede prevenirse desde los objetivos que tiene la garantía procesal.

> Decía Iván Cullen, en la convención constituyente de 1994, que es tan importante precisar este derecho o garantía jurisdiccional –se refiere al hábeas data- que estamos dando a la gente para que defienda su derecho a la reputación y a la honra –"*porque eso es lo que defiende el hábeas data*"-, para evitar ir en desmedro de la privacidad y el secreto profesional que puedan tener otros.

Una vez más se advierte la omisión de la norma reglamentaria porque nada ha dicho al respecto, aunque al sostener que persigue el "*restablecimiento del pleno ejercicio de los derechos a que se refiere la presente ley*", puede colegirse alguna amplitud, teniendo en cuenta que, a diferencia de otras cartas constitucionales, la nuestra no consagra explícitamente la defensa al honor, a la buena reputación, a la intimidad personal y familiar, a la propia imagen, al buen nombre, etc. que son cuestiones que, hipotéticamente, podrían argumentarse desde el hábeas data.

> Sostiene Bidart Campos: "…que el hábeas data haya surgido y funcione habitual y normalmente como garantía para preservar la autodeterminación informativa y la privacidad de datos personales no alcanza para agotar su funcionamiento en esa dirección: toda garantía constitucional debe ser tan *elástica* cuanto la realidad de una situación determinada lo demande; y ello a efectos de que rinda su efecto tutelar respecto del derecho que a través de esa misma garantía se pretende. Como en tantas otras cosas, nada de rigideces, estrangulamientos, reduccionismos, ni cosa semejante. Las garantías deben holgarse y si, acaso, nunca antes nos imaginamos que íbamos a precisar alegar un "derecho" a la verdad y a los datos de víctimas desaparecidas, ahora que se hizo necesario hay que buscar con aperturismo y activismo procesal y judicial la mejor vía conducente –en cada caso- para que haya una –o más- garantías a disposición de quien invoca aquel derecho. Si las garantías no sirven para el fin por el cual existen, no sirven para nada. Y esto no es tolerable ni admisible".

4.3 El derecho a la propia imagen

Seguramente en los tiempos actuales la comprensión del concepto de "imagen" se encuentra afectada por la idea de apariencia sobre lo que uno es y representa ante los demás. Antes, la imagen era una pertenencia de la persona que se violaba cuando, sin consentimiento, se reproducían sus rasgos físicos en forma reconocible a través de un soporte material cualquiera. Hoy la reputación se forja también desde la apariencia transmitida.

Es decir, ambas facetas se ocupan de proyecciones distintas de un mismo derecho. Mientras la imagen es el derecho que uno conserva para mostrarse ante los demás, y como tal, es un derecho intrínseco de la intimidad; el otro es el poder estrictamente individual de impedir el uso de nuestra fisonomía a través de un medio de reproducción cualquiera.

> La invención de la fotografía y el grabado, así como el extraordinario desarrollo que en la vida moderna ha alcanzado la publicidad y la propaganda mercantil e industrial plantearon, a partir del siglo pasado, según dice Concepción Rodríguez –siguiendo a Castán Tobeñas- la cuestión del derecho a la imagen.

Sin embargo, esta es una distinción no aceptada en legislaciones donde el "derecho a la propia imagen" se construye como límite específico de las libertades de expresión e información.

En efecto, en España doctrina de las más calificadas sostiene que el derecho a la propia imagen "*es un derecho innato de la persona, derecho que se concreta en la reproducción o representación de la figura de ésta, en forma visible y reconocible. Es un derecho subjetivo de carácter privado y absoluto. Es un derecho personalísimo, pero dotado de un contenido potencialmente patrimonial en cuanto que a través de su ejercicio pueden obtenerse bienes económicamente valorables, y además en cuanto a la posible indemnización pecuniaria en el caso de su violación. Es un derecho inalienable; como tal irrenunciable, y en general, inexpropiable. Es un derecho intransmisible mortis causa, bien que su tutela post mortem corresponda fundamentalmente a los más próximos parientes del difunto. Es, en fin, un derecho imprescriptible*" (Gitrama).

En tal sentido, por constituir la exteriorización de la imagen una misteriosa impronta de la personalidad, nadie, sin estar debidamente autorizado, puede propagar mediante ilustraciones la efigie de una persona aunque ella se muestre en público y el público la conozca. Y este razonamiento no meramente especulativo, lleva a la conclusión de que no son los bienes jurídicos del honor ni del secreto personal el contenido propio y genuino del derecho a la propia imagen; porque la reproducción arbitraria de una figura humana puede no lesionar el honor de la persona reproducida, ni quebrantar el secreto de una vida privada cuando se trata de exhibición popular *ad incertas personas*, en ellos desaparece aquel secreto o derecho a la reserva de la figura humana.

> El Tribunal Constitucional español ha dicho que "los derechos a la intimidad personal y a la propia imagen, garantizados por el artículo 18.1 de la Constitución, forman parte de los bienes de la personalidad que pertenecen al ámbito de la vida personal y familiar que queda sustraído a intromisiones extrañas. Y en este ámbito de la intimidad, reviste singular importancia la necesaria protección a la propia imagen frente al creciente desarrollo de los medios y procedimientos de captación, divulgación y difusión de la misma y de datos y circunstancias pertenecientes a la intimidad que garantiza este precepto" (STC, 170/87).

El derecho a difundir el nombre o la fotografía de una persona sin ocasionarle molestias o perjuicios depende en gran medida de la subjetividad que el individuo tenga respecto a su vida privada. Una persona cualquiera tiene derecho a que se la proteja en su vida y en su propiedad, y actualmente el primero ha llegado a significar el derecho a disfrutar de la vida, sin la publicidad o perturbación de una encuesta organizada sin autoridad. Los tribunales aseguran aquél derecho "a ser dejado en paz" que recuerda el derecho a estar a solas, propio de la privacidad.

Los derechos íntimos deben ser respetados al igual que los deseos y sensibilidades de la gente, los que pueden vulnerarse cuando se afecta la esfera inalienable de la imagen que ante los demás se tiene.

Ahora bien, la imagen se extiende a otras manifestaciones y perseguir una defensa particular en cada caso. Veamos:

- En una primera etapa (1839/1900) el derecho se relaciona con la propiedad intelectual y artística.
- Después (1900/1919) comienza a considerarse como un derecho esencial de la persona: es un atributo de la personalidad

> Sostiene Marcela Izascum Basterra, a quien seguimos en esta división de períodos para el reconocimiento del derecho a la imagen, que en 1902, en el marco del XXVI Congreso de Juristas alemanes, celebrado en Berlín, queda abiertamente reconocido el derecho a la propia imagen como uno de los derechos inherentes a la personalidad. Por otro lado, hacia fines del siglo pasado en Estados Unidos se conocía el célebre artículo de Warren y Brandais "*The right of privacy"* de 1890, que se refiere al derecho a la imagen personal como la forma más simple del *right of privacy*, y cuyo antecedente más inmediato es la expresión acuñada por el juez Cooley en 1879 *the right to be let alone* (el derecho a ser dejado en paz). Estos autores plantean que si la *Common law* cada vez ampliaba más su protección a las personas y a sus bienes, dicha protección debía extenderse a los particulares en su vida privada y si se tenían en cuenta las nuevas circunstancias sociales, tecnología y desarrollo de la prensa, crecimiento del interés informativo, etc., sería conveniente considerar al *right of privacy* como reconocido por la cuarta enmienda de la Constitución Americana.

- Entre 1910 y 1948 se consolida la garantía con jurisprudencia que la interpreta desde el derecho a la privacidad.
- A partir de la Declaración Universal de los Derechos del Hombre –1948- (art. 12) se protege especialmente la vida privada y la honra, transmitiendo a las cartas constitucionales del mundo el derecho consagrado.

> Vuelve a sostener Basterra que en nuestra Ley Fundamental no hay artículo que se refiera al derecho a la imagen propia, o al propio perfil, pero está implícito a través de las normas supranacionales que quedaron incorporadas a nuestra Constitución después de la reforma de 1994, en el art. 75 inciso 22. Por su parte el art. 43 establece la garantía de hábeas data como el acceso a los datos, y la finalidad que se dará a los mismos y la posibilidad según los casos de rectificación, supresión, confidencialidad y actualización de los mismos. Nada dice en relación a los derechos protegidos en doctrina, varios autores consideran entre los derechos tutelados por esta garantía, el derecho a la propia imagen.

En cada etapa se observa el paso de la defensa patrimonial de lo que es intrínsecamente propio (el producto del intelecto) al campo de lo espiritual (la tranquilidad de conciencia) y terrenal (vivir una vida propia sin interferencias). Por ello está bien que la imagen se considere como un derecho de la personalidad, o como una barrera que evita perturbar la dignidad humana. Ello es consecuencia de la evolución legislativa, pero también lo es, de la propia estima que el hombre reconoce sobre su persona.

> Dice Puig Brutau que "si se considera el derecho de la personalidad como una institución puesta al servicio de la persona para hacer valer su dignidad como tal, no cabe duda que la dignidad moral es un bien que merece ser protegido; por consiguiente, toda persona tiene derecho a recibir de los demás un trato acorde con la dignidad que el ordenamiento jurídico reconoce a todo sujeto de derecho, y en ese sentido cabe hablar de honor como una manifestación del derecho de la personalidad, que repercute además en la consideración que la propia persona tenga de sí misma".

Ahora bien, la imagen en sí misma puede transmitirse en dos formas: a través de la reproducción por cualquier medio de una figura propia, que sería un supuesto objetivo, inmediatamente reconocible. O bien, como creencia que los demás tienen sobre nuestra persona a partir de la imagen pública que expresamos, caso éste que resulta esencialmente subjetivo.

Por ello, mientras es posible actuar prontamente para la defensa de la imagen cuando esta se afecta en la publicación de fotografías o retratos producidos sin autorización del titular; resulta más difícil encontrar la vía de respuesta a las agresiones contra la reputación cuando ella no alcanza para lesionar el honor de la persona. Adviértase que en éste, el comportamiento atacado es aquél que pretende afectar la consideración social del individuo.

En uno y otro caso, el hábeas data no parece ser la herramienta más precisa, salvo claro está, que el camino aplicado para inferir el agravio sea un dato transmitido desde un archivo o base registral.

> Así pues –dice Herrán Ortiz- el derecho a la propia imagen debe identificarse con los derechos de libertad, de manera que al individuo le es garantizado el derecho a decidir libremente respecto a su imagen, adoptando en su caso las medidas que procedan para impedir la divulgación de imágenes o retratos de la persona, aunque la misma no dañe su honor, ni interfiera en su derecho a la intimidad. Claro que no se requiere la intención dañosa o injuriosa para que la libertad del sujeto, en cuanto a su imagen, se considere vulnerada, y constituye una realidad irrefutable que el simple hecho de divulgar, exhibir o publicar la imagen de la persona puede y debe ser cuestión que quede al exclusivo arbitrio de cada individuo.

La especialidad del proceso constitucional evita confundir el derecho a la propia imagen con el derecho a la intimidad o el derecho al honor, aunque no es necesario establecer una diferencia manifiesta entre ellos, pues en definitiva el derecho personalísimo que se tiene apunta a proteger la identidad personal mediante el hábeas data; mientras que el honor y la intimidad se tutela con herramientas específicas sustantivas (civiles y penales).

> De todos modos, al proteger a la persona de las invasiones ilegítimas (sea por reproducción gráfica o difusión escrita) contra esa parte de la vida que quiere mantener fuera del alcance de otros, evidentemente también se defiende la privacidad o el derecho a tener una vida privada.

4.4 La fama o reputación

La intimidad se podría representar, en forma figurada, cual si fuera una espiral cuyo núcleo contiene la más sagrada de las reservas que la persona quiere mantener. Aparece así una suerte de anillos donde el más expuesto hacia el exterior es el que los demás observan y conocen, y que puede asentar en la esfera de la fama o reputación.

> De manera similar, la doctrina alemana intenta profundizar el contenido de la intimidad distinguiendo en él tres esferas. Constituirían a modo de círculos concéntricos, representativos de una triple graduación de la vida privada, desde el más permisivo al más restringido. Novoa las explica diciendo que la más amplia, o *esfera privada*, comprende todos aquellos comportamientos, noticias y expresiones que el sujeto desea que no lleguen al conocimiento público. Se incluye aquí la imagen física de la persona y su comportamiento, aun fuera del domicilio, que no debe ser conocidos sino por quienes se encuentran en contacto con él. Le sigue la denominada *esfera confidencial*, que abarca lo que el sujeto participa a otra persona de confianza; de esta esfera quedan excluidos, aparte del público en general, aquellas personas que operan en la vida privada y familiar. Aquí se incluyen correspondencia, memorias, etc. Finalmente, como círculo concéntrico de menor radio, aparece la *esfera del secreto*, que corresponde a las noticias y hechos que por su carácter extremadamente reservado han de quedar inaccesibles a todos los demás.

En España, la ley de Tratamiento de Datos (derogada a fines del año 1999), identifica la defensa de la fama cuando ella supone reputación profesional. En la exposición de motivos se lee: *" …el conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor"*.

Esta inclusión en el terreno que el honor abona nos llevaría a interrogar si los actos lesivos dirigidos contra la fama pueden ser resueltos por las acciones que sirven a la defensa de la honorabilidad, o en su caso, si la herramienta precisa es el hábeas data.

Las posibilidades se alternan entre la visión patrimonialista que privilegia la atención sobre el daño provocado y, en consecuencia, la reparación a través de una indemnización por el perjuicio sufrido; o bien, la tutela del honor, ya sea en su aspecto interno afirmado en la autoestima, o en su faz externa integrado por el reconocimiento que los demás hacen de nuestra dignidad.

> El Tribunal Constitucional español ha terminado por incluir la fama o prestigio profesional dentro del concepto constitucional de honor en sentido trascendente, que no es otro que la opinión que la gente pueda tener de cómo trabaja cada cual y que respeto merece por ello.

No existen dudas respecto al derecho a la necesidad de protección jurídica que tienen ambas cuestiones, el punto a esclarecer es si el derecho se apoya en un derecho fundamental, o en su caso, en una solución material sostenida en la reparación de los perjuicios sufridos.

Cada profesión tiene códigos deontológicos que previenen las actitudes deshonrosas de los hombres que en el sector se desempeñan. Quienes no responden a esas normas de conducta moral o ética profesional, son sancionados. Una regla no escrita supone que a mayor responsabilidad, mayores son los deberes de conducta, y en consecuencia, más graves debieran ser las sanciones.

Ahora bien, afinando el concepto se advierte que cada vez más nos alejamos de la tutela prometida desde el hábeas data, en cuyo caso, esta vía solamente sería útil cuando en un archivo o registro se encuentren datos que descalifiquen o menosprecien la calidad del profesional.

Sin embargo, también en este punto hay que tener cuidado, pues los datos sobre una persona pueden capturar opiniones que otros tienen de ella a través de las publicaciones que constituyen críticas u observaciones que definen la expresión del arte, oficio o profesión que tiene.

> Bien apunta Cifuentes que es necesario buscar un punto de equilibrio entre la libre crítica y la ofensa de la persona. Esto será, por fatalidad, cuando alguien se siente ofendido en su condición profesional, desempeño de su especialidad o creación literaria, científica, artística, cultural y pública supeditado a la decisión judicial. El magistrado, según las circunstancias, pruebas y elementos objetivos y subjetivos del caso, deberá graduar la fuerza del cuestionamiento, de la ironía acusadora, del juicio desfavorable y sus comentarios y manifestaciones, a fin de establecer si se ha sobrepasado el mero disentimiento, para desmerecer la persona con aguda saña o en aspectos privados y propios de la honorabilidad profesional.

El acto de archivar, conservar y difundir datos que puedan lesionar la honorabilidad de una persona, o al menos, su reputación personal o profesional, se distingue de las vías positivas de defensa que el derecho tiene, pues el buen nombre vituperado solamente tiene indemnización económica, haciendo cierta la expresión que sostiene que, una vez que el dato se ha hecho público es inútil cualquier corrección, y lo único que queda, es la reparación patrimonial de un daño que, moralmente, no tiene sosiego.

Por ello, la ley incorporada resuelve el problema actuando preventivamente para evitar la difusión de comentarios hirientes o mal intencionados que persigan agredir el respeto personal o la fama profesional que se tenga.

Aun reconociendo que una lectura gramatical del artículo 43 no lo establece, no se puede privar a la ley de su auténtica interpretación axiológica del mensaje constitucional, al ocuparse en delante de la persona y sus datos personales como aspectos inherentes a su intimidad.

> Con el fin de apoyar este argumento, deberíamos considerar varios aspectos, algunos de los cuales son ampliamente aceptados, tales como la Directiva Europea* relativa a la protección de datos y libre circulación de los mismos. De hecho, varios de los artículos de la Directiva se refieren explícitamente a la naturaleza pública de ciertos datos a la hora de concluir que los datos personales que se han hecho públicos no se pueden proteger de la misma manera que los datos personales. Al menos tres de estas disposiciones deberían examinarse con más profundidad. Me refiero, a los artículos 8.2; 18.3 y 26.1.
>
> El artículo 8.2 de la Directiva relativo a las categorías especiales de datos (convicciones políticas, filosóficas o religiosas, datos personales que revelen el origen racial o étnico o la moral de cada persona) señala explícitamente que no se podrían tratar a menos que el interesado haya dado su consentimiento explícito.
>
> El artículo 18.3, exige que cualquier recopilación de datos debe ser anunciada a la autoridad encargada de la supervisión de los mismos. Este artículo presenta una exención para esta exigencia a las "recopilaciones destinadas a facilitar información al público y a la consulta abierta por parte del público".
>
> Para concluir, el artículo 26.1 admite una excepción a la exigencia de un nivel adecuado de protección para los datos objeto de comunicación transfronteriza, a saber: si los datos transferidos a un Estado que no proporciona dicho nivel de protección tienen su origen en "registros que están a disposición del público"

Desde otro punto de vista, también se puede enfocar el derecho que el individuo tiene para no descubrir facetas de su personalidad que le provocan deshonra o, al menos, son indecorosas para su imagen.

Surge así una suerte de relación confusa entre el engaño y la intimidad, una conducta que se puede ocultar y mantener al margen del conocimiento de otros porqué, de otro modo, caería el prestigio adquirido.

> Sostiene Catalán González que la relación entre engaño e intimidad es diacrónica: allí donde se dé un área de conducta que hoy tengo derecho a mantener al margen de la inspección de los otros, desde la correspondencia privada a la cuenta bancaria, desde el número de teléfono particular al seudónimo del concurso literario, desde el diario íntimo al secreto informático, allí se dio antes motivo para el engaño y el secreto. La intimidad así entendida, y con ella el engaño que la antecede, sólo podrían aprehenderse desde una perspectiva genética,

> atendiendo al precario equilibrio de fuerzas entre aquello que el grupo sabe del individuo y aquello que el individuo está dispuesto a reconocer ante el grupo; también, trasladando el ángulo de inspección, como un pacto entre ambas instancias donde cada una sacrifica algo para recibir algo a cambio, y, por último, como el reconocimiento simultáneo de que alguien no puede renunciar a ciertas actividades que le acarrearían consecuencias desagradables de ser conocidas.

Las inclinaciones sexuales, por ejemplo, son datos sensibles que tienen prohibida su difusión. Este sería un derecho al secreto que el hábeas data puede amparar; en cambio, divulgar que la fama de un autor literario se debe a que contrata servicios de otros para sus ediciones, es un hecho inconveniente para esa notoriedad alcanzada; aquí, la revelación de los servicios prestados afectaría el crédito logrado, aun cuando lo fuese mediando un intelecto que no le es propio y se vale de esa ocultación. Aun cuando parezca incómodo decirlo, el hecho no es delictual (aunque pueda ser cuasidelictual), y recobra aquella máxima que ponía en práctica "Anibal" en su lucha contra los romanos:

"Se debe luchar con la astucia cuando no se puede ser igual con las armas"

En términos similares se plantean otras diferencias sensibles que inciden en la reputación como "estigmas o descréditos", aunque de hecho no lo sean, y el individuo desea conservar en su más sagrada reserva; por ejemplo: los atributos físicos diferentes (v.gr.: enfermedades crónicas como la diabetes); las capacidades diferenciadas (v.gr.: sordera, tartamudez, etc.); las costumbres sociales o sexuales; el comportamiento doméstico, etc. En cada caso, existe una relación entre el encubrimiento y la intimidad.

La revelación se produce cuando la confidencia se hace pública; ese acto, además, agrede la fama o reputación.

> Las figuras de la "discreción" y la "ocultación éticamente justificada" del individuo ante el tanteo para saber más que ejercen los extraños o simples conocidos, son figuras morales que se remontan a fechas muy anteriores a la moderna eclosión de los valores de la vida íntima. Se pueden hallar en los textos de las grandes religiones y en los escritos morales de la antigüedad grecorromana. Nada tiene de extraña –agrega Catalán González- esta inveterada apreciación que constituye el bastidor invariable sobre el que se teje, como dijimos, el cambio social de valores; puesto que las relaciones sociales se asientan en el conocimiento que tengamos del otro, y ese conocimiento ha de ser mayor conforme aumente la mutua relación. El límite de los tanteos realizados para saber más de él, sin que ese tanteo pueda considerarse "indiscreto", no puede establecerse de una vez y para siempre, sino que varía conforme lo hacen las condiciones sociales.

En el fondo, la intimidad mejor protegida es la que oculta la información agraviante, a pesar de confrontar con ello la simulación del "yo" y el disimulo de lo inconveniente a la imagen.

> Por mucho que pueda repugnarnos a primera vista –afirma Catalán González- la aspiración al secreto bancario y al derecho del aspirante a un empleo a no revelar al empleador su "biografía moral" sufren de la misma dualidad pragmática: por un lado, aceptan la importancia del descrédito sociogénico; por otro, hacen uso de la capacidad reconocida de reserva para encubrir características de su comportamiento que saben desacreditables.

4.5 El derecho a la reserva y confidencialidad

Es común afirmar que la reserva y confidencialidad pertenecen y corresponden con los objetivos del derecho a la intimidad.

También se afirma que, entre los tipos de hábeas data, aparece el *reservador* (que sólo puede transmitirse a quien se encuentra legalmente autorizado y en las circunstancias en que corresponde), el cual involucra la confidencialidad del dato (supuesto de datos sensibles que se excluyen en todo tipo de información).

Sin embargo, es preciso afinar los conceptos, porqué el punto de partida no es la intimidad en sí misma, sino otro u otros derechos, que por ahora dejamos planteados sin definirlos.

Un dato es una fuente de información. No se obtiene sino a través de la pesquisa o de la revelación que haga la persona. Cuando es ésta quien lo da a conocer, pone en exposición un pensamiento, una característica de su personalidad, un gusto, una idea, o cualquier manifestación que hace a su identidad. En ese momento el dato deja de pertenecerle porqué lo ha transferido a otros. Esta actitud puede representar una confidencia y la obligación del otro es conservar el secreto revelado como un derecho que aquél tiene a la reserva.

Se observa así, como la intimidad, atraviesa por el secreto absoluto (porque sólo el individuo sabe del dato que transfiere), para llegar al secreto compartido donde se puede hablar, con mayor precisión, del ámbito de la reserva y confidencialidad.

> En definitiva –afirma Herrán Ortiz- si íntimo es lo que cada persona se reserva para sí y a los demás no es lícito invadir, confidencial es aquello que se revela a alguien con la intención o ánimo de que no sea revelado a los demás sin el consentimiento del interesado. De igual manera, no puede desconocerse que si bien en un primer acercamiento al derecho a la intimidad éste se puede relacionar estrechamente con el "secreto", debe admitirse que la intimidad no implica exclusivamente la ausencia de información sobre la vida de la persona; representa, por el contrario, una necesidad de "vida interior", o relación intra-personal, de reflexión de los propios sentimientos y pensamientos.

Cuando la información es producto de la investigación practicada sobre alguien, y éstas conciernen a la vida y personalidad, se puede presumir que esa búsqueda tiene alguna finalidad, más allá de la simple recopilación y almacenamiento. El individuo tiene desde el hábeas data la posibilidad de saber el objetivo del archivo y solicitar la confidencialidad como un medio de autopreservar su derecho a la intimidad.

> Por ello, la intimidad no es tanto una cuestión de ocultamiento o secreto, que corresponda a terceros en atención a las circunstancias que justificaron su revelación, sino de libertad del individuo, de posibilitar la plena disponibilidad sobre su vida y relaciones personales.

Por su parte la confidencia se resguarda en la confianza depositada en otro, quien se vale de su propia conducta para mantener el ocultamiento, y también, porque no, de cierto grado de complicidad con el dato revelado; el secreto pertenece a la intimidad, como la máxima expresión de la vida interior que no se transfiere. A su turno, la información pesquisada no pertenece al secreto (porque éste no se consigue sin la voluntad del individuo) sino a la intimidad, y el deber de quien obtiene datos que son expresiones de ese derecho, es conservar la confidencialidad como una obligación derivada.

> Por todo ello –concluye Herrán Ortiz- el deber de secreto constituye una de las manifestaciones del derecho a la intimidad, pero no se confunde con él. En ocasiones, el deber de ocultar se limitará a bienes de la personalidad, a la esfera interior de la persona, pero la más de las veces lo que se debe reservar del conocimiento ajeno serán informaciones no íntimas; sin embargo, también estas informaciones constituyen el deber de secreto. Así lo íntimo es lo más personal siendo, por tanto, todo lo íntimo secreto y reservado. Representa, por otro lado, una evidencia que cada persona puede develar, por decisión propia, parte de su intimidad a los demás, naciendo entonces un deber secreto en aquél a quien se ha confiado la intimidad. Por ello, determinados autores han querido ver en el derecho al secreto una especie del derecho a la intimidad.

La interesante diferencia entre secreto y confidencialidad, desde esta perspectiva, sirve para tomar distancias respecto de la protección penal establecida en los artículos 153 a 155 del código, en la medida que estas normas responden a un tiempo distinto, donde la protección se direccionó únicamente a la incolumidad de la correspondencia particular.

> No obstante la jurisprudencia ha buscado cierta actualización en la materia punitiva, habiendo inscripto al correo electrónico en el marco de la defensa penal.

> Confrontar para el caso la sentencia dictada por la Cámara Nacional Criminal y Correccional, sala VI, de fecha 4 de marzo de 1999, en la causa “Lanata”.

Actualmente, y fundamentalmente desde la reforma constitucional de 1994, cabe pensar que así como la justicia remoza los alcances de las normas penales, también la legislación ha evolucionado permitiendo extender la protección a los registros privados contenidos en computadoras o cualquier otro soporte, pues siempre existe en ellos un ámbito propio de la reserva de las personas.

4.6 El derecho al secreto

Esta es una de las cuestiones más difíciles de establecer en el alcance del hábeas data. Se parece a la reserva personal sobre hechos y pasiones que la persona conserva para sí, pero excede la privacidad determinada por uno al ser un aspecto que, pudiendo ser conocido por otros, no se quiere transferir el dato, el pensamiento o la característica, o la cuestión que fuera motivo de expreso ocultamiento.

> Para Santos Cifuentes, por secreto debe entenderse no lo reservado, la vida interior o en soledad, sino aquellas situaciones, pensamientos y datos en general que pertenecen a la persona y que, por su índole o porque así lo quiere aquélla, están destinados a no expandirse ni ser conocido por terceros. Es lo que se mantiene oculto, y si bien muchas veces el ocultamiento es diverso de lo puramente personal, no cabe duda que se refiere a un aspecto del derecho a la intimidad.

El secreto es un misterio individual; es algo que cuidadosamente se mantiene alejado de los demás. La similitud con el estudiado derecho a la reserva y confidencialidad es manifiesta, pero tiene algo más.

En primer lugar la relación entre intimidad y secreto no es permanente, aun cuando sea cierto que el fundamento de lo que se quiere preservar reposa, en última instancia, en una decisión individual que afinca en la parte más íntima de una persona.

> No todo lo secreto será íntimo; aquello que es revelado en determinadas circunstancias o a determinadas personas aunque no se identifique con la interioridad del individuo, con su esencia personal, deberá ser ocultado por aquellos a quienes se comunicó, es decir, tienen el deber jurídico, además de moral, de no compartir la información recibida con terceros extraños.

Si la explicación la abordamos desde la protección a la correspondencia y papeles privados, la cuestión puede ser más clara.

En efecto, el artículo 18 de la Constitución Nacional y distintas normas de los códigos civil y penal, garantizan la inviolabilidad de las cartas y otros papeles privados que contengan la expresión de un pensamiento aunque no esté destinada a ser comunicada a otro, siempre que estén dentro de la esfera de custodia de la persona.

Es decir, la garantía está en el secreto de lo que se dice o escribe, sin importar si las expresiones constituyen revelaciones de intimidades o son hechos intrascendentes. La idea es que la persona tenga libertad para expresar aquello que a otros comunica sin que nadie pueda interferir en forma directa o solapada. Por eso las intercepciones telefónicas son ilegítimas, como lo es también la apertura indebida de una carta, un pliego cerrado o un despacho telegráfico o de cualquier naturaleza.

En relación con ello la Convención Europea para la protección de los derechos humanos* resguarda la capacidad legal de mantener cierta información secreta o fuera del alcance de la autoridad estatal y de otras personas. El artículo 8º se preocupa e insiste sobre la inviolabilidad de la correspondencia, el domicilio y la vida privada y familiar, a excepción que una ley lo autorice expresamente y constituya una medida resuelta dentro de una sociedad democrática. Además, debe revestir el carácter de “necesaria” para sostener la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de las libertades y derechos de los demás.

> Informa Oteiza que la Corte de Estrasburgo interpreta con amplitud el texto de la Convención. En el caso Klass (sentencia del 6/9/78) se analizaba la legislación de

> la por entonces Alemania Federal que permitía un control genérico sobre la correspondencia, los envíos postales y las telecomunicaciones. Con respecto a las conversaciones telefónicas no mencionadas expresamente en el art. 8º el Tribunal estimó que ellas se encuentran comprendidas en las nociones de "vida privada" y de "correspondencia", agregando que el sistema de vigilancia previsto contiene diversas cláusulas destinadas a evitar a un mínimo indispensable el efecto de las medidas de control que limitan a la autoridad administrativa.

Ahora bien, ¿cómo se elabora este principio aplicado al proceso constitucional de hábeas data?

En primer lugar, dando por cierto que *secreto* es lo que cuidadosamente se tiene reservado y oculto, y por tanto que su alcance jurídico consiste en asumirlo como un hecho que se quiere mantener escondido por considerar que su conocimiento podría dañar a alguien. En ambos casos, el término dominante y coincidente es la ocultación.

En virtud de ello, el derecho a mantener oculto los datos obliga a pensar en un destinatario que está impedido de conocerlos, por eso, al hábeas data no es posible estructurarlo como un derecho al secreto personal, es decir, con relación a uno mismo.

En segundo término, el derecho al secreto es una garantía para la confidencialidad de las comunicaciones de cualquier tipo, en cuyo caso, el hábeas data queda fuera del mensaje, en razón de que si hubiera que reclamar por el incumplimiento o la violación del derecho, la vía judicial más idónea sería el amparo.

> Llegado a este punto habría que preguntarse con Velázquez Bautista, acerca de cuál es el contenido del derecho al secreto, y en particular, el "secreto de las comunicaciones". La idea sería que éste ampara tanto la "libertad de comunicación", como el mantenimiento en secreto de las mismas con independencia de cual es el contenido de los mensajes. Sin embargo, no se considerará violación de secreto cuando se autorice su intervención mediante mandato judicial o medie consentimiento.
>
> Por su parte, el artículo 8º de las Directivas de la Comunidad Europea sostienen: 1. *El organismo de telecomunicaciones deberá garantizar una protección adecuada, utilizando las técnicas más avanzadas, de los datos personales contra posibles accesos y usos no autorizados; 2. En caso de que exista un riesgo especial de violación del sistema de seguridad de la red, como por ejemplo, en el ámbito de la radiotelefonía móvil, el organismo de telecomunicaciones deberá informar a los abonados de dicho riesgo y ofrecerles un servicio de cifrado de extremo a extremo.*

4.7 El derecho a la información

El derecho a la información es producto de una sociedad democrática que reclama saber y conocer el complejo mundo que habita y las vicisitudes donde esta inserto.

Sostiene el Tribunal Constitucional español que "*la libertad de información juega un papel esencial como garantía institucional del papel democrático que inspira nuestra Constitución, el cual presupone, el derecho de los ciudadanos a contar con una amplia y adecuada información respecto a los hechos que les permita formar sus convicciones y a participar en la discusión relativa a los asuntos públicos. Es este aspecto el que puede explicar que este tipo de comunicados haya aparecido en otros periódicos sin que ello haya motivado la intervención de la justicia penal, como se desprende de la documentación acompañada en autos"*.

El derecho a estar informado tiene una doble e interesantes facetas. Mientras por un lado privilegia el derecho de los medios de comunicación a publicar y difundir sin restricciones ni límites a la libertad de prensa (inclusive en el artículo 43 se lee la previsión para que el hábeas data no afecte las "fuentes de información periodística); por otro se defiende el derecho individual de las personas para estar informado sobre datos que le conciernan y estén archivados o registrados en una base específica.

Además, puede ocurrir que una publicación ofenda o de una versión equívoca de los hechos, en cuyo caso, obrarán los derechos repulsivos consecuentes como la querella penal o el derecho de rectificación o respuesta, pero éstos no son temas de esta obra.

> El contenido de un derecho de la información -dice Gutierrez Castro- no se agota con el contenido de un derecho a la información, sino que, "la información" es hoy objeto de un tratamiento especial por los juristas y el derecho a ser informado por la prensa es sólo uno de sus aspectos, ya que tiene características propias y opera tanto como derecho individual, político y social, amén de su enorme interés como garantía institucional de la democracia. Así, junto al derecho a la información (libertad de prensa en toda su gama de aspectos y medios), aparecen otros derechos subjetivos que tienen como objeto directo "la información", tal es el caso, del derecho de acceso a documentos, registros, archivos y papeles del gobierno (transparencia de la administración).

Sí interesa observar cómo el derecho a la información puede aplicarse en el hábeas data como derecho a la verdad de saber si está en un banco de datos (derecho de acceso) y, en su caso, cuál es el destino que se quiere aplicar a ellos (con el fin de resolver su derecho a rectificar, actualizar, cancelar o solicitar la confidencialidad de ellos).

Nuestra Corte Suprema de Justicia en la jurisprudencia más actual ha desarrollado esta idea, interpretando con amplitud el sesgado artículo 43. El Juez Petracchi en la causa "Urteaga" sostuvo que "*proteger el derecho a conocer todo lo relativo a la muerte de un familiar cercano –ocurrido en luctuosas circunstancias que vivió el país- significa reconocer el derecho a la identidad y a reconstruir la propia historia, los cuales se encuentran estrechamente ligados a la dignidad del hombre*".

Ni más ni menos que saber lo que ocurrió: es un derecho a la información, y el hábeas data el camino apropiado.

Es igual la inteligencia que acuerdan otras constituciones, como Brasil* (art. 5.XXXIII) cuando dispone que todos tienen derecho a recibir de los órganos públicos informaciones de su interés particular, o de interés colectivo o general, que serán facilitados en el plazo señalado en la ley, bajo pena de responsabilidad, salvo aquellas cuyo secreto sea imprescindible para la seguridad de la sociedad y del Estado.

La causa "Ganora" fallada por el Tribunal Superior de Justicia de la Nación el 16 de setiembre de 1999, insiste y concluye que "*la obtención de información sobre datos personales obrantes en los organismos y fuerzas de seguridad halla adecuación legal en la acción de hábeas data; ello sin perjuicio de que el suministro de esa información pueda, eventualmente, afectar la seguridad, la defensa nacional, las relaciones exteriores o una investigación criminal, cuestión que en cada caso deberá ser invocada por el titular de la respectiva institución*".

Vamos entonces por un buen camino, logrando encausar los bienes jurídicos que el hábeas data respalda. El derecho a la información, sin lugar a dudas, es un fundamento esencial.

4.8 El derecho al olvido

Esta es una parte, un extracto del derecho a la información exacta. En la especie se trata de preservar la intimidad de la persona en sus actuales circunstancias, procurando que los datos compilados en su vida no lo conviertan en un reflejo de lo que fue antes de lo que es.

Existe otra vertiente que no escala en esta cuestión, y proviene del artículo 14.1 de la Convención Americana de Derechos Humanos que establece, con carácter vinculante, que *"toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley"*.

La facultad de requerir la cancelación o la corrección de los datos inexactos, otorga el denominado *derecho al olvido*, esto es, el principio a tenor del cual ciertas informaciones (v.gr.: antecedentes penales prescriptos) deben ser eliminadas de los archivos transcurrido un determinado tiempo desde el momento en que acaeció el hecho a que se refieren para evitar que el individuo quede prisionero de su pasado.

La corrección de los archivos puede efectuarse por el mismo sistema que los contiene, sea ya por la aclaración que se peticione, o por la información corroborada por la base de datos.

> En el mecanismo articulado por el Consejo de Europa, el Convenio 81 previene un "mínimo necesario" de exactitud en los registros, comprendiendo como tales, la pertinencia, la corrección y la conservación actualizada de los archivos. Estos organismos de registración, públicos o privados, generalmente pueden oponerse a las rectificaciones cuando ellas se promueven por quienes no son directamente interesados, excepción hecha de las pretensiones sostenidas por personas que invoquen un legítimo interés y la mantención de los datos les provocare riesgos o daños inminentes.

Por tanto, la subsistencia de un dato caduco en un archivo, registro o base de datos es ilícito, toda vez que no media correspondencia con la actualidad requerida y, además, no media consentimiento del interesado ni existe un interés público prevalente.

> Dato caduco es el que por efecto del transcurso del tiempo ha perdido virtualidad y ha devenido intrascendente a los efectos de cualquier efecto jurídico relativo a la ejecutabilidad. El Código Penal, por ejemplo, al referirse a los datos de reincidencia, dispone que "*el registro de las sentencias condenatorias caducará a todos sus efectos, después de transcurridos cinco (5) años desde su extinción para las condenas a pena de multa o inhabilitación. En todos los casos se deberá brindar la información cuando mediare expreso consentimiento del interesado…*"

De este modo queda emplazado en esta suerte de "derecho al olvido" un fundamento más para localizar los contenidos tutelares del hábeas data.

> Según Palazzi, el tema es complejo, pues plantea la posibilidad de aceptar en el proceso constitucional otros motivos distintos a la falsedad o discriminación, lo que ratifica como posible. De otro modo, la difusión de datos pasados puede lesionar el derecho a la privacidad.

4.9 El derecho a la identidad

En terreno de ir precisando el objetivo del artículo 43 párrafo tercero de la Constitución Nacional, se podría apurar una respuesta sosteniendo que la idea fue generar un marco de protección a los datos, pero que al estar inserto en el desarrollo del derecho al amparo, la persona humana encuentra un campo más propicio para ampliar el acotamiento natural que tiene la acción de hábeas data.

En los hechos, a partir de los derechos personalísimos donde la intimidad aflora como esencial y contundente, aparece el derecho a la identidad que supone, en los términos como De Cupis lo ensaya, el ser en sí mismo, la persona con sus propios caracteres y acciones, constituyendo la misma verdad de la persona que, por tanto, no puede en sí y por sí, ser destruida: porque la verdad, por ser la verdad, no puede ser eliminada.

> Según Cifuentes, intimidad e identidad difieren. La diferencia está en que la primera no tutela las reservas personales y familiares como un ámbito que tiene el sujeto para desarrollarse, sino la verdad de su perfil sociocultural. Y este perfil socio cultural puede estar en el exterior, no ser privado ni íntimo, sino por el contrario dado al público. Se ataca la intimidad mostrándose la verdad de lo que no se desea difundir. Se ataca la identidad desfigurando la personalidad del sujeto y mostrándola distinta de lo que es. Esta consiste en un conjunto de actividades públicas caracterizantes de dicha personalidad, que puede ser inexactamente deformada. En general, en la intimidad esa actividad pública no existe. Pero es claro que aprovechando lo recoleto del individuo, puede a la vez falsearse su perfil espiritual, con lo que podría verse producido un doble ataque de su persona: lo reservado y la identidad dentro de lo reservado.

La identidad tiene aspectos que no suponen, en principio, problemas que deban resolverse en la vía del hábeas data, tales como los derechos derivados del nombre o la propiedad intelectual. Aunque la ley 18.248* (ley del nombre) admita acciones para reclamar, contestar, suprimir u oponerse a decisiones vinculadas con la identificación personal, ellas no afectan derechos de naturaleza constitucional en la medida que se tratan de atributos jurídicos de la persona que tienen un reglamento especial para su tratamiento y consideración.

Lo mismo puede aplicarse a los derechos emergentes de la creación artística o literaria, los cuales a pesar de poderse registrar y archivar en un sistema informatizado, cuando son violados o amenazados encuentran un mecanismo particular para su defensa.

La identidad fundamental, como derecho personalísimo y englobado dentro de los derechos humanos, pretende amparar el perfil que hace a una personalidad. Es parte del derecho a la imagen, pero al mismo tiempo, lo comprende.

> La identidad del ser humano, en tanto éste constituye una unidad, presupone un complejo de elementos, una multiplicidad de aspectos esencialmente vinculados entre sí, de los cuales unos son de carácter predominantemente espiritual, psicológico o somático, mientras que otros son de diversas índole, ya sea cultural, religiosa, ideológica o política. Estos múltiples elementos son los que en conjunto, globalmente, caracterizan y perfilan el ser “uno mismo", el ser diferente a los otros, no obstante ser todos iguales en cuanto pertenecen a una misma especie, entendiéndose en definitiva “como identidad personal el conjunto de atributos y características que permiten individualizar a la persona en sociedad. Identidad personal es todo aquello que hace que cada cual sea “uno mismo” y “no otro”. Este plexo de características de la personalidad de “cada cual” se proyecta hacia el mundo exterior, se fenomenaliza y permite a los demás conocer a la persona, a cierta persona, en su “mismidad”, en lo que ella es en cuanto específico “ser humano”, para utilizar la expresión de Fernández Sessarego.

Cualquier información sobre este perfil puede ser motivo de la acción constitucional, por ejemplo, cuando se registra la pertenencia o afiliación política; o las cirugías practicadas en su cuerpo; o la filiación que le pertenece, etc.

> Agrega Cifuentes que es cierto que el sexo, la filiación y la edad registrables identifican. Es cierto que forman parte de la unidad-hombre y están en su proyección existencial desde el origen. También la formación genética forma parte de la combinación biológica, pero, sobre todas estas manifestaciones de la persona, domina, es primero y más visible, la conformación orgánica y los derechos respectivos. Creo que, ante todo, la ligadura de estos derechos se enraíza con las expresiones corporales del ser, y que desde el punto de vista de la caracterización diferenciadora, juegan allí un papel principal, siendo según ese orden la identidad cultural subordinada, secundaria. De todas maneras, cualquiera sea la ubicación del analista, la de la integridad orgánica o la de la identidad personal, son especies de derechos personalísimos que merecen tutela semejante. También la imagen debe distinguirse. No sólo por su condición ajena a la fuerza del movimiento cultural propia de la identidad, aunque pueda modificarse con la cirugía plástica o por accidentes, lo que no significa que sea una manifestación dinámica, sino también porque la violación es el aprovechamiento veraz, y, en la identidad, se trata de evitar la falsedad y mantener la verdad.

Observado atentamente, el derecho a la identidad puede ser atacado también desde la ofensa al honor. De este modo, si alguien expusiera un agravio contra la honorabilidad que identifica a la persona, evidentemente y más allá de las pretensiones penales que pudieran caber, el registro de esa expresión puede evitarse desde el hábeas data, sea a través de la supresión o la corrección por el dato exacto.

Y aún más lejos se puede llegar, por cuanto desde este derecho a la identidad se puede exigir el “derecho a la verdad”, y perseguir la revelación de datos que permitan conocer el origen familiar, como una legítima manifestación del derecho humano a saber la verdad de su historia.

La jurisprudencia acompaña esta proyección de acceder a los datos personales, entre los que se halla la ascendencia biológica que permite desentrañar la propia identidad del sujeto. Sin embargo, el hábeas data debe ser el punto de inflexión que permita el equilibrio prudente, en virtud de que un banco genético violaría el derecho a la identidad del niño.

En síntesis, el derecho a la identidad permite generalizar el objeto tutelado sin caer en el riesgo limitativo de las fórmulas constitucionales rígidas e inalterables, donde la precisión matemática no tiene cabida.

4.10 El derecho a la autodeterminación informativa

A medida que se tamiza el derecho constitucional creado, la última escala pareciera estar en la autodeterminación informativa. Es decir, desde la amplia libertad creadora que permite el derecho a la intimidad se llega al reducto de la libertad informática controlada por la persona respecto a sus propios datos.

Es verdad que entre uno y otro extremo se levantan voces polémicas para el reconocimiento propio e independiente de la autodeterminación o propiciando un refuerzo de las garantías de la intimidad, pero en ambos casos, queda de manifiesto que el problema está en el control que se tiene sobre los registros o archivos personales.

> Las constantes disquisiciones en torno a la independencia de un derecho a la autodeterminación informativa han evitado acuerdos coincidentes. Según Herrán Ortiz se distinguen dos sectores enfrentados, uno de los cuales rechaza la consideración del derecho a la autodeterminación informativa como derecho fundamental argumentando que es suficiente para ofrecer garantías individuales adecuadas una reformulación del derecho a la intimidad; el otro sector sostiene, por el contrario, la idea de la necesidad insoslayable de admitir la existencia de un nuevo derecho fundamental, cuya construcción se asienta sobre el reconocimiento al individuo de unas facultades de disposición y decisión respecto a sus propios datos personales que no sería posible deducir del tradicional derecho a la intimidad.

La autodeterminación, como lenguaje técnico, tiene reminiscencias equívocas que nos sugiere sustituirlo por el "*derecho a la libre disposición de los datos personales*".

Lo mismo sucede cuando se aplica el término "libertad informática" pues pareciera indicar la libre utilización de los medios informáticos en el tratamiento de los datos, cuando en realidad, se trata precisamente de lo inverso: poner límites y control a esa libertad.

De esta manera, el hábeas data surge como la mejor herramienta procesal para encausar el amparo prometido, sea para acceder a las informaciones que sobre él se tengan, así como para controlar la exactitud y autorizar, o no, la circulación de esos datos.

> Si se admite que el derecho a la autodeterminación informativa reconoce la facultad del individuo a decidir cuándo y cómo está dispuesto a permitir que sea difundida su información personal o a difundirla él mismo, esto es, la facultad de la persona de controlar y conocer los datos que sobre ella se encuentran en soportes informáticos, se reconoce al individuo una tutela legal para conocer y acceder a las informaciones almacenadas en ficheros de datos que les conciernen, así como la facultad de controlar por el interesado la calidad de los datos inexactos o indebidamente automatizados y consentir su transmisión que define el contenido que integra la libertad informática.

Sin embargo, la garantía no reposa en el reconocimiento de un derecho subjetivo propio e individual que pueda catalogarse, indeseablemente, como derecho patrimonial (tal como acontece con la profusa enumeración de derechos que emanan de los códigos sustanciales). La fuente que nutre la defensa constitucional no es sobre un derecho de propiedad sobre los datos, cual si ellos fueran el objeto de pertenencia exclusiva que resultan inalienables e intangibles. El basamento está en la libertad de resolver con

plena libertad sobre el destino que se pretende dar a los datos y, en su caso, si se autoriza o no el acopio informativo de ellos.

> Una interesante conferencia de la profesora de la Universidad de Buenos Aires, Adelina Loianno, expuso el carácter de derecho subjetivo del dato personal, confiriéndole el alcance de un derecho de propiedad. De esa manera, al subjetivizar el objeto, eliminó el problema del carácter constitucional de tal derecho, o si es preciso encontrar la garantía absorvida por el artículo 43 para dar respuesta a la protección de ellos.

Por eso, algunos autores prefieren hablar de intimidad informática para aludir al bien jurídico protegido frente al poder informático. Sería una proyección de los derechos personalísimos de fuente constitucional.

> En este sentido, Ruíz Miguel manifiesta que esta identificación constitucional constituye el medio idóneo para eludir las dificultades que se derivan de la protección de la persona frente a la utilización informática; así, entre las posibles dificultades cita a la problemática en torno al rango de la ley que desarrolle este derecho, el acceso al amparo ordinario y al constitucional reconocidos en el artículo 53.2 de la Constitución española.

Ahora bien, si uno aplica esta idea también puede tomar una dirección errada, pues la defensa constitucional emergente del artículo 43 quedaría circunscripta al campo de los archivos personales o familiares eludiendo la amplitud que antes le dispensamos.

De todos modos, la libertad para disponer sobre los datos personales sería una especie dentro de la generosa tutela judicial prometida a los derechos derivados de vida privada (intimidad y privacidad).

> Dice el Tribunal Constitucional de Alemania que *"no serían compatibles con el derecho a la autodeterminación informativa un orden social y un orden jurídico que hiciese posible al primero, en el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo sabe algo sobre él* (Cfr. Herrán Ortiz, cit., pág. 88).

La construcción de este nuevo derecho fundamental excede la tradición jurídica que tuvo el derecho a la intimidad, permitiendo que toda información que concierna a cualquier persona pueda ser controlada por él mismo como un freno al poder informático.

> Hoy nadie duda que la vida privada de la persona es un bien que debe respetarse, porque el ataque a la misma es susceptible de causar un daño irreparable a la persona en una sociedad como la actual cuyo único límite al almacenamiento y tratamiento de datos personales es el que procede de la imaginación humana. Información relativa al ocio, a los comercios o a la educación de los hijos, así como a las actividades profesionales no son inocuas en nuestro desarrollo personal y en la honorabilidad o imagen que se ofrece al exterior, por lo que oportunamente entrelazadas y almacenadas "dicen" mucho de cada individuo, y de su personalidad; inmiscuirse en ellas, para conocerlas y tratarlas sin consentimiento representa un peligro del que debe ser consciente si se quiere una sociedad libre y en igualdad de oportunidades. Sentir que constantemente se está siendo observado, seguro de que la totalidad de las acciones serán "registradas" impide el derecho a manifestarse en una sociedad con libertad y dificulta el libre desarrollo de la personalidad. Habida cuenta de los nuevos peligros y amenazas que el tratamiento informático trae consigo, se sugiere una conceptuación del derecho a la autodeterminación informativa a través de una extensión de su protección frente al uso ilícito o abusivo de la informática a cualquier información personal que represente una amenaza para la persona en "manos de terceros"; la interceptación no consentida de la información, debe controlarse y limitarse sin detenerse a averiguar la índole íntima o no de la información (Cfr. Herrán Ortiz, cit., pág. 105).

En pocas palabras, el derecho a la libre disposición de los datos personales supone recrear un derecho fundamental que, derivado del derecho a la vida privada del hombre, le permite resolver por sí mismo el tratamiento que quiera asignar a los datos que sobre su persona se almacenen con destinos diferentes. La garantía específica para salvaguardar el derecho es el proceso constitucional de hábeas data.

De este modo se responde a la especificidad que contiene la promesa constitucional, ampliando las fronteras de la intimidad, el honor y la propia imagen, para ocupar espacios mucho más ambiciosos que los recortados en el párrafo tercero del artículo 43 de la Ley Fundamental argentina.

> Una vez más transcribimos la opinión de Herrán Ortiz, quien concreta el alcance del derecho en estos términos: "Si la protección de datos personales no ha podido enmarcarse en los instrumentos de tutela propios del derecho al honor o a la propia imagen por la limitación conceptual y garantista que implican tales derechos, tampoco el derecho a la intimidad resulta de utilidad para explicar y fundamentar el fenómeno de la autodeterminación informativa. Desde la consideración de un sistema de resarcimiento o meramente indemnizatorio no sería deseable ni posible jurídicamente estructurar el sistema de protección de datos, porque, en ese caso, la protección de la persona se vería limitada a medidas de naturaleza represiva, con lo que un aspecto fundamental de la protección de los datos personales, cual es el carácter preventivo o precautorio, carecería de total relevancia jurídica. El sistema jurídico que se acoge desde el derecho a la intimidad no responde a unos criterios fundamentales de precaución sino que deben identificarse con un sistema puramente indemnizatorio para la víctima del agravio. Como fácilmente puede comprenderse, con este esquema parece especialmente complicada la configuración jurídica de la protección de los datos personales desde la perspectiva del derecho a la intimidad; al afectado, titular de los datos, se le atribuyen en las leyes de protección de datos personales derechos y facultades individuales que sólo pueden contemplarse desde la óptica de un derecho principalmente preventivo que dota al individuo de garantías suficientes para evitar y controlar la utilización abusiva o ilícita de la información personal registrada en soportes informáticos.

4.11 El derecho a la vida privada

Toda persona tiene derecho a vivir su propia vida; a desarrollarse conforme pueda y pretenda; a generar relaciones con otros o a mantenerse ajeno y en soledad. Los comportamientos del hombre serán externos cuando se proyecten hacia otros dando publicidad a esos actos; o serán internos e intransferibles cuando permanecen en el espacio interior de la persona. Este es el terreno de lo privado, lo propio, la esfera de máxima intimidad.

La vida privada es una parte esencial de la persona, que sin resultar secreta ni de carácter íntimo, merece el mayor de los respetos para garantizar el normal desarrollo de las libertades.

> La doctrina suele distinguir entre "vida privada", haciendo referencia a una esfera de retiro y aislamiento donde los demás dejan en paz al sujeto; e "intimidad" por la cual el individuo tiene un mundo propio, fuera de los ojos de los demás. Mientras el derecho a la intimidad tutela la zona espiritual, reservada, de la persona que permanece en su interior, referida a la conciencia de sí mismo como ser humano libre en su ámbito moral e intelectual; el derecho a la vida privada se manifiesta a través de la realización de actividades y comportamien-tos en un ámbito estrictamente personal, de amistad o familiar en que el sujeto decide desarrollar su existir, preservando esa esfera de su existencia del conocimiento general.

Es verdad aquella reflexión de Sartre cuando dice que la mirada del otro nos esclaviza, pues trasciende la metáfora, porqué cuando alguien nos mira nos juzga y, cuando nos juzga, de algún modo, nos domina.

La opinión pública se forma, en buena medida, con este juego sutil de la observación penetrante; de otro lado, la soledad, parece emerger como remedio que relaja la tensión que produce la presencia de quienes nos miran para analizarnos.

La presencia informática en la vida de las personas es cotidiana; se manifiesta continuamente desde nuestros primeros pasos en el día y no deja de abandonarnos en la práctica frecuente. A veces, la voluntad implícita de la persona reporta una autorización no pensada para quien está observándonos y registrando esos actos y costumbres (V.gr: encuestas; inscripciones en concursos; planillas que se completan a ciertos fines, etc.). Otras, la información se debe ofrecer como un requisito para "entrar" en un ámbito determinado (V.gr: asociaciones, entidades financieras; bancos; hoteles, etc.); también el Estado almacena nuestros datos con finalidades diversas (censo poblacional; identidad de las personas; historias médicas; etc.) y así, sucesivamente, el hombre encuentra que su vida está archivada prolijamente en un banco de información.

Lo trascendente no es el carácter más o menos íntimo de los datos personales que se cedan, sino las posibilidades infinitas de la técnica informática para tratar esos datos (posiblemente irrelevantes cada uno de ellos para la intimidad de su titular) y extraer de ellos informaciones precisas.

> Sostiene el Tribunal Constitucional español que *"el incremento de los medios técnicos de tratamiento de la información puede propiciar la invasión de la esfera privada, haciéndose necesario la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestos en práctica a través de cualquier instrumento que produzca tal efecto, y a incrementar las facultades de conocimiento y control que se otorguen al ciudadano para salvaguardar el núcleo esencial de su derecho…Las normas autorizatorias de recogida de datos, incluso con fines legítimos y de contenido aparentemente neutro, deben incluir garantías adecuadas frente a su uso potencialmente invasor de la vida privada, por lo que si no lo hacen pueden y deben considerarse vulneradoras de la intimidad"* (TC, Sentencia del 9 de mayo de 1994).

Por tanto no hay datos que sean secretos absolutamente sino en la medida que se han conocido, a cuyo fin, regresamos al punto de la confidencia o al derecho a la reserva que antes mencionamos.

Es decir, la garantía constitucional del proceso de hábeas data procura que la vida privada de los hombres no sea invadida ilegítimamente por el acopio o almacenamiento de datos personales, ni que ellos sean difundidos sin la expresa autorización del titular o de quien tenga derechos de representación.

> De algún modo, esta línea de pensamiento se asocia a la diferencia que hacía Nino y que explica con suficiencia Eduardo Oteiza cuando expone que la noción de privacidad pareciera abarcar dos conceptos independientes que garantizan ámbitos distintos. Por una parte, nos encontramos con las acciones privadas que no dañan a terceros y sólo afectan a la persona que las realiza. Ellas solamente entran en juego con la moral personal, al consistir en la elección de aquellos aspectos que conforman el plan de vida de cada individuo. En el plano normativo el artículo 19 de la Constitución Nacional acepta el principio liberal de la autodeterminación, que deja librada a la decisión individual las acciones privadas. Sin embargo, una lectura restrictiva, fundada en ideas perfeccionistas, que consideran el Estado puede interferir con conductas que no lesionan a terceros, bajo la pretendida defensa de sus propias convicciones y creencias sobre una proyección comunitaria, ha limitado el marco de libertad en áreas sensibles para la ética individual, apoyada en su propia apreciación de la moral pública.
>
> La diferencia entre moral pública y ética privada ha sido explicada a partir de la noción de privacidad, que se ha utilizado, también, para identificar a aquellas circunstancias que caen bajo el dominio exclusivo de una persona, por su voluntad de no dejarlas trascender a otros. Nino, siguiendo a Parent, vinculaba el concepto de privacidad con la posibilidad irrestricta de realizar acciones privadas que no son objeto de una moral pública, separándolo de la idea de intimidad. Asociaba a esta última con el derecho a que los demás carezcan de información

> sobre hechos personales, cuando el sujeto al que se encuentran asociados niegue su consentimiento. Consiste, entonces, -concluye Oteiza- en la exclusión de información documentada accesible al público, mediante la potestad de limitar el conocimiento sobre aspectos personales, cuando el mismo no se encuentre justificado por una razón que en la tensión entre la reserva y la publicidad ceda en favor de la primera.

A pesar de ello, no es la propia determinación sobre la transmisión del dato lo que caracteriza el derecho a tener una vida privada, sino el derecho a mantenerse ajeno a las intromisiones ilegítimas o legítimas pero infundadas.

Asimismo, muchas veces el límite entre intimidad y privacidad es difuso y no se podría hallar un derecho preciso que alimente la fuente de protección respectiva; en definitiva, todo conduce a sostener que la limitación que se persigue pretende, como mínimo, que nadie se entrometa en la vida de otro sin tener consentimiento para ello, y que el individuo mantenga la libertad de resolver, en todo tiempo y espacio, que aspectos de su vida personal quiere ocultar o trascender.

> En opinión de Bianchi, la distinción entre privacidad e intimidad es más aparente que real. Para ello se vale de algunos ejemplos: una reunión es íntima o privada cuando asisten a ella algunas pocas personas elegidas. La correspondencia que intercambian dos individuos es íntima o privada entre ellos y no debe ser conocida ni divulgada por otros. La relación carnal entre dos personas es íntima o privada entre ellos y no puede ser objeto de interferencia alguna. En todo caso –y con ánimo de formular alguna diferencia- podría decirse que íntimo, es más privado aun que lo privado. El fuero íntimo de una persona es lo que sólo le pertenece a ella y está exento de cualquier objetivación forzosa. Desde este punto de vista, afirma el prestigioso publicista argentino, el pensamiento es íntimo mientras no sea objeto de exteriorización y se transforma en privado cuando es divulgado en un pequeño o limitado círculo.

Cuando se estudia el derecho a la vida privada, en realidad, no se demanda que sea éste el fundamento del hábeas data, sino que es una parte de todo ese cuadro de derechos que mejoran el perfil del proceso constitucional creado.

Observado atentamente el fenómeno en el tiempo que transcurre, se puede advertir que la distancia está trazada entre la tutela que deriva del derecho a la intimidad y, en su caso, del carácter individual que tiene, y por ello, el signado de derecho personalísimo. Frente a la corriente que postula la relación con el "tratamiento de los datos", en cuyo supuesto la atención no se fija tanto en la persona como sí en el interés en preservar la veracidad de la información y el uso que de ella se hace.

> Sostiene Garzón que la categoría de "protección de datos" ha surgido para aplicarse a nuevas realidades jurídicas, que sólo parcialmente pueden ser descriptas o fundamentadas a través de la noción tradicional de "intimidad". El derecho a la protección de datos, según su propia expresión, pertenece al contexto de la era informática y ciertamente resulta atrevido afirmar que esta compleja disciplina legal estuviera ya implícita en las referencias generales al derecho a la intimidad inserta en cuerpos normativos de ámbito nacional o internacional de la era preinformática.

4.12 El derecho a la dignidad personal

La voz "dignidad", dice el Diccionario de la Real Academia española, cuando se usa de una manera absoluta, indica siempre buen concepto y se utiliza en contraposición a indigno.

También es la gravedad y decoro de las personas en la manera de comportarse.

De algún modo, la dignidad, en los términos como se presenta, puede englobar los supuestos de defensa al honor, la imagen y reputación que antes desarrollamos.

Sin embargo, es algo más.

> Miguel A. Ekmekdjian, que en nuestro país es pionero entre los autores que desarrollan el "derecho a la dignidad de las personas", afirma que el fundamento del *hábeas data* es otorgar una garantía especial al derecho a la intimidad. Agregando que el derecho a la privacidad o a la intimidad es una consecuencia o derivación del derecho a la dignidad.

Ese "plus" proviene de su propia generalización. Es un concepto jurídico que identifica varios presupuestos, pero donde se destacan especialmente dos: de un lado, la posibilidad efectiva de encontrar una respuesta positiva dentro del ordenamiento legal para defender los derechos de la intimidad, que es de carácter personalísimo; y por otro, la configuración en los correlativos términos de reserva de una esfera de acción humana y de la consiguiente capacidad de generación de una privacidad protegida mediante el correspondiente poder de exclusión.

> En cuanto al bien jurídico protegido –sostiene Martínez Sospedra- la doctrina más aceptada subraya que el mismo consiste cuasi exclusivamente en la libertad de disposición sobre el ámbito de lo íntimo, dimanante de la propia dignidad…La diferenciación entre asuntos privados y asuntos públicos, entre vida privada y vida pública, constituye una estructura cultural sin cuya preexistencia y hegemonía social, poco menos que absoluta, es impensable el mismo régimen de Estado, y en todo caso, sin la cual es impensable la concepción moderna de la libertad en términos de autodeterminación personal y del consiguiente poder legal de exigir a los demás, incluidos los poderes públicos, las conductas necesarias para asegurar su subsistencia y reproducción. En consecuencia es predicable de la vida privada, y de la intimidad con mayor motivo al ser ésta el eje o centro de aquella, la doctrina del papel institucional de las libertades que la amparan.

Si tomamos la dignidad como género desde el cual proyectar los contenidos que ocupa el hábeas data, se consigue vulnerar el reducto de los presupuestos que tiene el artículo 43 constitucional.

En efecto, la norma sólo menciona los casos de acopio informativo sobre las personas, con el fin de evitar inexactitudes en la transmisión de esos datos, o que el archivo donde los contiene sea una fuente de discriminación para los individuos. Este sería el campo del proceso constitucional.

Sin embargo, si la dignidad se aplica como marco de referencia que permite ampliar el objeto y las pretensiones, toma sentido y fundamento la sentencia de la Corte Suprema de Justicia de la Nación en el "caso Urteaga".

> Recordemos algunos párrafos de esta sentencia. Inicialmente se sostuvo que "la ausencia de normas regulatorias de los aspectos instrumentales de la acción de hábeas data no es óbice para su ejercicio, incumbiendo a los órganos jurisdiccionales determinar provisoriamente –hasta tanto el Congreso Nacional proceda a su reglamentación-, las características con que tal derecho habrá de desarrollarse en los casos concretos. El voto del ministro Bossert, ejemplifica la generalidad del caso y la apertura que se consigue desde esta visión. Dijo: "Los derechos de los hombres que nacen de su propia naturaleza, no pueden ser enumerados de manera precisa. No obstante dicha deficiencia de la letra de la ley, ellos forman el derecho natural de los individuos y de las sociedades, porqué fluyen de la razón del género humano, del objeto mismo de la reunión de los hombres en una comunión política y del fin que cada individuo tiene derecho a alcanzar.

Surge así una primera proyección en el llamado "derecho a la verdad" antes referido. De igual modo aparecen los derechos a la reserva y confidencialidad, que no deben asociarse a la idea del secreto absoluto de la persona o de la inabordable posibilidad de conocer aspectos de su intimidad.

En los hechos, la dignidad no supone que cuanto menos se conozca de uno, y cuanto más se conserve en secreto, permite reservar la intimidad en su mejor hábitat. En realidad, lo perseguido no es ocultar la información relativa a una persona, sino que ésta pueda desarrollar su vida con libertad y posibilidades de resolver, por sí mismo, que aspectos de su vida admite poner en exposición y conocimiento de los demás.

> Ya se ha indicado –dice Herrán Ortiz- que no es mayor el ámbito de intimidad cuanto menos se conozca de la vida personal y familiar, que la intimidad no se debe vincular directamente con la reserva u ocultamiento de la información relativa a la persona, sino con el libre desarrollo interior de una vida individual que faculta a la persona a conocerse y realizarse intelectual y psicológicamente. Es por ello, que aunque los demás penetren en la vida privada ajena conociendo aspectos del mundo interior, a ellos sólo acceden a través de lo que la persona les facilita, pero además, les será imposible acceder al "mundo interior", integrado por los más valiosos sentimientos, pensamientos y recuerdos de la persona, en los que cada individuo se recrea y proyecta como ser humano. En resumen, la intimidad constituye un bien personal al que, en modo alguno, puede renunciar sin resentirse en su dignidad humana.

Por eso intimidad y privacidad no son términos contrapuestos, sino manifestaciones de la vida. Una que se conserva "hacia adentro" y reposa en los deseos, los sentimientos, las inclinaciones, los miedos, etc.; y otra que ocurre en el diario vivir, el hombre "hacia afuera", con sus relaciones, sus compromisos, su imagen y formación de una personalidad social que, de alguna manera, se debe distanciar de la personalidad familiar. No porque sean diferentes, sino porque la privacidad es distinta.

En suma, todo queda enmarcado por la dignidad. Una vida digna tiene un aspecto ético y moral que hace a una filosofía personal de la conducta; y también una proyección necesaria de los límites que deben imponerse a los demás para evitar agresiones innecesarias a los derechos de la personalidad.

Bibliografía Capítulo I

Alvarez Larrondo, Federico Manuel, *El hábeas data argentino*, en Doctrina Judicial, 1999-3, pág. 10 y ss.

Baigorria, Claudia Elizabeth, *Algunas precisiones sobre la procedencia del hábeas data*, en Revista La Ley, 1996-C, págs. 472 y ss.

Basterra, Marcela I., *Hábeas data: derechos tutelados*, Revista Doctrina Judicial, 1993-3, págs. 77 y ss.

Belforte, Eduardo A. – Zenere, Gisela G., *Derecho a la identidad*, Jurisprudencia Argentina, semanario nº 6030 del 26 de marzo de 1997.

Bianchi, Alberto B., *Hábeas Data y derecho a la privacidad*, publicado en El Derecho, tomo 161 págs. 866 y ss.

Bidart Campos, Germán J., *¿Hábeas data o qué? ¿Derecho a la verdad o qué?*, en suplemento de Derecho Constitucional, Revista La Ley, del 15 de febrero de 1.999, págs. 21 y ss.

Castán Tobeñas, José, *Derecho civil español, común y foral*, tomo 1 volumen II, editorial Reus, Madrid, 1984.

Catalán González, Miguel, *Descrédito, intimidad y encubrimiento*, en "Sobre la intimidad", editorial Fundación Universitaria San Pablo C.E.U., Valencia, 1996.

Cifuentes, Santos, *Derechos personalísimos*, editorial Astrea, Buenos Aires, 1995.

Concepción Rodríguez, José Luis, *Honor, intimidad e imagen*, editorial Bosch, Barcelona, 1996.

Dalla Vía, Alberto R., - Basterra, Marcela Izascum, *Hábeas data y otras garantías constitucionales*, editorial Némesis, Buenos Aires, 1999.

De Cupis, Adriano, *I diritti della personalità*,editorial Giuffrè, Milan, 1982.

Ekmekdjian, Miguel Angel, *El hábeas data en la reforma constitucional*, en Rev. La Ley, 1995-E, págs. 946 y ss.

Fernández López, Juan Manuel, *El derecho a la privacidad y su frontera en los demás derechos humanos,* en "XX Conferencia Internacional de autoridades de protección de datos" (1998), editado por la Agencia de Protección de Datos, Madrid, 1999.

Fernández Sessarego, Carlos, *Derecho a la identidad personal*, editorial Astrea, Buenos Aires, 1992.

G. Garzón Clariana, *El marco jurídico de los flujos internacionales de datos,* IBI, Doc. TDF 206, Roma, 1984.

García San Miguel Rodríguez-Arango, Luis, *Estudios sobre el derecho a la intimidad*, editorial Tecnos-Universidad Alcalá de Henares, Madrid, 1992.

Gitrama González, Manuel, *Derecho a la propia imagen*, editorial SEIX XI, Madrid, 1962

Gozaíni, Osvaldo Alfredo, *El derecho de amparo,* editorial Depalma (2ª edición), Buenos Aires, 1998.

Gutierrez Castro, Mauricio, *Derecho a la información. Acceso y protección de la información y datos personales*, en 51º período ordinario de sesiones OEA/Ser.Q, 4/29 de agosto de 1997. CJI/SO/doc. 9/96 rev. 2, Río de Janeiro, Brasil.

Loianno, Adelina, *Conferencia pronunciada en las Jornadas Internacionales sobre Defensa de la intimidad y de los Datos Personales: Hábeas Data*, Universidad de Belgrano, 14 de agosto de 2000.

Herrán Ortiz, Ana Isabel, *La violación de la intimidad en la protección de datos personales,* editorial Dykinson, Madrid, 1999.

Herrero Tejedor, Fernando, *Honor, intimidad y propia imagen*, editorial Colex, Madrid, 1994.

Nino, Carlos Santiago, *Fundamentos de Derecho Constitucional*, editorial Astrea, Buenos Aires, 1992.

Novoa Monreal, Emrique, *Derecho a la vida privada y libertad de información,* editorial Siglo XXI, Madrid, 1981.

Oteiza, Eduardo David, *Información privada y hábeas data*, comunicación presentada en el XX Congreso Nacional de Derecho Procesal, San Martín de los Andes (Argentina), 1999.

Othon Sidou, J.M., *Hábeas corpus, Mandado de Segurança, Mandado de Injunçao, Hábeas Data, Açao Popular –As garantías atoivas dos direitos coletivos-*, editorial Forense, 5ª edición, Río de Janeiro, 1998.

Palazzi, Pablo, *El hábeas data y el derecho al olvido,* en Jurisprudencia Argentina, semanario nº 6030 del 26 de marzo de 1997.

Perez Luño, Antonio Enrique, *Ensayos de informática jurídica,* Biblioteca de Etica, Filosofía del Derecho y Política, distribuidora Fontamara, México, 1996.

Pierini, Alicia – Lorences, Valentín – Tornabene, María Inés, *Hábeas Data*, editorial Universidad, Buenos Aires, 1998.

Puig Brutau, José, *Fundamentos de derecho civil*, tomo I, editorial Bosch, Barcelona, 1979.

Ruíz Miguel, Carlos, *El derecho a la intimidad informática en el ordenamiento español,* en RGD, nº 607, Madrid, 1995.

Sagüés, Néstor Pedro, *Derecho Procesal Constitucional –Acción de Amparo-*, editorial Astrea, Buenos Aires, 1995.

Velázquez Bautista, Rafael, *Protección jurídica de datos personales automatizados,* editorial Colex, Madrid, 1993.

CAPÍTULO II. Derechos que el hábeas data protege

5. Derecho a la intimidad

Para lograr una aproximación más o menos certera al objetivo que persigue el proceso constitucional de hábeas data, es necesario tomar desde el comienzo una posición específica: *o centramos la tutela en la protección de los datos,* o expandimos los derechos defendidos hacia todo el universo que supone el *derecho a la intimidad*.

> La relación entre derecho a la intimidad y el derecho a la protección de los datos personales o a la autodeterminación informativa ha sido analizada de forma diferente por la doctrina. Groshan sostiene que los términos "protección de datos" y "protección de la intimidad" son dos nociones distintas, ya que el interés de proteger la veracidad de los datos y el uso que de ellos se hace no está relacionado necesariamente con la protección de la libertad individual. En Estados Unidos, la distinción se traza más que en el significado en los sistemas legales, apuntando que, los países de tradición legal de *common law* utilizan más frecuentemente la expresión "protección de la intimidad", mientras que los países de *civil law* prefieren la expresión "protección de datos".

Observemos entonces la redacción acordada al artículo 1° de la ley:

Capítulo I
Disposiciones Generales

Artículo 1º .- Objeto. La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas de registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.-

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

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

Es verdad que la revolución informática del siglo XX ha obligado a encontrar formas procesales que respondan a esa novedosa invasión a la esfera de intimidad de las personas.

En este terreno afinca el hábeas data como garantía jurisdiccional; pero no es menos cierto que los derechos interesados en esta dimensión no pueden ser, únicamente, individuales y abonarlos en el campo de la intimidad. La sociedad, todos, tienen un interés especial que trasciende el reducto de lo propio en esta cuestión. Así como es necesario, también, advertir que el fenómeno de la recolección y archivo de datos provoca un negocio que no siempre es ilícito como parece resultar del mensaje.

La búsqueda del dato posee finalidades de organización y conocimiento, de seguridad y certidumbre para la toma de decisiones, y por ello, es el Estado mismo quien debe garantir el derecho y poner límites a la expansión.

Tanto como existe un derecho a no ser perturbado en la vida privada; también existe el derecho de las empresas a comercializar la información que obtiene cuando ello no tiene fines ilícitos.

> Lo que tratamos de manifestar es que aquella concepción tradicional sobre el derecho a la intimidad que nos llega del "derecho a ser dejado a solas", se ha ido transformando en el contexto de la sociedad informatizada. Y tal como afirma Estadella Yuste, existen varios aspectos que hacen evidente esta evolución: 1) Aunque la información personal puede tener un valor económico, no deja, por ello, de tener un valor personal. La información personal forma parte de la intimidad individual y está relacionada con el concepto de autonomía individual para decidir, hasta cierto límite, cuándo y de qué información puede ser objeto de tratamiento automatizado; 2) La protección del derecho a la intimidad contra el uso de un tratamiento automatizado de datos personales no se plantea exclusivamente a consecuencia de problemas individuales, sino que también expresa conflictos que incluyen a todos los individuos de la comunidad internacional. La idea de que la persona titular de los datos –el afectado- tiene interés, como parte de un grupo, es controlar el tratamiento automatizado de datos es reciente, ya que no aparece así en la "primera generación" de las leyes protectoras de datos, orientadas exclusivamente a la protección de la persona como entidad individual; 3) En algunos casos el tratamiento de datos automatizado se ha llegado a convertir en un arma estratégica de manipulación de conductas individuales; 4) La aplicación de avanzados métodos telemáticos a información de carácter personal ha dejado de ser la excepción para convertirse en una rutina diaria; en consecuencia, hay que tratar el tema como una realidad y no como un problema hipotético.

Por ello, cuando se trata de establecer límites al sistema de circulación y registro de datos de las personas, se ha pensado que el mentado derecho a la intimidad no puede resultar afectado, al menos, en cuatro aspectos esenciales: vida privada, vida familiar, domicilio y correspondencia.

> El artículo 12 de la Declaración Universal de Derechos Humanos establece que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación". Prácticamente igual es el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

A su vez, la faz comercial o empresarial, que tiene el tratamiento de datos, obliga a considerar el desarrollo de las telecomunicaciones, o de tecnologías de la información, o la vigía permanente por satélites de teletransmisión que, en cada caso, provocan una suerte de libertad vigilada que afecta el derecho a la intimidad, pero que resultan inevitablemente necesarios para asegurar aspectos tales como la seguridad del Estado, o el derecho a la información.

> El Convenio 108 de la Unión Europea* establece un límite a los derechos de la autodeterminación informativa cuando ellos constituyen una medida necesaria en una sociedad democrática para la protección de la seguridad del Estado: seguridad pública, intereses monetarios, o imposición de infracciones penales, y cuando estén dirigidas a la protección de la persona concernida y de los derechos y libertades de terceras personas. Aparte de estas restricciones se admiten otras respecto a aquellos ficheros automatizados de carácter personal utilizados con fines estadísticos o de investigación científica, siempre y cuando no existan manifiestamente riesgos de atentado a la vida privada de los afectados.

Importante resulta advertir que la lesión al derecho de intimidad no se da en un acto único que caracterice la afectación, es decir, no se puede encontrar una libertad de intimidad única, sino referida a un valor agredido. Por eso, el bien jurídico "intimidad" no se autoprotege ni defiende por sí mismo, sino que requiere la presencia de algún otro interés vulnerado, como pueden ser, la imagen, el honor, la reputación personal, etc.

En definitiva, precisar el contenido de qué se puede demandar desde el hábeas data, es decir, saber para qué sirve y qué derechos tutela, es significativo y altamente complejo. No obstante, como punto de partida puede resultar útil el célebre informe *"Data och integritet"* de la Comisión Sueca sobre publicidad y secreto de documentos oficiales que en 1972 sostuvo que:

- *No se podía pretender que el derecho a la intimidad fuera considerado un derecho absoluto; el primer límite al mismo se encuentra en el derecho que ostenta la sociedad a exigir a sus miembros las contribuciones necesarias para la realización de los fines comunes y, que…*
- *Tanto los entes públicos como los privados se encuentran en la necesidad de recoger numerosa información referente a los individuos para cumplir con los diversos fines que les son propios; por ello, toda información relativa a la condición de los individuos puede tener relación con el derecho a la intimidad*

5.1 Derecho personalísimo

La intimidad es un bien personal, un derecho subjetivo individual que no se transfiere ni negocia, y que por esa calidad de "derecho personalísimo" obtiene, respecto al tema que nos ocupa, una característica determinante: el ser posesión exclusiva y excluyente de la persona humana.

Sólo el individuo puede resolver, sin interferencias ni perturbaciones, que aspectos de su vida admite compartir y que pensamientos, sentimientos o hechos de su vida interior pretende que otros conozcan.

> Para Herrán Ortiz, estas características facultan a que el derecho a la intimidad pueda ser un bien un derecho libremente determinado por la persona, permitiendo que ésta resuelva cuándo y hasta qué medida quiere exteriorizar su vida y ponerse en contacto con la sociedad. Como complemento de la existencia del ser humano debe ser protegido, en tanto que ha de considerarse esencial que cada individuo conserve una esfera de libertad y autonomía que pueda defender frente a intromisiones externas. Las manifestaciones concretas del derecho a la intimidad pueden transformarse con el transcurso del tiempo y a buen seguro que en el futuro se defenderá una idea diferente de la que actualmente se sustenta de este derecho.

La intimidad es entonces el género desde el cual se pueden bajar otras manifestaciones como la vida privada, familiar, el derecho al secreto, al honor, a la imagen, etc.

Es algo propio que se dispone con libertad; pero al mismo tiempo, es una obligación de los demás hacia ese derecho, y por tanto, se configura como un derecho de defensa y garantía esencial para la condición humana.

> Los derechos fundamentales deben considerarse garantías de la autonomía individual, derechos de defensa frente a las injerencias de los poderes públicos en la esfera privada de cada persona. Además, constituyen garantías jurídicas esenciales para el mantenimiento del orden y la paz económico-social. Si bien entre ellos se pueden observar notas comunes –afirma Herrán Ortiz- cada derecho representa una categoría independiente y, consecuentemente, debe ser interpretado y aplicado en forma autónoma. La esencia y naturaleza del derecho a la intimidad permiten su consideración como un derecho de defensa; se trata de una defensa en principio ilimitada y frente a toda injerencia en la esfera de la persona que debe permanecer reservada en su interior.

Tanto se permite reclamar por la defensa de la intimidad violada o amenazada; cuanto se puede exigir del Estado que prevenga eventuales intromisiones que lesionen ese derecho personalísimo.

En este sentido, el hábeas data puede ser la garantía procesal adecuada para ciertos aspectos del derecho a la intimidad; pero el proceso es un remedio *ex post facto* que ofrece soluciones a situaciones ya padecidas; lo importante será actuar en la etapa previa, formando y conscientizando para que los derechos se promuevan y ejecuten conforme sus premisas e ideales lo contemplan.

> Sostiene el Tribunal Constitucional español que "los derechos fundamentales no incluyen solamente derechos subjetivos frente al Estado, y garantías institucionales, sino también deberes positivos de parte de éste. Pero, además, los derechos fundamentales son los componentes estructurales básicos, tanto del conjunto del orden jurídico objetivo como de cada una de las ramas que lo

> integran, en razón de que son la expresión jurídica de un sistema de valores que, por decisión del constituyente, ha de informar el conjunto de la organización jurídica y política […]. La garantía de su vigencia no puede limitarse a la posibilidad del ejercicio de pretensiones por parte de los individuos, sino que debe ser asumida también por el Estado. Por consiguiente de la obligación de sometimiento de todos los poderes a la Constitución no solamente se deduce la obligación negativa del Estado de no lesionar la esfera individual o institucional protegida por los derechos fundamentales, sino también la obligación positiva de contribuir a la efectividad de tales derechos, y de los valores que representan, aun cuando no exista una pretensión subjetiva por parte del ciudadano" (STC, 53/85, sentencia del 11 de abril de 1985).

En suma, asentar el piso de marcha del proceso de hábeas data, a partir de la tutela de la intimidad, supone privilegiar la libertad de las personas para resolver qué aspectos de su vida permite se hagan públicos a través de la información compilada o la difusión consecuente.

A estos fines, la sola invasión en la vida privada o en la esfera de la intimidad permite considerar afectado el derecho a la intimidad, sin que resulte necesario buscar donde se encuentra la lesión individual.

Esta sustentación reconoce la exigencia constitucional para que el Estado garantice dicha libertad; y como acción frente a otro, a quien se reclama para que revele el conocimiento de los datos archivados y, en su caso, para que los conserve actualizados, los reserve en el marco de la confidencialidad o los suprima como un derecho derivado de la potestad de autodeterminación informativa.

5.2 Derecho personalísimo proyectado "hacia otros"

La base que razona este derecho no supone caracterizarlo, estrictamente, como un derecho subjetivo. Vale decir, como una potestad exclusiva y excluyente de la actividad de otros; ni exigir de ello la mentada relación entre daño directo y efectivamente sufrido que admite la intervención jurisdiccional.

Si fuera mantenida la condición para el ejercicio del derecho, evidentemente, poco se habría avanzado porqué la lesión a la intimidad, muchas veces, es ocasional o circunstancial y hasta puede no existir, toda vez que se trata de una estimación puramente subjetiva.

La defensa que promete el hábeas data no está circunscripta al daño, ni siquiera lo exige, como tampoco se requiere ilegalidad o arbitrariedad para los actos que recopilan la información individual. En los hechos, si la garantía pervive en la libertad de decidir sin interferencias sobre nuestra vida privada o familiar –entro otros- es evidente que el derecho se proyecta también a determinados aspectos de otras personas con las que se mantiene una estrecha vinculación, sea familiar o de amistad, y que como tales, inciden en la esfera de la personalidad.

> Resulta significativo -informa Herrán Ortiz- que el Tribunal Constitucional en su sentencia del 15 de noviembre de 1991 considere el derecho a la intimidad no como algo privativo de la vida de cada individuo, sino que también reconozca la existencia de circunstancias que sin afectar directamente al individuo son susceptibles de ser protegidas acudiendo al derecho a la intimidad que todo individuo ostenta. Sin embargo –agrega- el derecho a la intimidad no constituye, en modo alguno, un derecho absoluto, antes bien, se encuentra limitado, además de por el necesario respeto al derecho de los demás, por la necesidad de preservar otros bienes constitucionalmente protegidos que responden a una demanda de la sociedad cada vez más avanzada y en constante desarrollo.

Ahora bien, este diseño obliga a investigar la naturaleza de la defensa que trae el hábeas data y la legitimación procesal que admite y reconoce, porqué si no es un derecho personal ni colectivo; tampoco difuso o de incidencia colectiva; aun cuando sea personalísimo con ampliaciones en la cobertura "hacia otros", es evidente que estamos ante un nuevo derecho, una novedosa garantía que no puede capturar su naturaleza jurídica tras la silueta del amparo tradicional.

Un ejemplo de las causas que obliga a sincerar la amplitud del hábeas data se muestra con el fenómeno de las redes mundiales de comunicación y el ámbito del comercio electrónico que, por su propia globalización, necesitan una respuesta igualmente universal.

> Informa Ulf Brüehann (miembro de la Comisión Europea y Director de la Unidad "*Libre flujo de la información y la protección de datos, incluyendo aspectos internacionales"*, que el trabajo de la World Wide Web Consortium se orienta hacia la elaboración de una tecnología de filtración (conocida como P3P), gracias a la que los usuarios de Internet podrían regular su propio acceso a páginas web en función de sus propias preferencias de intimidad. Los protocolos técnicos que se trabajan tienen un efecto directo en el nivel de intimidad del que disfrutarán los usuarios de la línea en años venideros.

Lo mismo, aunque desde otra perspectiva, ocurre con los organismos que se ocupan de la defensa de los derechos humanos, sean organizaciones no gubernamentales o el propio Defensor del Pueblo (ombudsman), en la medida que tienen legitimación procesal suficiente basados en las actividades que celebran. Además, es obvio que la soledad intrínseca del derecho individual no puede ir contra los retos continuos de la acumulación de datos admitidos a sabiendas o sin ella, pues la utilización de tecnologías cada vez más avanzadas impone un tratamiento general que juzgue la pertinencia de esa actividad recolectora que invade permanentemente la intimidad de las personas.

> El Parlamento Europeo ha manifestado, reiteradamente, que el tratamiento de datos no puede reducirse a una mera defensa de los derechos individuales ofreciendo al afectado la única posibilidad de accionar, pues esa actitud significaría dejarlo auténticamente solo, sin ninguna defensa comunitaria.
>
> Resumiendo –agrega Estadella Yuste- se puede decir que en un primer momento los instrumentos internacionales de derechos humanos no recogían expresamente el derecho a la protección de datos o autodeterminación informativa, sino tan sólo un derecho "a la vida privada" o a la intimidad personal. Posteriormente éste se ha ido desarrollando y paulatinamente se han adoptado otros instrumentos internacionales reconociendo el derecho a la protección de datos. Ello es importante porque, si la protección de datos sólo se hubiera plasmado en leyes de ámbito nacional, habría sido más difícil que la comunidad internacional lo considerara como un derecho individual.

5.3 La vida privada [*]

La vida privada que atiende el hábeas data se vincula con todas aquellas manifestaciones que se registran o archivan con alguna finalidad sin tener consentimiento expreso de la persona.

Recordemos que el resonado caso argentino fallado por la Corte Suprema de Justicia de la Nación (CS, 11 de diciembre de 1984) en autos *"Ponzetti de Balbín c/ Editorial Atlántida s.a."*, sostuvo que el derecho a la privacidad e intimidad, en relación directa con la libertad individual protege un ámbito de autonomía individual constituida por sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física y, en suma, las acciones, hechos o *datos* que, teniendo en cuenta las formas de vida aceptadas por la comunidad están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significa un peligro real o potencial para la intimidad. En rigor, el derecho a la privacidad comprende no sólo la esfera doméstica, sino otros aspectos de la personalidad espiritual o física de las personas, tales como la integridad corporal, la imagen, y nadie puede inmiscuirse en la vida privada de una persona ni violar las áreas de su actividad no destinadas a ser difundidas, sin su consentimiento o el de sus familiares autorizados para ello, y sólo por ley podrá justificarse la intromisión, siempre que medie un interés superior en resguardo de la libertad de otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen.

---

[*] Ver parágrafo 61.11

> "Vida privada" hace referencia a una esfera de retiro y aislamiento, al ámbito donde los demás dejan en paz al sujeto, con tranquilidad para actuar y donde no tienen derecho a inmiscuirse. En tanto que la intimidad se refiere al individuo, a un "mundo propio" –en palabras de Herrán Ortiz-, fuera de los ojos de los demás, se trata de la esfera más sagrada de la persona.

Esta interpretación conlleva a fragmentar la defensa del hábeas data si aplicamos la jurisprudencia tal como se expresa.

Es decir, la privacidad se recorta en dos vertientes: la vida personal y la vida familiar, y en la misma línea, la inviolabilidad del domicilio y de la correspondencia particular.

Por eso la vida privada excede a la intimidad, y por tanto comprende, además de los bienes que el fallo enumera, otros como la imagen y el honor. En consecuencia, también las personas jurídicas tienen vida privada, aunque no posean intimidad.

> La distancia entre vida personal y derecho a la intimidad no supone que la primera necesite de una regulación legal expresa mientras la segunda cuente con respaldo constitucional, en razón de que nuestro país, de conformidad con el artículo 75 inciso 22 de la Ley Fundamental, reconoce varios tratados y convenciones donde se distingue la defensa que al domicilio, a la correspondencia, a la propia imagen y a la individualidad se dispensa.
>
> De algún modo puede coincidir con esta idea la opinión de Martínez Sospedra cuando expresa que "…de este modo aquellas áreas de la vida privada que exceden del ámbito de la intimidad y no se hallan protegidas ni por el derecho fundamental a la misma ni por los otros derechos fundamentales con incidencia en aquella obtienen protección constitucional mediante la internalización de las disposiciones de los tratados que reconocen el derecho a la vida privada que provoca la ratificación de los mismos. En sentido estricto no hay, pues, en nuestro ordenamiento (España) un derecho propiamente constitucional a la vida privada, pero si existe, mediante la vía señalada, una suerte de derecho paraconstitucional, si bien el mismo sólo es protegible en amparo en aquellos supuestos en que se puede obtener la cobertura del artículo 18 de la Constitución española".

En síntesis, el derecho a la vida privada contrae, al menos, las siguientes obligaciones:

- Recrear la doctrina del derecho a estar a solas, evitando que la persona humana sea invadida por intromisiones de cualquier naturaleza que afecten su vida íntima o privada.
- Auspiciar una defensa efectiva del individuo contra la publicidad de actos personales que se ponen a disposición del público interesado sin conocimiento ni permiso del afectado.
- Propiciar un régimen de control sobre el almacenamiento de datos personales y el destino que a ellos se asigne.
- Formular un criterio economicista respecto a la vida privada, a cuyo fin se la puede analizar como resultado de la difusión y retención de la información en el contexto comercial y personal.
- Dar un sentido amplio al derecho a tener una vida privada, para evitar el egoísmo de considerar únicamente el problema del tratamiento de datos, sin relacionar otras situaciones tan o más importantes que ella, como son las intercepciones telefónicas, la penetración de los correos electrónicos, la invasión domiciliaria de publicidad, etc.

5.4 La vida familiar

El derecho de exclusión que pervive en la defensa de la vida privada, en cuanto evitar o prevenir las intromisiones en la dimensión de lo que resulta absolutamente reservado y secreto de las personas; se extiende a la vida familiar como una proyección del derecho a la privacidad.

En este aspecto, la tutela constituye un avance necesario en la forma de resolver la invasión o perturbación en el reducto de lo íntimo, si se tiene en cuenta que la protección estuvo dirigida a salvaguardar la familia de la indiscreción y las consecuencias que traía a ella ese conocimiento de hábitos o costumbres.

> Sostiene Lyon que constituye una realidad que, si bien en sus comienzos la protección de la vida personal se salvaguardaba frente a la indiscreción ajena que, con más curiosidad que malicia, interfería en la intimidad de quienes por su profesión, condición o deseo se consideraban personas públicas, hoy la protección de la intimidad o de la privacidad de las personas adopta una nueva dimensión, más social, menos individual y que se proyecta en las circunstancias más cotidianas e irrelevantes de la existencia humana. Negar que la protección de la persona en la era de las computadoras ha superado el estricto ámbito de la intimidad, representaría la negación de una realidad constatable pero, igualmente, podría calificarse de parcial un estudio de la protección de la persona en la que la intimidad, como aspecto de la personalidad individual, no sea reconocida en cuanto ámbito personal digno de tutela frente a las agresiones informáticas.

La vida en familia representa un sin número de comportamientos que identifican el perfil del diario acontecer. Existen gustos, tolerancias, manifestaciones que identifican el carácter de los miembros, preferencias, etc. que, observadas y registradas, definen el ser cultural y económico del grupo. Cuando esa vigilancia es producto de intromisiones directas o indirectas, debe existir un control sobre ellas y una forma de prevenir el uso de ese archivo de costumbres.

A veces, la familia se encuentra invadida sin saberlo, aunque de hecho lo admite. El caso de medios electrónicos que conviven con ella es habitual. Por ejemplo, la televisión representa hábitos, promueve usos y costumbres. La utilización de la red Internet obliga a dejar datos y otros registros cuando se practica el comercio electrónico; el uso del teléfono es también un medio indirecto de invasión a la intimidad (por eso, saber quien nos llama antes que un servicio es un derecho).

> Cierto que, en principio –afirma Herrán Ortiz- el conocimiento de los comercios donde una persona adquiere sus enseres o el vestuario parecen datos irrelevantes y sin trascendencia, no obstante, adviértase que el conocimiento de estos datos debidamente relacionados pueden ofrecer una imagen de la persona, de sus gustos, aficiones o puede revelar, por ejemplo, su desmesura en el gasto. Datos, todos ellos que pueden perjudicar a la persona, no por su falsedad o por el desmerecimiento de su reputación, sino por el solo hecho de que el individuo no ha consentido su almacenamiento y, menos aun su utilización por terceros.

La utilidad para otros de estos hechos cotidianos seguramente es inasible o probablemente difuso. También es cierto que esa ausencia de daño, peligro o incertidumbre, no puede solaparse tras la defensa de la intimidad o la privacidad como derechos de contenido personal (subjetivos).

Lo que se procura mantener en la mira del hábeas data es el control sobre los registros, antes que evitar la recopilación propiamente dicha. Toda información de la persona, familia y amistades, ese reducto o círculo de "los íntimos" no puede ser observado con desinterés y tolerancia, seguramente tiene un fin y un objetivo. En consecuencia, es una amenaza y necesita una herramienta de control.

5.5 La inviolabilidad del domicilio

La Constitución Nacional protege el domicilio de las personas con un criterio amplio que comprende modalidades como la residencia transitoria, la simple morada, el alojamiento por horas y en general toda habitación o lugar cerrado o abierto, móvil o inmóvil, que permita el desenvolvimiento de la libertad personal en cuanto concierne a la vida privada.

La pretensión es operativa sin necesitar ayuda de la norma reglamentaria, y constituye una orden al Estado para que establezca límites en su accionar, impidiendo al menos, al allanamiento sin orden judicial o la violencia sobre los lugares donde una persona se encuentra, aun cuando utilice el lugar como refugio.

> Dice Bidart Campos que la norma del artículo 18 es directamente operativa y no vale decir que el domicilio carezca de inviolabilidad mientras no se dicte la ley reglamentaria a la que la cláusula se refiere. Lo que la norma significa es que para allanar el domicilio sin orden judicial es indispensable que una ley previa determine razonablemente los casos y justificativos.

El hábeas data, en este aspecto, no es una vía útil ni efectiva para impedir un allanamiento ilegal, o provocar en su campo la nulidad por ilegítimo de ese acto practicado. Una vez más, queda de manifiesto el marco acotado de la garantía procesal al tratamiento de datos, aunque es posible encontrar similitudes de encuadre si se confronta con el hábeas corpus.

5.6 La correspondencia y los papeles privados

La correspondencia particular y los papeles privados deben interpretarse con sentido amplio que admita el desarrollo tecnológico y evite la zona de grises que se encuentra aun sin definir.

En efecto, el caso de las cartas misivas debe capturar en su alcance los mensajes del correo electrónico, los informes del "pager" o "beeper" (pese a la intervención de un tercero que mediatiza el mensaje pero que participa de la confidencialidad), y todo tipo de mensajero que aplica esa función de correspondencia a particulares.

Lo mismo puede ser dicho respecto a los papeles privados, los cuales conservan el derecho al secreto y a su invulnerabilidad (por ejemplo: legajos personales, fichas de trabajo, historias clínicas, etc.). La extensión mentada se aplica a todo tipo de comunicaciones interpersonales, de forma tal que el medio utilizado no es trascendente como sí lo es la garantía que preserva la libertad de intimidad.

> Con la técnica moderna –agrega Bidart Campos- consideramos que la libertad de intimidad se extiende a otros ámbitos: comunicaciones que por cualquier medio no están destinadas a terceros, sea por teléfono, por radiotelegrafía, etc. Este último aspecto atañe simultáneamente a la libertad de expresión: la expresión que se transmite en uso de la libertad de intimidad no puede ser interferida o capturada arbitrariamente. La captación indebida tampoco puede, por ende, servir de medio probatorio. Sería extenso enumerar otros contenidos que quedan amparados en la intimidad, y sobre los cuales sólo puede avanzar una ley suficientemente razonable con un fin concreto de verdadero interés. Así, el secreto financiero y bancario, el retrato o la imagen, etc.

La dimensión de los derechos tiene presente, en definitiva, la seguridad individual y no es otro el sentido que orientan las normas del Código Civil, en particular el artículo 1071 bis, y el Código Penal que recepta el garantismo del artículo 18 constitucional.

> Apunta Oteiza siguiendo el criterio que se expone, que continúan en esta línea la ley 23.798 que se ocupa de distintos aspectos vinculados con el síndrome de inmunodeficiencia adquirida cuando impone la codificación de las fichas y los registros y la obligación de guardar reserva absoluta de los profesionales que intervengan en el tratamiento. La ley 11.723 que requiere el consentimiento de la persona fotografiada y que su difusión se vincule con fines científicos, didácticos o culturales. Las citadas disposiciones reciben en forma atenuada el derecho de evitar las invasiones sobre aquellos aspectos de la vida personal que no existe mérito para revelar, o que conocidos no deben ser dominados o empleados por terceros.

Con mayor preocupación el Pacto de San José de Costa Rica (art. 11), y otros tratados y convenciones (v.gr.: art. 12 de la Declaración Universal de Derechos Humanos; art. 17 del Pacto Internacional de derechos civiles y políticos) prefieren evitar toda intromisión arbitraria en la vida privada, domicilio, vida familiar y correspondencia privada, que son los numerales que acepta el derecho a la intimidad en sentido lato.

Ahora bien, ¿cómo trabaja el hábeas data en este campo de la correspondencia epistolar?.

En primer lugar debemos partir de la base de sostener que el concepto no está limitado a las cartas misivas, sino a todo tipo de comunicaciones que emitan información privada y que no importa que en el intercambio participen terceras personas. Esta actuación necesaria o contratada de otro individuo o de un medio técnico controlado por otro, no significa publicitar o dar sentido público al envío.

En segundo término, hay que resguardar y asegurar el derecho a mantener secreta cierta información que le concierne, de modo tal que no esté al alcance de persona alguna, a excepción de autorizaciones judiciales expresamente indicadas.

Un aspecto más se vincula con las nuevas modalidades de información que una persona investiga y que, sin saberlo ni quererlo, tiene "buscadores" que siguen sus preferencias para utilizar ese dato obtenido.

> Existen cuatro acciones calificadas como muy graves en la utilización de la red Internet: a) seguimientos de qué sitios en la red visita cada persona y utilización indebida de esa información; b) introducción en Internet de información sobre personas presente en registros públicos que permite la identificación de las mismas; c) lectura de mensajes de correo electrónico por personas a las que no van dirigidos; d) sitios de la red que recopilan direcciones de correo electrónico de sus visitantes para obtener listas de comercialización sin consentimiento ni autorización alguna.

La suma de cuestiones previas abre esperanzas para que la garantía creada en el párrafo tercero del artículo 43 constitucional permita, por ejemplo, saber qué registros se tienen de alguien que comercializa vía Internet y qué otro destino puede tener ese archivo; qué sentido tiene la persecución completa de datos para registrarse en un hotel; impedir la agresiva venta telefónica que invade permanentemente la línea celular, satelital u ordinaria que se ha contratado, en fin, toda inmiscusión en la zona de reserva y confidencialidad propia de los papeles privados, constituye un campo propicio para que el hábeas data resuelva.

Sin embargo, la cuestión no podrá seguramente tener solución ni por la ley ni a través de su garantía. La novedosa injerencia y penetración en lo que es propio obligará a complementar las leyes con acciones precisas destinadas a la protección efectiva, antes que la invasión se produzca. De otro modo, cualquier proceso será meramente resarcitorio porqué el daño se habrá producido.

> La normativa, por sí misma, no será suficiente para proteger el derecho a la intimidad en el próximo siglo –asegura Ann Cavoukian- ; será necesario emplear diversos instrumentos como complemento a la legislación y, en particular, herramientas de carácter tecnológico (herramientas de protección de la intimidad)…Puede adoptarse la legislación más estricta, como es el caso en la Unión Europea, pero si existe la posibilidad de eludirla mediante la aplicación de las diversas tecnologías, su valor disminuirá en gran medida. Además, en el mundo de Internet, en el que no se conocen fronteras políticas ni se observan leyes aplicables, no queda otra opción que recurrir a la tecnología…Quizás, las *plataformas para las preferencias de intimidad (*P3P) apoyen esta tecnología y pueden considerarse un paso adelante hacia la mejora en la protección de la intimidad

6. Derecho a la privacidad

Todas las manifestaciones de la libertad de intimidad asumida como derecho fundamental de las personas, o bien, del derecho a la intimidad interpretada como derecho subjetivo, permiten desplazar cada uno de los enunciados que en el capítulo anterior fueron presentados.

Es decir, desde la intimidad uno puede llegar al honor, a la propia imagen, a la fama o reputación, a la reserva y confidencialidad, al secreto, al derecho al olvido y a la verdad, etc. etc.; pero el marco donde ha de ubicarse el proceso de hábeas data requiere, siempre, del tratamiento de datos de una persona que por esa causa tiene interés. Luego de observar el uso y destino de ese archivo sobre alguien, se podrá colegir si está afectado el honor, la fama, el secreto, o cualquiera de los derechos antes enumerados. Y, en todo caso, si la vía procesal que se implementa es, efectivamente, la garantía constitucional creada y en estudio, para recién allí determinar la condición del acto lesivo.

Sobre esta base la cuestión parece demasiada compleja, cuando en realidad no lo es.

La defensa de la intimidad puede ser el género que amplía las fronteras del hábeas data; pero el derecho a la privacidad resulta más adecuado para recibir los bienes a tutelar por el proceso.

En efecto, *privacy* tiene un sentido activo que tiende a concretar la protección de los particulares impidiendo que terceros se ocupen de la vida privada de otros. Al mismo tiempo, implica que si el banco de datos es legal y permitido, sea también "privado", en el sentido de lograr confidencialidad y secreto, seguridad y privacidad en la transmisión que se efectúa.

No se tratan de bienes jurídicos diferentes, pues la privacidad que la persona prefiere, a veces no es posible, porque los registros se toman en diversas formas y manifestaciones (por ejemplo, ofrecer datos personales en un requerimiento de crédito o completar una planilla de inscripción para un sorteo ofrecido) y pocas veces puede conocer el uso posterior que se dará a esos datos.

Si interpretamos la privacidad en ambas dimensiones, los intereses se pueden conciliar. Tanto los del hombre y su derecho a la libertad de intimidad; como los de la empresa que en ejercicio de un comercio lícito debe resguardar la seguridad del sistema (privacidad en las comunicaciones).

De este modo, intimidad y privacidad no son realidades contrastables.

> "Nótese que se habla de la privacidad y no de la intimidad: aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservada de la vida de las personas –el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo" (párrafo de la Exposición de Motivos de la LORTAD* española).

Creemos que el ámbito natural del hábeas data es el derecho a la privacidad, en dos sentidos: uno se dirige como mensaje impeditivo o barrera que se pone para evitar que la vida personal sea accesible a otros cuando el titular no lo admite; el restante, como acción positiva tendiente a obrar preventivamente frente a las agresiones provenientes de la informática.

> La *privacy* se concibe por un sector doctrinal como una libertad positiva para ejercer un derecho de control sobre los datos referidos a la propia persona que, si bien han emergido al exterior, fuera de la esfera íntima de la persona, y se han incorporado a un archivo electrónico, nada impide que puedan continuar bajo control y salvaguarda de su titular. En definitiva, se identificaría con el mismo derecho a la autodeterminación informativa, porque ese es el significado y contenido de este derecho. Se confunde pues, el derecho en sí mismo como medio y respuesta jurídica de tutela de la persona, con el ámbito o bien jurídico tutelado, si la privacidad se identifica con los aspectos o ámbitos de la existencia personal que se preservan del tratamiento informatizado, no puede identificarse con el derecho que lo tutela.

Si en la defensa de la intimidad el fin fue evitar las intromisiones en la vida privada y espiritual de alguien; en la tutela que reserva el hábeas data el derecho se actúa, antes que previene. Es un ejercicio plenamente dispositivo de la libertad de control sobre los datos que le conciernen.

> Afirma Carballo que el derecho de privacidad no representa sino la expectativa individual de control que cada persona tiene respecto de la información sobre sí mismo y la forma en que esta información es conocida o utilizada por terceros.

En definitiva no se trata de defender a la persona en su hábitat individual, en su soledad absoluta o en la confidencia más extrema; porqué el hábeas data no es una cuestión de hermetismo o secreto, sino de otorgar un recurso a la privacidad, permitiendo con ello una vía de control a la esfera de reserva.

Sin embargo, no es bueno auspiciar que esta vía permita eludir todo tipo de registros o transmisión de datos que son necesarios para la vida social y para los intereses del Estado.

> No es posible instaurar un recurso a la privacidad para ocultar datos de carácter económico, patrimonial o penal, impidiendo con ello aquellas formas de control social que tutelan los intereses de la comunidad. Se trata, por tanto –dice Alpa- de la defensa de la persona frente a la intromisión, la recogida, difusión y utilización de aspectos de su vida pertenecientes a su privacidad, actos que hoy son frecuentes y ante los cuales no podía oponerse un conjunto de instrumentos jurídicos eficaces.

6.1 Las etapas en la transformación de la privacidad

Lo dicho en párrafos precedentes no debe conducir a la creencia de que el hábeas data se aloja únicamente en la vida privada o personal, ni que el Estado –o los particulares que comercializan con bases de datos- cuenten con una herramienta útil para legitimar el uso que aplican a esos registros.

Los derechos de la privacidad, en realidad, constituyen una gama muy compleja de situaciones que fueron transformándose en la historia del mundo hasta llegar a un estadio donde resultan plenamente imbricados con las acciones públicas y, por tanto, donde no es posible ni fácil resolver cuál de esos derechos tiene primacía.

En efecto, cuando se observa el desarrollo del mundo moderno, se advierte la influencia notable que tiene la sociedad en la vida de las personas. Existe en cada etapa una suerte de búsqueda por la burguesía porque instalados en esa posición resultaba más simple relacionarse y obtener influencia. Un mundo que abandonó la sociedad feudal requería del poder vinculado a los terratenientes pero con un sentido más social que económico.

> Sostiene Jürgen Habermas que el espacio público se constituye en la modernidad desde la búsqueda por la burguesía de una esfera donde proyectar su modo de experimentar la vida, en medio de sociedades donde el poder se articulaba desde la nobleza que lo ejercía en representación de todo el cuerpo social. La burguesía, basándose en las posibilidades y requerimientos de comunicación y noticias de un mundo en expansión, concibió, en oposición al Estado estamental, un espacio donde, utilizando la expresión oral y sobre todo la tecnología de la escritura (correspondencia, archivo, circulación de documentos), personas carentes del poder político legítimo, es decir, privadas, podían desarrollar relaciones sociales intensas mediadas por el razonamiento, generalizando idealmente sus experiencias subjetivas de vida en la familia nuclear. Recíprocamente, lo privado ha dejado de ser, como lo era en la sociedad feudal, el sitio de procura de las necesidades, o sea, un lugar de producción, puesto que el modo de producir había desbordado latamente las fronteras de la economía doméstica hacia el mercado, desterrando de ella el esfuerzo social para dejarla exclusivamente ocupada de las relaciones familiares. De este modo es que nacen íntimamente vinculadas las esferas de publicidad y privacidad.

La vida cortesana va a demostrar la influencia del orador y del escritor, cada uno con su público y su inagotable poder para instalar conceptos sobre temas que "a todos interesa". Esta primera etapa nos sirve para comprender la fuerza y pujanza de la opinión transmitida y de algunas de las razones por las que debe mantenerse esta suerte de libertad de expresión que forja una sociedad.

Sin embargo, la familia se reconduce hacia lo personal (*my home is my castle*). Se estrechan las relaciones y comienza una etapa donde la intimidad es el producto de la necesidad de pensar por sí mismos. El Estado, los burgueses, no podían continuar aquel estado de dominación.

> El estudio de Carlos Peña, en la compilación de monografías efectuada por la Universidad Diego Portales, es elocuente cuando expone:"…Allí es cuando la privacidad incorpora el ideal de la intimidad, como algo diverso tanto de lo propiamente público, el poder legítimo que no pertenecía a la burguesía, pero ante el que poseía una autonomía asegurada por la propiedad privada, por un lado; por otro lado, también respecto a la producción económica, de su dinámica de enfrentamiento racional en la publicidad del mercado, respecto del cual ofrecía el lugar adecuado para depositar los sentimientos, y en tercer lugar, en relación a la publicidad cultural de la "vida social" que hacía la burguesía, de la cual, sin embargo, era su antesala al asumir la familia la función educativa de los miembros de ella".

Cuando el individuo se convierte en ciudadano (Siglo XVIII), la polaridad entre lo público y privado se hace más intensa, en razón de que se institucionaliza la representación política y el poder de la opinión pública (eludiendo el significado que había tenido la burguesía en la vida cortesana); frente a la sociedad que, en definitiva, era un agrupamiento de personas privadas y esencialmente emancipadas del poder económico del Estado.

Así, la vida privada se transforma en una idea pública que al menos ideológicamente ofrece a toda la sociedad un espacio público ampliado (Peña).

La última etapa nos muestra el intervencionismo del Estado en las relaciones privadas y con una absoluta indiferencia por la intimidad y reserva que tenía el núcleo familiar. Se difumina la autonomía económica y comienza una sociedad de masas donde el consumo marca las preferencias. Queda en evidencia la destrucción del ideal de aislamiento (entre lo público y privado) y la defensa de lo propio se resuelve desde los derechos fundamentales, dando lugar a un nuevo orden internacional para los derechos humanos.

> En esta etapa –dice Peña- se produce la degradación de la autonomía privada, ideal radicado en el hogar familiar, la cual pierde su fundamento en la propiedad privada disponible arbitrariamente y ahora sobre regulada y con ello disgregada, mudándose en una autonomía de consumo. El consumo, a su vez, tampoco es esencialmente privado, por cuanto muchas veces empiezan a depender del Estado para procurar sus necesidades básicas. De este modo es que la familia pierde toda relación con el mundo del trabajo. Ello traerá por consecuencia el descargar a la familia también de su capacidad de intimación personal, debido a la férrea dependencia de la vida familiar del Estado social y la sociedad organizada. Dicha situación tiene dos paradigmáticas expresiones que nos interesarán: el fracaso del ideal del aislamiento, tanto física (en la gran urbe) como psicológicamente (desvalorización de la vida solitaria), y la socialización inmediata de las personas a través de los medios de comunicación social (con lo que pierde la familia su función protectora respecto de lo público, quedando a merced, antes bien, más que de lo público en sentido político, de lo semipúblico).

El tránsito por distintas etapas evidencia la transformación del concepto de privacidad, como la tensa relación entre el dominio de lo público y lo privado.

La aspiración de ser dejado a solas; de vivir una vida propia con el mínimo de injerencias exteriores; de autodeterminar sus relaciones sociales; de desarrollar la personalidad sin ataduras ni compromisos, cada una de estas expresiones que son, definitivamente, derechos de las personas, tienen ante sí las dificultades de su propia concreción.

Las citadas etapas, en la explicación del derecho a la intimidad o bien, acotando la mención, del derecho a la privacidad, son presentadas habitualmente bajo dos teorías posibles que, en realidad, pretenden focalizar –cual si fuera el haz de luz de una linterna- qué derechos deben protegerse.

> Estas teorías son las denominadas "de las esferas" y "del mosaico". Mientras la primera refiere al derecho de la intimidad representado en círculos concéntricos donde el anillo central es la esfera de máxima reserva y los demás, dirigidos hacia el exterior, van hilando sucesivamente, las esferas del secreto, la confidencialidad, la confianza, hasta llegar a las cercanías de lo público que

> constituyen las relaciones del hombre con los demás persiguiendo crear una imagen de sí mismo.
>
> La teoría del mosaico –explicada por Diana de Slavin- resalta los diferentes roles que desempeña el individuo. Este conforma un complejo de informaciones, y según se articulen éstas el resultado final será diferente. Aquí se debe entender no solamente el carácter intrínseco del dato, a su intimidad, sino también a quienes tienen derecho para acceder a él.

Concretar la defensa constitucional en terreno de lo público o lo privado, frente a la situación que advierte un desarrollo simultáneo en ambos niveles, obliga al poder del Estado a promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas. Han de removerse los obstáculos que dificulten o impidan la plenitud del derecho constitucional creado, de forma tal que los siguientes derechos proyectados desde la privacidad, pueden encontrar una auténtica respuesta:

a) *La intromisión en el ámbito de reserva y soledad* que una persona pretende crearse (intrusión que se puede dar hacia los bienes o en la intimidad del hogar). Derecho que se afecta de manera directa con la grabación de conversaciones privadas, las intervenciones telefónicas, la filmación intrusiva de actos de la vida familiar, la observación vigilante de la familia o de la persona, el acoso irrazonable en el círculo de una persona, etc. También son agresiones indirectas la publicidad estentórea (a viva voz, por medios parlantes aéreos o viales, etc.) en horas pensadas para la tranquilidad y reposo; las llamadas telefónicas que no reconocen origen (por eso, como antes dijimos, la localización del número desde nos llaman, antes que un servicio es un derecho).

b) *La divulgación de hechos privados*, dados en secreto o confidencialidad. No importa que la exposición pública afecte o no el honor de la persona, pues la lesión se produce en la intimidad. Recordemos el caso *Melvin c/ Reid* en el cual la jurisprudencia americana sostiene que se violenta el derecho de toda persona al olvido, al narrarse en una película su pasado como prostituta.

c) *La difamación* que consiste en hacer públicos hechos relativos a un individuo, presentados en forma disimulada, totalmente falsos o con una imagen distorsionada con el fin de afectar o dañar a la persona concernida. Se incluyen aquí las protecciones que necesita el nombre, la voz, la imagen, y en definitiva, la fama o reputación.

d) *La falsificación de atributos,* por el cual una persona pretende atribuirse identidades o características que a otro pertenecen, pretendiendo con ello utilizar una imagen ajena.

e) *La identidad*, por el cual una persona persigue ser reconocida por su nombre y apellido, sus calidades personales, sus atributos intelectuales, y todo aquello que hace a su personalidad. Por eso, cuando un banco de datos contiene información inexacta, desactualizada o equívoca, es menester corregir el archivo desde la garantía del hábeas data.

6.2 La defensa del derecho a la privacidad sobre las cosas

La legislación comparada permite confrontar la preferencia de algunos para indicar espacios o lugares donde no se puede penetrar sin afectar el derecho a la privacidad.

> Novoa Monreal sostiene como privados a los hechos que presentan las siguientes características: a) ser desconocidos para los extraños o ajenos al círculo familiar, o que no suceden normalmente a la vista de ellos; b) cuyo conocimiento provoque generalmente turbación moral en el sujeto, por dañar su pudor o recato; 3) que el sujeto no quiera que otros los conozcan.

De este modo, si los actos se ejecutan en el interior de una vivienda o espacio exclusivo, sin importar el tiempo o el motivo en que ello suceda, al lugar se le garantiza la reserva y exclusividad.

Es este un sistema objetivo casuista que emplea el criterio de tutela de acuerdo a las circunstancias donde y como se produce.

> De alguna forma es una oposición al sistema subjetivo que distingue entre lo público y lo privado según la calidad de la persona en cuestión. Si es un funcionario o tiene una actividad que lo expone al contacto general del público, se interpreta que esa actuación le limita su derecho a tener una vida privada absolutamente intangible; situación que tienen también otras personas notorias o famosas.

6.3 La privacidad de los datos

La evolución tecnológica produjo una intromisión impensada en la intimidad de las personas, y sobre todo, demostró que la defensa tradicional de los derechos individuales, era absolutamente insuficiente.

> Se ha dicho que la utilización de nuevas tecnologías y la entrada de nuevos intervinientes exigen esfuerzos continuamente renovados para consultar y educar, tanto al ciudadano particular acerca de los derechos que le asisten, como a los sectores público y privado acerca de las obligaciones que tienen de tratar la información personal de manera responsable y lícita. Aquí, las autoridades de control de todo el mundo para la protección de datos y la intimidad tienen un papel clave y una gran responsabilidad (Brüehann)

Primero fueron las Convenciones Internacionales las que advirtieron la penetración del fuero íntimo mediante la técnica de recolección de datos para su posterior transmisión con objetivos diversos, o simplemente con fines de archivo estadístico o informativo.

El concepto de intimidad varió, como amplió asimismo la idea acostumbrada para resolver las invasiones ilegítimas en el reducto de lo personal. Se habló de un campo propicio para una libertad nueva: la informática y el uso responsable del dato.

> Ya vimos como se produce este fenomenal cambio y de que manera sucede la aparición del hábeas data como proceso destinado a resolver el problema de la penetración de los derechos a través de la informática. De todos modos es conveniente recordar que en el ámbito de la contratación individual una persona no puede disponer de los derechos de la personalidad, teniendo en cuenta que no tienen contenido patrimonial y, como tales, resultan intransferibles, fuera del comercio. Lo que no puede ocurrir –sostiene Peña- es que un sujeto enajene su derecho al honor, a la intimidad, a la privacidad o a la imagen, quedando en definitiva privado de los mismos.

Es el campo donde anida, esencialmente, la protección derivada del hábeas data, y que sigue principios internacionales respecto a formas, modalidades y controles que debe mantener el individuo cuando se archivan sus datos en bancos destinados a cualquier efecto.

Ellos son:

a) El principio de la *calidad de los datos*, por el cual se pretende que los archivos o registros sean absolutamente fidedignos. Además, la *pertinencia* obliga a que la recolección y el tratamiento sean acordes con los fines del banco, incurriendo en ilegalidad cuando se aplica a objetivos diferentes a los autorizados (art. 4°).

b) El principio de *información del afectado,* que supone mantener informada adecuadamente a la persona sobre el motivo por el que se lo incluirá en un fichero (art. 6°).

c) El principio del *consentimiento* que inspira la participación de la persona en las tres etapas posibles en que actúa el registro. Primero, cuando se toma el dato; después para el mantenimiento y conservación en el archivo, y finalmente, para la cesión o transferencia a terceros de información que le concierne (art. 5°).

d) El principio de *protección de los datos sensibles*, que se vincula con la información estrictamente confidencial por su carácter privado y personalísimo (V.gr.: raza, credo, religión, salud, inclinaciones sexuales, hábitos y costumbres, etc.). La LORTAD los clasifica en tres

tipos: -los relativos a la ideología, religión o creencias; los datos relativos al origen racial, a la salud o a la vida sexual y, los datos relativos a los antecedentes penales (art. 7°).

e) El principio de *seguridad de los datos*, considerado a los fines de evitar la introducción de terceros al archivo, de manera directa o indirecta, legítima o ilegítima, para preservar la confidencialidad y, también, para conseguir que los registros no se pierdan, alteren o modifiquen por accesos no autorizados (art. 9°).

El hábeas data otorga al individuo la posibilidad de concretar el cumplimiento de cualquiera de estos principios, sea mediante el acceso inmediato, irrestricto y sin condiciones económicas que lo dificulten o esterilicen; o para la actualización, rectificación o supresión del dato que le concierne.

> Según el Convenio 108 de la CEE, estos principios pueden ser limitados cuando constituyan una medida necesaria para una sociedad democrática para la protección de la seguridad del Estado: seguridad pública, intereses financieros, imposición de infracciones penales, y cuando están dirigidas a la protección de la persona concernida y de los derechos y libertades de terceras personas. Señala Garzón que, en circunstancias normales, las medidas restrictivas de los Estados deber ser, en primer lugar, motivadas y han de fundamentarse en una de las razones reconocidas internacionalmente; en segundo lugar, la acción del Estado debe emprenderse de buena fe; y por último, las medidas no deben ser discriminatorias para los individuos sometidos a la jurisdicción del Estado, ni deben suponer un trato discriminatorio en las relaciones económicas internacionales.

7. Derecho a la identidad personal [*]

Fuera de los casos especiales que observamos al presentar el derecho a la identidad, y que pueden tomar caminos diferentes según el tipo de reparación que deban intentar (v.gr.: nombre, imagen, propiedad intelectual, etc.), el hábeas data va recortando su perfil para encontrar en este derecho uno de sus más preciados fundamentos.

En efecto, la identidad constituye una suerte de carta de presentación personal. Es la radiografía de la vida, y en buena medida, el atributo central de la personalidad.

Teniendo en cuenta que los bancos de datos registran información, ha de aceptarse que la veracidad del archivo pueda ser controlada por el propio interesado que se ha visto registrado; y aun frente a la posibilidad de incertidumbre acerca de la existencia del registro, es posible ingresar al mismo persiguiendo conocer la verdad compilada.

Por tanto, el derecho a la identidad supone además de la acción para reclamar información que le concierne, la proyección de requerir al banco de datos toda información que se conserve sobre alguien que pertenece al ámbito de intimidad de la persona, con lo que se advierte la extensión del derecho hacia una legitimación procesal más amplia que la tradicional.

> La protección de la intimidad de los ciudadanos requiere que éstos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados donde las Administraciones Públicas conservan datos de carácter personal que les conciernen, así como cuáles son esos datos personales en poder de las autoridades. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración Pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el artículo 18 de la Constitución española, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos…Al desconocer estas facultades, y no responder a las peticiones deducidas, la administración del Estado hizo impracticable el ejercicio de su derecho a la intimidad, dificultando su protección más allá de lo razonable,

[*] Ver parágrafo 61.9

> y por ende vulneró el art. 18 de la Constitución (TC, 254/93, sentencia del 20 de julio de 1993).

De esta manera, se comprende que la identidad colectada no resulta un derecho privativo de cada individuo, porque admite la existencia de circunstancias que, sin encontrar una afectación directa, es susceptible de ser protegido por otros acudiendo al derecho a la intimidad que toda persona ostenta.

> Afirma Herrán Ortiz que la jurisprudencia ha acogido como característica del derecho a la intimidad su eficacia general, unida a ello, su categoría como derecho absoluto, donde la lesión no se da, ni surge acción para su protección, en tanto se cumple el deber privado de respeto. No hay acción allí donde falta el interés nacido de la agresión. Surge el derecho a la intimidad como derecho general, con capacidad para proteger a la persona frente a cualquier intromisión o ataque a su vida privada. Ahora bien, impera una consideración dogmática general o comprensión preinformática de la intimidad, que permite dudar y recelar de la posibilidad de fundamentar sobre el derecho a la intimidad la totalidad del sistema de protección de los datos personales, lo que llevaría a admitir la necesidad de reconocer la existencia de un nuevo derecho fundamental sobre el que asentar la protección de los datos de carácter personal.

La necesidad de ampliar los objetivos de tutela de la libertad de intimidad se motiva en la propia conversión del derecho tradicional. No se trata aún de la defensa de la persona en sus aspectos más recónditos, sino de comprender que existe un derecho al desarrollo de la personalidad y de todas las vicisitudes que ella abarca, donde anida, entre otros, el derecho a la verdad. Verdad a que se sepa quien es uno; verdad a saber nuestros orígenes y la de quienes nos rodean; verdades que se quieren ocultar a otros.

> El caso Garkin resuelto por el Tribunal Europeo de Derechos Humanos versa sobre el principio de acceso individual a documentos e información sobre la infancia de un huérfano, recogida en el fichero de un orfanato. Las autoridades locales denegaron el acceso argumentando que sería contrario al interés público, puesto que si los datos fueran revelados violarían la confidencialidad con la que fueron creados por enfermeras, profesores, padres adoptivos, etc., perjudicando el sistema de ayuda y protección de los niños, ya que los profesionales se negarían a redactar de nuevo tales documentos. A la vista de lo importante que era la petición de acceso del Sr. Gaskin, la dirección del orfanato intentó ponerse en contacto con todas las personas que habían contribuido a la creación de aquellos documentos para solicitarles su consentimiento en la revelación de la información. El resultado fue que algunas personas no pudieron ser localizadas y otras se opusieron, aunque sin argumentos consistentes.
>
> El Tribunal Europeo sostuvo que era necesario examinar y encontrar un equilibrio entre los intereses generales de la comunidad y los del individuo. Entendió que había existido una violación al artículo 8 porque tales datos concernían a la vida privada y familiar del reclamante, constituyendo un interés vital para el individuo, ya que de lo contrario sería incapaz de entender su infancia y adolescencia. Además el Tribunal añadió que una denegación de acceso a los ficheros basado en argumentos de que las personas que han intervenido en su creación no fueron localizadas o que se opusieron injustificadamente, exigía la existencia de una autoridad independiente que decidiera si procede el acceso o no. La ausencia de esta autoridad impidió que el demandante tuviera garantizado el respeto de su propia vida privada y familiar, por lo que se violó el art. 8 del Convenio Europeo de Derechos Humanos (Gaskin vs. Reino Unido, sentencia del 7 de Julio de 1989).

En nuestro país, el caso resuelto por la Corte Suprema de Justicia de la Nación, caratulado:" *Urteaga, Facundo R. c/ Estado Mayor Conjunto de las Fuerzas Armadas"* (Octubre 15/1998)* dejó establecido que el hábeas data ampara la identidad personal y permite ampliar la cobertura sobre el sentido personalísimo de ese derecho.

En este sentido se afirmó que la protección garantizada facultaba al hermano de la víctima (desaparecida años atrás y de la cual no existían noticias ciertas) a esclarecer las circunstancias en que se produjo la muerte de su familiar, y en su caso, el destino dado al cadáver.

> El voto unánime de la Corte fue sostener que *"…de acuerdo con lo expuesto, lo afirmado por la Alzada en cuanto a que la finalidad perseguida en la presente acción no se compadece con el texto constitucional, se aparta de las circunstancias de la causa. Ello es así en la medida en que la presentación inicial –entre otras peticiones- incluía la de obtener información existente en registros o bancos de datos públicos que permita al recurrente establecer el fallecimiento de la persona desaparecida y, en su caso, conocer el destino de sus restos, es decir, acceder a "datos" cuyo conocimiento hace al objeto de la garantía de que se trata.*

7.1 El derecho a la verdad

La extensión que promete la garantía protegida por el hábeas data se fundamenta en el derecho que "toda persona" tiene para saber la verdad sobre los hechos que le conciernen, que se tornan ineludibles cuando esta de por medio la libertad de intimidad.

La pauta que crea el artículo 43 constitucional abarca manifestaciones distintas como son el derecho de amparo, la tutela de la supremacía de la ley fundamental, la exigencia de licitud, lealtad y exactitud en la información contenida en archivos o bancos de datos públicos y privados, la defensa de la libertad ambulatoria, entre otras garantías afincadas en el contexto.

Un análisis circunspecto y preciso sobre la letra de la ley, pareciera indicar que el hábeas data no se encuentra disponible a otros sino, tan sólo, a quienes tienen una afectación directa y personal.

Esta es la tendencia legislativa que reglamentan las constituciones de Portugal, de España, los Países Bajos, Hungría, Suecia y Perú, entre otros. Y es, por su parte, la opinión que en "Urteaga" domina el pensamiento del Ministro Fayt.

> Dice el Juez Superior en el Considerando 9 de su voto que *el núcleo del tema es la libertad del individuo frente al procesamiento de datos, es decir, la protección del individuo contra la evolución técnica de la informática. En tal sentido, la Declaración de Derechos y Libertades Fundamentales de 1989, aprobada por el Parlamento Europeo, reconoce a las personas el derecho a la intimidad en su art. 6 y les confiere el derecho de acceso y de rectificación de los datos que les afecten en los documentos administrativos. En cuanto al control sobre los datos acumulados y procesados en registros o bancos de datos públicos y privados, se trata de un derecho individual reconocido únicamente al afectado…*

Sin embargo, el derecho a la identidad se relaciona profundamente con el derecho a la intimidad, y como ya hemos dicho, ambos usan al hábeas data como instrumento destinado a evitar injerencias extrañas en la vida privada, y en la medida de sus posibilidades, responde también para reparar el honor agraviado, la imagen perturbada o la identidad igualmente afectada.

La personalidad de un individuo está conformada por ese conjunto de atributos que lo destacan (nombre, imagen, reputación, etc.), de forma que ella se mantiene como un derecho inalienable a la identidad. Si esa malla de protección se penetra por actos abusivos, autorizados o no, y registran datos de esa persona ofreciendo un archivo documental sobre la misma, es justo y legítimo que la base mantenga una verdad refleja de la identidad.

La persona concernida tiene, efectivamente, un derecho a ser informado sobre las características del registro; la duda que cabe plantear es si es un derecho transmisible o, en su caso, si finaliza con la muerte del interesado.

En nuestro parecer, el problema no está en la prosecución del derecho por otros, sino en el mantenimiento del archivo que, por tanto, conserva datos que pueden ser importantes para situaciones distintas.

La Corte Nacional completa la idea en el voto del Dr. Petracchi en la citada causa "Urteaga", por el cual se sostiene que la negativa del Estado a proporcionar la información que estuviera registrada acerca del destino de una persona posiblemente fallecida, afecta indudablemente la vida privada de su familia, en tanto ésta ve arbitrariamente restringida la posibilidad de ejercer derechos tan privados como el del duelo o el de enterrar a los propios muertos.

> Agrega el citado ministro que *…dado que el hábeas data se orienta a la protección de la intimidad, el giro "datos a ella referidos" debe ser entendido como el reaseguro del derecho básico protegido por la norma, como medio de garantizar que sea el titular de los datos el que pueda obtener el desarme informativo del Estado, o de quien fuere, para poder decidir acerca del destino y contenido de dichos datos. Pero, además, en tanto el texto constitucional permite ejercer un control activo sobre los datos, a fin de supervisar no sólo el contenido de la información en sí, sino también aquello que atañe a su finalidad, es evidente que se trata, a la vez, de un instrumento de control. Por lo tanto, no es posible derivar de la citada expresión un permiso genérico para que el Estado se exima de su "deber de información", pues ello significaría revertir su sentido fundamental.*

La identidad resulta así proyectada a un derecho justo como es reconstruir el pasado de alguien que pertenecía a nuestra intimidad y que desaparece sin causas, al menos, razonablemente lógicas. Saber la verdad es también aquí el derecho que se garantiza desde el hábeas data.

> Insistimos con el carácter de *leading case* que tiene "Urteaga", y en lo profundo de sus votos. Por ejemplo, en párrafos finales, agrega Petracchi que *…en la medida en que lo solicitado representa el ejercicio de un interés legítimo, y en tanto ello no vulnera en modo alguno la intimidad de terceros, no cabe restringir la legitimación activa del recurrente, con base en que no se trata de "datos referidos a su persona". Pues proteger el derecho a conocer todo lo relativo a la muerte de un familiar cercano ocurrida en las circunstancias referidas significa, en última instancia, reconocer el derecho a la identidad y a reconstruir la propia historia, los cuales se encuentran estrechamente ligados a la dignidad del hombre.*

Es evidente, en consecuencia, que los vínculos jurídicos familiares, que determinan el estado de familia, integran la identidad de la persona y, en la perspectiva funcional y dinámica que alentamos para la garantía creada, puede obtener tutela el tercero que tiene el derecho a saber la verdad.

> También la Corte Nacional en el precedente "Suarez Mason" (agosto 13/1998), sostuvo en el voto del Dr. Boggiano que "*…la actora tiene derecho a obtener la información que existiera en los organismos públicos requeridos pues, tal como ha sido expresado anteriormente, la Constitución ha consagrado el derecho a conocer los datos que el Estado pudiera tener de su persona que, en la causa, concierne a su hija…Pues tal como ha juzgado este tribunal, el derecho consagrado en el art. 19 de la Constitución Nacional protege jurídicamente un ámbito de autonomía individual constituido por los sentimientos y las relaciones familiares de proximidad existencial y, por lo tanto, el desconocimiento de la verdad acerca de las circunstancias de la desaparición de su hija y de dónde se hallan sus restos afecta gravemente su derecho a la identidad y a la intimidad, que en su fase positiva, habilita la presentación efectuada en autos.*

7.2 La potestad de control sobre el dato

A medida que se avanza en el perfil del hábeas data se advierte que la preocupación central asienta en el uso racional de los datos personales que se compilan en archivos y registros, informático o no, y cualquiera sea su carácter (públicos y privados).

> Es clásica la expresión utilizada por Perez Luño al referir a una "libertad informática" que asegura, por un lado, la identidad de las personas ante el riesgo de que sea invadida o expropiada por determinados usos (más bien abusos) de las nuevas tecnologías. Para ello pone en manos de las personas los instrumentos procesales pertinentes para ejercer su derecho a acceder y controlar las informaciones que les conciernen y, por el otro, contribuye a conformar un orden político basado en la equilibrada participación cívica y colectiva en los procesos de información y comunicación que definen el ejercicio del orden en las sociedades informatizadas de nuestra época.

Frente a la probable dificultad para evitar el origen de la base de datos se ha previsto la participación del involucrado permitiendo que sea éste quien defina la calidad del registro que le concierne.

Este control le posibilita corregir el dato equívoco o inexacto; suprimir la información incorrecta y, aun resolver la transmisión del mismo. Claro está que para ello, existe un derecho natural al acceso a la información que debe preferirse en la dispensa de tutela con el fin de evitar la evasión del mencionado derecho al control sobre la base de datos.

La potestad que referimos suele nominarse como "autodeterminación informativa", en el sentido de dispensar al hombre un derecho de administrar la información personal que le concierne propiciando que controle los datos registrados y resuelva cuáles son aquéllos que admite su transmisión a terceros.

En síntesis, es una garantía básica de la persona decidir por sí misma cuándo y dentro de qué límites procede revelar situaciones referentes a su propia vida.

> Sostenía el Tribunal Constitucional Alemán en el año 1983 que "la libertad informática ya no es la libertad de negar información sobre los hechos privados o datos personales, pretensión que hoy no podría encontrar adecuada tutela en muchos casos, sino la libertad de controlar el uso de los propios datos personales insertos en un programa informático. Es el *hábeas data* correspondiente al antiguo *hábeas corpus* del respeto debido a la integridad y libertad de la persona…Por tanto, derecho de acceso a los bancos de datos, derechos de control sobre su exactitud, derecho de puesta al día y de rectificación, derecho de secreto para los datos ´sensibles´, derecho de autorización para su difusión, todo este conjunto es lo que hoy constituye el ´right to privacy´".

7.3 El derecho de identidad de las personas jurídicas

Una de las dificultades más importantes que encuentra la determinación de los bienes jurídicos que tutela el hábeas data está en saber si la garantía se puede extender a las personas jurídicas, a cuyo fin nos detendremos para su análisis en el estudio del sujeto activo del proceso.

No obstante, el párrafo final del artículo 1° de la ley extiende la vigencia y aplicación de la ley a las personas ideales.

De todos modos podemos coincidir con aquellos que sostienen que las empresas tienen un derecho de identidad (marca o registro), un nombre que las identifica; un prestigio que proteger, o una trayectoria que conservar. Por todo eso, el archivo que reúne información debe ser cierto y confiable, circunstancias que permitirían defender el derecho a una propia identidad.

> Considera Palazzi –reproducido por Puccinelli- que se puede hablar de un derecho a la identidad de las personas jurídicas que se proyecta en el nombre comercial o en el valor del fondo de comercio o de la marca de sus productos, por poner algunos ejemplos. Por ello comparte la opinión de Rivera para quien, frente a un ente ideal el hábeas data protege un derecho a la verdad sobre los datos sociales que se encuentran en un determinado registro y que hagan a la reputación, fama y buen nombre del afectado.

La conclusión no significa afirmar que el hábeas data sea el remedio procesal preciso para lograr la protección que se persigue, pues aunque sea lógico que las entidades jurídicas puedan disfrutar de un derecho

de acceso o de corrección sobre la información que le concierne; también es cierto que el derecho constitucional que se garantiza es un valor para el hombre y sus libertades, mientras que el mundo de los negocios se presenta dando preferencia a valores económicos; y el honor y la imagen, entre otros derechos, tienen en este aspecto un tinte crematístico innegable.

> ¿Poseen las personas jurídicas el mismo derecho a la intimidad que las físicas? Se interroga Estadella Yuste. En su parecer es difícil negar que las personas jurídicas carezcan de un derecho general de conducir sus actividades en secreto, o de evitar que cierta información confidencial pase a manos de la competencia o del público en general. No obstante, la necesidad de proteger ciertos secretos empresariales o la confidencialidad de información comercial no implica que se pueda atribuir a las entidades jurídicas un derecho individual a la intimidad, ya que el significado de éstos términos no es el mismo. En mi opinión –agrega-, la conveniencia legal que se haya podido encontrar en atribuir a las entidades jurídicas una "personalidad", no implica que éstas sean humanas y que tengan que disfrutar de los mismos derechos que los individuos. Parece ser más apropiado atribuirles derechos y obligaciones propios de la actividad que desempeñan y relacionarlos con aquellas ramas del derecho encargadas de regular tales actividades, en lugar de fundamentar sus Derechos en instrumentos legales que no han sido diseñados para personas jurídicas.

8. Derecho a la información

Vinculado al proceso constitucional de hábeas data aparece este derecho a la información que representa varias cosas importantes.

En torno a los fundamentos que le ofrece a la garantía constitucional creada es evidente que el derecho, desde esta perspectiva, permite al individuo exigir al banco de datos la información que tenga sobre su persona.

Sin embargo, debemos recordar que en el conjunto de posibilidades que encuadra el derecho a la información aparecen la libertad de expresión, la libertad de prensa y de imprenta, la libertad de opinión y otras que, confrontadas con las potencialidades que ofrece el hábeas data, pueden ocasionar algunas reservas. Quizás, pensando en ellas, el constituyente dejó asentado que el hábeas data no podía afectar el secreto de las fuentes periodísticas.

Ahora bien, como el derecho a la información resume en los hechos tres actividades: a) la libertad de investigar; b) la libertad de difundir y c) la libertad de recibir información y opiniones; cada una de ellas tiene el correlato de la responsabilidad, razón por la cual existe otro derecho personal a no recibir información distorsionada, y su reflejo en el derecho a no ser objeto de una información falsa o abusiva.

> El tema lo explica acertadamente Uicich al agregar que por libertad de investigar se entiende la posibilidad irrestricta de utilizar toda la información obtenida legalmente y todos los medios existentes en procura de información. La libertad de difundir es la consecuencia de la facultad de investigar. Toda esa información obtenida, en la medida que no perjudique el legítimo interés de los terceros, goza de la facultad de ser difundida por cualquiera de los medios de comunicación. La libertad de recibir información es la faceta pasiva de la ecuación. Así como el ser humano, por ser tal, goza de la libertad de investigar y de difundir, él mismo es titular del derecho a ser informado, a exigir que la información le sea brindada…El derecho a la información comprende pues la faceta de quien tiene la facultad de acceder a la información cuanto la del sujeto pasivo de esa información de que no sea distorsionada o no sea revelada en tanto afecte su intimidad y no exista cuestión de orden público o de seguridad del Estado que lo justifique.

De esta manera el derecho afianza la potestad de control sobre el derecho a la verdad, tanto para el sujeto activo que esta en el archivo o registro, como para quien recibe la información.

> El problema, a juicio de Gutierrez Castro, se plantea en un conflicto de intereses, es decir, no sólo de legalidad, sino que sobre todo de legitimidad, vale decir de justicia y racionalidad en el ejercicio de un derecho. Por decirlo de otro modo, ambos derechos valen, el de quien informa y el de quien se informa. Pero valen dentro de límites razonables de modo que cuando se abusa del derecho de informar este se ejercita ilegítimamente; o sea, no es que un derecho se imponga a otro por su mayor peso, es que no puede coexistir dos conductas lícitas y legítimas contrapuestas, una debe ceder en el caso concreto ante otro y cuando se cede o es porque no se tenía derecho (legalidad) o porque se llegó a su límite razonable (legitimidad).

8.1 El derecho de información a los sujetos que están en el archivo

Los bancos de datos registran información muy diversa que, por lo general, no es de conocimiento público y, menos aun, de la persona que en él se encuentra.

El acopio y obtención de datos es bastante simple si se quiere. Todo depende de la finalidad que el registro persiga (por ejemplo, lograr información respecto a litigios que tenga una persona, causa y estado de cada expediente se puede conseguir hasta desde un ordenador con su módem respectivo) y del destino que piensa asignar a esa información compilada.

Precisamente por esta presunta facilidad en la recopilación, algunas legislaciones establecen que no se puede evitar el carácter público del dato destinado a facilitar información general que, para ello, está abierta al público.

> El crear una base de datos –afirma Marcel Pinet- a partir de datos personales que sean públicos, aunque sea sólo por un instante, llevaría a la modificación de la naturaleza de la información. Un ejemplo sirve para ilustrar este punto de manera más que suficiente: en cualquier democracia, la vista de un procedimiento penal en la que se dicta sentencia es pública, pero en todas y cada una de nuestras democracias los antecedentes penales, que son los archivos de las condenas que se dictaron de manera pública, son uno de los archivos más protegidos y menos accesibles. Esto es un ejemplo de como cuando se recopila información, ésta toma un valor informativo específico.

Por ello, es más importante trazar el límite de divulgación que tiene el registro, antes que determinar cuando un dato se puede o no hacer público de acuerdo a la instancia individual.

En este sentido, el derecho de acceso a los archivos es una garantía derivada del derecho a la información.

> En el ámbito de las telecomunicaciones es bien conocido el ejemplo de los directorios inversos: se crean con los mismos datos que se utilizan para los directorios públicos de los abonados telefónicos, pero se invierte el criterio de búsqueda: en vez de utilizar un nombre y una dirección conocidos para encontrar un número de teléfono, se usa un número de teléfono para averiguar el nombre y la dirección del abonado. El criterio que se use para acceder a los datos puede cambiar radicalmente el uso que se vaya a darles. En ambos casos (directorios normales e inversos) la información es la misma y, a no ser que el interesado se haya opuesto de manera explícita, está al alcance del público en general. Sin embargo buscar el nombre y dirección de una persona si sólo tiene su número de teléfono supone buscar información que, tal vez, esa persona no pensaba dar; supone descubrir información suya sin su consentimiento y saber más de lo que esa persona quería revelar.

Y ese acceso está especialmente previsto como un mecanismo de vigilancia sobre el dato y la difusión que del mismo se pretenda realizar. Obviamente, mientras perdure la ausencia de una ley para el tratamiento de datos, es imprescindible resguardar el derecho de acceso a la justicia como la máxima garantía; al mismo tiempo que se debe facilitar el ingreso a la información que nos concierne.

8.2 El derecho a la información veraz

Con la misma preocupación con que se agiliza la defensa de la persona registrada, se debe proteger al usuario de ese banco de datos (principio de exactitud).

Veracidad de la información supone mantener actualizado el archivo y conservar la información oportunamente tomada de acuerdo con las reales circunstancias en que sucedieron (situación real del afectado).

La transportación del informe por la vía que sea, exige responsabilidad en el llamado "tratamiento del dato".

Tomemos como ejemplo la ley española que en el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, de "*Protección de Datos de Carácter Personal*" * evidencia el problema que afrontamos:

Artículo 29. Prestación de servicios de información sobre solvencia patrimonial y crédito.

1. *Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.*
2. *Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.*
3. *En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.*
4. *Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.*

Dado que el responsable de la veracidad del informe no es el acreedor, pues no tiene competencia para modificar o cancelar los datos inexactos que se encuentran en el archivo, aquella recae exclusivamente sobre la persona que comunicó el dato, a quien podría llamarse "responsable de la anotación" para distinguirlo del responsable de la base de datos que es el titular de la responsabilidad global. La inclusión de los datos en un fichero ajeno, supone un tratamiento automatizado de estos. Por ello, no han existido dudas en la interpretación de la ley española acerca de que cualquier incumplimiento respecto de la calidad de los datos incluidos en el fichero, salvo que fuera imputable a la exclusiva responsabilidad del titular del registro, deba ser imputado a la persona que introdujo los datos, al responsable de la anotación como se dijo, quien deberá garantizar la calidad de los datos.

9. Derecho a la "autodeterminación informativa" *

El resumen de derechos que tutela el hábeas data muestra que el punto de mira no es sólo impedir intromisiones ilegítimas en la esfera privada, sino evitar que los datos obtenidos sean utilizados o transferidos

* Ver parágrafo 61.10

sin el resguardo y control que pueda tener la persona; de este modo se elimina –al menos parcialmente- el llamado "rumor informático" y se instala una valla a las empresas que hacen de las bases de datos su fuente de comercialización.

> Inclusive, afirma Panuccio, se impone una doble vertiente de responsabilidad al titular del banco de datos: diligencia en el mantenimiento de la calidad del contenido de la misma, en términos de veracidad, licitud y caducidad, y la obligación de responder por las consecuencias lesivas que su negligencia, en términos de responsabilidad objetiva, pueda ocasionar el afectado.

Precisamente, como la figura no tiene antecedentes en nuestra legislación, más allá de las actuaciones logradas en materia civil respecto a la tutela de la intimidad; o en el derecho penal en aras de la defensa del honor y la confianza, lo cierto es que el hábeas data tiene un perfil acotado que se resuelve desde la pretensión del afectado. Es un derecho individual que, partiendo desde el derecho a la intimidad y con posadas en la privacidad, la identidad o la dignidad de la persona fragmenta su unidad como proceso para aplicar su garantía a otras cuestiones como la tranquilidad espiritual, el derecho al aislamiento, la protección del nombre civil o comercial, la integridad física, el secreto profesional, etc.

Esta es una primera visión del derecho fundamental creado por el artículo 43 de la Constitución Nacional. La promesa de protección a la intimidad es amplia, sin embargo, no procede si el acto lesivo (la afectación, propiamente dicha) no proviene de un tratamiento informático o manual de nuestros datos compilados en una base, archivo o registro.

Por ello, la garantía antes que una herramienta procesal, es un derecho disponible por el individuo que encuentra de esta forma una vía de acceso a información que le concierne, e inmediatamente, la potestad de resolver, por sí mismo –con algunas pocas limitaciones- si quiere que esos datos se transmitan a otros, se conserven bajo reserva o confidencialidad, o se supriman por afectar la sensibilidad de la persona. Este conjunto de atributos suele nominarse como "derecho de autodeterminación informativa".

> Se hace notar que el derecho a la autodeterminación informativa se construye tomando como fundamento el concepto de intimidad o vida privada; puesto que trata de ofrecer tutela a la persona respecto a sus datos de carácter personal una posible utilización abusiva de los mismos mediante la informática u otro tratamiento automatizado. Ahora bien, que nadie se confunda –dice Herrán Ortiz-, mediante el derecho a la autodeterminación informativa no se salvaguardan tan solo los datos que se denominan sensibles, sino también aquellos que sin pertenecer a la esfera más próxima al individuo, son susceptibles de daños su imagen o el ejercicio plano de sus derechos. Más aún, ni tan siquiera los considerados como datos sensibles representan siempre información íntima o secreta de la persona, el origen racial o determinadas enfermedades son tan evidentes y reconocibles externamente que de ellas poco permanece reservado en la intimidad del individuo y, sin embargo, no puede dudarse de su carácter sensible como informaciones personales.

La subjetividad natural que impera en esta potestad de control sobre la base de datos caracteriza, entonces, al derecho emergente como:

a) Un derecho individual, previsto para atacar las intromisiones en la intimidad concretadas con un fin específico (en el caso, compilar las acciones para registrarlas en un archivo).

b) Un derecho de acceso irrestricto, a excepción de fuentes de información que puedan mantener su secreto por razones de seguridad justificadas (V.gr.: datos policiales; registros fiscales; etc.).

c) Un derecho de requerir la verdad del registro (principio de exactitud y actualidad del dato archivado), o de promover su rectificación o supresión.

d) Un derecho de exigencia por el cual se pretende que el titular de la base de datos utilice la información compilada con la finalidad concreta para la que fue autorizado el archivo.

A su vez, el proceso garantista, si bien sujeto al principio dispositivo (*ne proceda iure ex officio; nemo iudex sine actore*), por sí mismo constituye un sistema cautelar o preventivo, que no requiere de

reglamentación para obrar en tal sentido, dentro del marco de posibilidades que el derecho otorga (amparo, conocimiento, rectificación o cancelación).

> La ley española parte de un "derecho a la autodeterminación informática" que se inspira en el principio de que ha de ser el sujeto quien decida qué datos pueden ser almacenados, por quién y para qué fines, lo cual comporta una capacidad de decisión que descansa en una información previa o en el requerimiento inicial de su consentimiento para recabar, tratar o ceder los datos sensibles a él referentes. Estamos pues ante el "hábeas data" en virtud del cual la persona tiene la facultad de controlar la información que le concierne y que se encuentra recogida en el fichero automatizado; le asegura una esfera de libre decisión con respecto a una categoría de datos sobre los cuales el ordenamiento le confiere la facultad de prestar su consentimiento para ser objeto de tratamiento automatizado.

10. Advertencia: *addenda*

Señalamos con anterioridad las dificultades que tiene encontrar la naturaleza jurídica de la garantía que emerge del párrafo tercero del artículo 43 constitucional. El derecho comparado muestra, entre otros casos, una suerte de opción: o se prefiere la regulación como derechos concedidos desde una ley específica; o tal como resulta en Argentina, se define un proceso especial (proceso constitucional) destinado a la protección y defensa de los derechos específicos que la norma constitucional señala.

Sin entrar, por ahora, en las ventajas o inconvenientes que tiene esta elección del constituyente, el paso siguiente se da para resolver el tipo de proceso habilitado, donde encontraremos algunas incertidumbres para saber si es una especie o sub tipo de amparo o un procedimiento especial y autónomo.

> En las conclusiones del XX Congreso Nacional de Derecho Procesal (San Martín de los Andes,octubre de 1999) se dieron dos lecturas en torno a la naturaleza procesal del hábeas data: la primera, siguió mi opinión respecto a que el hábeas data no es una modalidad del amparo, sino una vía con carriles propios; de carácter autónomo y que no recibe los presupuestos y condiciones del amparo tradicional. La segunda, consideró que se trataba de una modalidad del amparo con características propias, sin que le sea aplicable la idea básica de la primera parte del artículo 43 C.N. (arbitrariedad o ilegalidad manifiesta), y sí en cambio el carácter incondicionado (expedito), como vía rápida, en cuya aplicación la jurisdicción opera en función protectora.

Pero al llegar a los derechos tutelados desde el hábeas data, se van recortando interpretaciones disímiles que ocupan extensiones animadas desde la jurisprudencia (por ejemplo el caso Urteaga que abre la legitimación procesal) o acotamientos procesales que reducen la significación del hábeas data a las posibilidades de acceso, conocimiento, actualización, rectificación, supresión o confidencialidad del dato.

De mantenerse esta incógnita el proceso puede llegar a constituir una aventura de riesgo, tal como aconteció en Perú y que llevó a tener que modificar la ley constitucional al poco tiempo de creada.

> Sostiene Eguiguren Praeli que la extensión del hábeas data a la protección del honor y la buena reputación, la intimidad familiar y personal, la voz e imagen propias, y al derecho de rectificación en los medios de comunicación social, configuró un gravísimo exceso del constituyente de 1993. Siendo que conceptualmente el hábeas data busca proteger la intimidad personal y la privacidad frente a posibles abusos del poder informático, mediante el registro y difusión de datos sensibles, la aplicación genérica de este remedio procesal constitucional a cualquier clase de afectación a la intimidad y, lo más serio, la inclusión a otro conjunto de derechos que podrían verse afectados a través de los medios de comunicación, revela una muy acusada falta de conocimiento y de idoneidad técnica.
>
> Si la extensión, anómala y desnaturalizada del hábeas data, a los derechos antes referidos no fue producto de una confusión, sino que obedeció a una decisión

explícita –como sostienen algunos- el asunto puede resultar incluso más delicado. Y es que la intensión sería impedir la difusión de datos o informaciones obtenidos a través de la investigación periodística, alegando la afectación de la buena reputación o intimidad de ciertos personajes públicos.

Bibliografía Capítulo II

Alpa, Giuseppe, *Compendio del nuovo Diritto Privato*,editorial UTET, Torino, 1985.

Bidart Campos, Germán J., *Tratado elemental de derecho constitucional argentino*, tomo 1: *El derecho constitucional de la libertad*, editorial Ediar, Buenos Aires, 1986.

Brüehann, Ulf, *La escena internacional y la directiva comunitaria: 5 semanas antes de su entrada en vigor*, en XX Conferencia Internacional de autoridades de protección de datos (1998), editado por Agencia de Protección de Datos, Madrid, 1999.

Carballo, Elvira, *Informática y protección de datos: Antecedentes para el proyecto de una ley nacional*, en Revista del Colegio de Abogados de Buenos Aires, nº 3, 1986.

De Slavin, Diana, *Mercosur: La protección de los datos personales*, editorial Depalma, Buenos Aires, 1999.

Eguiguren Praeli, Francisco J., *El hábeas data y su desarrollo en Perú,* en *Liber amicorum Héctor Fix Zamudio*, volumen 1, editorial Secretaría de la Corte Interamericana de Derechos Humanos, San José, Costa Rica, 1998.

Estadella Yuste, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales*, editorial Tecnos, Madrid, 1995.

Garzón Clariana, G., *Flujo de datos transfronteras, protección de datos y derecho internacional*, IBI, Documentos TDF 102, Roma, 1981.

Gutierrez Castro, Mauricio, *Derecho a la información. Acceso y protección de la información y datos personales*, en 51º período ordinario de sesiones OEA/Ser.Q, 4/29 de agosto de 1997. CJI/SO/doc. 9/96 rev. 2, Río de Janeiro, Brasil.

Habermas, Jürgen, *Historia y crítica de la opinión pública*, traducción de Antoni Domenech, Ediciones de Gustavo Gili, Barcelona, 19994.

Herrán Ortiz, Ana Isabel, *La violación de la intimidad en la protección de datos personales*, editorial Dykinson, Madrid, 1999.

Herrero Tejedor, Fernando, *Honor, intimidad y propia imagen*, editorial Colex, Madrid, 1990.

Lyon, David, *El ojo electrónico. El auge de la sociedad de la vigilancia,* editorial Alianza, Madrid, 1995.

Martínez Sospedra, Manuel, *Sobre la intimidad. Derecho a la intimidad, vida privada y* privacy. *El art. 18 CE* in principio *en la jurisprudencia del Tribunal Constitucional,* en *Sobre la intimidad,* editorial Fundación Universitaria San Pablo C.E.U., Valencia, 1996.

Medina, Cecilia – Mera Figueroa, Jorge, *Sistema jurídico y derechos humanos*, editorial Escuela de Derecho de la Universidad Diego Portales, Santiago de Chile, 1996.

Novoa Monreal, Eduardo, *El derecho a la vida privada y libertad de información. Un conflicto de derechos*, editorial Siglo XXI, México, 1979.

Oteiza, Eduardo D., *Información privada y hábeas data,* en *Estudios de Derecho Procesal en homenaje a Adolfo Gelsi Bidart*, editorial Fundación de Cultura Universitaria, Montevideo, 1999.

Palazzi, Pablo, *Conferencia en "Impacto de la reforma constitucional en la actividad empresaria"*, Universidad Argentina de la Empresa, 25 de octubre de 1994.

Panuccio, Vittorio, *Banche de dati e diritti della persona*, editorial CEDAM, Milan, 1985.

Perez Luño, Antonio Enrique, *Los derechos humanos en la sociedad tecnológica*, en la obra colectiva *Libertad informática y leyes de protección de datos personales*, editorial Centro de Estudios Constitucionales, Madrid, 1989.

Pinet, Marcel, *Datos públicos o datos a los que puede acceder el público y protección de datos personales*, en XX Conferencia Internacional de autoridades de protección de datos (1998), editado por Agencia de Protección de Datos, Madrid, 1999.

Prosser, Williams, *Privacy (a legal analysis)*, en California Law Review, nº 48, ps. 338 y ss., 1960.

Puccinelli, Oscar Raúl, *El Hábeas Data en Indoiberoamérica*, en *El Amparo Constitucional, perspectivas y modalidades*, editorial Depalma, Buenos Aires, 1999.

Uicich, Rodolfo Daniel, *Los bancos de datos y el derecho a la intimidad*, editorial Ad Hoc, Buenos Aires, 1999.

CAPÍTULO III. Las bases de datos

11. La información y los datos

¿Qué es un dato? La pregunta constituye el punto de partida para reconocer la preocupación constitucional y la pretensión objetiva que trae la garantía creada.

El dato es una referencia. Puede ser descriptivo, indicador, dar una pauta, pero no se vincula a la información mientras el conocimiento no se transmita. Igual sucede con las noticias o las investigaciones.

> Afirma Puccinelli que el vocablo "dato" se refiere a un elemento circunscripto y aislado (v.gr.: nombre o nacionalidad), que no alcanza a tener el carácter de información, pues para que se transforme en ella se requiere la interconexión de esos datos de manera que, vinculados, se conviertan en una referencia concreta (v.gr.: nombre y nacionalidad).

La misma voz (dato) es anfibológica: define varias cosas y mantiene incertidumbre. Por lo general muestra una característica parcial que se utiliza como indicio o fuente.

El dato tiene referencia en algo o alguien, igual que la información. Sin embargo difieren.

> Algunos entienden "datos" a la representación de hechos, conceptos o instrucciones bajo una forma adaptada a la comunicación, a la interpretación o al tratamiento por seres humanos o máquinas; y por "informaciones" al significado que toman los datos de acuerdo con convenciones vinculadas a estos datos. Asimismo se interpreta por "sistemas de información", los ordenadores, instalaciones de comunicación y redes de ordenadores y de comunicación, así como los datos e informaciones que permiten conservar, tratar, extraer o transmitir, incluidos los programas, especificaciones y procedimientos destinados a su funcionamiento, utilización y mantenimiento.

Los datos de alguien son personales y tienen el derecho a la reserva y confidencialidad o a la cobertura mayor de la libertad de intimidad. Por su parte, el derecho a la información es una garantía de las sociedades libres y democráticas, lo cual supone no poner trabas a sus mecanismos de expresión y difusión.

Entre ellos impacta el fenómeno informático que toma los datos como fuentes de información para darles un uso determinado. El ejercicio dinámico del registro para actividades diferentes (V.gr.: comercio electrónico –*e-commerce*); la transferencia de datos por medios de comunicación que no reconocen fronteras; la comunicación a través de redes, etc., muestra sin dificultades de qué manera la sociedad convierte en públicas las acciones privadas y, por ello mismo, la necesidad de encontrar un límite natural a esta invasión impensada en la intimidad de las personas.

> Hay que diferenciar estos tres conceptos –dice Davara Rodríguez- que, aunque es evidente que tratan distintas cuestiones, tienen una incidencia grande en el momento de analizar cualquier normativa sobre protección de datos. Si entendemos por dato el antecedente o noticia cierta que sirve de punto de partida para la investigación de la verdad y aceptamos que ese dato se encuentra en un documento o soporte –físico o lógico- con la calidad de testimonio, debemos distinguirlo de información, entendiendo por tal la acción de informar o dar noticia de alguna cosa. El dato es difícil que, por sí solo, pueda tener una incidencia grande o grave en la llamada privacidad. Esto es, mientras el dato no resuelva una consulta determinada, no sirva a un fin, no dé respuestas o no oriente la posible solución a un problema, es el antecedente o punto de partida para la investigación de la verdad; pero, en el momento en que ese mismo dato da respuesta a una consulta determinada, o sirve a un fin, o se utiliza para orientar la solución de un problema, se ha convertido en información. En este sentido se expresa el apartado primero de la exposición de motivos de la ley española de

protección de datos, indicando que: "*…el conocimiento ordenado de esos datos (los de carácter personal) puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor, y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos*".

La breve descripción de relaciones entre información, dato y uso informático, releva de alguna manera, cuál es la actividad que se piensa establecer para los jueces. La idea sugiere interpretar que el hábeas data tiende a dejar en manos del Juez la información referida a una persona contenida en un soporte convencional o mecánico (base o banco de datos), para que pueda ordenar sobre su uso y destino.

En síntesis: que el Juez tenga los registros, o los datos, significa hábeas data.

Luego, la función tuitiva, abarca el control sobre las bases de datos (cumplimiento de principios mínimos para su constitución y funcionamiento); la estimación acerca de cuando un dato debe ser protegido en el sentido de las acciones que el hábeas data recibe (acceso a los archivos, confidencialidad del dato o rectificación o supresión del mismo); la tarea de supervisar, a pedido de parte interesada, la forma como se recolectan los datos y el tratamiento que a ellos se asigna, donde aparecen otras manifestaciones como la cesión y las responsabilidades emergentes.

11.1 La información, los archivos y la evolución histórica

En la evolución de la figura se verifica un cambio importante que proviene del desarrollo tecnológico y de las ciencias de la información.

> Perez Luño dice que en otros períodos históricos el progreso de la ciencia y de la técnica venía entendido, las más de las veces, como aportación al desarrollo de la humanidad en términos cuantitativos y, por ello, independiente respecto a los valores. Por el contrario, el signo distintivo de nuestra época es que en ella el progreso tecnológico se halla inescindiblemente ligado a elecciones o valoraciones éticas y políticas. Ello obliga a someter cada innovación tecnológica al correspondiente *technology assesment*, esto es, a una tasación crítica de sus consecuencias. A esta exigencia son especialmente sensibles las sociedades más desarrolladas. En ellas se teme el coste que, para el disfrute de los derechos fundamentales, puedan representar determinados progresos tecnológicos e, incluso, se ha llegado a aludir, en algunos sectores de la teoría social anglosajona, al peligro de una contaminación de las libertades en el seno de las sociedades tecnológicamente avanzadas.

El derecho a la intimidad está ahora acosado por la transformación y el progreso de las herramientas técnicas. Inclusive, la información sobre las personas constituye un dato relevante y revelador de las fuentes de conocimiento sobre el desarrollo de la sociedad.

La posibilidad de aislamiento, otrora posible, está afectada por la intromisión permanente de los medios en el hogar, los que son inevitables y paradójicamente imprescindibles.

El dilema no es la perturbación en sí misma, tampoco la invasión en el reducto privado del ambiente familiar. El problema es que cuando se obtiene un dato y se lo asocia a otro, comienza a elaborarse un perfil de la persona, o del grupo al que pertenece, o también, interesando la sociedad donde está inserto.

En definitiva, se ha producido un tratamiento (procesamiento) de los datos que posteriormente se recopilan, se compendian y archivan para darles un destino del cual, esas personas quizás jamás tengan conocimiento.

> Es cierto –recuerda Estadella Yuste- que antes de la era del ordenador ya se utilizaron archivos manuales con información personal, los cuales fueron usados por ciertas autoridades nacionales para repetidos intentos de aniquilación de un sector de la sociedad, por ejemplo, en Alemania por Hitler, Por esta razón, la

> automatización de ficheros de datos personales es vista, muy a menudo, con cierto recelo.

El avance tecnológico le permite al hombre común que disponga de interés para conseguirlo, la posibilidad de tomar fotografías desde puntos tan lejanos que serían imposibles de captar desde el objetivo; se pueden escuchar conversaciones a distancia; se testimonian hechos por la reconstrucción computarizada; y, entre tantas más, se levantan datos y registros de personas con la finalidad de formar archivos que dan las características generales de la sociedad donde se vive.

Muchas veces estas actividades no tienen el consentimiento o el sometimiento voluntario de las personas a quienes se afecta. Aparece así la manipulación y la introducción de la técnica en la vida íntima de los hombres, agrediendo en consecuencia, la esfera de sus libertades individuales.

Algunos afirman que es recién en los años sesenta del siglo XX cuando se advirtió la amenaza que la intimidad personal sufría por las nuevas tecnologías, comenzando un proceso de legislación internacional, regional y local que sigue hasta nuestros días.

> Los derechos humanos han sido objeto, a lo largo de la historia, de una serie de mutaciones que les permiten ser clasificados por generaciones. Tal como Perez Luño ha puesto de manifiesto, la primera generación correspondería a los derechos humanos considerados como derechos de defensa de las libertades del individuo, es decir, los que exigen la no injerencia de los poderes públicos en el ámbito privado; la segunda generación corresponde a los derechos económicos, sociales y culturales, los cuales requieren una política activa de los poderes públicos para garantizar tales derechos; y en la tercera generación se encontrarían los derechos humanos que complementan las libertades individuales y los derechos sociales, es decir, son los que se presentan como una respuesta al fenómeno de la contaminación de las libertades; dentro de esta categoría se destacarían el derecho a la libertad informática o protección de datos, derechos de los consumidores, etc.

El desarrollo normativo, no obstante, ha debido equilibrar la importancia que tiene la acumulación informativa a los fines de la organización política (por ejemplo, planificación estratégica, política fiscal, economía social, estadística, etc.) con la protección del hombre en su derecho a la privacidad, que constituye, por estos tiempos, un avance moderno de la libertad de intimidad.

11.2 La dimensión normativa

La elaboración de un conjunto de leyes que se haga cargo del problema enfrentado con las bases de datos, puede clasificarse a grandes rasgos, en tres sistemas:

a) El sistema internacional

b) El sistema regional

c) El derecho interno (constitucional, legislativo y jurisprudencial)

El primero de ellos es una proyección sobre la inteligencia que cabe asignar a las cláusulas que tienen, sobre el tema del derecho a la intimidad, las convenciones internacionales.

Tomemos por ejemplo el caso de la "*Declaración Universal de Derechos Humanos*" (1948) que declara su fe en los derechos fundamentales del hombre, en la dignidad y el valor de la persona humana y en la igualdad de derechos de hombres y mujeres, expresando la resolución de la comunidad universal de elevar el nivel de vida dentro de un concepto más amplio de libertad.

La Resolución 217 A (III) del 10 de diciembre de 1948 * consagró el derecho de todo individuo a la libertad de opinión y expresión, incluyendo en esa garantía, el derecho a no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, el de difundirlas sin limitación de fronteras por cualquier medio de expresión.

Sin embargo, entre libertad de información y derecho a la intimidad hubo roces inevitables, los que sólo *pueden* remediarse a través de una lectura inteligente de las cláusulas.

Ese fue el paso que dieron los sistemas regionales.

En el seno del Consejo de Europa, en 1967, se creó una comisión consultiva para estudiar el impacto de la tecnología informativa en los derechos de las personas, dando lugar la investigación a la Resolución 509 * sobre "*los derechos humanos y los nuevos logros científicos y técnicos*". A partir de esta decisión el Comité de Ministros elaboró una serie de reglas relativas a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector privado y otra similar pero referida a los bancos de datos del sector público. En ambos casos, se debía armonizar entre el derecho a ser informado y a tener una vida privada, a cuyos efectos se dieron las pautas siguientes:

- La información debe ser exacta, mantenida al día, apropiada para el fin para el que fue almacenada y obtenida por medios legales.
- Todo ciudadano tiene derecho a conocer la información archivada sobre sí mismo.
- Las personas que deben operar sobre las bases de datos tienen que estar bajo severas normas de conducta para el mantenimiento del secreto y para poder prevenir el mal uso de los datos.
- La seguridad debe ser extremada al máximo para impedir el acceso a las bases de datos a personas no autorizadas o para evitar el desvío de la información, mal intencionadamente o no, hacia sitios no previstos.
- Si la información va a ser utilizada con fines estadísticos se revelará de tal forma que sea totalmente imposible relacionarla con ninguna persona en particular.

Tiempo después de da el "*Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal*" (Estrasburgo, 1981) conocido como Convenio 108, el cual fue largamente demorado en su ratificación por los estados partes.

En Estados Unidos de América, en 1974, se sanciona la "*Privacy Act*" que reza en su exposición de motivos: *"El Congreso estima que la privacidad de un individuo es afectada directamente por la captación, conservación, uso y difusión de información personal por entes y órganos federales…, el creciente uso de ordenadores y de una tecnología compleja de la información, si bien es esencial para el funcionamiento eficiente de las administraciones públicas, ha aumentado sensiblemente el detrimento que para la privacidad individual puede derivarse de cualquier captación, conservación, uso y difusión de información personal"*.

> Algunos autores observan en este desarrollo normativo una relación con la evolución de los derechos. "Una primera generación –dice Fappiano- de leyes sobre protección de datos personales (*Datenschultz*, del Land de Hesse de 1973, *Landesdatenschutgesetz* de Renania-Palatino, 1977, *Data Sueca* de 1973, etc.) tiene como objetivo garantizar los derechos individuales estableciendo determinados límites al empleo de la informática. Se interpretó que la eficacia de la protección reposaba en la autorización previa del banco de datos y en el posterior control de su gestión mediante órganos específicos de vigilancia. Era la época de las computadores escasas y de hardware voluminosos y, por consiguiente, localizables con facilidad.
>
> "Las leyes de segunda generación (*Privacy Act* de 1974, *Informatique aux fichiers et aux libertes* francesa de 1978, Constitución de Postugal y España) centran su inquietud en asegurar el derecho de acceso de las personas a las informaciones que les conciernen, mostrando especial atención por la ´calidad de los datos´ y no del hardware que los memoriza, mediante cláusulas específicas de protección de las informaciones consideradas sensibles por su directa incidencia sobre la vida privada o sobre el ejercicio de las libertades.
>
> "En tanto que la tercera *generación* (Convenio Europeo de 1981; *Data Protection Act* inglesa de 1984) e hace cargo de los cambios en la tecnología provocados por la revolución microinformática y, también, de la necesidad de conciliar la defensa

> de los datos personales con las exigencias de una sociedad en la que la transmisión de informaciones constituye un compromiso social, económico, político y cultural ineludible. Es la época de los ´personal computers´"

El tercer tiempo fue de los Estados en particular; cada uno diseñó una estrategia para llevar a buen puerto la defensa de la intimidad frente a la agresión informática.

Algunos han optado por la incorporación expresa en el texto constitucional (como es el caso del Hábeas Data de Brasil); otros lo proyectan entre sus garantías constitucionales (por ejemplo, el caso de Argentina que lo trasciende desde el derecho de amparo); algunos prefieren establecer con claridad el derecho a tutelar (intimidad, privacidad, control sobre los datos, etc.) y dejar abierto el tipo procesal (por ejemplo, Perú).

La opción reglamentaria no está ausente y para ello se crean diversidad de textos legales que explicitan el derecho constitucional (Costa Rica); mientras que la preferencia jurisprudencial es reticente, quizás por la desconfianza reinante en las instituciones judiciales.

> Según García Belaúnde, las constituciones latinoamericanas prefieren elevar el Hábeas Data a un nivel constitucional, y otras no, como lo es en países europeos y lo es en Estados Unidos.

11.3 Libertad de información y derecho a la privacidad

La libertad de información trasciende el quid que, en su tiempo, produjo la libertad de expresión. Mientras ésta pretende resolver el problema de la intervención de los poderes públicos en materia de censura o prohibición previas, la libertad informativa tiene que afrontar una dimensión muy diferente a la de otrora, si se tiene en cuenta el alcance inusitado de los medios de comunicación y la mentada globalidad que ella alcanza.

> John Stuart Mill dijo que la necesidad de libertad de opinión y de libertad de expresión se sostenía en cuatro fundamentos. Primero, una opinión reducida al silencio puede ser verdad. Negarlo es asumir nuestra infalibilidad. En segundo lugar, aunque la opinión censurada sea un error, puede contener algo de cierto. Tercero, aun en el caso de que la opinión general sea no sólo verdadera, sino toda la verdad, se tendrá como una suerte de prejuicio con escasa comprensión de sus fundamentos racionales a menos que sea contestada de manera seria y enérgica. Y cuarto, de convertirse en un dogma, se traduciría en un obstáculo e impediría el desenvolvimiento de otras convicciones.

Mientras en origen la libertad de manifestarse (expresar ideas y reunirse sin obstáculos ni impedimentos de orden legal) era un expreso reconocimiento a una sociedad libre; actualmente la libertad admitida no se puede interpretar sin límites.

Es evidente que hay múltiples maneras de colegir el concepto, tantas como existen formas de pensar y actuar la comunicación humana. De la expresión deriva el conocimiento, la inteligencia, la sensibilidad ante los valores humanos, y en definitiva, la capacidad para emitir un juicio objetivo. Estas son referencias lógicas y algunos las utilizan como pautas para afirmar la imposibilidad de establecer limitaciones.

Sin embargo, en la búsqueda de información aparece una etapa previa de reunión de datos, noticias, investigación, entre otras actividades que pueden comprometer la vida privada de las personas.

Por ejemplo, si en la compilación de antecedentes es preciso buscar en archivos o registros los conocimientos logrados se obtienen conociendo datos que hipotéticamente son reservados o confidenciales.

> Podría definirse como "fuente periodística" –dicen Pierini, Lorences y Tornabene-, al sólo efecto de presentar la cuestión y sin ánimo de ser plenamente abarcativos de todas las hipótesis, toda noticia, informe, comentario, trascendido, rumor, etc., y toda actuación de informantes –voluntarios o involuntarios- que sirva para obtener la información. Se trata de la etapa previa a la publicación, y comprende la información recibida y la investigación. Entendida como tal, está

> expresamente prevista en el artículo 43 de la Constitución Nacional y es allí donde se produce la controversia sobre la preeminencia de un derecho sobre otro.

Comienza así el conflicto entre preferencias. ¿Qué es más importante? ¿Proteger la libertad de información ó la libertad de intimidad? ¿Acaso es posible establecer jerarquías?.

Inclusive, hasta se podría establecer una diferencia entre Europa y América sobre la forma de entender este fenómeno y optar por uno de ellos o compatibilizarlos.

Tocqueville comparó el periodismo europeo con el americano indicando una severa distancia en el estilo de practicarlo. Uno respetaba la libertad de las personas en el sentido individual que ello supone; el otro también lo respetaba pero desde la generalidad de sus conductas y el interés que ellas tienen hacia los demás. Uno reserva la información, el otro la divulga.

> El espíritu del periodista, en América, es el de atacar groseramente, sin ambages ni arte, las pasiones de aquellos a quienes se dirige; el de dejar a un lado los principios y hacer prensa en el hombre; el de seguir a éste en su vida privada y poner al desnudo sus flaquezas y sus vicios.
>
> De esta forma, afirma Aznar Gómez, los medios de comunicación servirían para conjurar el peligro de una sociedad individualista, donde cada uno en su retiro privado ignoraría el destino común y compartido de lo público.

Una distinción demasiada efímera, elástica, absolutamente discrecional y peligrosa para la seguridad jurídica y la certidumbre que requieren las conductas humanas.

Por ello es preciso hurgar en la vida privada para saber –o reconocer- aquello que es intangible y que, aun invocando libertades fundamentales, no pueden socavarse por la dignidad que exige la persona humana.

En este sentido, la intimidad individual y familiar, la honra, la propia imagen, la reputación son valores que la prensa no puede comprometer amparada por la libertad de expresión y opinión.

Esto, reflejado en la dimensión del hábeas data, supone que los datos conocidos de fuentes informativas registradas en soportes manuales o informáticos, no pueden publicarse o darse a conocer, sin caer en responsabilidad por esa actitud imprudente.

> Conviene recordar la diferencia que existe entre invasión de la intimidad y publicación de información sobre la vida íntima o privada. Y ello, porqué a diferencia de otras faltas legales y morales cometidas en el ámbito de la información, en el caso de la intimidad su violación constituye de por sí un daño. Por ejemplo, en lo relativo al honor o la verdad se requiere, necesariamente, la publicación de la información para que exista la falta. Los rumores que en gran cantidad circulan día a día en las redacciones de los periódicos no constituyen faltas si no se difunden o editan. Sin embargo, ocurre algo muy distinto en el caso de la intimidad: aquí la persona experimenta ya un daño moral al sufrir la violación de su privacidad, al sentirse desprotegida o invadida su intimidad. Por consiguiente –concluye Aznar- las exigencias éticas y legales de respeto a la intimidad comienzan en el mismo momento de la obtención de la información.

Aun así, uno se podría interrogar si aspectos de la intimidad como la fama o reputación constituyen violaciones cuando la revelación por la prensa pone al descubierto actitudes simuladas o apariencias solo mantenidas para cubrir verdades que no son tales.

> Para Espinar Vicente, en principio, todo pensamiento, afecto o asunto de un individuo que tenga un carácter antijurídico o que sirva para la construcción de su fama social puede y debe ser conocido más allá del ámbito que el sujeto pretende mantener reservado para sí mismo o su familia. De lo contrario, el derecho a la intimidad personal y familiar se convertiría en un instrumento al servicio de una doble moral de costumbres, poco compatible con la idea prefacial de establecer una sociedad democrática avanzada, amén de operar como un factor susceptible de extraer ciertas actitudes y conductas de la esfera de ordenación del Derecho.

La primacía de la información sobre la intimidad pareciera inmediata, aunque para reafirmarlo es necesario establecer otros criterios que no sean tan abiertos como el caso mencionado.

En efecto, la intimidad tiene un plano de vida privada y familiar que permite la realización de la persona sin interferencias ni intromisiones. Este es un punto sin discusión.

La averiguación de datos sobre una persona puede constituir una actividad lícita cuando la forma de practicarlo no se inmiscuye con artilugios en la vida privada, o a través de maniobras que eluden el consentimiento necesario para lograr la información. Por eso es inviolable el domicilio, son secretas las comunicaciones y la correspondencia, y se impiden las escuchas de conversaciones realizadas por medios técnicos invasivos (intervención en líneas telefónicas; irrupción en los correos electrónicos; grabación de conversaciones, etc.).

Igualmente existen datos que por su sensibilidad con la persona no se pueden registrar (y, de serlo, deben tener el consentimiento del afectado) ni divulgar (vinculados con la ideología, el credo, las preferencias íntimas, las inclinaciones de conducta, enfermedades, etc.).

Por otra parte, en el derecho a la información la necesidad de expresar la verdad y conocer la verdad son aspectos esenciales para ella y un límite preciso para su justificación. Informar lo que no es cierto transforma la difusión en una calumnia.

En cambio, uno puede expresar ideas o pensamientos a través de la prensa sin involucrar a terceros, ejerciendo un legítimo derecho que no refiere a la información. Por eso, la libertad de expresión es más amplia que la libertad de información.

> A los medios de comunicación no se les puede dar carta blanca –sostiene Concepción Rodríguez-, dejando a los particulares sin protección. La prensa (en un sentido amplio) tiene una función social y política que cumplir y en la mayoría de los casos es perfectamente cumplimentada a través del ejercicio responsable de la función periodística…La importante función que desempeñan los medios de comunicación y periodistas conlleva no sólo el reconocimiento de derechos y garantías del ejercicio libre de la profesión, sino también ciertas obligaciones consistentes en suministrar una información de calidad, evitando abusos y violencias morales. De ahí que los propios periodistas, los ciudadanos y los poderes públicos estén interesados en dotar a los profesionales de una organización y una regulación de su actividad informadora.

Simplificando la presentación (porqué el tema merece un tratamiento mucho más amplio que lo acotado de estas referencias) entre la libertad de expresión y el derecho a la intimidad existe un conflicto que sólo se puede resolver con prudencia y adecuación a los tiempos y las personas.

Cuando los individuos tienen una exposición al público casi permanente (políticos, artistas, etc.) la inmiscusión en sus reductos privados suele consentirse más que en supuestos de personas comunes, o de menor trascendencia social.

Sin embargo, existen algunas reglas que no pueden olvidarse:

a) Sólo la defensa del interés público justifica las intromisiones o indagaciones sobre la vida privada de una persona sin su previo consentimiento.

b) En el tratamiento informativo de los asuntos en que medien elementos de dolor o aflicción en las personas afectadas, el periodista evitará la intromisión gratuita y las especulaciones innecesarias sobre sus sentimientos y circunstancias.

c) Las restricciones sobre invasiones en la intimidad deberán observarse con especial cuidado cuando se trate de personas ingresadas en centros hospitalarios o en instituciones similares.

d) El periodista deberá evitar nombrar en sus informaciones a los familiares y amigos de personas acusadas o condenadas por un delito, salvo que su mención resulte necesaria para que la información sea completa y equitativa.

e) Se evitará nombrar a las víctimas de un delito, así como la publicación de material que pueda contribuir a su identificación, actuando con especial diligencia cuando se trate de delitos contra la libertad sexual.

f) Los criterios indicados en los dos principios anteriores, se aplicarán con extremo rigor cuando la información pueda afectar a menores de edad. En particular, el periodista deberá abstenerse de entrevistar, fotografiar o grabar a los menores de edad sobre temas relacionados con actividades delictivas o enmarcables en el ámbito de la privacidad.

g) El periodista, asimismo, deberá evitar la publicación de datos (sobre la raza, color, religión, origen social o sexo de una persona, o cualquier enfermedad o minusvalía física o mental que padezca), salvo que guarden relación directa con la información publicada.

Las consideraciones expuestas –según son explicadas por Aznar Gómez- corresponden al Código Deontológico de la Federación de Asociaciones de Prensa de España, y reflejan una situación tan variable y circunstancial como es la relación entre información e intimidad. Igualmente, manifiestan la imposibilidad última de dar una respuesta definitiva, sin conocer cada caso en concreto. Hay pues un margen siempre abierto para la reflexión del propio profesional. Los medios, como entorno habitual de trabajo donde se dan estas situaciones, deben hacer lo posible por proveer los medios y mecanismos para que los profesionales puedan ejercer dicha reflexión y llevar a cabo un aprendizaje moral tan valioso o más que el puramente técnico.

En suma, simplificado el tema en relación con la amenaza o violación a la vida privada y otros derechos de la personalidad, el problema es más profundo pues afecta y va a dañar más en el futuro a la libertad y a la igualdad, pues resulta evidente que al ser vulnerada la vida privada o la privacidad, en su caso, el equilibrio se rompe y se establece una relación de dominio y control de quien posee la información sobre la persona a quien desnuda; y en consecuencia todo dominio personal restringe la libertad e impone desigualdad entre quien posee información y quien no tiene acceso a ella.

12. La creación del archivo

La base o banco de datos se constituye para un fin determinado; circunstancia que la diferencia de una fuente de información que puede estar en las cosas o lugares.

El régimen legal creado especifica en el artículo 2º: " ***Archivo, registro, base o banco de datos****: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.*

Oportunamente, el Decreto 165/94* en su artículo 1º inciso b) definió el significado de "base de datos": "*Se entenderá por base de datos, incluidos en la categoría de obras literarias, a las producciones constituidas por un conjunto organizado de datos interrelacionados, compilados con miras a su almacenamiento, procesamiento y recuperación mediante técnicas y sistemas informáticos*".

Informa Uicich la Resolución del Consejo de Ministros de la Organización de Cooperación y Desarrollo Económico (OCDE) europea del 23 de setiembre de 1980 que en el artículo primero de su Directiva define a las bases de datos como: "*Toda colección de obras o materiales ordenados, almacenados y accesibles mediante medios electrónicos, así como el material electrónico necesario para el funcionamiento de la misma, por ejemplo: su diccionario, índice o sistema de interrogación o presentación de información, no quedarán comprendidos en la definición de los programas del ordenador utilizados en la realización o el funcionamiento de las bases de datos*".

Un ejemplo testimonia con facilidad la distinción: si alguien necesita conocer la solvencia económica de una persona, recurre a un registro bancario o a una oficina comercial creada para estos efectos; en cambio, si lo buscado es un dato aislado, por el caso: fecha de nacimiento o de deceso; la fuente de información llega desde el lugar donde fue la persona sepultada, o del archivo documental que emite la partida de nacimiento o el certificado de defunción.

> Cabe destacar que un gran número de datos se encuentra fácilmente disponible para quien los necesite. Desde aquellos que se toman de la simple información cotidiana como de otros que están al servicio de la sociedad para fines diversos. Por eso el problema no es la disponibilidad de la información que concierne a una persona, sino de los datos que éste admite que sean públicos o que pretenda estén reservados o absolutamente confidenciales.

Los archivos existen desde tiempos inmemoriales; ellos han dejado constancia de los nacimientos, las defunciones, los matrimonios, las enfermedades, entre tanta información recopilada y guardada con fines históricos o para ensayar comparaciones científicas.

El cambio operado se produjo con la aparición de la tecnología, que desaparece el límite antes fijado por el espacio y el tiempo. La crónica anterior fue suplida por la telemática (que supone hacer posible la consulta de una base de datos desde cualquier distancia) y el tratamiento de la información permitió generar otras deducciones, y lo que fue más importante, dejó de estar en sólo un lugar para instalarse en un sistema de acceso mundial con la sola pulsación de una tecla (Internet).

> En el ámbito de las telecomunicaciones es bien conocido el ejemplo de los directorios inversos: se crean con los mismos datos que se utilizan para los directorios públicos de los abonados telefónicos, pero se invierte el criterio de búsqueda; en vez de utilizar un nombre y una dirección conocidos para encontrar un número de teléfono, se usa ese número para averiguar el nombre y la dirección del abonado.

De esta manera allí donde ya existía un archivo, un registro, una copia de datos o un respaldo documental, con la aparición de la informática surge una abundancia informativa que hace necesaria la clasificación, la comparación, la sistematización y la recuperación de la misma, convirtiendo la simple reunión informativa en un grandioso archivo de perfiles, de preferencias, de gustos, de estructuras económicas, etc., etc.

Este cambio, evidentemente, provocó la dispersión de los datos y la pérdida del control sobre ellos. Las redes informáticas difundieron en escala dichas fuentes de información, y la tecnificación (digitalización, escaneo documentario, recuperación de textos, etc.) han multiplicado al infinito las posibilidades de búsqueda y de organización.

> La estructura abierta de la red Internet se fomentó para evitar que los datos fuesen conservados en un solo lugar. Para el Pentágono –afirma Marcel Pinet- se trataba de la máxima medida de seguridad: la dispersión de los datos estratégicos permitía esconderlos de las fuerzas enemigas a la vez que permitía conservar la posibilidad técnica de una recuperación instantánea. Esta es la característica que ha abierto nuevas posibilidades: primero para las Universidades y ahora para las empresas comerciales.
>
> Ahora, los datos nominativos se esparcen por la red por varias razones: para facilitar la cooperación científica existen directorios de investigadores; publicaciones de organigramas que describen la organización de la administración o de empresas privadas, en los que se incluyen anotaciones biográficas de las personas que ostentan los cargos de responsabilidad; transmisión de directorios preexistentes, como los de los abonados telefónicos, anuncios por palabras, etc.

La antigua privacidad de los archivos, habitualmente conservados en registros manuales escritos, rápidamente se transformó en unos pocos *bits* almacenados en la memoria de una computadora que, desde la

generalización de las redes virtuales como Internet, facilitan la transmisión. De suyo, los datos antes reservados y ciertamente confidenciales pasaron a ser públicos y disponibles para cualquiera.

Es preciso aclarar que algunas legislaciones prefieren no hablar de "archivos" optando, por ejemplo, por "ficheros", quizás influenciados por el significado que el primero tiene en el sentido informático, como conjunto de datos que ocupan un espacio en el disco (duro o flexible), a los que se asigna un nombre y tienen un autor determinado. Su característica es similar a la de un libro, solo que la extensión se mide en *bites (binary digit* o dígito binario) y tiene un atributo determinado.

> Nosotros utilizamos la noción de "archivo, registro o banco de datos" que tienen en nuestro vocabulario mayor comprensión que las voces usadas en Europa.

Las primeras manifestaciones contrarias a esta suerte de invasión en los dominios de lo secreto de los archivos llegaron de la tarea legislativa. Suecia con el Acta de 1973*, y Estados Unidos a través de la *Privacy Act** de 1974 (hoy complementada por la *Electronic Communications Privacy Act** de 1986 y el *Computer Matching and Privacy Protection Act** de 1988) reaccionaron estableciendo reglas y principios para la creación de los archivos y, esencialmente, para dar alguna seguridad con el tratamiento de los datos y el derecho a la intimidad.

> La interacción entre las disposiciones que afectan a los registros públicos y la legislación en materia de protección de la intimidad puede ser compleja, afirma Bruce Slane. La utilización de la libertad de información en este contexto puede, innecesariamente, agravar aún más la situación. En mi opinión –agrega-, la libertad de información no encaja fácilmente con la institución de los registros públicos y, sin embargo, se utiliza en Nueva Zelanda para exigir la publicación de datos en masa. Este tipo de aplicación de la legislación sobre libertad de información es demasiado estricto y no sirve ni para el cumplimiento de la función encomendada a los registros ni para la propia libertad de información.

De esta manera, la creación de los archivos han debido respetar ciertas reglas y principios, pero al mismo tiempo, reconocen derechos al individuo afectado (concernido) por el registro, y también, al titular de la base de datos. Se establecieron procesos y procedimientos para el almacenamiento, la conservación, la seguridad interna del archivo, y las fases para el tratamiento (circulación y venta de la información).

12.1 Archivos públicos y privados

Es necesario distinguir el tipo de archivo del dato propiamente dicho. Mientras uno se refiere al gestor que desarrolla la base, propiamente dicha, el restante diferencia la calidad reservada o disponible de la información. Es decir, mientras un archivo público puede ser propio y natural para la gestión social y económica del Estado, el dato que allí se encuentra puede ser público por su disponibilidad como fuente de conocimiento para todos. En cambio un archivo privado puede tener finalidades diversas (*e-commerce*; confianza crediticia; perfiles para la venta potencial, etc.) y el dato allí contenido suele ser confidencial por la naturaleza del banco de datos, aunque la circulación de ellos sea producto de la propia actividad desarrollada.

> De todos modos, conviene anticipar que algunos autores suelen distinguir entre datos reservados y datos públicos y hacen diferencias en cuanto a los alcances de la protección que debe asignárseles a uno y otro. Los típicos datos reservados –sostienen Beltramone y Zabale- son aquellos que contienen algún tipo de información de la calificada como "sensible" y que atañe a cuestiones íntimas de las personas (religión, raza, conducta sexual, opinión política, etc.). Los datos denominados "públicos" serían, entonces, para esa doctrina, aquellos de menor importancia o que pueden ser obtenidos fácilmente (como un número telefónico o una dirección, por ejemplo). De modo que los primeros, y dado precisamente su carácter de "reservados", merecen una mayor salvaguarda que los segundos.

La división entre "tipos" de archivos posibles, permitiría una clasificación más extendida. Por ejemplo, archivos de datos personales; de información crediticia; de movimientos comerciales; de antecedentes penales; de inversiones; y en definitiva, de cuanta actividad se disponga a almacenar en un banco informático.

Sin embargo, la pregunta inmediata es ¿para qué sirve tal clasificación? La respuesta puede ser totalmente inesperada: "para nada", salvo que exista un tratamiento diferencial entre archivos públicos y privados. Pero como bien afirma la doctrina, el problema no está en la condición del archivo, sino en la calidad del dato, y aun así, reconocer que ello es una diferencia contingente.

> Afirma Bianchi que no hay datos públicos o privados sino situaciones concretas que los califican como tales. Agregando Beltramone y Zabale que las creencias religiosas o las prácticas sexuales, son normalmente un dato reservado, pero también puede serlo el domicilio de una persona o su número telefónico, en el caso de que exista una amenaza de un atentado contra ella. Por otra parte, un dato insignificante puede carecer de importancia, pero la suma de ellos puede llegar a desnudar la intimidad de las personas.

En nuestro país, el artículo 43 de la Constitución, y su ley reglamentaria los iguala. Los archivos pueden ser *públicos o privados* y, a los fines del hábeas data, deben estar *destinados a proveer informes*. Por registros o bancos de datos públicos debemos entender los existentes en los organismos del Estado, de cualquier naturaleza, ya que la ley sólo establece las siguientes excepciones:

> Art. 23 (Supuestos especiales) .-
>
> 1. Quedaran sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia: y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.
>
> 2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados queda limitado a aquellos supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad publica o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categoría, en función de su grado de fiabilidad.
>
> 3. Los datos personales registrados con fines policiales se cancelaran cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Esto incluye no sólo a las reparticiones de la Administración Pública nacional centralizada, sino también a los entes descentralizados, autárquicos, empresas públicas y sociedades estatales, así como dependencias provinciales y municipales.

> Para Sagüés, la expresión *registros o bancos de datos públicos* no debe ser interpretada en el sentido de registros públicos, por oposición a registros reservados o secretos, ya que la norma se refiere a los titulares u operadores de los registros o bancos de datos. La redacción del texto abona esta interpretación ya que armoniza con la referencia a '*los privados destinados a proveer informes*'.

Han sido incorporados como sujetos pasivos de la acción de hábeas data, los registros o bancos de datos privados '*destinados a proveer informes*', que son, básicamente, los operados por las empresas o personas individuales dedicadas a recolectar información personal para suministrarla a sus clientes. Es el caso de las empresas de informes comerciales o financieros, que proveen a bancos, financieras, comercios y a quienes conceden crédito en general, información sobre situación patrimonial, reclamos pecuniarios judiciales o extrajudiciales, etc.

Es indudable que también se incluyen en esta categoría otras entidades, tales como los colegios profesionales, establecimientos educativos, clubes deportivos, y toda organización manual o informática que tenga registros de personas físicas sobre las cuales debe preservar reglas y principios antes de circular la información que tiene.

En tal sentido son las disposiciones de los artículos 21 y 22 de la ley reglamentaria, cuyo contenido analizamos más adelante.

En España la Ley de Protección de datos dispone:

Artículo 39. El Registro General de Protección de Datos.

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros de que sean titulares las Administraciones públicas; b) Los ficheros de titularidad privada; c) Las autorizaciones a que se refiere la presente Ley; d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley; e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Sin embargo, la ausencia de un criterio uniforme sobre quienes están obligados a cumplimentar los requisitos de seguridad enunciados, apareció manifiesta en la Ley 24.745* (vetada por Decreto 1616/96*) cuando eliminó de la ley sobre hábeas data y protección de datos personales:

a) A los registros o bancos de datos de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general.

b) A los registros o bancos de datos mantenidos por personas físicas con fines exclusivamente personales.

c) A los registros o bancos de datos de información judicial, científica, tecnológica o comercial, que reproduzcan datos ya publicados en boletines, diarios o repertorios judiciales.

d) A los registros o bancos de datos mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas reconocidos, con relación a sus afiliados, asociados, miembros y ex miembros, y sólo en cuanto estén referidas a una finalidad específica, sin perjuicio de la cesión de datos…

e) *Los registros o bancos de datos de las personas físicas o jurídicas dedicadas a la actividad periodística por cualquier medio de comunicación social. En ningún caso podrá afectarse el secreto de las fuentes ni pretender que las mismas sean reveladas.*

Además se había establecido en la misma norma (art. 2º) disposiciones específicas para:

a) Los registros o bancos de datos pertenecientes al Registro Nacional de Reincidencia y Estadística Criminal y al Registro Nacional de las Personas.

b) *Los registros o bancos de datos regulados por la legislación sobre régimen electoral.*

Frente a tanta diversidad en el almacenamiento de datos resulta necesario elaborar una clasificación de los archivos (ficheros, en el nomenclador que utiliza España), teniendo presente que algunas veces los datos son fácilmente conocidos, y otras que, aun siendo de personas fallecidas, conserva gran interés conocer el antecedente para sistematizarlos.

Con esta tendencia la ley sancionada incorpora un régimen para los archivos, registros o bancos de datos públicos y privados destinados a proveer informes, por el cual, además del dato personal que se categoriza genéricamente, se establecen singularidades para:

a) Los datos sensibles

b) Los hábitos personales o preferencias de consumo

c) Los antecedentes penales y contravencionales y

d) Los datos relativos a la salud

> Expresa Pinet que cuando un legislador estipula que una determinada información sea accesible al público no quiere decir necesariamente que esa información tenga la consideración de *res nullius.* Del mismo modo, cuando una persona decide hacer públicos unos datos, bajo ciertas condiciones, no quiere decir que dicha persona pretende renunciar a todos sus derechos.

12.2 Registros, archivos o bancos de datos

En la práctica no suelen clasificarse los tipos de ficheros (manuales o informáticos), porque se pretende resolver la aplicación de los principios fundamentales de la denominada "libertad informática" sobre la calidad del dato que se guarda o transmite. A partir de allí se deriva su relación con el derecho a la intimidad y otras reglas y principios que se aplican a quienes trabajan sobre datos de las personas físicas y jurídicas.

Archivar es guardar papeles o documentos en un archivo; y *archivo* significa el lugar donde se resguardan cosas importantes o curiosas. En otro sentido, pero vinculado, se dice de quien conserva secretos o intimidades que se le confían.

> Actualmente, en lenguaje informático, archivar es registrar un conjunto de información que tiene similar estructura. El archivo puede ser *lógico* y estar referido a un sistema de ingreso y búsqueda; o ser *físico* y permanecer en un lugar establecido.
>
> Toda base de datos contiene información para el usuario y, una vez dentro del sistema, cada dato abre nuevas variables. Estas suelen clasificarse en *características (data dictionary),* y *relaciones (relationships),* que vinculan los archivos a través de una tabla (que es la que almacena por segmento o grupo) o por documentos (*file*) que establece campos de búsqueda e interxconexión.
>
> Los archivos se denominan "*maestros*" cuando contiene los registros de la base de datos, donde cada cual tiene un conjunto de longitud variable que se identifica con un número o nombre.
>
> Son archivos "*invertidos*" aquellos que contienen términos que pueden usarse como puertos de acceso para la recuperación de información, pero desde una pauta diferente a la tradicional. Por ejemplo, si se busca información de alguien, en lugar de buscar su nombre y apellido, se localizan sus rasgos físicos u otros.
>
> Se denominan "*archivos Any*" los que permiten agrupar términos asociados y lograr un perfil por disociación. Por ejemplo, cuando se quiere saber cuál es el gasto anual de una persona que pertenece a un grupo profesional. Estos asimismo se vinculan con los llamados "*Archivos cruzados*" que facilitan la interconexión y el tratamiento de los datos.

Registrar es transcribir en los libros de un registro público las resoluciones de la autoridad o los actos jurídicos de los particulares. Se registra cuando se dejan señales de identificación de un lugar, cosa o personas.

Un *registro* es el libro en donde se apuntan datos o noticias, y tiene una diversidad de manifestaciones (V.gr: Registro Civil; Registro de la propiedad inmobiliaria; Registro de la propiedad intelectual; Registro de la propiedad industrial; entre otros).

También constituyen *registros* las anotaciones informáticas que se incluyen en un soporte mecánico, y son las piezas que fundan los bancos de datos.

Las *bases de datos* son el conjunto organizado de informaciones que han sido objeto de "tratamiento" o *"data mining"* que permite realizar entrecruzamientos y prospecciones para interpretar los datos almacenados.

Finalmente, se denomina como *"tratamiento"* las operaciones y procedimientos técnicos, de carácter automatizado o no, que permiten almacenar, grabar, elaborar, modificar, resguardar, disociar y eliminar datos de carácter personal, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

El artículo 2º de la ley, aclara que es **"Tratamiento de datos":** *Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.*

Para hacer referencia a los sistemas de documentación informática se utilizan las expresiones *banco de datos (*data bank) y *base de datos* (data base). En ocasiones –dice Perez Luño- se ha tratado de establecer diferencias entre ambos términos. Así, por ejemplo, se ha indicado que mientras las bases de datos se refieren a sistemas de documentación que operan con títulos o referencias, los bancos de datos almacenan textos o documentos. Otras veces, se ha considerado que la expresión base de datos es propia del lenguaje técnico informático y hace referencia al conjunto de programas dirigidos a organizar la documentación, mientras que los bancos de datos sería la expresión propia del lenguaje de las ciencias sociales y del derecho que aludiría al conjunto de informaciones pertenecientes a estos campos del saber y que se hallarían organizadas en una o varias bases de datos.

El hecho de que en inglés la abreviatura BD sirva para aludir a *data banks* y *data bases*, indistintamente, ha determinado un uso indiferenciado entre ambas expresiones. Por tanto, parece ocioso tratar de establecer contrastes, más o menos sutiles, cuando las diferencias entre ambos términos han sido abolidas por la práctica.

Se puede observar que cuando se habla de protección de los datos, inmediatamente aparece la necesidad de dar seguridad a las personas que están contenidas en cualquiera de esas modalidades de anotación, con el fin de evitar invasiones en la intimidad de ellas.

Sostiene Gils Carbó que el tratamiento de los datos almacenados no admite clasificaciones pues todo dato puede tornarse "sensible" en la medida en que la sumatoria de datos no sensibles, que permitan hacer un seguimiento en la vida de las personas, también puede representar una afrenta a la privacidad.

La defensa de la privacidad tiende a instalar reglas y principios en la formación de los bancos de datos. Asimismo, se restringe la interconexión de registros, con el fin de anular la manipulación informativa que no tiene el consentimiento anterior del afectado.

La realidad de los registros evidencia que no todos tienen finalidades informativas, es decir, que sean transmisibles a terceros. Esta característica, en consecuencia, lleva a resolver cuál es la protección que la persona ostenta: si lo es para evitar que el archivo ingrese sus datos y con esa incorporación afecte, probablemente, la privacidad; o en su caso, si la tutela se vincula a la reserva y confidencialidad (y eventual supresión) que los datos deben conservar, evitando que se concrete una hipotética transferencia que violente la intimidad de la persona al hacer públicas sus características.

En los hechos, ambas son las actitudes defensivas que tiene un individuo. Sólo que una vía se concreta desde la ley de protección de datos; y la otra, a través del hábeas data y sus posibilidades concretas de demanda (V.gr.: acceso, actualización, rectificación, confidencialidad, reserva, o cancelación).

12.3 Base de datos: clasificación

Siguiendo la pauta establecida en el punto anterior, se pueden señalar algunos archivos que se forman para especiales funciones que, por ello, quedan excluidas de la injerencia que el hábeas data establece.

> Los principios de la protección deben aplicarse a cualquier información relativa a una persona identificada o identificable. Para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona. Los principios de la protección no se aplican a aquellos datos hechos anónimos de manera tal que no sea posible identificar al interesado.

Testimonio de este apartamiento es el artículo 28 de la ley cuando elimina del régimen a los archivos, registros o bancos de datos relativos a encuestas públicas.

> Perez Luño establece tres modelos de bases de datos: a) bases de datos *jerárquicas,* en las que los datos están organizados por relaciones de jerarquía que pueden representarse de forma arborescente a partir de una raíz común; b) bases de datos *reticulares*, en las que las distintas informaciones se organizan a través de una pluralidad de puntos de acceso; c) bases de datos *relacionales*, en las que los datos se estructuran sistemáticamente en relaciones homogéneas que permiten al usuario seleccionarlas y adaptarlas a sus necesidades operativas.

Una guía provisional clasifica los registros en dos grandes sectores que, posteriormente, se van segmentando para centrar su principal actividad.

a) *Archivos públicos* y *privados*

Públicos son los registros que tiene el Estado para el almacenamiento de datos relativos a una actividad que, por seguridad jurídica, se debe mantener custodiada y con un respaldo documental. Pueden transferirse a terceros, y por lo general, son informaciones que están disponibles a cualquiera sin más requisitos que la solicitud fundamentada.

Privados son los archivos que se conservan por personas físicas o jurídicas con una finalidad determinada. Si resultan para una simple información personal (V.gr.: base de datos científica; archivos con perfiles sociales; etc.) no afectan la intimidad mientras no se logre identificar a persona alguna en particular (en cuyo caso, el afectado podría requerir el acceso a la base y requerir explicaciones sobre la finalidad del registro).

Esta sutil diferencia que tiene solamente en cuenta el agente que origina el banco de datos (público o privado) no es suficiente para controlar la invasión a la intimidad. Basta confrontar un hecho cotidiano para advertir la indefensión de la persona para detener llamados telefónicos o cartas que llegan a su nombre ofreciendo cosas, lugares o servicios. Esa injerencia permanente es una intromisión indeseable en un reducto propio y contamina la privacidad.

> Según Horacio Lynch, una investigación publicada en el año 1996 calculaba que en Estados Unidos una persona generaba 150 registros electrónicos diarios. Porque cuando se completan formularios, cupones, encuestas, por ejemplo, o en la simple utilización de la tarjeta de crédito, o al depositar un cheque en la sucursal bancaria, esa información se carga en una computadora que la guarda o distribuye donde debe. Luego, esa información privada y reservada es la que conforman las bases de datos. Tan necesarias para el trabajo de unos y tan valiosas para los negocios de otros; pero que al mismo tiempo, provocaron un mercado ilegal que, en el mejor de los casos, se utilizan con fines comerciales o de promoción política.
>
> Un ejemplo más muestra porqué no es útil la diferencia entre el archivo que se origina desde el Estado y aquél que resulta creado por un particular con fines comerciales. El Estado tiene en sus bases de datos, por ejemplo de la ANSES

> (Administración Nacional de la Seguridad Social) una fuente de información grandiosa al contar con una variable de registros que van desde los habituales identificadores hasta el de profesiones e ingresos promedios anuales. En cierta ocasión fue descubierta una operación de compra de esos datos por una cifra muy significativa de parte de una empresa comercial que pretendía con ello obtener un perfil de clientes a quienes seducir con sus productos. Asimismo, hay bases de datos creados por personas que buscan compradores tradicionales (por ejemplo, empresas de telemarketing, que venden sus productos a través del teléfono o del correo), lo cual supone una actividad perfectamente lícita. Sin embargo, alguna vez un banco oficial (del Estado) con la idea de vender más tarjetas de créditos, persiguió adquirir estos archivos que tenían identificadas y clasificadas a las personas por su nivel de ingresos, solvencia económica, ingresos anuales, deudas hipotecarias pendientes, juicios civiles o penales en su contra, etc., informaciones –todas ellas- de carácter confidencial, que se vendían a razón de un valor ínfimo por dato, pero que en la suma llegaba a un múltiplo verdaderamente sorprendente.

En España la ley de tratamiento de datos divide los ficheros según la titularidad sea pública o privada, pero en ambos casos, se tiene en cuenta la finalidad prevista para el archivo, las formas como se efectuará el almacenamiento de información, la descripción de los datos que se pretende relevar, las cesiones o transferencias que se prevean, los órganos que son responsables del fichero y los servicios que se presten a las personas identificadas cuando ellas pretendan ingresar al banco de datos y ejercer actos de control sobre el mismo.

Es el temperamento adoptado en la reglamentación del hábeas data. El principio, en ambos casos, es que la persona debe prestar consentimiento para estar en las bases de información. Ha de quedar en claro que, esta pretensión, si bien ideal, constituye muchas veces una utopía (mucho más cuando se advierte que la toma de registros, a veces, se produce desde Internet y resulta imposible conocer las probables interconexiones de datos).

b) *Archivos manuales* e *informáticos*

La protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual.

Los archivos manuales constituyen una parte de la historia del mundo, como lo acreditan las leyes *Aelia Sentia* y *Papia Poppaea* de la Roma del emperador Augusto en el año 9 a.C.; fueron la modalidad habitual desde la creación de la imprenta y uno de los grandes poderes de la iglesia con sus actas de fe. En los últimos siglos los registros constituyeron el testimonio manifiesto del derecho de propiedad.

La informática, como hemos dicho largamente, modificó sustancialmente el espacio y el tiempo para conservar la información.

Por todo ello el alcance de la protección no debe depender de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de elusión.

> La Comunidad Económica Europea a través de la Directiva sobre Tratamiento de datos señala, en cuanto respecta al tratamiento manual, que sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas. En particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva.

c) Archivos de Seguridad del Estado

En Europa, tanto el Convenio 108* del Consejo emitido en el año 1981, como la Directiva 95/46* y las legislaciones locales que ratificaron el criterio allí mentado, han sostenido que existen datos cuya protección es manifiesta (ordinaria) y otros que merecen una defensa especial al implicar un riesgo mayor para la intimidad de las personas, en cuanto son los que revelan ideología, creencias religiosas, afiliación sindical, origen racial, salud y vida sexual (datos sensibles).

Los archivos de seguridad, generalmente están excluidos de la injerencia del hábeas data, lo cual no obsta a que se pueda efectuar un control directo sobre las bases de datos, toda vez que, siendo bancos de información del Estado, la reserva y confidencialidad queda limitada por el conocimiento y admisión expresa que el afectado pueda tener sobre el registro.

> El caso Urteaga sostiene en una de sus partes que "*…dado que el hábeas data se orienta a la protección de la intimidad, el giro ´datos a ella referidos´ debe ser entendido como el reaseguro del derecho básico protegido por la norma, como medio de garantizar que sea el titular de los datos el que pueda obtener el desarme informativo del Estado, o de quien fuere, para poder decidir acerca del destino y contenido de dichos datos. Pero, además, en tanto el texto constitucional permite ejercer un control activo sobre los datos, a fin de supervisar no sólo el contenido de la información en sí, sino también aquello que atañe a su finalidad, es evidente que se trata, a la vez, de un instrumento de control. Por lo tanto, no es posible derivar de la citada expresión un permiso genérico para que el Estado se exima de su "deber de información", pues ello significa divertir su sentido fundamental* (C.S., octubre 15/998, in re *Urteaga, Facundo Rául c/ Estado Nacional – Estado Mayor Conjunto de las Fuerzas Armadas s/ amparo –ley 16.986"*.

Los registros de datos de personas físicas solamente pueden quedar intangibles cuando la causa del secreto justifique la reserva, al punto que si la pretensión de difusión o conocimiento que reclama el presunto afectado, pueda vulnerar la razón de Estado que autoriza la confidencialidad estricta.

> En España, la Ley establece en el artículo 22 sobre *"Ficheros de las Fuerzas y Cuerpos de Seguridad"* lo siguiente:
>
> *1) Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley. 2) La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad. 3) La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales. 4) Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.*

La decisión, obviamente, es jurisdiccional, porqué sólo los jueces están en el punto de equilibrio exacto que la resolución merece.

> El artículo 23 inciso 2º establece que: *"El tratamiento de datos personales con fines de defensa nacional o seguridad publica por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad publica o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categoría, en función de su grado de fiabilidad*".

En suma, todos los datos personales contenidos en bancos de datos han de sufrir mínimas limitaciones en el acceso a la información y consecuencias que de ella deriven.

Si se toleran excepciones, como las que menciona el artículo 17, ellas deben ser fundadas y obliga a categorizar la calidad de los archivos; cuestión que se ha delegado en el Poder Ejecutivo de la Nación.

> Art. 17 (Excepciones) .-
>
> 1. Los responsables de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión de datos de carácter personal en función de la protección de la defensa de la Nación, o de la protección de los derechos e intereses de terceros.
>
> 2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.
>
> 3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.

d) Archivos históricos

Un ejemplo lo presta el "Archivo General de la Nación" creado en 1821 donde conviven las historias públicas y privadas de quienes nos precedieron, con sus proyectos, sus esperanzas y también sus fracasos, porqué la historia –tal como se presenta al Archivo en su página web- se construye con la totalidad de los acontecimientos y de sus protagonistas.

El archivo histórico contiene intimidades de héroes y personajes de la vida y tradición de los pueblos, que se exponen al conocimiento público como una muestra de sus personalidades.

En principio, podría afirmarse que la historia se cuenta por experiencias de investigación y análisis, y lo que se transmite es producto de esa labor; sin embargo, ¿puede un dato histórico ser eliminado por afectar la intimidad de un prócer?. Si fuera afirmado que tal o cual personaje era adicto a tal estupefaciente; o, eventualmente, que era afecto a inclinaciones sexuales morbosas o diferentes, ¿puede el historiador, un familiar, una línea de descendencia, provocar la rectificación del dato o la supresión del mismo?.

Evidentemente, son exposiciones de características muy personales de nuestros antecesores, y la probable justificación de ser hombres públicos, aparentemente, no sería causa bastante para fundamentar el dato publicado. Por ello, la afectación a la intimidad sería evidente, e hipotéticamente, procedería el hábeas data.

Sin embargo la afirmación no puede ser rotunda ni perentoria toda vez que el archivo histórico conserva una información periodística, o un documento oficial o privado del cual surge el dato, o el producto de una investigación, o bien un libro que cuenta esa parte de la historia personal, y como tales son fuentes que hipotéticamente no pueden revertirse por el hábeas data, sino a través de una nueva investigación, o del derecho a réplica cuando el archivo es reciente y el afectado puede entablar la acción reparatoria.

e) Archivos penales

La información sobre antecedentes personales es diferente del registro de conductas penadas por la ley. Por ello, el hábeas data procede en cualquiera de los supuestos ya citados con el fundamento de resolver el tratamiento de datos automatizados de carácter personal cuando la base o archivo ofrezca una definición de características personales o un perfil individual; no así cuando la información proporcionada refiere a los antecedentes penales de la persona.

El artículo 7 inciso 4º establece que: *Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas*.

Un solo ejemplo sirve para ilustrar este punto de manera más que suficiente: en cualquier democracia, la vista de un procedimiento penal en la que se dicta sentencia es publica, pero en todas y cada una de nuestras democracias –afirma Marcel Pinet- los antecedentes penales, que son los archivos de las condenas que se dictaron de manera pública, son uno de los archivos más protegidos y menos accesibles. Esto es un ejemplo de como cuando se recopila información, ésta toma un valor informativo específico. Esta es la razón por la que un fallo del Tribunal Supremo de los Estados Unidos, del 22 de marzo de 1989, denegó la petición de unos periodistas para serles comunicadas las sentencias de varias personas ligadas a la mafia, aunque éstas se habían dictado públicamente. El tribunal precisó que al evaluar los intereses en conflicto, *"la infracción del derecho al respeto de la vida privada de un ciudadano, resultante de la difusión de sus antecedentes penales, superaba el interés público que se obtendría del ejercicio de la libertad de prensa".*

El antecedente penal, puede incorporarse entre los registros o bancos de dato de información judicial, y en este grupo se advierte la trascendencia del problema a resolver cuando se difunde un dato proveniente de dichas fuentes.

En efecto, las bases de datos incorporan decisiones judiciales tomadas respecto a personas físicas y jurídicas; algunas veces, son resoluciones adoptadas en el curso del procedimiento (lo cual supone su provisoriedad) de modo tal que solamente con la sentencia (firme y definitiva) el dato es actual y exacto.

Pero un conflicto habitual en los medios de comunicación es transferir situaciones procesales no firmes como si fueran tales, afectando en consecuencia algunos principios o garantías procesales que se destinan hacia la persona (en la dimensión de sus propias libertadas, como la presunción o estado de inocencia; o la continuidad de la empresa en los procesos fallimentarios) y hacia el órgano judicial (debido proceso, defensa de las personas, imparcialidad del juez, etc.). En estos casos, el dato se obtiene de una fuente judicial fidedigna, es verdad, pues el acceso a la información no está vedada en las actuaciones jurisdiccionales, salvo en situaciones muy especiales. El inconveniente aparece en la forma como se difunde el dato.

> Estas informaciones en las que puede aparecer nuestro nombre y apellido, se reflejan periódicamente en los medios de comunicación como fruto del ejercicio del derecho a la información, y por lo que a este punto se refiere –sostiene Velázquez Bautista- "sentencias", su difusión responde también al principio de publicidad de la actuación judicial. También se tratan informáticamente por personas que no forman parte o son colaboradores de la administración de justicia, constituyendo así, bases de datos que se utilizan con finalidades diversas.

Creemos que el hábeas data no es la vía idónea para impedir la difusión del dato penal (o judicial), en la medida que las actuaciones judiciales no son bases o bancos, ni archivos o registros, y aún a pesar de la existencia del registro de sentencias (Cfr. Art. 17 inciso 2º).

La situación debiera entender dos problemas diferentes. El que transmite la información debiera reservar en la difusión sólo el dato consistente en la situación procesal, y nada más. Es imprescindible resguardar la reserva y confidencialidad de otros datos que surgen del relevamiento jurídico efectuado en las etapas sumariales donde necesariamente se investigan aspectos de la personalidad que no son parte de la información a comunicar.

> La manipulación y la posibilidad de conocerse al momento de celebrar un contrato u otorgar un crédito por una institución financiera también debe ser limitada, al menos en el tiempo, porque las personas tienen derecho a ser perdonadas. A esta situación alude el *artículo 22 del Título III (proyecto* para Chile), que intentando terminar con los registros o boletines llamados "históricos", se preocupa de fijar plazos para proveer o suministrar información a terceros (lo que no hace propiamente un acreedor sino más bien empresas comerciales que lucran —y "Abusan del Derecho"— prestando servicios de solvencia patrimonial). Según el proyecto no puede hacerse pasados 3 años desde que la obligación se canceló o transcurridos 10 años desde que la obligación se extinga por cualquier causa legal.
>
> Agrega Jijena Leiva que, los datos patrimoniales "positivos" tales como monto de ingresos, de acciones que se poseen, de participaciones en sociedades, de depósitos bancarios, de bienes muebles e inmuebles, etc., no deben por regla general o en principio ser procesados y menos perfilados o cruzados con otros.

Por ello, en 1997 la Comisión de Bélgica afirmaba que *la posibilidad de usar bases de datos centralizadas o integrales para buscar los antecedentes penales de una persona crea riesgos para la*

protección de datos que son totalmente desproporcionados respecto a los medios tradicionales de acceso o publicación de los casos judiciales…La evolución tecnológica debe ir acompañada de una mayor discreción respecto a la revelación de la identidad de las partes que se encuentran en los archivos de los casos judiciales".

El otro aspecto del tema es qué puede hacer el afectado cuando se transmite información sensible además de aquella que se vincula con sus antecedentes penales.

En estos casos el registro de antecedentes penales, o el de sentencias, o toda información que surja de un expediente judicial, debe permitir al interesado el derecho de exigir que la información que se transmita sea únicamente respecto a la decisión final adoptada sin agregados. Por ejemplo, si la sentencia decide la exclusión del hogar de una persona y el embargo de sus bienes, no se podría complementar la información indicando cuales son los inmuebles o valores afectados ni el lugar del que se lo excluye.

El Consejo de Europa ha recomendado la eliminación inmediata de todo dato personal que no sea necesario para el sumario policial, a cuyo fin se establecieron tres categorías de actuaciones de investigación: en primer lugar las dirigidas a prevenir o, en su caso, reprimir amenazas graves e inminentes para la defensa del Estado, orden y seguridad pública, siempre que sean cometidas por bandas o grupos organizados; en segundo lugar, las previstas para prevenir otros peligros reales para la seguridad pública, distintos de los anteriores; y en tercer lugar, las que reprimen infracciones penales que requieran la utilización de datos personales, sean o no especialmente protegidos.

Los criterios para la cancelación de oficio de los datos personales son diferentes en cada categoría de actuaciones, de suerte que los datos personales registrados para investigaciones relacionadas con la primera categoría de actuaciones policiales estarán sujeta para su cancelación a los regímenes procesales locales; los datos recabados para las investigaciones relativas a la segunda categoría de actuaciones se cancelarán en el plazo de cinco años a contar desde el momento en que no se incorporen nuevos datos a la investigación concreta de que se trate; y finalmente, en relación con los datos recabados para las investigaciones a que se vincula la tercera categoría, se cancelarán en el plazo de cinco años siempre que recaiga sentencia condenatoria; el plazo comenzará a contar desde que se cumpliere la misma o desde el indulto o remisión de la pena. Asimismo procederá la cancelación inmediata de los datos cuando recaiga sentencia firme absolutoria o auto de sobreseimiento libre por no ser los hechos constitutivos de delito.

> Otro aspecto al que se debe prestar atención, es la transmisión del dato penal requerido por otro Juez interviniente, pues si lo que se pretende es mantener la confidencialidad, no debiera en caso alguno solicitarse por el Juez civil o penal o de cualquier otra jurisdicción, más datos de los que son absolutamente necesarios. También, es preciso garantizar la reserva del trámite, de modo tal que en el mismo intervengan sólamente aquellos que pueden ver la información. Inclusive, para las partes el alcance del secreto debiera extenderse impidiendo la extracción de copias del expediente donde figure la información sensible.

f) Archivos científicos o de investigación

Las bases de datos que, generalmente, se constituyen con fines de investigación están excluidos del ámbito donde actúa el hábeas data. No interesa que la información sea transmitida a otros o se negocie con el almacenamiento logrado.

> El art. 8º dispone (Datos relativos a la salud): *"Los establecimientos sanitarios públicos o privados y los profesionales vinculados a la ciencia de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquellos, respetando los principios del secreto profesional"*.

La única excepción resulta cuando en el archivo, o en la cesión, se mencionan expresamente personas físicas a las que se da un perfil determinado, una vez efectuado el tratamiento de los datos que le conciernen.

Por ejemplo, en la investigación científica sobre una enfermedad (v.gr.: SIDA, Diabetes, Cáncer, etc.) suelen tomarse casos testigos que, ineludiblemente, vinculan a personas determinadas que padecen el mal. Estas son identificadas, caracterizadas, seguidas permanentemente hasta en mínimos detalles, y todo ello se registra y archiva en el banco de datos.

Esta información personal que divulga a otros un dato sensible, no obstante ser un archivo con finalidades científicas, necesita protegerse a sí mismo para lograr mayor seguridad, evitando transferir datos que afectan la intimidad de los seres investigados.

> Debe considerarse –afirma Herrán Ortiz- que el almacenamiento de determinadas informaciones relacionadas con la salud conlleva un peligro añadido, en otras palabras, no será preciso para conocer la enfermedad de un paciente registrar ésta explícitamente, porqué a través de la información relativa a determinados fármacos, puede deducirse fácilmente la enfermedad que padece la persona.

La recomendación nº 81 del 23 de enero de 1981 del Consejo de Europa* sostuvo entre sus fundamentos que era imprescindible considerar la relevancia del tratamiento automatizado de los datos médicos de una persona pues éstos forman parte de la esfera más íntima de las personas y *la divulgación injustificada de los datos personales de carácter médico puede ser luego el origen de diferentes tipos de discriminaciones y también de violaciones de derechos fundamentales.*

> La actual recomendación sobre datos médicos R.97/5* se detiene especialmente en tratar el problema de la investigación científica y los datos médicos, estableciendo el principio general del tratamiento anónimo de los datos médicos con dicha finalidad, si bien cuando no sea posible no impedirá de forma absoluta la realización de las investigaciones.

Un desvío potencial es la adquisición de la base informativa por parte de laboratorios que pretenden anticipar resultados con la producción de fármacos; o desde otra perspectiva, la segregación laboral de personas que padecen una determinada enfermedad (lo cual, quizás tampoco sea materia del hábeas data –pues el dato es preciso aun siendo sensible- aunque permita una acción de amparo por segregación).

> En Francia, las personas portadoras del virus del SIDA deben incorporarse inmediatamente a una base de datos a cuyo fin el médico está obligado a dar la información (Decreto del 31/10/82). Luego, informa Herrán Ortiz, pensando en las investigaciones epidemiológicas y estadísticas de la enfermedad, se ha adoptado una disposición que trata de garantizar los derechos de la persona seropositiva, imponiendo la necesidad de la autorización expresa del afectado con anterioridad al registro de la información y al empleo de un proceso criptográfico de archivación, logrando que la información permanezca disociada incluso para el profesional que interviene en el procedimiento.

g) Los servicios estadísticos

El relevamiento estadístico se realiza respetando los principios de reserva y confidencialidad, porqué el resultado que se obtiene de la actividad no es aplicable a una persona en particular sino a la sociedad toda a través de medidas específicas que al efecto se resuelven.

> En el secreto estadístico –afirma Bacaria Martrus- existe un doble vínculo obligacional: por una parte la obligación legal de declarar los datos para la realización de actividades estadísticas; de otra, el imperativo legal de mantenimiento del secreto estadístico y también la obligación legal de difusión pública de los resultados alcanzados.

Idéntica conclusión se aplica a los servicios estadísticos efectuados por empresas o particulares. Un ejemplo de actividad estadística es el censo poblacional que se concreta cada diez años, para el cual cada individuo debe prestar su colaboración (Cfr. Ley 17.622* y su reforma por ley 21.779*).

A los fines de precisar la injerencia del hábeas data sobre estos bancos de información es preciso conocer que la estadística, antes que una base de datos, es una actividad que tiene por objeto la comparación

de datos y su interrelación para la medición de diversos programas (para algunos, es la ciencia que aplica las leyes de la cantidad y de su representación gráfica para condensar los hechos sociales y medir su intensidad, deducir las leyes que los rigen y hacer una predicción próxima).

> El secreto estadístico se puede considerar –a criterio de Bacaria Martrus- como secreto profesional. Es fundamentalmente, una obligación específica de un colectivo concreto y se aplica al personal de los órganos estadísticos y al de otros servicios estadísticos de las administraciones públicas como un elemento de su régimen jurídico, a la vez que se hace extensiva a cualquier otra persona física o jurídica que entre en contacto o tenga acceso a los datos estadísticos individuales o individualizados, por razón de su participación en operaciones estadísticas.

El Consejo de Europa establece en el Convenio 81* (art. 5º) que estos servicios *registrarán finalidades determinadas y legítimas y no se utilizarán de una forma incompatible con dichas finalidades;* además, *serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado.*

> En España la ley 12/89 de la Función Estadística Pública considera como datos estadísticos, tanto los que se obtienen para los servicios estadísticos, como a aquellos recolectados por otros órganos de tipo administrativo. Datos que son útiles a efectos estadísticos, por lo que se facilitan a estos servicios, diluyéndose así –dice Velázquez Bautista- en este caso, la tradicional separación entre datos de carácter administrativo y servicios estadísticos.

La confidencialidad y reserva del trabajo estadístico, unido al carácter de la actividad, lo exime como sujeto pasivo del hábeas data, aunque se puede exigir al banco de datos que ellos realizan, la aplicación de los principios que imperan para el tratamiento de datos en general.

> En España, la Ley 12/1989 de la Función Estadística Pública sostiene: *"1. Cuando los servicios estadísticos soliciten datos, deberán proporcionar a los interesados información suficiente sobre la naturaleza, características y finalidad de la estadística, advirtiéndoseles, además, de si es o no obligatoria la colaboración, de la protección que les dispensa el secreto estadístico, y de las sanciones en que, en su caso, puedan incurrir por no colaborar o por facilitar datos falsos, inexactos, incompletos o fuera de plazo.*
>
> *"2. En todo caso, serán de aportación estrictamente voluntaria y, en consecuencia, sólo podrán recogerse previo consentimiento expreso de los interesados los datos susceptibles de revelar el origen étnico, las opiniones políticas, las convicciones religiosas o ideológicas y, en general, cuantas circunstancias puedan afectar a la intimidad personal o familiar".*

La denuncia de los peligros que reporta la cesión de los datos logrados desde un censo poblacional, se puede evitar disociando la información, esto es, procesando los datos de manera que no se pueda establecer vínculo alguno entre el titular de los datos y la información que se obtiene.

> Según Herrán Ortiz, así lo ha entendido el legislador español, que ha prohibido cualquier información particularizada sobre los datos personales contenidos en el censo electoral, garantizando a la persona el respeto a su intimidad personal y familiar, ya que de otro modo podría vulnerarse el derecho a la libertad individual al obtener un completo retrato de la persona a través de los datos personales que se encuentran registrados en el censo electoral.

Asimismo, los funcionarios que por razón de sus cargos u oficios tomen conocimiento de datos estadísticos o censales, están obligados a guardar sobre ellos absoluta reserva.

La ley sancionada sostiene en el artículo 28 que:

> (Archivos, registros o bancos de datos relativos a encuestas):"*1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a la ley 17.622, trabajos de prospección de mercados,*

investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable; 2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna".

h) Los bancos de datos genéticos y los bancos de órganos

Los bancos de datos genéticos contienen información que permite estudiar enfermedades y otras características de la persona humana a partir de su estructura genética.

> Informa Uicich que en Islandia se ha permitido a una empresa manejar la información genética y las historias clínicas de los habitantes de ese país. La ley sancionada en 1998 le otorgó por 12 años el estudio de los factores genéticos que inciden en las enfermedades de los habitantes de la nación isleña, quienes han conservado su genealogía desde 1915 y no muestran rasgos de mezcla genética hasta la segunda guerra mundial (lo cual los constituye con una genética propia). Según la empresa, esta base de datos tiene por objetivo comprender los factores genéticos que inciden en las enfermedades, generar una medicina predictiva y mejorar el resto de la administración de salud.

Más allá de los beneficios indudables que reporta el estudio de los cromosomas para determinar fisonomías clínicas y resolver causas y tratamiento para los padecimientos de salud, lo cierto es que el tratamiento de estos datos por inescrupulosos (v.gr.: guerras químicas que destruyen a los hombres manteniendo la arquitectura de las ciudades) provoca un riesgo que es preferible no correr.

Estos datos pueden identificar al ser humano en detalles que hasta para él mismo podrían ser desconocidos, circunstancia que demuestra la penetración de la intimidad y la necesidad de lograr un punto de equilibrio entre los derechos potenciales que se enfrentan.

Lo mismo sucede con los bancos de órganos (por ejemplo: Incucai) que cumplen una función informativa esencial para la vida de las personas a quienes concierne. Estos archivos informáticos localizan órganos humanos de donantes que voluntariamente asumen el transplante a otro quien sufre por la pérdida o afectación del mismo órgano vital.

Son fuentes de datos médicos, evidentemente, pero la acumulación de informaciones sobre la persona del donante y del destinatario es tan variada que podría comprometer la intimidad de ellas.

En nuestro parecer, estos bancos de datos se encuentran en las mismas condiciones que los bancos científicos, por lo cual las conclusiones de ellos les alcanza.

i) Las empresas de venta de información crediticia

Informar sobre la solvencia económica de alguien, tiene en las operaciones financieras una importancia trascendente porque disminuye el riesgo y facilita la toma de decisiones en la asignación de créditos.

Los bancos de datos que se ocupan del tema tienen como objetivo informar a quien lo requiere y paga por ese servicio, sobre el comportamiento comercial y crediticio de una persona o empresa.

Las actividades de estas entidades son básicamente dos: la información sobre la solvencia económica, y la relativa al cumplimiento y morosidad de obligaciones dinerarias. Mientras la primera se refiere a la capacidad económica de una persona, permitiendo al interesado tener una visión sobre la confiabilidad patrimonial; la restante amplía el historial al comportamiento adoptado para responder por los créditos tomados.

Ambas situaciones son permitidas en el artículo 26 de la ley de tratamiento de datos personales, pero introduce una variable significativa en torno a la forma de conocer el dato y proceder a su archivo.

Mientras para el supuesto de la *"solvencia económica y crédito"* se exige la facilidad obtener la información o el consentimiento libremente prestado para el archivo; en el caso del *"cumplimiento de las obligaciones"* se tiene en cuenta la legalidad del registro cuando éste informa sobre deudas ciertas, vencidas y exigibles que hayan sido previamente intimadas de pago. De este modo, aun sin tener sentencia firme (condenatoria o absolutoria) el archivo puede informar sobre la verdad que constata, sin infringir intimidad comercial alguna.

La información ofrecida se recaba de las operaciones financieras efectuadas (v.gr.: compraventa de inmuebles o muebles registrables; cumplimiento en transacciones menores como la adquisición de electrodomésticos a plazos; gastos realizados con tarjetas de crédito, etc.), y de resultar moroso en los pagos o demandado en litigios por cobro de sumas de dinero, se da noticia sobre juicios en trámite, sentencias condenatorias, inhibiciones y embargos, entre otra información disponible.

Por lo general estos informes de solvencia y confiabilidad se reportan como confidenciales, prohibiendo su exhibición o divulgación a terceros, especificando que en caso alguno los datos implican abrir juicios de valor sobre las personas concernidas.

> En Argentina, Organización Veraz S.A. (empresa dedicada al rubro que se analiza) suele afirmar en sus escritos judiciales que todos los cambios que sufren los informes efectuados por cualquier acto o hecho nuevo que modifica el anterior, es comunicado al cliente que solicitó el informe. Los datos de los hechos u actos registrados de la persona física o ideal se dan de baja a los diez años de vencido el plazo de vigencia de cada uno de ellos, en tanto en el interín no se hayan producido reiteraciones de igual naturaleza, en cuyo caso los diez años empiezan a contarse desde el último producido.

En nuestro país, existe bajo la órbita del Banco Central de la República Argentina, el denominado "*Sistema de Telecomunicaciones del área financiera*"*, por el cual se administra información vinculada con las inhabilitaciones de las personas físicas o jurídicas para operar en cuentas corrientes bancarias; deudores de entidades financieras que se encuentran en liquidación; entre otra información reportada. Además, existen sendas centrales sobre control de riesgo e información crediticia.

No se ha previsto la intervención de la persona concernida, de modo tal que la información suministrada es el producto de una relación entre partes. Actualmente existen proyectos que pretenden abrir un banco de datos sobre riesgo crediticio donde pueda el afectado tomar conocimiento de los informes que sobre su persona se brindan*.

No obstante, cabe señalar que el inciso 5º del art. 26 crea una "doble obligación de notificación" para el operador de la base de datos y para el acreedor hacie el deudor anoticiándolo de su posible inclusión en una base de datos de información crediticia por el incumplimiento de su obligación en el supuesto de que el acreedor no lo hiciera.

¿Cuál es el problema en torno de estos archivos?.

En su inmensa mayoría los procesos de amparo que contra ellos se deducen argumentan que la producción de informes personales violenta el derecho a la intimidad, además de provocar un daño inmediato al privar de crédito y apoyo económico a las actividades que se pretenden realizar.

La respuesta suele fundamentarse en que los datos informados son de fácil acceso para cualquiera por ser públicos y registrados, y que no se afecta la intimidad de persona alguna al permitir el acceso a las fuentes de información y facilitar a los concernidos las quejas que contra los datos tuvieren.

Asimismo, hay que tener en cuenta que, si la función del banco de datos es *informar* objetivamente sin emitir juicios de valor, el suministro del archivo personal responde al fin para el que fue creado y no podría, en principio, catalogarse como ilegítima esa actividad.

> Desde un aspecto subjetivo, se plantean dudas sobre si son aplicables las garantías de la protección de la privacidad a quienes operan en una actividad empresarial como ejecutivos individuales, esto es, si es o no aplicable el régimen de protección de la intimidad a la parte empresarial de la vida particular de un individuo.

> El desarrollo jurisprudencial en nuestro país tiene el mismo sesgo restriccionista, porqué sólo procede el proceso constitucional cuando la información proporcionada es falsa o discriminatoria. Por ejemplo, se ha dicho que "*corresponde rechazar la acción de hábeas data intentada si los actores no manifiestan que la información proporcionada sea falsa, ni que revista características de discriminatoria (*en el caso se solicitaba la intimación al banco de datos demandado para que cesara de informar sobre circunstancias y hechos precluidos y comunicara a las instituciones bancarias que los actores no registraban antecedentes) –CNCom., Sala E, diciembre 13/994 *in re* Molina, Alberto V. y otros c/ Organización Veraz S.A.-

La dualidad entre derecho a la información y derecho a la privacidad aparece, una vez más, en juego. Aunque en este caso, el límite se puede encontrar en las posibilidades reales que encuentre el afectado para acceder y controlar los datos que de él se ocupan.

> El objeto de protección normativa que tiene la Lortad (actualmente derogada pero vigente en esta idea) –dice Salom- es la privacidad, entendida como aquella que tutela la vida privada que se afecta cuando las actuaciones cotidianas del ciudadano se observan, y la información procedente de ellas se acumula y conserva, formando lo que se denomina perfil del afectado, perfil que puede ser utilizado con fines de diversa índole. La protección de la privacidad que se garantiza no supone sino la posibilidad real de que la persona tenga el control de los usos y finalidades a que se destina dicha información y pueda oponerse, en consecuencia, a que la información que genera su perfil sirva a propósitos que él rechaza.

Sin embargo, el perfil constitucional que trae el artículo 43 se muestra sesgado en los bancos de datos destinados a proveer informes (en el particular, información crediticia). En efecto, si el archivo proporciona información almacenada desde fuentes de acceso público, la transmisión que genera no produce en los hechos afectación alguna a la privacidad o al derecho que tiene toda persona sobre sus datos personales. En todo caso, la actualización, rectificación, supresión o confidencialidad, debiera plantearse al órgano estatal que recopila o guarda dicha información.

Por eso, se ha dicho que la acción de hábeas data sólo procede cuando los registros tienen inexactitudes y, a consecuencia de ello, se provoque cierta o determinada discriminación. Si no es así, *no corresponde hacer lugar al pedido tendiente a suprimir un dato caduco si ambas partes –actor y demandado- están contestes en que el contenido de la información existente en los archivos carece de inexactitudes por tener los mismos expresos agregados con asiento de las fechas en que las inhabilitaciones han vencido* (cfr. CNCiv., Sala G, mayo 10/996, *in re* Falcionelli, Esteban P. c/ Organización Veraz S.A.).

El artículo 26 de la ley aprobada sostiene: "(Prestación de servicios de información crediticia):

1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

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

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

4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico- financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el

deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho.

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

Tal plataforma introduce algunas limitaciones temporales para el registro que se puede efectuar y ceder a terceros. Se trata la información de cinco años del requerido y se le otorga un derecho al olvido cuando cumple sus obligaciones, permitiendo reducir a dos años la fecha límite para el almacenamiento.

¿Desde cuando se cuenta este límite temporal?

Una primera lectura puede afirmar que el plazo comienza a correr desde la mora del deudor; en cambio otra puede sostener que corre desde la inclusión en la base de datos.

Una y otra posibilidad es incongruente, además, con los tiempos disímiles que la ley establece, porqué los cinco años de mora frente a los dos de permanencia en la base porqué pagó, supone generar una desigualdad de criterios frente a una misma situación ante el cumplimiento de las obligaciones. La diferencia estaría en que en el segundo caso se otorga una franquicia (derecho al olvido) por haber superado el estado moratorio.

Lo más conveniente, a nuestro entender, es contar el plazo de cinco y de dos años a partir del momento de la cancelación de la obligación contraída. Será el mejor incentivo para el deudor a realizar los pagos en forma oportuna evitando el riesgo que se corre con el deudor renuente que puede especular con una interpretación diferente y aprovechar la diferencia de los tiempos.

Este pareció ser el criterio asentado en el artículo 47 (Disposiciones transitorias) –vetado por el Decreto 995- *que disponía:* Los bancos de datos prestadores de servicios de información crediticia deberán suprimir, o en su caso, omitir asentar, todo dato referido al incumplimiento o mora en el pago de una obligación, si ésta hubiese sido cancelada al momento de la entrada en vigencia de la presente ley".

Pero esta lectura no elimina el problema que sufrirán muchos argentinos a partir de ahora, en la medida que la categoría de riesgo crediticio que hace el Banco Central, comienza a sufrir criterios desiguales. Los registros de créditos negativos –es decir, por mora o deudas que pasaron a la vía judicial- quedarán anotados por cinco años, o dos si se cumple con la obligación. Si la deuda tiene un origen diferente, por ejemplo servicios, la anotación cae automáticamente; mientras que si la morosidad se constata en un proceso de quiebra, la anotación se mantiene por diez años.

Además, se establece la obligación de informar al afectado las transferencias efectuadas en los últimos seis meses, cuando aquél lo solicite expresamente al banco de datos.

También, antes de enviar un informe crediticio a un banco de datos, y como requisito para que este lo reciba, la entidad acreedora deberá enviarle al deudor un requerimiento de pago, haciendo constar de que es una deuda líquida y exigible, comunicando a qué registro se lo esta enviando.

Cuando una entidad financiera reciba un informe que considere negativo, es decir, que le otorgue bases para resolver la denegatoria al pedido de crédito, deberá notificar al perjudicado de esa situación informando el motivo por el cual rechaza la solicitud de un producto financiero. Este sistema actualmente no existe, de forma tal que se arbitra un mecanismo por el cual el supuesto deudor podrá corregir el dato inexacto o la información desactualizada, si ello fuere así.

La cuestión siguiente estaciona para saber si el mismo derecho lo tienen las personas jurídicas, en atención a que la garantía procesal parece extenderse a ellas, siguiendo la redacción estricta del artículo 43 constitucional, y el artículo 2º parte final de la ley. Tema que abordamos más adelante.

En otro sentido, los archivos de información crediticia se clasifican en *negativos*, cuando acumulan datos sobre insolvencia e incumplimientos en obligaciones dinerarias; y *positivos*, que son aquellos que

reúnen datos sobre comportamiento crediticio vigente. Es decir, mientras el primero registra "morosos", el segundo lo hace con los créditos pendientes.

> A diferencia del fichero negativo, el fichero positivo no está contaminado por el concepto de lista negra, que puede dificultar la aceptación psicológica de los archivos. Con este sistema, los prestatarios no se encuentran inducidos a ocultar la verdadera situación de sus deudas. Sin perjuicio de ello, el sistema de almacenamiento positivo contribuye a hacer más responsables a las partes.

En definitiva, los archivos de información crediticia son bancos de datos que procesan información obtenida directamente o por cesión de otras fuentes de acceso público. Si el objeto del giro comercial de ellas se centra en el suministro de información objetiva sobre la actividad comercial y crediticia de las personas, pero no datos de otra índole, a lo que cabe sumar la ausencia de un juicio de valor sobre el sujeto de que se trate, su patrimonio o su solvencia, no puede tildarse de parcial, discriminatorio o incompleto (y por ende falso) al informe que se brinda.

Así lo ha interpretado nuestra jurisprudencia, agregando que en tales casos, *no se puede obligar a la empresa a que integre su negocio con un plexo informativo que permita formarse un juicio integral o que suprima la información que a criterio del propio interesado sea incompleta, por cuanto es a éste a quien le cabe suministrar estos elementos a las personas o entidades que hayan requerido la información sobre él* (cfr. CNCiv., Sala M, noviembre 28/995, *in re* Groppa c/ Organización Veraz S.A.).

Además, es criterio aceptado que el derecho de exigir confidencialidad en los datos no se aplica a la información de alcance comercial o financiero, pues la misma, por su carácter, está destinada a divulgarse entre todas las entidades financieras del país, tal como lo prevé la circular OPASI 2 del Banco Central *.

> La recientemente sancionada ley 25065 *, sobre Tarjetas de Crédito, establece en el artículo 53 la prohibición de informar: *"Las entidades emisoras de tarjetas de créditos bancarias o crediticias tiene prohibido informar a las bases de datos de antecedentes financieros personales sobre los titulares y beneficiarios de extensiones de tarjetas de crédito u opciones cuando el titular no haya cancelado sus obligaciones, se encuentre en mora o en etapa de refinanciación. Sin perjuicio de la obligación de informar lo que correspondiere al Banco Central de la República Argentina. Las entidades informantes serán solidaria e ilimitadamente responsables por los daños y perjuicios ocasionados a los beneficiarios de las extensiones u opciones de tarjetas de crédito por las consecuencias de la información provista"*.

Por todo ello, al individuo hay que asegurarle:

- El derecho de información que supone tener acceso al archivo de información de crédito y solvencia para tomar conocimiento de los datos que a su respecto se registran.
- Garantizar la información suficiente en torno a cómo se recabaron los datos, de qué fuentes y, en su caso, identificando el cesionario que brindó la información personal de un tercero.
- Ofrecer la posibilidad de actualizar los datos inexactos o rectificar aquellos que fueran erróneos.

j) Archivos de entidades financieras

La incorporación a una entidad bancaria o financiera comienza con el llenado de fichas informativas de datos personales, habitualmente muy exhaustivas, que persiguen formar un perfil del nuevo cliente.

Esta base debiera ser confidencial y reservada, y aplicarse para la toma de decisiones respecto a la relación bancaria específica. Sin embargo, es frecuente el intercambio de información en el sistema financiero nacional.

> El negocio de la circulación de datos no es necesariamente ilegal. No siempre que se llena un cupón en un comercio se envía información a una boca de lobo

> delincuencial. Pero a quienes se preocupan por mantener sus empresas dentro de la ley, casos como los ocurridos en Argentina como la venta del banco de datos del ANSES o del padrón electoral, les causan más que un dolor de cabeza. No obstante, es sabido que entre las entidades financieras existe una suerte de cooperación, con un centro informativo en el Banco Central, que les permite conocer al cliente a través de las experiencias tenidas entre las sedes y sucursales del sistema financiero.

Considerando que el hábeas data local se encuentra previsto para controlar todo registro o banco de datos, público o privado *destinado a proveer informes*, cabe la duda respecto a determinar si la cooperación informativa no onerosa, puede ser controlada por este mecanismo constitucional.

La respuesta debe ser afirmativa, porqué la información voluntariamente suministrada, como requisito ineludible para acceder al sistema (igualmente sucede cuando nos alojamos en un hotel; o al completar un formulario para un sorteo; o para suscribir una editorial, etc.) se ingresa como parte de un convenio, donde la confidencia integra el conjunto. Es evidente que la ausencia de control y la falta de recursos o herramientas en manos de los particulares para poder defenderse ante una real desviación de poder en el uso de los datos revelados, puede significar no solamente perjuicio material, sino, además, una honda lesión a los derechos de la personalidad humana.

No obstante, este derecho a exigir confidencialidad no se extiende al comportamiento financiero que el interesado muestra en sus actos, pues la reserva se aplica a los datos denominados sensibles o esenciales.

> El derecho de exigir la confidencialidad de datos no se extiende a aquella información de alcance comercial o financiero. Ello es así pues tal información (cierre de una cuenta corriente por haber producido el tercer rechazo de cheques sin provisión de fondos), por su carácter, está destinada a divulgarse entre todas las entidades financieras del país tal como lo prevé la circular OPASI 2 del Banco Central (*CNContenciosoadministrativa, Sala 4ª, setiembre 5/995*, ver Jurisprudencia Argentina, 1995-IV, 350)

El Banco Central de la República Argentina (BCRA) ha dictado una normativa que crea y regula una de las bases de datos públicas que mayor repercusión tiene en el mercado del crédito: la "Central de Deudores del Sistema Financiero" (CDSF). Se trata de una regulación típica de la era del derecho informático y entre sus normas se consagra un derecho de acceso al que Pedro Dubié ha denominado Habeas Data Financiero.

> Pedro Dubie ha dicho que la CDSF establece, entre otras normas, parámetros definidos para la calificación de cumplimiento de los clientes del sistema financiero (1), crea un procedimiento de revisión de las calificaciones (2), y fija una autoridad de control (3), que es el propio BCRA. A su vez el BCRA, en tanto autoridad de aplicación del sistema financiero, está sujeto a la revisión judicial de sus actos, y todo este andamiaje jurídico que analizaremos se asienta en el Habeas Data consagrado en el art.43 tercer párrafo exhibiendo una clara coherencia en la pirámide jurídica.
>
> En setiembre de 1997 el BCRA creo la CDSF, fundiendo en un solo régimen informativo la Central de Deudores y la Central de Información Crediticia, pero continuó diferenciando la clasificación de los deudores con relación al monto del préstamo, esto es por debajo o por encima de la barrera de los $ 200.000. Propio de la era del derecho informático, en la Sección 8 de la 2729 se establece uno de los derechos más desconocidos y menos practicados. Posterior a la consagración del habeas data constitucional en 1994, la 2729 emula del art. 43 tercer párrafo un derecho de acceso y conocimiento a la información que contiene la CDSF.
>
> El art. 8.1, titulado "*Informaciones a suministrar*" reza: "*A solicitud de cada cliente, dentro de los 10 días corridos del pedido, la entidad financiera deberá comunicarle la ultima clasificación que le ha asignado, junto con los fundamentos que la justifican según la evaluación realizada por la entidad, el*

importe total de deudas con el sistema financiero y las clasificaciones asignadas que surjan de la ultima información disponible en la "Central de Deudores del Sistema Financiero. Los clientes deberán ser notificados de que tienen la posibilidad de requerir esos datos, en el momento de presentarse las solicitudes de crédito, mediante una formula independiente de ellas".

El sujeto legitimado es el cliente de una entidad financiera y tiene una clara meta informativa. El BCRA ha querido garantizarle al solicitante de un crédito y al deudor, desde el primer momento de la relación precontractual, el conocimiento previo de que su conducta de pago será calificada una vez concedido el préstamo. Establece una obligación para la casa bancaria de informar en forma previa que el cliente podrá en todo momento solicitar a la entidad financiera explicaciones acerca del encuadre calificativo de su comportamiento crediticio que realice la entidad conforme las pautas fijadas por la autoridad de control.

El BCRA, siguiendo la tendencia de las leyes de Protección de Datos, indica que este derecho de acceso y conocimiento se comunique en una fórmula separada junto a las solicitudes de crédito. Este Derecho de Acceso, como dijimos, practicamente reproduce, si bien en forma parcial y circunstanciada, la primera parte del art. 43 tercer párrafo de la CN: *"Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos o privados destinados a proveer informes"*. Hubiera sido deseable también un final como el del primer párrafo del 43: *"y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad, o actualidad de aquellos."*.

Pero aunque el art. 8.1 no lo diga expresamente este Derecho de Acceso específico, se completa con el derecho a solicitar la actualización, rectificación o supresión ante la presencia de falsedad en la información de la CDSF. Va de suyo que el Derecho de Acceso cumple una doble funcionalidad: o (1) se agota en sí mismo luego que cliente ha tomado conocimiento efectivo de la información solicitada; o (2) se comporta como un derecho de medio, para la petición legítima posterior de actualización, rectificación o supresión.

La complementación hermenéutica es informada por el art. 43 tercer párrafo de la C.N. que viene en auxilio de la incompletitud del art. 8.1 de la 2729 que no ahonda en un procedimiento de corrección. El derecho a una información personal verdadera tiene rango constitucional y es una de las finalidades del habeas data.

En el caso "Cadaveira, Enrique c/ Banco Central de la República Argentina s/ habeas data", la Cámara dijo: "Que si bien el caso "Urteaga" no tiene un punto de contacto con los que se debaten en el sub lite, interesa poner de resalto por su trascendencia, el hecho de que el Alto Tribunal se inclinara por una hermenéutica flexible de la norma... *No es suficiente que el B.C.R.A. se limite a suprimir la base de su información errónea y a no volver a repetirla... De manera que la mera supresión del dato deja subsistente una cierta ambigüedad o falta de certeza sobre la situación en que se encontró el deudor en el lapso antes indicado...* Con lo cual podrá, acaso, haberse respetado formalmente la letra del art. 43 de la Constitución Nacional, pero no se habrá asegurado el cumplimiento de su elevado fin que no es otro que asegurar la difusión de la verdad" (Cfr. Walberg de Iturbe, Elizabeth c/ Banco de la Nación Argentina s/ habeas data", Juz. Fed. Río Cuarto, 23-11-98. Revista Derecho y Nuevas Tecnologías, Año 1 Números 2-3, pag. 259, Director Pablo Palazzi).

El contenido de la información que debe suministrar la entidad es amplio. Cuatro son los aspectos que debe cubrir el informe.

1) *"...comunicarle la ultima clasificación que le ha asignado..."*. Cuando se refiere a la última clasificación o calificación asignada, entendemos que se refiere a aquella calificación que la entidad financiera remitió al BCRA, y que este se encargó de difundirla en forma pública en su carácter de autoridad y administrador de la CDSF. Esta calificación es de acceso público, y es habitual que el deudor se entere de ella en forma indirecta. No obstante, entiendo que el cliente también tiene derecho a conocer la última calificación asignada aunque esta no sea pública aún, justamente porque de su revisión se puede impedir la divulgación de un dato inexacto o falso, especialmente cuando el deudor tiene sospechas fundadas que se le podría estar calificándole en forma errónea. Existe un lapso entre que el banco remite la información al BCRA y este la hace pública. Hasta el presente, como causa del procesamiento informático, la información del BCRA deviene naturalmente desactualizada en tres meses aproximadamente.

2) *"...junto con los fundamentos que la justifican según la evaluación realizada por la entidad..."*. Por regla, la calificación que asignan las entidades financieras no es discrecional, ya que debe conformarse en orden a criterios objetivos preestablecidos por el BCRA, aunque hay algunas excepciones como veremos más adelante. Esto significa que la entidad satisface el requerimiento del deudor cuando describe el comportamiento crediticio del cliente subsumido en cada categoría de la 2729 para un mes determinado.

3) *"... el importe total de deudas con el sistema financiero..."*. Junto con la clasificación se publica el monto total adeudado. Este monto como luego veremos es la sumatoria de tres cifras: (1) los préstamos efectivamente transferidos al patrimonio del deudor (ej: un crédito hipotecario, un crédito prendario, un simple mutuo, más (2) el límite hasta el cual puede endeudarse el cliente (ej: descubierto en cuenta corriente, límite en la tarjeta de crédito) y (3) las garantías dadas a terceros.

4) *"... y las clasificaciones asignadas que surjan de la ultima información disponible en la "Central de Deudores del Sistema Financiero"*. Nos preguntamos si la entidad financiera debe poner en conocimiento de las otras clasificaciones asignadas por las demás casas o se refiere a las anteriores clasificaciones informadas por el banco. Nos inclinamos a pensar que se trata de la propia información y no de las demás casas, ello por varias razones: resulta imposible que el banco pueda dar explicaciones por las calificaciones ajenas a su propio giro comercial; es conducente que el deudor no solo controle la última clasificación sino también las anteriores de forma que su historia crediticia de cumplimiento refleje la realidad, es decir, se corresponda con la verdadera historia de pago. En este último sentido, de nada valdría rectificar una calificación si ello no se refleja en la base de datos del BCRA y este no la comunica a toda la plaza financiera en su calidad de fuente de información de acceso público.

Por *Entidad de Crédito* no debe entenderse solamente a la entidad financiera o entidad bancaria (Ley 21.526) autorizada por el BCRA para funcionar como tal. Desde 1996 el BCRA incorporo como entidad sujeta a la obligación de informar a las entidades no financieras emisoras de tarjetas de crédito bajo la modalidad de

Por la misma razón que resulta vital para el sistema de crédito distinguir a los deudores con relación al grado de cumplimiento de sus créditos, es fundamental que la información sea verdadera, porque de lo contrario podría apartar a un cliente del crédito mismo.

El BCRA en tanto recepta en forma continua la información remitida por el sistema financiero y administra la CDSF, a pedido del deudor tiene las suficientes facultades para:

1) Interrumpir la difusión de la calificación cuestionada.

2) Solicitar informes a la entidad financiera informante.

3) Pedir a la entidad financiera que remita los antecedentes que dieron lugar a la calificación.

4) Evaluar, en su carácter de policía financiera, la procedencia de la calificación cuestionada, y en su defecto

5) Cambiar, como autoridad del sistema, en forma fundada la calificación del cliente.

6) Modificar su propio bancos de datos (CDSF).

7) Ordenar a la entidad financiera para que registre en su banco de datos el cambio de calificación.

8) Difundir a través de los medios que dispone, esto es el Sistema de Telecomunicaciones del Area Financiera (STAF), página web, disco compacto o comunicaciones tipo "C", el cambio de status del cliente o el mensaje aclaratorio correspondiente para los casos de falsedad (*Cadaveira, Enrique c/ BCRA s/ habeas data"*, Juz. Nac. Civ. Com. Fed de la Capital Federal , 22/12/98. Ver revista Derecho y Nuevas Tecnologías, pag. 281)

De todas maneras, no hay que confundir la posibilidad de transferir la conducta del cliente en las operaciones de crédito y cumplimiento de sus obligaciones, con el *secreto financiero*, que supone el deber de la entidad de mantener con discreción y sigilo los datos y bienes sobre los cuales obtiene información a raíz del contrato entre ellos suscripto.

> La justicia comercial ha manifestado que: *"Toda entidad bancaria puede –sin violar el secreto bancario- ofrecer información acerca de los datos identificatorios de su cliente; no así respecto de las operaciones por éste realizadas por cuanto ella es reservada, ya que desde el momento en que el cliente circula cheques, debe aceptar que los portadores de éstos están habilitados para indagar respecto de la identidad e identificación del librador" (*CNCom, Sala A, mayo 5/983 *in re* Lon, Fanny c/ Noguera Canto, Juan).
>
> Igual temperamento sigue la Sala B, al expresar que "*el secreto bancario establecido por la ley 21.526, en su art. 39, alcanza a las informaciones que los clientes brindan a las entidades financieras a raíz de las operaciones que éstos realicen en el marco de dicha ley. Por ello, la declaración de bienes efectuada por el demandado en oportunidad de la apertura de la cuenta corriente en la entidad bancaria, se encuentra amparada por dicha norma"*.

La ley 24.244 ha limitado el deber de secreto a las operaciones pasivas, beneficiando al público en general toda vez que ahora se puede conocer quiénes son los deudores de la entidad financiera donde se piensan colocar los fondos y, por consiguiente, se pueden evaluar los riesgos a asumir si efectivamente son depositados.

> Así lo afirma Vázquez Arzaguet, agregando que "pese a ello, esta modificación no adquiere la entidad que, prima facie, podría pensarse que tiene. Opino que en virtud de nuestra legislación actual, puede ser revelada en sí misma toda operación de activos o de servicios, según sea el caso, pero no sucede lo mismo con los informes que se brindaron al banco para concretar la operación. Lo contrario, importaría violación al derecho de propiedad y al deber de secreto, el que no se encuentra específicamente relevado en este aspecto".

k) Los archivos fiscales

Los bancos de datos en materia fiscal se forman esencialmente con las declaraciones juradas que efectúan los contribuyentes amparados por el secreto y confidencialidad del sistema.

En la clasificación antes vista, son archivos públicos que se conservan con la finalidad de controlar el cumplimiento de las cargas públicas; y no tienen otro destino que ese, por lo cual, son personales y afectan la relación entre Estado y ciudadano. Es decir, este tipo de datos no se puede transferir a terceros.

> Sostiene Christensen que la Constitución en lo que hace a los registros públicos no fija el requisito que si contempla para los privados, de que los datos estén destinados a ser informados a terceros. En el caso de los registros o bancos de datos públicos no existe tal condicionamiento, por lo que torna procedente a pedido de persona interesada, la acción de hábeas data contra la Administración Federal de Ingresos Públicos; ya que la clasificación de públicos y privados está dada sobre la base de la persona que es titular de los registros o bases de datos, no a quien accede o pueda acceder a la información de los mismos.

El secreto fiscal está dispuesto en el artículo 101 de la Ley 11.683*, reserva que se extiende a toda la documentación que se expone incluyendo los papeles privados de los que el Fisco toma conocimiento, sea por requerimiento o declaración voluntaria.

> Por Decreto de necesidad y urgencia nº 606/99* se modificó el artículo 101 de la Ley 11.683 limitando el secreto fiscal que ampara las declaraciones juradas, manifestaciones e informes que los responsables o terceros presenten, y bs juicios de demandas contenciosa en cuanto consignen dichas informaciones. Asimismo, la norma establece que los magistrados, funcionarios y empleados de la administración fiscal están obligados a mantener el más absoluto secreto de todo lo que llegue a su conocimiento en el desempeño de sus funciones.
>
> Evidentemente, al levantarse el secreto fiscal sobre este tipo de actos de confidencialidad, se pretende establecer una especie de sanción al renuente o al incumplidor con la presentación de las declaraciones juradas correspondientes a obligaciones tributarias, lo que es absolutamente inconstitucional.

Sin embargo, es manifiesta la intención de los organismos recaudadores –algunas veces concretada- de informar los sumarios o investigaciones que se practican a quienes pueden haber violado el deber de decir verdad en las declaraciones de impuestos. La exposición como vergüenza pública afecta la intimidad, sin perjuicio de otros intereses afectados.

> Entra dentro del análisis que se efectúa, las comunicaciones que realiza el Fisco al Banco Central sobre supuestas deudas, que aun sin estar firmes por ser litigiosas, se comunican como si fueran tales; así como los potenciales incumplimientos de la seguridad social. Hace un tiempo –agrega Christensen- el Fisco remitía una nota a los bancos con los que operaba el contribuyente o responsable en los términos del artículo 12 de la Ley 14.449 y de la Circular 1703 del BCRA, a los fines de inhabilitarlo para conseguir créditos de parte de la institución bancaria.

La publicidad de las presuntas infracciones (que son de este carácter al no tener sentencia que las declare e imponga las condenas pertinentes, en el caso de verificarse la violación al principio de buena fe), se convierten en un sutil mecanismo de provocación a un acto espontáneo –aunque sea obligatorio- que viola la privacidad de quien los realiza.

> El presidente de la Agencia de Protección de Datos de España, contaba en oportunidad de visitar Argentina en el año 1999 que con las cuentas bancarias de contribuyentes había surgido un problema que llevó a sostener que el conocimiento de las cuentas bancarias era necesario para proteger el bien

> constitucionalmente protegido, que es la distribución equitativa del sometimiento de los gastos públicos. El tema que se planteaba era si la informatización por parte de la Hacienda Pública, al pedir datos a los bancos para averiguar si las declaraciones de impuestos se habían efectuado correctamente, vulneraba o no el principio de la intimidad de las personas: y dice que no; porque hay otros valores protegidos. A la vez un pronunciamiento del propio Tribunal de 1986 sostuvo que "no hay derechos ilimitados, por lo cual, si no hay duda de que en principio los datos relativos a la situación económica de una persona y entre ella los que tienen su reflejo en las distintas operaciones bancarias en las que figura como titular entran dentro de la intimidad constitucionalmente protegida, no puede haberla tampoco en que la administración está habilitada también desde el plano constitucional, para exigir determinados datos relativos a la situación económica de los contribuyentes"

De todos modos, el problema que presentamos (violación del secreto y confidencialidad) es diferente del que trae el sistema de registro o archivo de los datos vinculados con la actividad comercial o profesional de una persona.

En efecto, actualmente se ha implementado un nuevo sistema, denominado "OSIRIS"* para la recepción de pagos y de los datos contenidos en declaraciones juradas por medio de soportes magnéticos, de las obligaciones impositivas y previsionales correspondientes a los contribuyentes y/o responsables.

El objetivo tenido en consideración al instrumentar el referido sistema es el de optimizar el ingreso de datos y pagos mediante un proceso que, en forma paulatina, lleve a la supresión del papel como soporte de datos, para recibir la información declarada.

Para alcanzar esta meta se ha hecho conveniente establecer un régimen de transferencia electrónica de datos, para la recepción de la información contenida en las declaraciones juradas de obligaciones tributarias que se presenten en las entidades bancarias habilitadas para operar en el mencionado sistema "OSIRIS".

Este nuevo régimen se instrumenta mediante la firma de un contrato de adhesión depositado en el banco receptor habilitado, la elección por el usuario de una clave de seguridad e identificación personal y la presentación de las declaraciones juradas mediante su transmisión electrónica remota.

> La aceptación voluntaria de las reglas para presentar las declaraciones juradas, no debe suponer manifestación expresa de voluntad para que la administración ceda información aunque lo sea en miras a dar mayor eficacia al sistema de ingresos públicos. El punto debiera enfocarse en dos posiciones: en primer lugar, la información que adquiere la dirección de impuestos debe reconocerse como necesaria para el desarrollo de sus actividades; y en segundo lugar, que sólo esa información puede aplicarse para el ejercicio de sus propias competencias. Se configura así, un límite a los límites, ya que si la actividad de la administración dentro de los cauces legales constituye una valla para el ejercicio del derecho fundamental al control sobre las bases de datos que le conciernen, en tanto le impone el deber de facilitar información y le impide el acceso a la misma, no debe llevar a que, fundamentado en el cumplimiento de sus competencias, abuse de esas atribuciones legales cual tuviera un cheque en blanco para vulnerar las garantías de la libertad de intimidad y el derecho al secreto de las informaciones fiscales.

La seguridad de la base de datos (que pasa a ser eminentemente informática) se resuelve por un conjunto de mecanismos compuesto por reglas de filtrado en los ruteadores,

listas de control de accesos, paredes de fuego (*firewall*), y mecanismos de encriptar por equipo (hardware) las claves de seguridad e identificación personal de los usuarios y los algoritmos de encripción.

La comunicación que se establezca entre el contribuyente y el servidor estará encriptada en tiempo real.

Las claves de seguridad e identificación personal se resguardan en un equipo con estrictas medidas de seguridad física y lógica. Ante cualquier violación, mecanismos de seguridad lógicos deberán impedir la recuperación de los datos allí almacenados.

l) El registro electoral y las fichas de los partidos políticos

El padrón electoral es una típica base de datos con información elemental para autorizar la emisión del voto en los sufragios de elección de representantes y autoridades.

> Los datos que releva un padrón son mínimos y hasta parecen superficiales. Sin embargo, en el mercado de compra y venta de datos de un paquete básico –informa Revista Viva del domingo 21/3/99- cuesta cincuenta centavos. El costo de la información varía según la cantidad y la magnitud de los datos solicitados. Por ejemplo: el alquiler por dos meses del padrón de la ciudad autónoma de Buenos Aires salía cinco mil trescientos diez pesos ($ 5.310). Para alquilar el de la provincia de Buenos Aires había que pagar dieciseis mil seis cientos dieciocho ($ 16.668). Si el cliente deseaba durante dos meses el padrón nacional completo, con los datos de los 22.713.000 electores, el precio escalaba a cuarenta y cuatro mil quinientos sesenta y ocho ($ 44.568)

Si bien la consulta a estas bases es accesible en tiempos preelectorales, se mantiene en reserva cuando no lo son, aunque se permite conocer los datos si la petición se realiza con patrocinio de abogado y se paga un arancel.

El carácter de archivo público unido a la función que tiene, impide considerar al hábeas data como vía procesal idónea para acceder y solicitar algunas de las pretensiones establecidas en el artículo 43, toda vez que las correcciones que se debieran hacer por actualización o rectificación deben tramitar ante la justicia electoral.

Es diferente la situación de los padrones de afiliados a partidos políticos.

> Los ficheros a que nos referimos –dice Velázquez Bautista- son para los partidos políticos como los ficheros de clientes para una sociedad mercantil. Por ello, elemento esencial en la vida de los partidos, los cuales sin una militancia cohesionada y participativa, registrada en un fichero, perdería gran parte de su potencial convirtiéndose, al menos durante un tiempo, en una fuerza testimonial. Y en función de los recursos y la aceptación del electorado, en un producto presente en la sociedad a través de un gabinete de prensa y relaciones públicas pero con un futuro incierto.

Una ficha de afiliación partidaria suele requerir datos históricos de la persona. Quizá el más importante, más allá de la expresión abierta hacia un dogma, sea el domicilio y no otros como la ocupación u oficio.

La cuestión que se presenta con estos registros es la disponibilidad a terceros de una manifestación que no siempre se pretende hacer pública. Por eso, la cesión del dato a través del potencial informe necesita el consentimiento del afectado. En la ley el dato de filiación y creencia política se considera sensible, al igual que lo estiman otras leyes similares.

> *En España el dato ideológico se considera sensible pues de acuerdo con el Artículo 7 de la ley, son datos especialmente protegidos:*

> *"1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo. 2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. 3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. 4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual".*

Evidentemente, el archivo partidario es público y no debiera ser objeto de cesión o informes a terceros, precisamente por la disponibilidad de los datos. Por tanto, el acceso al mismo es irrestricto, y las pretensiones de actualización, corrección y supresión de datos (sensibles) tramitan por el hábeas data. No así la exclusión del archivo, porqué esa manifestación supone desafiliarse lo cual tiene su carril pertinente.

> En nuestro país, la justicia ha dicho que *las tristes experiencias de persecución ideológica vividas justifican plenamente –a través del hábeas data- la tutela de la información relativa a la filiación política, las creencias religiosas, la militancia gremial, o el desempeño en el ámbito laboral o académico, entre muchos otros datos referidos a la persona titular del derecho, que no corresponde que se encuentren a disposición del público o de ser utilizados por órganos públicos o entes privados, sin derecho alguno que sustente su uso (*CNCiv., Sala H, mayo 19/995, in re Rossetti Serra, Salvador c/ Dun & Brandstreet S.R.L., en Jurisprudencia Argentina, 1995-E, 294).

m) Los registros sociales y culturales

Los archivos o registros de entidades sociales, culturales o deportivas, son de uso estrictamente interno para resolver el acceso a la institución, y posteriormente, mantener informado al adherente sobre actividades y obligaciones emergentes de la asociación.

La calidad de fichero privado que no está destinado a proveer informes, en principio, lo desplaza de la injerencia del hábeas data.

> Se ha dicho que, si el objeto de la acción de hábeas data es tener acceso a la información relativa al peticionante, el retiro de la credencial que lo autorizaba a ingresar al casino militar no es un hecho sobre el que haya que emitir opinión jurisdiccional. Por ello, la denegatoria a la admisión como socio de un club, no se halla incluida dentro de los presupuestos de admisibilidad del hábeas data, *salvo que para tal negativa se haya tenido en cuenta algún dato descalificante o discriminatorio que conste en sus propios archivos*, pero no alcanzan esta categoría ni el listado de socios ni el registro de pago de cuotas (C.Fed. Bahía Blanca, Sala 1ª , enero 18/995, Rev. La Ley, 1996-A, 316)

n) Los archivos profesionales y ocupacionales

Las fuentes de información no necesariamente están ordenadas en bancos o archivos específicos, a veces, el simple ordenamiento de los papeles privados que se reúnen con motivo o en ocasión del trabajo, forman un archivo de datos que, posiblemente, contengan información íntima de las personas a quienes se atiende.

El abogado, el médico, el periodista, entre tantas profesiones y ocupaciones conservan materiales de uso particular que involucra a otros a quienes se debe reserva y confidencialidad.

Probablemente, la sofisticación de estas bases de datos y la penetración de otras fuentes de información mediante sistemas informáticos, termine considerando a estos archivos o ficheros, como "bancos de datos privados", tal como acontece en legislaciones demasiado proteccionistas.

> La vetada ley 24.745 excluye a los registros o bancos mantenidos por personas físicas con fines exclusivamente personales, del mecanismo creado para la salvaguarda de los datos personales.
>
> El inciso e) del artículo 2º dispone también la inaplicabilidad para *los registros o bancos de datos de las personas físicas o jurídicas dedicadas a la actividad periodística por cualquier medio de comunicación social.*

Actualmente, el art. 24 de la ley sostiene: (Archivos, registros o bancos de datos privados): *Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21.*

Sin embargo, el problema no es la formación del archivo sino la transmisión del dato sin el consentimiento de la persona.

Por tanto, la cuestión tiene una dimensión vinculada con la privacidad del fichero personal, que por su calidad se debe incluir en el concepto de "papeles privados" del artículo 18 de la Constitución Nacional; y otra vertiente que refiere a la responsabilidad del profesional que conoce el dato y lo cede a otros sin el consentimiento del concernido.

> Dalla Vía y Basterra opinan que los registros o bancos personales para uso privado no están comprendidos dentro de los registros con posibilidades de acceso; sí estarían comprendidos aquellos bancos de datos de profesionales que puedan tener uso público, y si bien una ley reglamentaria determinará los casos en que es posible el acceso, en definitiva los jueces decidirán en cada caso concreto si es procedente o no la acción.

Bibliografía Capítulo III

Aznar Gómez, Hugo, *Intimidad e información en la sociedad contemporánea,* en "Sobre la intimidad", editorial Fundación Universitaria San Pablo C.E.U., Valencia, 1996.

Bacaria Martrus, Jordi, *El secreto estadístico (contenido jurídico)*, en Revista Informática y Derecho, números 6/7, editorial UNED, Mérida, 1994.

Beltramone, Guillermo – Zabale, Ezequiel, *El Derecho en la era digital –Derecho informático a fin de siglo-*, editorial Juris, Rosario (Argentina), 1997.

Bianchi, Alberto, *Hábeas Data y derecho a la privacidad,* Revista El Derecho, tomo 161 págs. 868 y ss.

Christensen, Eduardo Alberto, *El hábeas data como tutela en el derecho tributario,* en "Libro de Ponencias" del XX Congreso Nacional de Derecho Procesal, celebrado en la ciudad de San Martín de los Andes del 5 al 9 de octubre de 1999.

Concepción Rodríguez, José Luis, *Honor, intimidad e imagen*, editorial Bosch, Barcelona, 1996.

Davara Rodríguez, Miguel Angel, *La protección de datos en Europa*, editorial Universidad Pontificia Comillas, Madrid, 1998.

Dubie, Pedro, *El Hábeas Data Financiero*, comunicación presentada a las Jornadas Internacionales sobre *Defensa de la Intimidad y de los Datos Personales: Hábeas Data*, Universidad de Belgrano 14 y 15 de agosto 2.000

Espinar Vicente, José María, *La primacía del derecho a la información sobre la intimidad y el honor,* en "Estudios sobre el derecho a la intimidad", editorial Tecnos, Madrid, 1992.

Estadella Yuste, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales,* editorial Tecnos, Madrid, 1995.

Fappiano, Oscar Luján, *Hábeas data: Una aproximación a su problemática y a su posible solución normativa,* en "Liber Amicorum" Héctor Fix Zamudio, volumen 1, editorial Secretaría de la Corte Interamericana de Derechos Humanos, San José, Costa Rica, 1998.

García Belaúnde, Domingo, *El Hábeas Data y su configuración normativa (con algunas referencias a la Constitución peruana de 1993),* en Liber Amicorun Héctor Fix Zamudio, volumen I, editorial Secretaría de la Corte Interamericana de Derechos Humanos, San José de Costa Rica, 1998.

Gils Carbó, Alejandra, *Qué dice la ley en otros países* (sobre el hábeas data y la defensa de la privacidad), nota en Revista Viva, Diario Clarín, del 21 de marzo de 1999.

Herrán Ortiz, Ana Isabel, *La violación de la intimidad en la protección de datos personales,* editorial Dykinson, Madrid, 1999.

Jijena Leiva, Manuel, *carta…,* publicada en Boletín Hispanoamericano de Informática y Derecho, ano I nro. 5, Octubre-Noviembre, 1998.

Mill, John S., *On liberty,* editorial Cambridge, 1989.

Perez Luño, Antonio –Losano M.G. y Guerreo Mateus F., *Libertad informática y leyes de protección de datos personales*, en Cuadernos y Debates, editorial Centro de Estudios Constitucionales, Madrid, 1993.

Perez Luño, Antonio, *Ensayos de informática jurídica,* editorial Fontamara, México, 1996.

Pierini, Alicia – Lorences, Valentín – Tornabene, María Inés, *Hábeas Data,* editorial Universidad, Buenos Aires, 1998.

Pinet, Marcel, *Datos públicos o datos a los que puede acceder el público y protección de datos personales*, en "XX Conferencia Internacional de autoridades de protección de datos" (1998), editado por la Agencia de Protección de Datos, Madrid, 1999.

Puccinelli, Oscar Raúl, *El hábeas data en el constitucionalismo indoiberoamericano finisecular,* en *El amparo constitucional*, editorial Depalma, Buenos Aires, 1999.

Sagüés, Néstor Pedro, *Derecho Procesal Constitucional –Acción de Amparo-*, editorial Astrea, Buenos Aires, 1995.

Salom, Javier Aparicio, *Tratamiento de datos de solvencia patrimonial*, en "XX Conferencia Internacional de autoridades de protección de datos" (1998), editado por la Agencia de Protección de Datos, Madrid, 1999.

Sanchez Gonzalez, Santiago, *La libertad de expresión*, editorial Marcial Pons, Madrid, 1992.

Slane, Bruce, *Publicación masiva de registros públicos: una perspectiva Neozelandesa*, en "XX Conferencia Internacional de autoridades de protección de datos" (1998), editado por la Agencia de Protección de Datos, Madrid, 1999.

Tocqueville, Alexis de, *La democracia en América*, editorial Sarpe, Madrid, 1984.

Vázquez Arzaguet, Gabriel A. – Mighetti, Carlos M., *Secreto financiero*, editorial Depalma, Buenos Aires, 1999.

Velázquez Bautista, Rafael, *Protección jurídica de datos personales automatizados*, editorial Colex, Madrid, 1993.

CAPÍTULO IV. Reglas y principios para los bancos de datos

13. Límites constitucionales

El fenómeno actual del *tratamiento de datos* debe ser analizado en consonancia con el tiempo en que transcurre y avizorando el futuro que nos llega, pues el derecho comparado que actualmente se dispone, probablemente, está adecuado a circunstancias y necesidades de cada lugar, y proyectadas, puede ocasionar en otras sociedades una modificación o una interpretación distinta a sus reglas y valores.

En este sentido, es evidente que la era de las comunicaciones que se avecina y constituye hoy una realidad palpable, transforma algunos conceptos y derechos fundamentales. Por ejemplo, la noción de privacidad que tanto espacio dedicamos en los capítulos precedentes, donde la idea de estar solos afinca el derecho individual, personalista y de profundo contenido singular (como derecho de propiedad), es evidente que torna hacia otra inteligencia, por la cual, ese mismo derecho a la soledad se refiere al libre desenvolvimiento de la persona en sus esferas privadas (propia y familiar) y públicas (actuación social y profesional).

Es el cambio que obliga a adecuar las normas y principios fundamentales. No para variar su finalidad, sino para darles posibilidad de eficacia evitando declamaciones que no puedan ser realidades (como tantas existen en nuestra Ley suprema).

> Para Herrán Ortiz, el estudio de los procedimientos idóneos para la defensa de la persona frente a las prácticas abusivas, significa tener que adecuar las esferas de los derechos y libertades fundamentales, como son la intimidad, el honor, la imagen, la libertad de conciencia, entre otros, al fenómeno del tratamiento automatizado de datos personales, que viene a introducir una penetración diferente a la conocida en el reducto de la privacidad.

En consecuencia, pensar que se podrá evitar la inmiscusión informática en el ámbito de lo personal, cuando la práctica cotidiana nos lleva a vivir una sociedad plenamente informatizada, parece una utopía, lo que no impide que se formulen reglas y principios que lleven a la convivencia armónica entre la persona y los medios, y en definitiva, a obrar con sentido preventivo antes que reparador.

> Nos parece que la regulación constitucional del hábeas data tiene dicho sentido garantista que actúa *ex post facto*, cuando la sensación de seguridad debe partir antes de que el conflicto suceda; razón por la cual, la garantía procesal necesita de una Ley de protección de datos que tenga en cuenta lo trabajado en convenciones y tratados internacionales y nuestra particular idiosincrasia.

Por ahora, la interpretación constitucional necesita obrar con elasticidad evitando el aislacionismo tradicional de la jurisprudencia vigente, que continúa atrapada en el concepto de derechos subjetivos, propios e intangibles, que eluden el compromiso con la sociedad donde está inserta.

> Testimonia el proceso de amparo ese concepto egoísta que atiende, únicamente, el derecho socavado con manifiesta arbitrariedad y que repara, solamente, el hecho lesivo provocado, pese a la promesa que encierra el párrafo constitucional cuando permite proceder esta vía frente a las amenazas.

En esta materia, la tutela de la intimidad amenazada o violada por el uso de datos personales, no tiene en la Norma Fundamental respuestas suficientes.

La reglamentación del artículo 43 genera un marco procesal que evita el reduccionismo del amparo (por lo cual, no puede considerarse al hábeas data como un subtipo de este proceso constitucional),

consagrando una vía rápida de tipo sumarísima que facilita con holgura actuar en los términos como se la emplaza (tal como lo vino permitiendo alguna jurisprudencia).

El artículo 18 ha de ampliar la idea tuitiva para los papeles privados y la correspondencia particular; y los tratados y convenciones internacionales que se incorporan a la Constitución señalar el rumbo para una defensa efectiva de los derechos humanos.

En suma, la supremacía de los derechos y garantías que de la Constitución emana, lleva a fundamentar una serie de reglas y otra de principios sobre los cuales se desenvuelva el uso de los datos personales.

> La ley francesa (nº 78 del 6 de enero de 1978) establece en el artículo 1º que: "*La informática debe estar al servicio de cada ciudadano. Su desarrollo debe desenvolverse en el marco de la cooperación internacional. No debe afectar la identidad humana ni los derechos humanos, ni la vida privada, ni las libertades individuales o públicas"*
>
> *"Ninguna decisión judicial, que implicara apreciación en cuanto al comportamiento humano, podrá tener por fundamento la definición del perfil o de la personalidad del interesado dada por un sistema automatizado de informaciones…"*(art. 2º, aplicado con idéntico sentido a las decisiones administrativas y privadas)

La dignidad humana puede instalarse como punto de partida, para ocupar derechos como la identidad, el honor, la imagen, la reputación personal, y el derecho a que la vida privada no sea alterada por invasiones informáticas no queridas.

Cuando el consentimiento para el uso de los datos no sea manifiesto, el principio a rescatar será el denominado por otras legislaciones como "autodeterminación informativa", base del proceso de hábeas data que facilita el acceso al banco de datos y permite formular las pretensiones consecuentes.

> Explica Casallo López que el consentimiento o "autodeterminación informativa" debe considerarse como un principio general, ya que toda norma tiene excepciones. Esto significa que el titular del dato es el que debe dar su consentimiento para que el mismo pueda ser recogido y transferido a un tercero: sin el consentimiento expreso del interesado ninguno de sus datos personales puede ser tocado. Más aún, para que ese consentimiento sea válidamente emitido tiene que ser libre y, fundamentalmente, suficientemente informado por el titular, porque si carece de la necesaria información el sujeto puede estar consintiendo algo que desconoce y automáticamente nos hallaríamos ante un consentimiento nulo, o viciado de nulidad.

Con esta plataforma, ensanchada por la tutela amplia al derecho de intimidad, la persona ha de promover sus derechos a la información (a saber si está en la base de datos y para qué fines fue almacenado); a la privacidad (persiguiendo la eliminación de fastidios directos o indirectos a su vida familiar y personal); a exigir que los datos consignados sean fehacientes y veraces; y a ejercer un control activo sobre los archivos que le conciernen.

Los principios se basan, en consecuencia, en la libre determinación de las personas para resolver por sí mismas el estar en una base de datos y autorizar el uso de esa información a terceros.

Ahora bien, como es fácil suponer, en un mundo sin fronteras como representa la globalidad informática, resulta prácticamente imposible saber cuándo, dónde y cómo se archivan y colectan nuestros datos, problemas que se deben arreglar sobre la base de reglas que los bancos o archivos han de cumplimentar, bajo estrictas y severas penas por su incumplimiento.

De igual manera, el derecho a ejercer una industria lícita, como es el relevamiento informático de datos, y comerciar con ellos no puede observarse como una actividad a contrarrestar, teniendo en cuenta que la misma reporta múltiples utilidades, bien conocidas en la sociedad de la información.

> Por eso, Herrán Ortiz dice que no habría ningún obstáculo jurídico que pueda imponerse al establecimiento o constitución de empresas cuyo objeto o fin social se encuentre en la explotación mercantil o utilización de bases de datos. Por tanto, se alza en límite para el desarrollo y regulación legal del derecho a la autodeterminación informativa el derecho a la libertad de empresa, en tanto que no le estaría permitido al legislador restringir el uso de la informática hasta el punto de prohibir o impedir la constitución de empresas cuyo fin consista en la creación y explotación de bases de datos personales.

14. Límites legales

La implementación de bancos de datos con archivos personales es un fenómeno difícil de impedir, de modo tal que, al menos, deben fijarse límites para su operatividad.

El primer aspecto a considerar es la creación del archivo, y el potencial control que sobre él se puede ejercer.

El segundo, ha de establecer las reglas para autorizar su funcionamiento y fijar los derechos que tengan las personas para acceder y conocer las finalidades que tiene el almacenamiento de sus datos.

El tercer problema se refiere a los principios que debe respetar el banco de datos para la guarda, recuperación, conservación, secreto y seguridad de la información que contiene.

> La Lortad (reformada a fines del año 1999) agrupa en dos grandes apartados los principios fundamentales para la protección de los datos. El primero de ellos –expone López Muñiz- es el grupo de derechos que corresponden al sujeto de datos y que son los siguientes: a) el del consentimiento, previo a la incorporación a un fichero de los datos personales; b) el derecho de información, que corresponde al conocimiento de lo que realmente existe o se ha incorporado al fichero; c) el derecho de acceso, o comprobación por el interesado, de una forma periódica, de lo que se mantiene en el fichero; d) el derecho de rectificación, para que los datos incorporados a un fichero sean exactos; e) el derecho a la veracidad de los datos, es decir, que los de carácter personal incorporados a un fichero deben actualizarse para que permanezcan acordes con la realidad; f) el derecho de indemnización de los perjuicios que pueden ocasionarse por el uso indebido de la informática.
>
> El segundo grupo es el conjunto de principios relacionados con el propio fichero que contiene los datos personales. Aquí podemos considerar: a) el principio de legalidad en la captación de los datos; b) el principio de unicidad, o la necesidad de que los datos captados respondan a la finalidad del fichero, sin que puedan difundirse o tratarse fuera de esa finalidad; c) el principio de la adecuación, según el cual los datos recogidos, serán los pertinentes y no excesivos, teniendo en cuenta la finalidad del archivo; d) el principio de caducidad, que exige que los datos incorporados a un fichero no se conservarán en el mismo más tiempo que el necesario para cumplir su finalidad; e) el principio de seguridad, tanto informática como general, para garantizar la conservación de los datos y la no revelación de los mismos salvo dentro de la finalidad del fichero.

El Capítulo II de la ley reglamentaria establece el princio de la inscripción para considerar legal el registro de datos personales.

Inmediatamente, enumera y establece los requisitos que los archivos deben cumplimentar: a) Calidad de los datos; b) Consentimiento; c) Información; d) Datos sensibles, estadísticos, científicos, relativos a la salud y de antecedentes penales y/o contravencionales (clasificación de los datos), e) Confidencialidad y f) Cesión y transmisión internacional.

14.1 Reglas para la creación de archivos

Tanto la Resolución de la Asamblea General de la O.N.U. adoptada en la sesión 45ª sobre "*Directivas para la regulación de ficheros automáticos de datos personales"* (Doc. A/Res.45/95 del 29.1.91*), como las instrucciones del Parlamento Europeo y del Consejo de la Comunidad Económica que dieron lugar, el 25 de octubre de 1995, a la *"Directiva 95/46/CE"*, se preocupan por establecer una suerte de reglas para la creación de archivos que contendrán datos de carácter personal.

En líneas muy generales, se parte de considerar, antes que la autorización para funcionar, los principios que cada fichero debe cumplir para actuar con legitimación suficiente.

La legalidad se establece para cada etapa que tiene el tratamiento de los datos, es decir: a) la recolección o toma de información personal; b) el intercambio de datos que supone, tanto la transmisión a terceros, como la interrelación o "data mining"; c) la cesión propiamente dicha, y d) el control interno y externo del archivo.

> Todas las leyes de protección de datos que tiene Estados Unidos de América como las desarrolladas por los Estados miembros de la Unión Europea, recogen la idea del Convenio 108 del Consejo de Europa *, por el cual se crean principios básicos para la protección de la persona a quien se concierne con la recolección y tratamiento de sus datos; dejando que el archivo o fichero se origine sin demasiadas reglas mientras respete dichos principios.
>
> Estos, al decir de Davara Rodríguez, se pueden resumir en los de legalidad y lealtad al recabar los datos, al tratarlos, al utilizar el resultado de su tratamiento y al, en su caso, cederlos a terceros, y los de pertinencia y adecuación al fin y secreto del responsable, complementados con los derechos de información, acceso, rectificación y cancelación, que se constituyen en una constante en el articulado de las diferentes normas.

De alguna manera, es una decisión prudente que no ha soslayado la notoria dificultad de establecer reglas para la creación de archivos que se originan constantemente con finalidades diversas.

Por ejemplo, Internet moviliza un flujo constante de información entre millones de usuarios por día, que acceden a bases de datos diferentes que no tienen control directo ni frontera reconocida. Obviamente, el sitio se origina como un producto y la página informa con reglas similares a las de la tradicional compraventa (v.gr.: comercio electrónico).

> La naturaleza sin fronteras de Internet –según Manganelli- contrasta claramente con el enfoque proteccionista o localista adoptado, por la mayoría de los países, en la pertinente normativa. Existen barreras legales que se derivan tanto de los diferentes códigos comerciales (como la responsabilidad de las partes interesadas) y de las leyes de protección de la intimidad, de propiedad intelectual y de censura. Debido a la ausencia de reglas internacionales, se han implantado con frecuencia "criterios de jurisdicción local" –reglas, criterios y conceptos legales- que por estar muy relacionados con el mundo real no encuadran adecuadamente al entorno virtual de la red.

Precisamente, la diversidad normativa, la imposibilidad concreta de establecer reglas comunes para un sistema enlazado mundialmente, y las diferencias notables entre continentes para ocuparse en armonía del complejo tema de los bancos de datos, lleva a un problema interno que no es fácil resolver.

Cada país tiende a dictar leyes de protección de datos personales que se automatizan para ingresar en una cadena intangible de archivos, fuentes de información y carriles de comunicación, que en la aplicación concreta, legislan para el lugar donde la persona se considera afectada (en los hechos, la jurisdicción local que tiene el archivo que lo registra), sin atender que el fenómeno está en la necesidad de armonizar y, de ser posible, unificar con reglas y principios, el funcionamiento de estos bancos de datos.

> Comprar y vender datos personales puede ser un gran negocio en América, pero es por demás dificultoso en Europa, porqué la Directiva sobre protección de datos pone mucho cuidado en evitar la transferencia entre fronteras de datos personales de consumidores, a menos que ese país haya dado los pasos oportunos para garantizar que los datos personales continúen siendo privados. En Estados

Unidos, ni la "*Electronic Comunications Privacy Act"* * de 1986, ni la "*Computer matching and privacy proteccion act"* * de 1988, han resuelto la dificultad de mantener intangible a la persona.

Por otra parte, bien apunta Manganelli cuando dice que "los europeos no se acercan, de ninguna forma, a la información que, acerca de sus administraciones públicas, disfrutan los estadounidenses a través de su administración y leyes protectoras de la libertad de información, tan abiertas y valiosas. También aceptan los estadounidenses mucha más intrusión de las administraciones públicas en sus vidas, a menudo sin rechistar".

En nuestro país, siguiendo el modelo español, la creación de archivos y el control sobre ellos, fue previsto en un organismo especialmente destinado al efecto, pero fue resistido en el veto presidencial (Decreto 1616/96 *) por las atribuciones que se le confería.

El artículo 20 de la ley española dispone para los ficheros públicos:

"Creación, modificación o supresión"*: 1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente. 2. Las disposiciones de creación o de modificación de ficheros deberán indicar: a) La finalidad del fichero y los usos previstos para el mismo. b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos. c) El procedimiento de recogida de los datos de carácter personal. d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo. e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros. f) Los órganos de las Administraciones responsables del fichero. g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición. h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible. 3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción"*.

En España se distingue entre ficheros públicos y privados, pues a estos últimos se los autoriza cuando contengan datos de carácter personal que resulten necesarios para el logro de la actividad y cumplan la finalidad prevista para su origen.

Actualmente, el artículo 3º establece*:*

"La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la ley y las reglamentaciones que se dicten en su consecuencia.

"Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública"

14.2 Reglas para el funcionamiento del archivo

La distinción entre archivos públicos y privados, antes que una razón metodológica, es una necesidad que surge del control efectivo que sobre ellos se puede concretar. Mientras los primeros responden al principio del acceso sin interferencias y de la transmisión de datos con libertad; el segundo tiene mayores dificultades para la fiscalización en cualquiera de sus etapas (creación, tratamiento y cesión de la información compilada), circunstancias que motivan el establecimiento de reglas comunes pensadas en dos cuestiones esenciales: a) los derechos de las personas, y b) las obligaciones del archivo.

La exposición de motivos de la Lortad (actualmente derogada, pero vigente en lo que respecta a este comentario) dice: "…Con la pretensión de evitar una perniciosa burocratización, la Ley ha desechado el establecimiento de supuestos

como la autorización previa o la inscripción constitutiva en un registro. Simultáneamente, ha establecido regímenes diferenciados para los ficheros en razón de su titularidad, toda vez que, con toda evidencia, resulta más problemático el control sobre la titularidad privada que el de aquellos de titularidad pública. En efecto, en lo relativo a estos últimos, no basta la mera voluntad del responsable del fichero sino que es precisa norma habilitante, naturalmente pública y sometida al control jurisdiccional, para crearlos y explotarlos, siendo en estos supuestos el informe previo del órgano de tutela el cauce idóneo para controlar la adecuación de la explotación a las exigencias legales y recomendar, en su caso, las medidas pertinentes".

Los derechos de las personas asientan en los siguientes principios:

a) Toda persona física debe prestar consentimiento expreso para que sus datos personales sean incorporados a un banco de datos. No existe voluntad presunta.

b) Toda persona que se considere afectada por el almacenamiento de sus datos tiene derecho a saber las razones por las cuales ellos fueron registrados.

c) Se debe asegurar el derecho de acceder a los bancos de datos como una proyección del derecho a la información y en salvaguarda del derecho a la privacidad, para que sea el mismo afectado quien resuelva sobre el destino de sus datos personales.

d) En tal sentido, y como consecuencia del principio anterior, se debe asegurar el control sobre el archivo con el fin de mantener la exactitud de los datos, o en su caso, requerir la actualización o corrección de la información errónea o desactualizada.

e) Toda persona tiene derecho a exigir restricción para transmitir sus datos personales.

f) Toda persona puede solicitar, como derecho al secreto, que sus datos más íntimos se reserven y mantengan en la confidencialidad del archivo, o en su caso, exigir la supresión.

g) El afectado podrá solicitar una reparación pecuniaria cuando los datos personales que se registraron sin consentimiento, y se transmitan a terceros, le cause un perjuicio cierto.

Los archivos, por su parte, deben cumplir con las siguientes obligaciones:

a) La acumulación de datos personales debe estar autorizada por la persona concernida y limitado a los que sean congruentes con el fin para el que el archivo fue creado.

b) La pertinencia de los datos personales responde al principio de *unicidad*, por el cual, se establece la buena fe en la recolección y el destino adecuado a la finalidad del banco de datos.

c) No se podrán archivar ni registrar datos que no sean proporcionados por la parte y afecten su derecho a la intimidad (datos sensibles).

d) La calidad del registro supone la obligación de mantener actualizada la base de datos, y de expurgar la información que haya caducado (supresión de oficio del dato, o derecho al olvido).

e) Es deber del titular del registro mantener la confidencialidad y secreto de la información que almacena, debiendo cederla únicamente en los supuestos expresamente autorizados por la ley o el particular afectado.

f) Toda base de datos debe ser segura y secreta, debiendo el titular proteger la información, evitando por los medios que fueran, toda invasión o penetración ilegítima.

Según Puccinelli, las primeras normas europeas sobre datos personales contienen diez principios comunes, los cuales fueron calcados por la Constitución de Río Negro *, al regular el hábeas data: a) el de justificación social, según el cual la recolección de datos debe tener un propósito general y usos específicos socialmente aceptables; b) el de limitación de la recolección, el cual estatuye que los datos deben ser obtenidos por medios lícitos, es decir, con el conocimiento y

consentimiento del sujeto de los datos o con autorización legal, y limitarse al mínimo necesario para alcanzar el fin perseguido por la recolección; c) el de calidad o fidelidad de la información, que implica la obligación de conservar los datos exactos, completos y actuales; d) el de especificación del propósito o la finalidad, para que los datos no sean usados con fines diferentes; e) el de confidencialidad, conforme al cual el acceso de terceros a los datos debe tener lugar con el consentimiento del sujeto o con autorización legal; f) el de salvaguarda de la seguridad, por el cual el responsable del registro de datos personales debe adoptar medidas adecuadas para protegerlos contra posibles pérdidas, destrucciones o acceso no autorizado; g) el de política de apertura, que implica asegurar el conocimiento, por parte del público, de la existencia, fines, usos y métodos de operación de los registros de datos personales; h) el de limitación en el tiempo, que entraña su conservación hasta que sean alcanzados los fines perseguidos; I) el de control público, que implica la necesaria existencia de un organismo responsable de la efectividad de los principios contenidos en la legislación; j) el de participación individual, que consagra el derecho de acceso a los datos y los derechos conexos.

Actualmente el artículo 21 establece:

"1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.

"2. El registro de archivos de datos debe comprender como mínimo la siguiente información:

a) Nombre y domicilio del responsable;

b) Características y finalidad del archivo;

c) Naturaleza de los datos personales contenidos en cada archivo;

d) Forma de recolección y actualización de los datos;

e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;

f) Modo de interrelacionar la información registrada;

g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;

h) Tiempo de conservación de los datos;

i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

3) Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro.

El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el Capítulo VI de la presente ley.

14.3 Reglas para el control del archivo

El cumplimiento de las reglas y principios para el funcionamiento de los archivos se deja en manos de un organismo creado a tal efecto. Al menos es el temperamento adoptado por el derecho europeo, y que ha seguido nuestra ley reglamentaria, tal como lo hicieron buena parte de los proyectos de hábeas data existentes en Argentina *.

Alemania (Ley de Hesse que refiere referencia a un Comisario para la protección de datos, actualmente suplantado por cuatro funcionarios: Delegado federal para la protección de datos, Comisarios encargados, funcionarios particulares y consejos locales y regionales); Austria (Comisión para la protección de datos; y Consejo para la protección de datos); Bélgica (Comisión para la protección de la vida privada); Dinamarca (Autoridad de vigilancia de registros); España (Agencia de protección de datos); Francia (Comisión Nacional de la Informática y las libertades); Finlandia (Comisión de protección de datos); Gran Bretaña (con dos órganos, el Tribunal de protección de datos y el Registro para la protección de datos); Holanda (Cámara de registros); Italia (Garante para la tutela y el respeto del tratamiento de datos personales); Luxemburgo (Comisión consultiva sobre protección de datos); Portugal (Comisión Nacional para la protección del Tratamiento automatizado de datos); Suecia (Consejo de inspección de datos)

Esta fiscalización no impide el acceso a la justicia, que es el modelo americano de la denominada "Ley de privacidad" del 31 de diciembre de 1974*.

La vigilancia a través de una agencia particular de derecho público permite auspiciar funciones de relevancia para la eficacia de la tutela prometida.

Entre ellas se pueden mencionar, el efectuar un relevamiento (censo) de archivos públicos y privados destinados a brindar información; establecer un marco normativo apropiado para la defensa del derecho a la privacidad amenazada por el fenómeno informático; crear un código ético entre los bancos registrados (de carácter obligatorio) y no registrados (aplicado en sede judicial); emitir instrucciones para dotar de seguridad a los archivos, entre otras misiones que se pueden cumplir.

El artículo 29 de la ley establece (órgano de control): " 1. *El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:*

a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;

b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;

c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;

d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley;

e) Solicitar información a las entidades públicas y privadas, las wue deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos de carácter personal que se le requieran;

f) Imponer las sanciones administrativas que se dicten en consecuencia;

g) Constituirse en querellante en las acciones penales que se promovieren por violaciones a la presente ley;

Los incisos 2 y 3 fueron vetados por el Decreto nª 995/2000

2. El órgano de control gozará de autarquía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia de la Nación.

3. El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el poder ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia.

El Director tendrá dedicación exclusiva en función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones, incapacidad sobreviniente o condena por delito doloso.

El Director como así también el resto del personal están obligados a guardar secreto de los datos de carácter personal que conozcan en el desarrollo de su función.

La Fiscalía Nacional de Investigaciones Administrativas, a través de un Fiscal General competente en la materia, podrá ejercer las facultades previstas en el art. 45 de la Ley 24.946 respecto de la observancia de la presente por parte de todos los archivos, registros y bancos de datos públicos. Dictaminará en los asuntos de importancia sometidos a consideración del Director; en los casos en que se haya denegado el acceso o rectificación de datos invocando las causales del art. 17 incisos 1 y 2 su intervención será obligatoria".

A su vez, el afectado por la información archivada (afectación que puede ser directa o indirecta) tendrá disponibles los mecanismos procesales tradicionales como el reclamo administrativo y la demanda judicial de hábeas data con las modalidades de pretensión que menciona el artículo 43, constitucional y a través de la vía administrativa consagrada en el art. 14 y la tutela judicial conferida por la reglamentación en los arts. 33 y siguientes.

Es conveniente, no obstante, tener en cuenta que el control no puede estar disperso. En España, el gobierno de Cataluña denunció la inconstitucionalidad de la Ley Orgánica 5/92 en relación con la distribución de competencias, porque afirmó que la distinción entre ficheros de titularidad pública, controlados por la misma administración del registro; y los ficheros de titularidad privada que quedan en la órbita de la Agencia de protección de datos, no atendía que la gestión de los archivos no era un criterio legal para la asignación de competencias, porqué la ley se debe cumplir y hacer respetar por las autoridades locales donde el archivo se encuentra. (Criterio difícil de cumplir con los archivos virtuales como Internet).

15. Principios aplicables al archivo

Los principios deben diferenciarse de las obligaciones, pues mientras los primeros hacen al conjunto reglas que determinan la legalidad del archivo; los segundos refieren a los deberes que debe cumplir el titular y el administrador del registro en cualquiera de las etapas (recolección, procesamiento y cesión).

Es importante acotar, antes de seguir con los principios y responsabilidades, que las obligaciones son del archivo en sí, y no de la persona que los administra. El titular del archivo puede ser una persona física o jurídica, de carácter público o privado, mientras que el administrador de los datos, necesariamente, ha de ser una persona física.

Además, el criterio de legalidad se impone interpretarlo como defensa de los derechos de todas las personas (y no por la mera inscripción del archivo en un registro que los ordene y clasifique a los fines del control subsiguiente), de manera que la protección que se ofrece desde el cumplimiento de cada uno de los principios, reporta a la idea de asegurar que los datos se mantengan en el registro sin afectar la libertad de intimidad de cada concernido.

Por su parte, cada individuo tiene derechos contra el banco de datos y acciones posibles para entablar.

En síntesis, son normas mínimas que fundamentan la legalidad del archivo, pero que no impiden a cada Estado que reglamente la tutela de los datos personales, ampliarlos con sus disposiciones internas.

El fin inmediato de cada principio es asignar un valor preferencial al dogma establecido, pensando que con ello se afianza el respeto por los derechos individuales, al mismo tiempo que se instrumenta un mecanismo procesal (hábeas data) que limita el abuso informático.

> Por eso, agrega Herrán Ortiz, la normativa en materia de protección de datos debe conformar sus medidas e instrumentos de limitación del uso de la informática en atención a los objetivos de garantía y respeto de los derechos de la persona; así, se debe instaurar un conjunto de medidas que sean apropiadas, prácticas, reales y proporcionadas al objeto que se pretende salvaguardar, que no es otro que la "privacidad" de individuo y los demás derechos de las personas. De igual manera, la configuración de las fronteras a que debe circunscribirse la utilización informática de los datos personales no debe consistir en imprecisas e indeterminadas medidas jurídicas que imposibiliten su efectiva aplicación y dificulten la consecución del fin perseguido.

Obvio resulta que la protección a los datos no supone la represión del desarrollo informático, ni levantar vallas contra la creación de archivos, bases, bancos o registros que tengan una finalidad útil que los fundamente.

Se trata, nada más, que establecer una suerte de indicadores o referencias; un marco de orientación del cual tomar un mínimo de requisitos; en definitiva, son principios básicos que no pueden estar ausentes en la constitución y desarrollo de cualquier archivo.

La legislación comparada suele colocar a este conjunto en torno de un sólo principio que es el de "*calidad de los datos"*, reposando la obligación antes que en el archivo, en el producto logrado.

El art. 4 (Calidad de los datos) de la ley dice:

"1.- Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para las que se hubieren obtenido.

"2.- La recolección de datos no podrá hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

"3.- Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

"4.- Los datos serán exactos y deben actualizarse en el caso que ello fuere necesario.

"5.- Los datos total o parcialmente inexactos, o que sean incompletos, deben ser cancelados y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.

"6.- Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

"7.- Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recabados".

La ley española califica como *adecuados y pertinentes* los datos que se almacenan respondiendo a la finalidad y ámbito del fichero, agregando que tampoco podrán ser *excesivos en relación* con la causa *explícita y legítima para las que se hayan obtenido.*

Los principios son:

15.1) Principio de legalidad

Como antes señalamos, el art. 4 de la reglamentación acordada al art. 43 constitucional dispone que la formación de archivos es lícita cuando se encuentran debidamente inscriptos; esto supone, entonces, que ante la posibilidad de revisar al tiempo de la presentación los fines y objetivos de los bancos de datos y de contar con la autorización pertinente, se tiene una presunción de legalidad por el sólo hecho del control de funcionamiento otorgado.

Por este principio, además, se establecen algunas reglas básicas:

1) Licitud en la recolección de datos (art. 4º inciso 1º; art. 5º inciso 1º)
2) Buena fe en la búsqueda de información, como en las etapas sucesivas de almacenamiento, tratamiento, interconexión, cesión y transferencia (art. 4º inciso 2º);
3) Lealtad hacia la persona que resulta concernida (art. 4º inciso 3º);
4) Participación del individuo en la incorporación al banco de datos (cuando fuese pertinente requerir autorización y consentimiento para tomar sus datos personales) (art. 5 inciso 1º);
5) Exclusión inmediata de los datos sensibles (art. 7 inciso 1º).

Cada uno tiene un requisito particular a cumplir, y en conjunto representa la justificación del archivo contra eventuales acciones que le atribuya abuso o intromisiones ilegítimas.

Ahora bien, ¿es suficiente cumplir cada aspecto reglado para aceptar socialmente al archivo?, ¿basta encuadrar y ajustarse a cada uno de las reglas para ampararse en un marco legal dispuesto?.

Responder estos planteos obliga a considerar cada uno de los puntos puestos como exigencias.

Por ejemplo, *licitud en la recolección de datos* supone que las acciones emprendidas para la obtención de informaciones personales han dado cumplimiento a una pauta general de buena fe y lealtad hacia las personas interesadas.

> "Se prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos", indica la Ley de protección de datos española. Mientras que la *Data proteccion act* (Gran Bretaña) dice que "la información contenida en la data personal deberá ser obtenida y deberá ser procesada en forma justa y de acuerdo a la ley", para agregar más adelante –según expone Uicich- que "al determinar si la información se obtuvo de manera justa, se deberá tener cuidado en el método por el cual se obtuvo, incluyendo en particular si cualquier persona a través de la cual se haya obtenido dicha información haya sido engañada o confundida en cuanto al propósito o propósitos para lo cual se ha poseído, usado o revelado dicha información. Se considera que una información ha sido obtenida en forma justa si se ha alcanzado a través de una persona que sea autorizada por o bajo cualquier estatuto o por algún convenio u otro instrumento que imponga una obligación internacional en el Reino Unido; y para dicho proceso no se considerará ninguna revelación de la información que se autorice o requiera por o bajo cualquier ley o requerida por tal convenio u otro instrumento mencionado anteriormente"

La toma de información puede ser *directa* y lograda del mismo interesado en aportarla; o *indirecta* y obtenida por adquisición o penetración en la intimidad de una persona.

En el primer supuesto, la buena fe se demuestra con la información dada a las personas para que sepan que los datos que aportan serán incorporados a una base de datos. La ocultación, el engaño, la apariencia, el sigilo, o cualquier otra maniobra elusiva de la verdad, será causa suficiente para advertir la deslealtad y penar al archivo por este comportamiento.

Por eso, el artículo 5º establece que *"1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso o informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias…".*

La nueva ley española de protección de datos, establece con la finalidad de informar adecuadamente al interesado, una serie de requisitos a cumplir en la toma de datos. Dice el artículo 5 (*Derecho de información en la recogida de datos)*

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y

de la identidad del responsable del tratamiento así como de los derechos que le asisten".

En el caso de intercepción de datos, la ilegalidad es inmediata, salvo en supuestos donde se obtengan de fuentes accesibles al público, o se recojan para el ejercicio de funciones propias de la administración pública en el ámbito de sus competencias, o bien, se refieran a personas vinculadas por un negocio jurídico, una relación administrativa y sean necesarias para el mantenimiento de las relaciones o para el cumplimiento del contrato.

> En el derecho argentino la invasión a través de sistemas informáticos no está penada, pero puede significar una clara intromisión ilegítima en los derechos de las personas. La conducta de ingresar a un sistema de información o programa, sin autorización, es decir, violando los medios de control establecidos para su acceso, se denomina *hacking* y el agente que la lleva a cabo *hacker*, cuyos objetivos pueden ser diversos, tales como copiar información, destruir archivos, cambiar su contenido, simplemente ver el mismo, o sortear el mecanismo de seguridad en sí mismo. Así lo afirma Galíndez, quien agrega que, sin desconocer los beneficios que la tecnología puede proporcionar, el tratamiento computarizado de la información puede llegar a constituir una invasión a la privacidad, tal como ocurre cuando un particular ingresa en la base de datos de una Universidad y toma de su servidor información que no está disponible al público. Lo mismo puede suceder con las personas, afectando su intimidad.

Buena fe y lealtad, reglas indicadas en los numerales dos y tres antes dichos, se asocian al de legalidad en la medida que se considera ilegítima (ilegal) la apropiación de datos obtenidos con prácticas engañosas (por ejemplo, grabando conversaciones, interceptando comunicaciones telefónicas, penetrando en archivos informáticos, etc.) u hostiles (V.gr.: violencia en los medios utilizados para lograr la información; seguimiento de la vida privada; etc.).

Cuando se piden datos, es necesario informar para qué se solicitan, donde se archivarán y el destino pensado para ellos. Eso es *lealtad hacia la persona concernida*; no obstante, buena parte de los bancos o registros privados se nutren con información indirecta, por el sistema de interconexión o tratamiento de las bases, logrando resultados sorprendentes que depuran al máximo los datos hasta llegar a la individualización de las personas.

> En España, afirma Estadella Yuste, las únicas excepciones que se pueden admitir para no informar, se dan cuando la autoridad nacional considera que, por razones muy concretas –por ejemplo, en actividades de investigación criminal-, no es apropiado que el afectado conozca la recogida de datos.

La forma prevista para detener estas actitudes producidas por el impacto informático se basan en el *principio de limitación* que otros refieren. Esta regla previene la recolección ilegítima y pone trabas al archivo de los llamados "datos sensibles".

> El principio de limitación está íntimamente ligado al de legalidad y es casi una consecuencia lógica del mismo en su aspecto negativo. El objetivo que se persigue –dice Estadella Yuste- es evitar la creación o existencia de ficheros con datos de carácter personal elaborados de forma arbitraria, y sin un objetivo específico para impedir su transmisión internacional. El principio de limitación no prohibe la recogida, el almacenamiento o el procesamiento de datos, sino que simplemente establece márgenes temporales y cuantitativos.

Algunas veces, la petición de datos requiere la *participación de las personas.* Es el recaudo previsto idealmente en buena parte de los ordenamientos jurídicos como autorización expresa que se otorga al archivo para registrar informaciones personales y permitir su circulación.

El consentimiento en la entrega de información personal depende, muchas veces, de la naturaleza del requerimiento. Puede ser obligatorio (por ejemplo, censo poblacional) o voluntario (V.gr.: encuesta de

hogares), y a veces, puede el interesado negar su voluntad de colaboración o apoyarla expresamente suscribiendo un documento de aceptación.

Son modalidades que asumen con variables de procedimiento las distintas agencias de protección de datos.

15.2) Principio de finalidad

Finalidad se relaciona con pertinencia, por eso suele llamarse a este principio con cualquiera de ambas referencias. En las dos, significa que el archivo esta autorizado para registrar datos solamente en la actividad prevista al tiempo de su creación.

A veces, se denomina "*principio de unicidad*" por el cual se entiende que, finalidad exige conocer desde el primer momento las razones por las que se recaban datos, justificándose así la necesidad de obtener y procesar algún tipo de información sensible.

El art. 4º inciso 3º especifica que: *"Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención"*

> Las excepciones autorizadas se llaman "cláusulas humanitarias", y permiten al archivo tomar datos personales de carácter sensible cuando el propósito sea la protección de derechos humanos o libertades fundamentales, o en su caso, la asistencia humanitaria.
>
> Según Estadella Yuste, hay directrices que también reconocen excepciones cuando están implicados temas de soberanía, seguridad nacional y orden público, aun cuando se exige que estas excepciones sean las mínimas posibles y que se pongan al conocimiento del público.

Este principio se relaciona con el anterior en cuanto a los límites que fija para la recolección y la conservación de los datos en el banco creado.

En efecto, ningún archivo puede colectar datos que no estén vinculados con el fin que persigue su objeto, y de serlo, surge un nuevo impedimento para la interconexión en la medida que está prohibido desviar la información de su propósito original.

Asimismo, la permanencia del dato en la base debe estar relacionada con los motivos del registro, y mantenerse en él hasta que el mismo se alcance.

Tal es el objetivo del art. 4º inciso 7º al establecer que: *"Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido colectados"*.

15.3) Principio de congruencia

Todo dato debe ser congruente con las finalidades que se buscan al archivarlo. Se trata de bosquejar una suerte de adecuación material y objetiva según la cual cada registro debe colectar y trabajar sin variar los fines de su creación.

Sin embargo, entendemos que es bastante difícil dar cumplimiento a este principio, porqué los datos informatizados se suelen buscar y clasificar aleatoriamente.

> Es de esperar que reglamentariamente –dice López Muñiz- se establezca qué criterios van a imponerse en este terreno, ya que es lógico pensar que deban especificarse los campos que compongan cada registro, y cuáles de ellos van a ser los que sirvan como elemento de recuperación. Igualmente se espera que deberán constar en la Agencia de Protección de Datos los sistemas de recuperación de la información.

También se nomina a esta regla como "*principio de proporcionalidad*", con la idea de colegir que los datos no deben ser más de los necesarios para la información que persiguen. Vinculado, claro está, al principio de limitación anterior.

> Esta solución parece postular –en el pensamiento de Estadella Yuste- en favor de la existencia de datos inofensivos que se conservan en el fichero mientras no se apliquen al fin buscado; pero puede resultar peligroso, ya que al almacenar datos personales sin un objetivo concreto puede facilitar que, en un futuro, se establezca un nexo identificador que permita utilizar la información para finalidades diferentes de las que existían originariamente.

En nuestra opinión, todo el conjunto hasta aquí expuesto, y que puede nomenclarse como de "*calidad de los datos*" (legalidad, finalidad y pertinencia), no responde más que a un postulado ideal que puede ser muy difícil de llevarlo a cabo.

El interés comercial en los datos personales es un atractivo creciente que moviliza sumas millonarias. El negocio de adquisición difiere de la tradicional compraventa y, a veces, solo se trata de un pasaporte de entrada (*password*) o un código cifrado que abre las puertas a un mundo magnífico de información generalizada que no reconoce fronteras.

Del mismo modo, el problema se plantea cuando se trata de resolver la ley aplicable. ¿O son acaso estos principios reclamados en el reducto donde se localiza el archivo?. Pareciera urgir, como lo veremos más adelante, la necesidad de crear una especie de *Código Mundial* o *principios éticos* donde han de abrevar los operadores de bancos de datos.

> Para Marcel Pinet, sería vano creer que se podría combatir una tendencia tan irreversible como la del interés comercial por los datos, es decir, el valor por el que pueden ser comercializados, mediante la creación de un principio que prohibiera el uso de estos datos para hacer propaganda comercial. Aquellos países en los que los operadores de mercado no pueden acceder a las fuentes de datos si no cumplen ciertas condiciones, tienen que admitir su derrota; los operadores de mercados compran datos personales de forma ilegal.
>
> Por eso, propone un nuevo principio al que llama de "*realidad"* que significa que también tenemos que darnos cuenta de que el uso excesivo de los datos personales para propósitos comerciales incita a poner restricciones en los datos personales que se encuentran al alcance del público.

El compromiso de los bancos de información debiera sustentarse, básicamente, en la legalidad y necesidad, según los cuales, la operatoria de búsqueda, localización, archivo y tratamiento de los datos se realice a través de sistemas legítimos, esencialmente no invasivos ni intrusos en la vida íntima de quien no quiere participar en la colección de datos. Asimismo, el dato debe resolver una finalidad útil (y que sea con fines económicos no le quita ese carácter), y no pensar que toda circulación de ellos ocasiona un gravamen a la libertad de intimidad.

> Agrega Pinet que, las leyes que permiten el libre acceso del público a la información deben ser más precisas a la hora de establecer los posibles usos. Esto se lograría proponiendo algunas prohibiciones sencillas, especialmente se debería prohibir el uso de estos datos con fines publicitarios, ya sea propaganda política o publicidad comercial. Aunque la ley no lo prohiba, resulta difícil argumentar que no puede hacerse…Todavía se necesita progresar mucho en este ámbito. La multitud de fuentes de difusión de datos, el gran número de operadores y la posibilidad de recuperación a distancia hacen que la creación de una única dirección de protección de datos sea una necesidad esencial. De esta manera se evitaría que los interesados tengan que realizar los mismos pasos una y otra vez con cada operador, tal y como sucede en muchos de nuestros países en relación con los directorios de los abonados telefónicos.

15.4) Principio de corrección

También suele llamarse principio de exactitud, o verdad de los datos, esto es, que reflejen con autenticidad y fehaciencia la información que compilan y transmiten.

Se relaciona con la "actualidad" del registro, en virtud de que los datos se deben guardar y conservar "al día", obligando en consecuencia, a un trabajo permanente de control sobre ellos.

El carácter de principio hace a la legalidad del archivo, y se convierte en obligación para el titular o administrador, quienes son responsables por la inexactitud informativa.

Por eso señala el art. 4º inciso 4º que *los datos deben ser exactos y actualizarse en el caso que ello fuere necesario*. Además, *los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados por el responsable del archivo o base de datos, cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate,* sin perjuicio de los derechos establecidos en el artículo 16 de la reglamentación.

> Nuestra jurisprudencia registra el caso de una base de datos condenada por no haber actualizado la información en ella contenida. La sentencia sostuvo que "*cabe responsabilizar a la entidad operadora de un banco de datos que, habiendo tomado conocimiento del error en virtud del cual se había incorporado al actor dentro de la base de datos del Banco Central no procedió a borrarlo de sus respectivos registros, pues no existe norma alguna que le impdiera dejar sin efecto tal incorporación…Habiendo quedado demostrado que el actor ha sido erróneamente incluido en la base de datos del Banco Central; sin que esta obligación pueda verse condicionada al cumplimiento de ciertos requisitos contenidos en una disposición interna de aquél que no ha sido aun publicada en el Boletín Oficial, pues no se trata de una norma vigente en los términos del art. 3º del Código Civil. Tanto más que, en el caso, el demandante ni siquiera operaba con el banco que le comunicó la errónea información a la entidad de contralor…Si bien es cierto que, en el caso, el banco que le comunicó al Banco Central la errónea información respecto del actor que provocó la inclusión de este dentro del registro de deudores del sistema crediticio, no tiene la obligación de borrarlo de ninguna base de datos propia, también lo es que los aquí codemandados Banco Central y Organización Veraz S.A. sólo podían desafectarlo de sus registros una vez que se les hubiese informado el error cometido, por lo cual, la mencionada entidad bancaria deberá ser responsabilizada por no haber realizado oportunamente tal notificación…Dada la ligereza y la falta de prudencia con que se opera en orden a la información pública que se brinda a través de las bases de datos, y habida cuenta de los perjuicios que con ello se puede provocar a los ciudadanos, que no pueden justificarse en función de la mayor agilidad que tal operatoria puede reportar para el comercio, resulta necesario que este hecho sea puesto en conocimiento del Honorable Congreso de la Nación a fin de que en ejercicio de su propia competencia adopte las medidas legislativas que estime corresponder"* (CNContenciosoadministrativa, Sala I, abril 21/999, in re "Finoli, Leonardo Luis c/ Banco Central de la República Argentina y otros s/ hábeas data", en Rev. El Derecho, del 21/10/99).

La norma impone un deber de estar informado permanente. De otro modo, sería imposible de cumplir por el titular del banco, archivo o registro, con el mandato legal.

Ahora bien, ¿cómo se logra responder este deber sin violar el principio de la calidad de los datos?

Evidentemente, el mayor problema está en la decisión a tomar por el responsable. Por ejemplo, si piensa que el dato es caduco ¿qué resuelve? Si es la supresión y sustitución inmediata del dato inexacto por el actual no hay inconvenientes, pero ¿qué ocurre cuándo mantiene la incertidumbre? ¿debe suprimir la información? ¿debe actualizarla dando

intervención al titular del dato? ¿acude a la fuente de información a los efectos de sustituir el informe incorrecto?.

De acuerdo con los términos legales, la obligación del archivo es mantener actualizada y exacta la información que contiene, pero no se resuelve cómo se debe proceder para mantener en tal sentido a la base de datos. Si la respuesta fuera en alguna de las alternativas que ofrece el artículo 5º el problema surge en que esos son datos que no ingresan en los deberes legales del responsable de la base informativa, y por tanto, la única manera factible de conocer la desactualización, posiblemente sea a instancias del interesado o afectado directo o potencial.

Correlato de este principio es la facultad del afectado para requerir la actualización de sus datos a través de la acción de hábeas data.

Ahora bien, el dato debe ser exacto mientras esté en el archivo; una vez que ha cumplido la finalidad para el que fue colectado, es deber del titular de la base, cancelar la información suprimiéndolo. No obstante, como se dijo con anterioridad, la colección de datos resulta a veces aleatoria, de modo tal que la posibilidad de conservar la realidad acopiada puede ser más que difícil, en cuyo caso, se debería establecer un mecanismo de actualización periódica o la disociación de los datos.

> La UNESCO ha propuesto que esta actualización se efectúe anualmente, salvo que el propio sistema operativo permita comprobaciones rutinarias sobre la veracidad de la información (Cfr. Doc. A/44/606 del 24 de octubre de 1989, en sesiones de la ONU *).
>
> Por su parte Estadella Yuste propicia que los instrumentos internacionales debieran considerar la propuesta a los siguientes fines: 1) para asegurar el principio de calidad de la información; y 2) que tal actualización fuese comunicada de oficio (y en caso contrario pudiera reclamarse responsabilidad) a todos los ficheros automatizados de otros países a los que se hubiese efectuado, con fecha anterior, una transmisión de tales datos.

Dato correcto no supone dato completo, es decir, la verdad que registra puede ser parcial, y para revestir de integridad la información necesitar de complementos que el archivo no ha recabado.

Esta deficiencia no ilegitima la base, sólo provoca que los datos sean incompletos pero nunca incorrectos.

No obstante, siguiendo el criterio de la comunidad europea, nuestra ley reglamentaria dice que el dato incompleto debe suprimirse y sustituirse por el correcto.

> La normativa comunitaria europea piensa que todo dato incompleto es inexacto y la permanencia en el fichero depende de los propósitos perseguidos en la creación.
>
> En Europa se ha establecido un acuerdo de cooperación para que los datos transfronterizos no sufran controles independientes, permitiendo su libre circulación entre los países signatarios y la actualización constante de la base mediante el aporte de cada uno. Se denomina *"Acuerdo Schengen"* y contiene información referente a: a) personas buscadas a efectos de extradición; b) personas desaparecidas; c) personas extranjeras incluidas en las "listas de no admisibles"; d) personas en interés de su propia protección o para prevenir amenazas; e) testigos protegidos.
>
> La característica central está en que los datos compilados no pueden ser más que éstos: a) nombre, apellido o seudónimo; b) rasgos físicos; c) primera letra del segundo nombre; d) fecha y lugar de nacimiento; e) sexo; f) nacionalidad; g) indicación de que la persona de que se trate está armada; h) indicación de las

personas de que se traten son violentas; I) motivo de la inscripción; j) conducta que debe observarse.

Este acuerdo esta suscripto entre Francia, Alemania, Bélgica, Holanda y Luxemburgo.

15.5) Principio de seguridad

Dice el Art. 9º . (Seguridad de los datos) :

1. *El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado y que permitan detectar desviaciones, intencionales o no, de información, y a sea que los riesgos provengan de la acción humana o del medio técnico utilizado.*
2. *Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.*

Los bancos de datos deben resguardar la seguridad de sus archivos, para evitar accesos no autorizados, o la penetración de la red informática por personas distintas a las que administran y están autorizadas para hacerlo.

El problema de la seguridad del archivo tiene dos facetas importantes: una atiende la protección de los datos en particular; la otra, el cuidado especial que se debe tener con las personas que tratan la información y custodian la seguridad general del archivo.

En líneas muy amplias, este principio persigue el estricto cumplimiento de los derechos a la reserva y confidencialidad de la información personal almacenada, propiciando que los responsables en el tratamiento de los datos resuelvan los riesgos de filtración, inmiscusión directa, robo de información, y eventualmente, la pérdida parcial, destrucción total, o alteración de las bases.

> El objetivo que se persigue –según Estadella Yuste- es mantener la confidencialidad e integridad de los datos personales frente a actos exteriores que puedan ponerlos en peligro y, consecuentemente, perjudicar los intereses y derechos individuales. Asimismo, se informa que por un estudio realizado sobre las categorías principales relacionadas con la seguridad del procesamiento de datos, son atribuibles a los siguientes factores: equivocaciones 65%; empleados deshonestos 13%; infraestructura inadecuada 8%; varios 5%; personas externas a la actividad del fichero 3%.

Los objetivos del principio de seguridad abarcan personas y equipamientos, y especialmente los sistemas de atención sobre los datos y los sistemas de comunicación.

Por tanto, es conveniente puntualizar el alcance de cada uno.

1) El **primer problema** aparece con la seguridad que manifiesta el archivo en su calidad intrínseca, en suma se trata de asegurar la confianza de las personas sobre la reserva y confidencialidad que mantiene el banco de datos que almacenó informaciones personales.

Para ello es necesario afianzar la responsabilidad del registro en tres niveles sucesivos: a) controles realizados sobre las personas que trabajan para el archivo y toman conocimiento de los datos personales de otros; b) qué se hace para asegurar al sistema informático, en sí mismo; y c) cómo se controla o impide el ingreso de terceros (directo o indirecto) a las bases de datos.

En este aspecto se dan los niveles de seguridad siguientes:

a) Seguridad técnica

La seguridad técnica, evidentemente, cambia y se transforma constantemente, al punto que no es posible sentar reglas sobre tal o cual mecanismo para certificar el cumplimiento de la regla.

No obstante, existen algunas guías: "*las protecciones han de ser físicas y lógicas (entre éstas últimas están los paquetes de control de accesos), y existir una separación de entornos y una segregación de funciones, además de una clasificación de la información; y deben existir los medios para garantizar su eficiencia: asignación de responsables de los ficheros, administración de la seguridad, auditoría informática interna y posible contratación de la externa*".

> La opinión transcripta es de Miguel A. Ramos, quien agrega la necesidad de efectuar controles, que suelen dividirse en: a) *controles preventivos*: los que contribuyen a evitar que se produzcan hechos como incendio, acceso ilegítimo, etc.; b) *controles detectivos*: los que, una vez producidos, ayudan a conocer el hecho y actuar hacia el futuro; c) *controles correctivos:* que contribuyen a restaurar la situación de normalidad, como la recuperación de un fichero dañado a partir de copias de procesos anteriores.
>
> Asimismo cabe agregar lo dispuesto en el Estatuto de la Agencia de Protección de Datos (España)* que aconseja las siguientes funciones inspectoras: a) sobre los soportes de información que contengan datos personales; b) sobre los equipos físicos; c) requerir el pase de programas y examinar la documentación y algoritmos de los procesos; d) examinar los sistemas de transmisión y acceso a los datos; e) auditorías sobre los sistemas informáticos.

En materia informática la seguridad técnica supone la integración de elementos externos al equipamiento (hardware y software) para que los controlen y aseguren de riesgos normales y anormales. En este sentido sería numerosa la enunciación de acciones posibles, aunque básicamente se refieren a las instalaciones donde funciona el archivo; sensores infrarrojos; blindajes; cámaras de televisión; contraseñas; seguros de riesgo, etc. etc.

b) Seguridad lógica

Se vincula con la intromisión que pueda sufrir una base de datos, sea desde otras terminales (locales o remotas), y las acciones que se pueden intentar para evitarlo.

En definitiva, son medidas organizacionales que deben adoptarse frente a la debilidad de los sistemas para contrarrestar las interferencias en la información.

> Es importante resaltar –dice del Peso Navarro- que hasta el momento presente en muchas empresas los datos de carácter personal han sido datos de segunda categoría toda vez que la preocupación principal estaba en garantizar la seguridad y la integridad de los datos de carácter simplemente económico, que eran los que se tenían que cuadrar y que podían reflejar el estado financiero de la empresa, teniendo más importancia que los datos de carácter puramente personal.
>
> La Lortad vino a modificar ese temperamento, pues el objeto de la misma no es regular el sistema de seguridad de los archivos de las empresas con todas las implicancias que esto lleva, sino desarrollar un derecho fundamental de la persona que figura en la Constitución.

Como en el caso anterior, son múltiples las posibilidades de protección, pero cuentan con un problema de costos que han demostrado la reticencia de las bases de datos para asumir con decisión los programas de protección que deben tomar.

> El Convenio 108 del CE (28/1/81), así como las Directivas 95/46 y 97/66 relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de ellos, han afincado en el sector de las telecomunicaciones algunas medidas de seguridad que se deben cumplir en los ficheros automatizados; pese a que todas las normas continúan la imprecisión o nominado abierto, como cuando se dice que las medidas de seguridad deberán tener un nivel de seguridad apropiado con los riesgos que presente el tratamiento y con la naturaleza de los datos que deben protegerse, debiendo tener presente para conseguir tales fines, no sólo los conocimientos técnicos existentes en cada momento sino también el coste que pueda suponer su aplicación.

Las medidas más frecuentes tienen en común los pasos que orienta el llamado "*libro naranja*" del Departamento de Defensa de los Estados Unidos de América, del que se toman diez procesos: a) control de acceso; b) medios de almacenamiento; c) control de memoria; d) control del usuario; e) control de acceso específico; f) control de comunicación; g) control de insumos; h) control de encargos; I) control de transferencias, y j) control de organización.

Un mecanismo lógico de protección es el "*encriptado*" que asegura, en condiciones de acceso libre a los datos, un sistema de filtración al que sólo pueden llegar quienes tienen permitida la entrada (lo cual se consigue a través de la firma digital o de claves de identificación).

> Existen dos tipos de criptografía, explica Erica Baum:
>
> 1. La de *clave de llave secreta o simétrica*: consiste en una clave compartida por dos entidades, una transmisora y otra receptora, que solo es conocida por ellas. Se dice que el sistema es simétrico porque requiere de un proceso de especificación de la clave.
>
> 2. La de clave de llave pública o asimétrica: en la cual se usan dos claves (sistema binario) una pública que, como su nombre lo indica, es de público conocimiento y otra privada, la cual no es revelada ni transmitida a persona diferente a la cual la misma pertenece. En este sistema asimétrico la clave pública se usa para cifrar el mensaje y la privada para descifrarlo.
>
> La ventaja de este sistema respecto del anterior es que permite a través de la firma digital o autenticación digital mantener en confidencia tanto la identidad de quien envía el mensaje como la integridad del mismo.
>
> Por lo tanto, la firma digital torna imposible la alteración de la firma y permite verificar con certeza la identidad de quien dice ser el firmante, quien no podrá a la postre alegar adulteración o falsificación de la misma.
>
> Para hacer uso de la firma digital es necesario que la persona posea un certificado de autenticación, el cual solo puede ser extendido por una autoridad certificante legítimamente habilitada a tal efecto y cuya función es otorgar respaldo acerca de la información contenida en el certificado. Dicho certificado es un documento digital firmado digitalmente por un certificador de clave pública, que asocia esa clave pública con su titular durante el período de vigencia del certificado.
>
> Es atribución del estado nacional garantizar a sus ciudadanos el derecho constitucional a la seguridad e intereses económicos y a una información adecuada y veraz. En Argentina, el 16 de abril de 1998, mediante Decreto 427/98 * se aprobó la implementación de esta tecnología en el ámbito de la Administración Pública Nacional con el objeto de hacer más eficientes los circuitos administrativos.

c) Seguridad organizada por vía reglamentaria

El Convenio 108 del Consejo de Europa (CE) ha resuelto que se tomen medidas de seguridad adecuadas para la protección de datos personales con el fin de evitar inconvenientes derivados de la

destrucción, pérdida accidental o provocada, así como para eliminar en el mayor grado de certeza posible, la intromisión en los archivos y la difusión no autorizada.

> En la exposición de motivos se confirma el sentido de las medidas al exponerlas en relación con las funciones que se deben asegurar: a) la vulnerabilidad de los datos (por eso, los datos sensibles exigen medidas de prevención más estrictas); b) la necesidad de que el acceso sea restringido; c) que el archivo o recolección de datos tenga en cuenta el tiempo que permanecerá disponible el dato; d) los riesgos propios de cada archivo; e) la finalidad prevista.

En países donde el tema está en ciernes, existe un vacío legislativo evidente que permite interferir las bases de datos sin que la acción tenga prevista una consecuencia punible. Por eso, buena parte de la tarea que se viene será resolver la complejidad del problema y orientar con medidas las acciones a concretar.

Tomemos por ejemplo, la "Agencia de Protección de Datos" de España, aprobada por el Real Decreto 428 del 26 de marzo de 1993 que se ha dado para sí un Estatuto y dos reglamentos.

La profusión normativa asigna una de los conjuntos legales para el tema de la seguridad de la información y la forma en que ésta ha de ser aplicada por los responsables de los ficheros.

> La publicación de la ley ha creado cierta alarma en los medios empresariales y ha servido también para llevar cierta inquietud a más de un directivo del sector privado. Según Del Peso Navarro, esto no ha sido así en el sector público, y las razones pueden ser de dos tipos: una empresarial y otra personal. Respecto de la primera se afirma que está motivada por la inexistencia en el mundo empresarial español de una cultura de la seguridad en sus tres aspectos físico, lógico y jurídico; mientras que en otros países, además de dar mayor importancia a los problemas relacionados con la seguridad, han pasado ya por tres generaciones de leyes de protección de datos y por tanto la entrada en vigor de leyes de este tipo no ha supuesto ningún trauma pues esta cultura de la seguridad se ha ido imponiendo poco a poco y su aplicación no ha representado sacrificios económicos; el problema personal se analiza desde la perspectiva de la misma ley que hace pensar a los directivos de empresas privadas que son ellos los responsables del archivo y, por tanto, sobre quienes pesa el riesgo patrimonial frente a las eventuales crisis del sistema.

La imposibilidad de generar por vía normativa una consigna sobre medios y acciones técnicas y lógicas que resuelvan la seguridad de los archivos con datos personales, ha sugerido el establecimiento de niveles para identificar donde ha de asentarse la mayor preocupación.

En tal sentido se establecen escalas de riesgo:

- *Nivel básico:*

Orienta a que el responsable del archivo tenga un manual de instrucciones de conocimiento obligatorio para todas las personas que actúan bajo su dependencia y, sobre todo, de aquellos que tienen la tarea de incorporar datos y procesarlos a los fines que el registro ha previsto. Este documento debe contener, como mínimo, el ámbito de aplicación y los recursos protegidos; las medidas, normas, procedimientos y estándares aplicados; las funciones y obligaciones del personal; la estructura de los archivos o bancos de datos con la descripción de los sistemas de información que los tratan; los procedimientos de notificación, gestión y respuesta ante las eventuales incidencias; procedimientos previstos para la actualización permanente del manual, entre otras.

En este nivel es obligatorio que exista una relación de personas que tengan derecho de acceso, y establecer procedimientos de identificación y autenticación para dicho acceso. Es, en otros términos, el método de identificación del usuario.

Cuando el mecanismo de autenticación se base en contraseñas existirá un procedimiento de asignación, distribución y almacenamiento de claves que garantice su confidencialidad e integridad. Las contraseñas –agrega Martínez Sánchez, a quien seguimos en este punto- se cambiarán con una periodicidad que tendrá que estar establecida en el documento y se registrarán en forma ininteligible (cifradas).

- *Nivel medio*

En este nivel la actividad de simple colección de datos agrega el aditamento del tipo de archivo creado y, por ello, la mayor intensidad en los sistemas de seguridad.

Hablamos de registros sobre infracciones administrativas, penales, crédito, situación patrimonial, servicios financieros, etc., en los cuales, además de cumplir las medidas señaladas anteriormente para el nivel básico, deben tener un responsable de la seguridad, encargado del control directo y auditoría permanente del sistema.

En este nivel, afirma Martínez Sánchez, las auditorías –al menos bienales- son obligatorias y deben dictaminar sobre resultados logrados en las medidas de seguridad y adecuación de ellas con el sistema reglamentario del archivo. La identificación del usuario es más exigente, agregándose a la autenticación el recaudo de operar en lugares cerrados donde el acceso sea restringido.

- *Nivel alto*

Es el nivel destinado para al tratamiento de datos sensibles.

La Directiva 95/46 CE, en el artículo 8 (Tratamiento de categorías especiales de datos) dice:

1. 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 los datos relativos a la salud o a la sexualidad.

2. Lo dispuesto en el apartado 1º no se aplicará cuando:

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 en 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 con 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 sus 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 de 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.

3. El apartado 1º no se aplicará 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 de secreto.

4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2º, bien mediante su legislación nacional, bien por decisión de la autoridad de control.

5. El tratamiento de datos relativos a 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. Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.

6. Las excepciones a las disposiciones del apartado 1º que establecen los apartados 4 y 5 se notificarán a la Comisión.

7. 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.

Las medidas de seguridad se extreman, así como las responsabilidades por su violación son superiores. El establecimiento de prevenciones ha de ser permanente y las infracciones penadas y multadas.

2) El **segundo problema** es la protección directa sobre los datos personales que se han colectado para el archivo.

El nivel de seguridad difiere en los de fácil acceso respecto a los denominados sensibles.

En unos (por el caso, nombre y apellido, domicilio, teléfonos, identificación, estado civil) la simplicidad del acceso y la multiplicación de lugares de búsqueda, impiden sentar reglas demasiado estrictas.

En otros datos más privados y personales (o personalísimos como la ideología, enfermedades, hábitos sexuales, etc.) se reserva un tratamiento más severo requiriendo un alto nivel de seguridad para impedir el acceso a ellos.

Las tareas que se encargan a los formadores de archivos y sus responsables, no impiden el diseño de programas generales de protección hacia los datos personales, como los desarrollados por *la World Wide Web Consortium* (W3C) con el fin de mejorar la defensa de la intimidad.

Se trata de un protocolo denominado P3P, o *plataforma para las preferencias de privacidad*, por el cual mediando un intercambio de información entre el usuario y el sitio en la red, ésta le informa qué posibilidades tiene para ocultar sus datos ofreciendo opciones que se resuelven y comunican a través del navegador.

> El funcionamiento es bastante sencillo. Un usuario de Internet expresa que no quiere dejar sus datos personales para que sean revelados a terceros pero que lo hará a los fines de concretar una adquisición que, posteriormente a ella, lo podrá identificar de un modo codificado. Según Ann Cavoukian, el acceso a la información necesaria para las operaciones de red puede dificultarse aún más mediante la navegación basada en la utilización de un dispositivo específico (*Web anonymizer*) que permite una actuación completamente anónima. El usuario tiene la capacidad de mantener el anonimato y revelar de todos modos ciertos datos no identificativos (como el equipo deportivo para acceder a una página de noticias, la ciudad de residencia para recibir previsiones metereológicas, etc.).

Otra opción son los sellos para la protección de la intimidad, por los que cualquier persona que no se quiere identificar puede exigir a la firma que opera en comercio electrónico, la certificación del respeto al secreto y confidencialidad de la operación. De esta calidad son firmas como WEBTrust (algo así como Instituto de Censores Jurados de Cuentas de Estados Unidos) o el "*Privacy seal program*" (Programa de sellos para la protección de la intimidad).

> Cabe recordar también las llamadas "*Listas Robinson*" que fueron implementadas con la finalidad de impedir la molestia que ocasiona la venta telefónica de productos o su oferta por correo. Para ello, quienes desean no recibir esa información se anotan en las listas y quedan automáticamente excluidos.

16. Obligaciones del archivo

Una de las cuestiones a esclarecer de inmediato consiste en saber quien debe responder por el cumplimiento de los principios establecidos y asumir las consecuencias derivadas.

A veces el tema se presenta desde el "*principio de responsabilidad*" por el cual se exige la identificación del titular del fichero, sea nacional o extranjero, a fin de poderle asignar una serie de responsabilidades proyectadas desde las obligaciones legales sobre la protección de datos de carácter personal.

> Este planteo lo hacen muchos autores que han interpretado la Ley de protección de datos española. Particularmente, Estadella Yuste dice que hay que averiguar si la responsabilidad por incumplimiento debe recaer exclusivamente sobre el titular del archivo, o si debe ser compartida entre las personas involucradas en la recogida, procesamiento o transmisión de datos personales.
>
> Hellner se ha manifestado en contra de que las disposiciones sobre responsabilidad estén demasiado relacionadas con el concepto de control general sobre el sistema computarizado, pues interpreta que el tema de responsabilidad se debe juzgar separadamente.

En todo caso la situación tiene que establecer la diferencia entre: a) administrador del archivo; b) persona encargada del tratamiento, c) características del servicio; d) interconexión de los datos.

Administrador del archivo puede ser una persona física o jurídica, de carácter estatal o particular, que por las funciones que lleva a cabo puede resolver sobre la finalidad, contenido y destino de los datos personales que almacena. Es el verdadero responsable porqué tiene el control y el poder de decisión. También se denomina *usuario*, cuando la persona –pública o privada- realiza a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos o a través de conexión con los mismos.

Encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento. En otros términos, es el operador de las bases, quien está obligado por el código de confidencialidad que debe tener el lugar donde trabaja.

La ley reglamentaria prefiere una simple definición: *Responsable del archivo, registro o banco de datos es la persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos (*art. 2º).

Finalmente, donde mayores inconvenientes se encuentran, es en la eventual *interconexión de los datos* que puede llevar a que el tratamiento sea realizado por terceras personas contratadas para ello.

De suyo, el administrador o titular del archivo no elimina su responsabilidad, ni la descarga en otro; la situación a resolver es el alcance de la obligación al tercero que viola el secreto conferido cuando se le encargó el trabajo.

El art. 10 (Deber de Confidencialidad) establece que:

"1. *El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aún después de finalizada su relación con el titular del archivo de datos.*

"2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública".

Esta situación merece ser considerada en la doble dimensión que supone. Por un lado el deber del archivo, registro o banco de datos para dar estricto cumplimiento con los principios y deberes a que se encuentra obligado; y por otro las sanciones civiles (resarcitorias) y penales (represiones) que la violación determine.

El primer aspecto tiene varias cuestiones que después analizaremos, donde basta por ahora señalar que la ley ha introducido la figura de la "presunción legal" del daño ocasionado acordando el derecho inmediato a la indemnización (art. 46).

Asimismo el art. 31 establece:

"1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000) a cien mil pesos ($ 100.000), clausura o cancelación de la autorización del archivo, registro o banco de datos;

2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso".

Otra cuestión es la incorporación que se hace al Código Penal para reprimir al que revela información almacenada de la cual toma conocimiento en razón de su oficio.

El inciso 2º del art. 32 dice:

Incorpórase como artículo 157 bis del Código Penal el siguiente:

" Será reprimido con la pena de prisión de un mes a dos años el que: 1º . A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos accediere, de cualquier forma, a un banco de datos personales;

2º Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".

De esta forma se resuelven ambos frentes derivados de la responsabilidad emergente por la administración de los datos personales de los individuos concernidos.

> Interpretando la ley española, Herrán Ortiz afirma que la responsabilidad del titular del fichero frente al afectado por el incumplimiento de las obligaciones, ya se realice materialmente por él o por un tercero a su cuenta, está regulado en la misma normativa. De forma tal que el titular es el responsable, aunque ello no obsta a que, en aquellos supuestos en que sea posible individualizar la responsabilidad en otro sujeto interviniente, se pueda actuar solidariamente contra ambos, eso sí, sin excluir la responsabilidad del beneficiado por el tratamiento y a cuyo nombre se verifica, que en ningún caso quedaría librado de sus obligaciones, sin perjuicio de que pueda repetir contra el tercero causante del daño cuando él haya soportado las consecuencias de dicha actuación.

Veamos ahora las obligaciones que tiene el archivo:

16.1 Obligación de registro o inscripción

La posibilidad de ejercer una fiscalización efectiva sobre los bancos de datos personales no podría concretarse sin saber cuáles son ellos y qué finalidades reportan.

Las *características del servicio* obedecen a la característica pública o privada del banco de datos, determinando obligaciones diferentes pero un régimen igual. En ambos casos se ha dicho que *todo archivo, registro o banco de datos público y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control* (art. 21 inciso 1º).

Mantener la voluntad de control en la acción de hábeas data corre el riesgo de dispersar los esfuerzos en favor de proteger la intimidad solamente a partir de la disposición del particular, sin que el banco de datos observe un mecanismo de vigilancia sobre sus actos.

Por ello el Capítulo V genera un "Órgano de control", al que le otorga un cúmulo de tareas para la total observancia de la ley sancionada.

> Todos los proyectos de ley que tiene Argentina, prevén la creación de un organismo de control bajo diferentes denominaciones. La Ley 24.745 fue vetada, entre otros argumentos, porqué se creaba una Comisión Bicameral de Seguimiento de Protección Legislativa de Datos, sin especificar ni delimitar las facultades que se le otorgaban; lo que llevó a sostener en el Decreto 1616/96 * que "*aquellas devienen de tal amplitud que vulneran la distribución constitucional de incumbencias estatales, dado que en nuestro sistema legal el único poder con atribuciones para resolver sobre la protección de los derechos de los individuos es el Poder Judicial de la Nación*".
>
> El art. 29 ya reproducido fija las bases de esta entidad de control.

16.2 Obligación de publicidad e información personal

El trabajo sobre datos personales no puede ser desconocido para los afectados ni para la sociedad en general. Aun sin exigir difusión publicitaria masiva, es necesario que el banco de datos haga pública su actividad proclamando así el derecho a la información que todos merecen.

> Sin la proclamación del principio de publicidad de los derechos de los ciudadanos se resentirían y padecerían una grave quiebra en su efectividad y satisfacción, ya que la actuación de la persona y su defensa frente a los posibles abusos pasan por el conocimiento veraz de las circunstancias relativas no sólo a la obtención y tratamiento de los datos, sino también de las que se refieren a los ficheros, sus titulares y las finalidades de aquéllos; informaciones precisas para que el

> interesado pueda contrastar y evaluar la incidencia y alcance que en sus derechos y libertades fundamentales va a tener el tratamiento automatizado de datos personales.

Esta obligación de publicidad, a veces, se consagra como "principio de transparencia", debiendo el archivo informar, además de los datos identificatorios de sus actividades, el sistema y los procedimientos que aplicará para el tratamiento de datos personales.

> Para Estadella Yuste, este es una parte del principio de calidad de los datos, porqué calidad supone garantizar la información y evitar consecuencias dañosas a los individuos.

La publicidad se convierte en notificación expresa, como "deber de información individual", cuando se vayan a solicitar a la persona datos que puedan ser objeto de posteriores procesos.

La obligación se cumple con el pedido de colaboración expreso, dando noticias suficientes e inequívocas sobre los motivos para los cuales se requieren los datos personales, sin ocultar la finalidad y destino que a ellos se aplicarán.

> En España, la ley se preocupa en afirmar el objeto de la información que debe darse al individuo, comenzando por la indicación sobre si es o no obligatoria su respuesta, las consecuencias de la obtención de datos y, en su caso, los inconvenientes que tendría por el silencio dispuesto. También, deberán darse a conocer los derechos de acceso, rectificación y supresión, así como la identidad y dirección del responsable del archivo.

En nuestro país, la Ley establece en el artículo 6º: *"Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) La finalidad para la que serán tratados y quienes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro o banco de datos, electrónico o de cualquier tipo de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos".*

Cuando los datos se recaben a través de encuestas, cuestionarios preimpresos, opinión casual requerida, cupones de sorteo, y otras modalidades que especifican el destino para el cual los datos se aportan, la información suficiente esta en la misma propuesta.

Sin embargo, el desvío de los datos hacia otras fuentes, o bien para darles un tratamiento diferente, hace responsable directamente a quien los solicita y archiva, por haber violado el deber de confidencialidad naturalmente contenido al tiempo de la voluntaria prestación.

En síntesis, las obligaciones emergentes del derecho a la información son esencialmente dos: la primera pone énfasis en el deber del archivo de dar a conocer sus actividades y responsables; la segunda, consiste en notificar expresamente a la persona concernida sobre las razones y destinos que se hará con sus datos personales, a los fines de que éste otorgue o no su expreso consentimiento.

> Para Estadella Yuste el titular del fichero está obligado a: a) que la recolección y operaciones automatizadas se hagan de conformidad con finalidades legítimas y aceptadas socialmente; b) que se respeten las limitaciones cuantitativas y temporales en la recolección y almacenamiento de datos; c) que se observen los

requisitos de la calidad de la información personal; d) que se especifiquen los propósitos para los cuales se crea el fichero; e) que se adopten medidas de seguridad necesarias que protejan los intereses y derechos de las personas respecto de los datos personales que les afecten. La segunda clase de obligaciones tiene un carácter más específico, procedente de los derechos individuales reconocidos a los afectados, y relacionados con las disposiciones legales nacionales sobre protección de datos. El titular del fichero debe: a) informar al afectado sobre los datos que son objeto de registro, de la finalidad del archivo, de la identidad del titular y su localización; b) comunicar el contenido de los datos que son objeto procesamiento automático, de almacenamiento, o de transmisión internacional, mediante una copia o fotocopia de los datos; c) rectificar, cancelar, borrar o bloquear los datos que a instancia de la persona concernida son inexactos o no se ajustan a las disposiciones normativas sobre protección de datos; d) cumplir los requisitos sobre inscripción de ficheros, notificar a la autoridad nacional sobre un cambio de domicilio o de titular de fichero, solicitar la licencia para la transmisión internacional de datos, en los casos que proceda según las disposiciones nacionales; e) garantizar que en las transmisiones internacionales de datos no se intente violentar los principios básicos de protección y que el destinatario de ellos, utilizará los datos personales transmisitos en forma adecuada; f) solicitar permiso a la autoridad nacional para el cambio de finalidad de ficheros; g) adoptar códigos de conducta interno que sean fiel reflejo de los principios básicos de protección de datos".

16.3 Obligación de seguridad

Esta es una obligación para el archivo y un principio de legalidad para sus actos.

Las medidas que comentamos anteriormente constituyen un deber inexcusable que no debieran requerir de leyes o directivas "marco", toda vez que se trata de justificar con plenitud la custodia del valor más importante que registran: los datos personales.

Sin embargo, es reconfortante ver la manera como se ocupan los países para encontrar niveles de protección equiparables a los que pueden adoptar lugares donde la contaminación informática es arroladora.

Claro está que las diferencias han de ser atendibles, pero nunca la obligación de asegurar, sin burocracias, los procedimientos que garanticen el acceso, y con ello, el secreto y la confidencialidad del registro.

16.4 Obligación de mantener actuales los datos

Observamos en el *principio de corrección* el deber de los archivos de mantener actualizada la información contenida; obligación que se mantiene entre los acciones que deben implementarse en esta parte, con la diferencia que ahora hay que especificar la forma como se cumple.

La exactitud de la información depende del modelo que genera la tarea de acopio y los sistemas de procesamiento de datos. Implica la necesidad de auditorías permanentes sobre los mecanismos y la facilidad que se ha de otorgar al afectado para que, a través de su propia disposición, coopere con la actualización correspondiente

De igual manera, la finalidad del archivo se relaciona y proyecta entre las obligaciones a cumplir, porqué una vez que el informe ha cumplido la razón de su almacenamiento, debe eliminarse sin necesidad que el interesado (afectado) lo peticione. Si este lo planteara obraría dentro de la garantía constitucional de hábeas data.

La supresión de oficio del dato caduco es una obligación emergente del deber de mantener actuales los archivos (art. 4 inciso 5º).

> Adviértase –dice Herrán Ortiz- la relatividad de esta obligación en tanto que se permite la conservación de los datos cuando se realizan operaciones de disociación de los datos respecto a su titular. Pugna con la idea misma del respeto a la finalidad la conservación de los datos personales cuando su utilización responde a fines diferentes, o incluso incompatibles con el que motivó su obtención; y en nada desmerece a dicha observación, el hecho de que el legislador español haya previsto la disociación de los datos respecto del titular, ya que ninguna garantía ofrece esta obligación a la vista de los avances que la tecnología proporciona a quienes de ella se benefician.

La cancelación de datos puede tener otras variables que se actúan por decisión del afectado, mientras que la obligación establecida en este campo se refiere solamente al dato que ha perdido la causa para su archivo (art. 4 inciso 7º).

La ley ha tenido en cuenta también el problema de la falsificación de los datos:

> En el artículo 32 (Sanciones penales) se prevé la incorporación al Código Penal de una norma (art. 117 bis) por la que se establece que: *1º) Será reprimido con la pena de prisión de un mes a dos años el que insertare o hiciere insertar a sabiendas datos falsos en un archivo de datos personales; 2º) La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales; 3º) La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona; 4º) Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo de la condena.*

El sistema tiene prevista una escala de ilicitudes: La primera es la simple modificación del dato personal insertando información inexacta que vulnera el perfil almacenado aportando con ello una imagen distorsionada de la persona. Si ello provoca al afectado un daño, la escala penal punitiva aumenta, y cuando el agregado fuere hecho por funcionario público en ejercicio de sus funciones (por ejemplo, el Director o Responsable del Banco de Datos) se aplica la accesoria de inhabilitación para el desempeño de cargos públicos por el doble tiempo de la condena que se fije.

16.5 Obligaciones económicas

La reparación por uso ilegítimo, abusivo o arbitrario del dato personal no tiene un régimen diferente al que establecen las normas sustanciales. El *daño* se debe alegar y probar, para obtener el derecho a la indemnización. Sin embargo, la novedad está en que la ley "presume el perjuicio sufrido", encadenando la culpa de manera directa e inmediata.

> En efecto, dice el art. 46:
>
> *"En los supuestos en que se demande judicialmente el resarcimiento de los daños ocasionados, la existencia de perjuicio se presumirá siempre que se acredite la violación o intromisión ilegítima en los derechos reconocidos por esta ley. La indemnización se extenderá al daño moral que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida. La condena podrá incluir la difusión y/o publicación de la sentencia por los medios que resulten necesarios para la adecuada compensación del perjuicio causado. La indemnización nunca será inferior a $ 5.000".*

La obligación económica que tratamos no se vincula con la condena hipotética que surge de una sentencia judicial, sino con un derecho autónomo que nace de la misma ley reglamentaria de tratamiento de datos.

La ley española dice en el ***artículo 18**, "Tutela de los derechos":*

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine. 2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación. 3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses. 4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

***Artículo 19**. "Derecho a indemnización". 1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.*

2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas. 3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

La penalidad actúa como sanción a las infracciones que puedan ocurrir sobre las reglas, principios y derechos que se establecen en la Constitución y por vía reglamentaria.

En particular, se considera que incurren en falta los archivos que no realizan los registros en forma estricta, o no informan con fehaciencia y certeza a la persona; o desplazan hacia el futuro los procedimientos de seguridad, o sean éstos insuficientes o irregulares; o violan el secreto y confidencialidad de los datos que no están autorizados a divulgar, ceder o transmitir a terceros.

Sin perjuicio de las acciones que cupieren al particular, el órgano de control hará responsable al archivo en cualquiera de las infracciones advertidas, y lo obligará a cumplir con penalidades distintas (Cfr. Art. 31 de la ley reglamentaria, ya transcripto).

Finalmente, la obligación económica que determina el resarcimiento que cuenta como derecho el afectado, en nuestro parecer, no necesita daño efectivamente sufrido, debiendo el interesado demostrar únicamente el incumplimiento del banco de datos con las reglas y principios que preservan la tutela de la intimidad.

En particular, la violación o intromisión ilegítima en los derechos que tutela le ley de protección de datos personales y que fueron vistos en los capítulos 1 y 2 con un análisis particular de cada caso.

> ¿Es este un sistema de responsabilidad objetiva? Se pregunta Herrán Ortiz. Agregando, "…no parece que pueda decirse tanto; en otras palabras, cierto es que el responsable del fichero representa una figura jurídica en la Lortad a quien se imponen las consecuencias del incumplimiento de las normas; pero también es verdad que esta circunstancia en ocasiones se ve alterada en determinados supuestos. En efecto, cuando el incumplimiento en las obligaciones procede de un defectuoso cuidado en el sistema de seguridad, cuando el responsable del fichero no haya empleado la diligencia exigible a su condición y cualidad profesional para evitar los perjuicios y así se demuestre, ninguna responsabilidad podrá exigírsele, si bien se le impone la carga de la prueba. Bien es verdad que en los demás supuestos, tales como la obtención indebida de datos personales, tratamiento ilícito y cesión de los datos, impedimento al ejercicio de los derechos de las personas, o incumplimiento de las obligaciones en relación con la actualización, rectificación o cancelación, la responsabilidad se exige al responsable del fichero, y sólo a él, sea o no quien realizó la actuación infractora, aunque nada excluye que luego éste repita contra quien materialmente causó el perjuicio.

17. Derechos del archivo

Los derechos de los titulares o administradores del archivo se reflejan en distintas exigencias que pueden requerir para el cumplimiento de la finalidad que persiguen.

Es decir, son derechos que reposan en la eficacia que se busca conseguir para los archivos, registros o bancos de datos, y en particular, versan sobre el acceso a la información que almacenan, y la colaboración que pueden requerir a quienes consulten; también, en la etapa de tratamiento, propiamente dicho, donde han de resolver algunos problemas derivados de la exclusión de datos registrables; y en el ciclo de cesión o transferencia, que presenta un marco un tanto difuso frente a la ausencia de normas que consideren el tratamiento de los datos personales.

En suma, son los derechos emergentes de las tres etapas: recolección, tratamiento y cesión de los datos personales.

17.1 Derecho a conocer los datos

La finalidad del archivo se cumple si la base informativa lograda es autosuficiente y precisa. Para ello, es menester legitimar la búsqueda y tratamiento de los datos a partir del reconocimiento legal que, por ahora, está ausente.

Esto supone que la actividad pueda ser ejercida con libertad, aceptando las restricciones emergentes de los principios, particularmente respecto a la pertinencia y proporcionalidad de la información colectada.

En España se denomina esta potestad como "*derecho a la información*", lo que parece confuso frente al derecho de la sociedad que tiene el mismo nominativo. Preferimos aceptar un derecho a conocer los datos y establecer alguna distancia según la información se tome directamente de la persona, o a través de mecanismos indirectos que obliguen a dar mayor seguridad a la tutela del derecho a la intimidad.

> Dice Puccinelli que los especialistas en derecho informático sostienen que la mayor parte de los datos son vacantes y, por tanto, accesibles a todos, en un Estado de derecho en el cual se reconoce el pluralismo de la información y la libre investigación científica. Estiman, asimismo, que el derecho a la información permitiría recolectar los datos vacantes (o públicos) para crear libremente el bien "información" e incluso, cuando se tratara de información privada, daría derecho a obtener el acceso libre e igual a tal información desde que ella fuese hecha pública.

Actualmente existe este temperamento por el cual se acepta el derecho a que la información personal se confiere voluntariamente o se exija por los medios legales especialmente previstos al efecto.

La jurisprudencia ha dicho que el derecho a exigir la confidencialidad de los datos no se extiende a aquella información de alcance comercial o financiero, pues la misma, por su carácter, está destinada a divulgarse entre todas las entidades financieras del país tal como lo prevé la Circular OPASI 2 del Banco Central *.

Por eso están fuera de la exigencia del consentimiento, los datos que revistan estas características:

Dice el art. 5 inciso 2º. No será necesario el consentimiento cuando:

a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal,

c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio.

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

e) se trate de datos que tengan fines estadísticos a los que se les hubiera aplicado una operación de disociación.

f) se trate de información proveniente de operaciones comerciales o financieras que realicen los socios de asociaciones empresarias de informaciones comerciales, sin fines de lucro, con la condición de que esa información se utilice exclusivamente entre los socios de tales asociaciones.

En cambio, diríamos que otros datos no pueden lograrse ni exigirse si no es manifestado libremente por el interesado, tal como ocurre con los datos sensibles, o cuando se pretende la información a través de medidas cautelares, de hecho improcedentes.

> "No es procedente la acción de hábeas data para tomar conocimiento de los datos insertos en una historia clínica mediante la obtención de una fotocopia de la misma ante la negativa del sanatorio que la conserva en su poder" (CNCiv., Sala C, julio 6/995, Rev. El Derecho 165-255).

17.2 Derecho al tratamiento de los datos

La tarea de procesar información no es sencilla y como tal se debe especificar. Así lo han hecho buena parte de las leyes de tratamiento de datos cuando afirman que esta labor comprende las operaciones efectuadas, en todo o en parte, con ayuda de medios automatizados que facilitan la búsqueda, localización y depósito, a los que se aplican operaciones lógicas o aritméticas, o de ambas en su caso, para interconectar información, modificar, borrar, recuperar y difundir a terceros el fruto generado.

El artículo 2 define al tratamiento de datos, como aquellas operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

El tratamiento ocupa varias secuencias, o en otros términos, se compone de etapas que se reconocen inescindibles a los fines previstos para la creación del archivo.

A partir del banco de datos que se origina (compuesto básicamente de una red central de proceso, un ordenador con su teclado y pantalla, los soportes o memorias donde se registran los datos, el sistema operativo, los programas de aplicación, un módem de comunicaciones y otros periféricos adicionales), comienza una tarea bastante compleja para almacenar información de todo tipo y procesarla para los fines previstos en la creación de la base.

Cuando esa información sea personal, el derecho que tiene reconocido el archivo para colectarla, se encuentra limitado porqué existen datos que no pueden registrarse por diversas situaciones (Por ejemplo, sensibilidad de la información; seguridad militar; secreto de Estado o profesional; etc.).

De igual modo, la colección de datos puede servir para elaborar perfiles o preferencias de alguien, pero ello no somete al individuo, quien tiene derecho a su propia realidad.

El art. 20 (Impugnación de valoraciones personales sostiene que:

"1.*Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración sobre conductas humanas no podrán tener como único fundamento el resultado del tratamiento informatizado de datos de carácter personal que suministren una definición del perfil o personalidad del interesado.*

2. Los actos que resulten contrarios a la directiva precedente serán insanablemente nulos".

17.3 Derecho a la cesión de los datos

La etapa de transferencia de datos tiene, en los hechos, la mayor importancia porque refleja las razones por las que el archivo se creó. Pueden ser beneficios científicos, culturales o económicos, pero en cada uno, el derecho a dar a conocer a otros el producto del tratamiento de datos está implícito en el reconocimiento original.

No interesa si la información se vende, cede o intercambia a un particular o se difunde públicamente, el principio es la libertad de transferencia, con algunas restricciones más estrictas que las observadas al tiempo de la registración.

> En tren de analizar las excepciones –agrega Puccinelli- a la regla del libre expendio, debemos remitirnos: a) a toda aquella información que está prohibido almacenar (v.gr.: conducta sexual; b) a aquélla registrable pero que sólo puede ser utilizada por determinados sujetos habilitados para ello (v.gr.: el juez penal que investiga una estafa), y c) a aquella que, en principio, no debiera ser proporcionada (v.gr.: listado de enfermos de SIDA remitidos a los fines estadísticos).

El derecho tiene base constitucional, en la garantía de ejercer toda actividad lícita, de modo que si tiene el archivo autorización para funcionar, debidamente conferida, no pueden encontrarse más obstáculos que los legalmente establecidos, para la cesión de datos a terceros.

18. Los códigos tipo: reglas éticas para el uso de datos personales

La necesidad de principios deontológicos establecidos en un código tipo, es una necesidad inevitable en el uso por otros de datos personales. La inmiscusión en la intimidad es inevitable desde múltiples formas y variadas expresiones. Se convive con la tecnología, la hemos aceptado, y casi sin darnos cuenta, nos sometimos a ella perdiendo individualidad.

La proliferación de bancos de datos, multiplicados al infinito desde la aparición de Internet, moviliza cotidianamente datos personales que se registran y procesan para un sin fin de razones.

Por ello, surge este anhelo internacional de contar con normas éticas que guían las conductas de los usuarios y titulares de los archivos.

De ello se ocupa el artículo 30 de la reglamentación:

1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley.

2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.

En particular, se ha continuado la consigna emitida en Europa por la Directiva 95/46 CE, que dice:

Artículo 27

1. 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.
2. Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales. Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes.
3. Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo 29. Éste se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo.

Con un carácter esencialmente autorregulatorio e implicando tanto a las empresas que se adhieran como a las asociaciones de usuarios, la Asociación Española de Comercio Electrónico ha presentado el primer "Código Etico de Protección de Datos" *, pionero en Europa, que centra su actividad en asegurar a los internautas el conocimiento y control del potencial uso que se derive de los datos personales introducidos en Internet.

Con el apoyo de la Agencia de Protección de Datos, se trata de un sello o logo que acompañará la página de toda empresa solicitante y que cumpla las condiciones de protección de datos. El citado identificador mantendrá un enlace directo a una página donde el usuario podrá contemplar la política de defensa que se efectúa en cada compañía para el uso de los datos.

El Código se basa en cuatro normas voluntarias, como son el derecho de oposición del usuario al almacenamiento y utilización de su información; la protección de menores mediante la limitación y clarificación del uso de los datos que éstos aporten; la posibilidad de rechazar el uso de correo electrónico para actividades comerciales y el sometimiento de las empresas a un Comité de control del cumplimiento que realizará auditorías periódicas al azar.

Bibliografía Capítulo IV

Casallo López, Juan Martín, *Protección de datos*, en Temas de Interés, nº 3, Escuela Nacional de Inteligencia (Argentina), Buenos Aires, 1999.

Cavoukian, Ann, *Comercio electrónico: las personas necesitan protección, no perfección*, en XX Conferencia Internacional de autoridades de protección de datos (1998), editado por Agencia de Protección de Datos, Madrid, 1999

Correa, Carlos M. – Nazar Espeche, Félix A. – Czar de Zalduendo, Susana – Batto, Hilda N., *Derecho informático*, 1ª reimpresión, editorial Depalma, Buenos Aires, 1994.

Davara Rodríguez, Miguel Angel, *La protección de datos en Europa*, editorial Universidad Pontificia Comillas, Madrid, 1998.

Del Peso Navarro, Emilio, *La figura del responsable del fichero de datos de carácter personal en la LORTAD*, en Revista "Informática y Derecho" números 6/7, editorial UNED, Mérida (España), 1994.

Estadella Yuste, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales*, editorial Tecnos, Madrid, 1995.

Galíndez, Maricel, *Acceso ilegítimo a sistemas informáticos. La informática y el derecho a la intimidad. Necesidad de una reforma*, en El Derecho, diario del 7/10/99.

Hellner, John, *From data proteccion to knowledge machines*,editorial Kluwer, Deventer, 1990.

Herrán Ortiz, Ana Isabel, *La violación de la intimidad en la protección de datos personales*, editorial Dykinson, Madrid, 1999.

López-Muñiz Goñi, Miguel, *La Ley de regulación del Tratamiento automatizado de los datos de carácter personal,* en Revista "Informática y Derecho" números 6/7, editorial UNED, Mérida (España), 1994.

Manganelli, Claudio, *Internet,* en "XX Conferencia Internacional de autoridades de protección de datos" (1998), editado por la Agencia de Protección de Datos, Madrid, 1999.

Martínez Sánchez, Mar, *Medidas de seguridad de las bases de datos,*en XX Conferencia Internacional de autoridades de protección de datos (1998), editado por Agencia de Protección de Datos, Madrid, 1999.

Pinet, Marcel, *Datos públicos o datos a los que puede acceder el público y protección de datos personales*, en XX Conferencia Internacional de autoridades de protección de datos (1998), editado por Agencia de Protección de Datos, Madrid, 1999.

Puccinelli, Oscar Raúl, *El Hábeas Data en Indoiberoamérica*, en *El Amparo Constitucional, perspectivas y modalidades*, editorial Depalma, Buenos Aires, 1999.

Ramos, Miguel Angel, *La seguridad y la confidencialidad de la información y la LORTAD*, en Revista "Informática y Derecho" números 6/7, editorial UNED, Mérida (España), 1994.
Uicich, Rodolfo Daniel, *Los bancos de datos y el derecho a la intimidad*, editorial Ad Hoc, Buenos Aires, 1999.

CAPÍTULO V. Los datos personales

19. Clasificación de los datos

La información personal que registran los archivos proviene de fuentes *directas* (datos voluntariamente prestados por su titular) o *indirectas* (adquisición de otras bases; interconexión; transferencias, etc.) que determinan el origen o lugar de procedencia.

Esta diferencia es importante para resolver el tema de la notificación de los derechos que tiene la persona al incorporar sus datos a un registro público o privado. Si el dato se otorga de manera directa la comunicación ha de ser inmediata; mientras que en el segundo caso se debe asegurar el conocimiento de los derechos bajo apercibimiento de aplicar el órgano de control las sanciones correspondientes.

Los datos se pueden clasificar con los siguientes criterios:

- *Por la identificación del titular del dato,* se divide en:

a) Nominativo: es el dato de una persona física o jurídica conocida e identificada.

> Uicich sostiene que dato nominativo es aquél que está referido a una persona determinada. Y lo divide de acuerdo a como se llegue a identificar a la persona en: a) directos: cuando lo identifica sin necesidad de proceso alguno, b) indirectos: cuando permite la identificación pero no lo hace en forma directa sino agrupando datos.

El Consejo de Europa en el Convenio emitido en el año 1981 aclaró que la protección de datos personales sólo corresponde a las personas físicas independientemente de que ellos se manipulen por administraciones o empresas; pero que las personas ideales son amparadas con relación a informaciones que vinculen a grupos de personas, asociaciones, fundaciones, sociedades, organizaciones comerciales u otros similares, tengan o no personería jurídica.

> Para Velázquez Bautista, el Convenio se aplica a todo tipo de ficheros que contuvieren datos sobre personas físicas, con independencia de quien los trate, salvo las excepciones establecidas; de esta forma se llega a "el reconocimiento de un derecho individual de acceso a los ficheros de personas jurídicas en el supuesto de que las informaciones registradas fueren utilizadas con miras a adoptar una decisión que pudiere ser invocada en contra de la persona interesada (por ejemplo, denegación de un crédito, de un seguro, etc.)".

La identificación más simple o sencilla, supone que del individuo se tengan datos provenientes de su documento o él mismo aporte otros que permitan conocerlo sin ninguna dificultad ni probabilidad de error. En cambio, si para identificar la persona se deben aplicar procesos, el dato compilado seguirá siendo nominativo pero indirecto.

b) Innominativo o anónimo: es el dato de uso estadístico o científico que no identifica a persona alguna porqué la información archivada no se refiere a él sino a sus actividades.

Es información tomada a un cierto fin y no se puede utilizar ni aplicar para otra cosa incompatible con ella.

- *Por la confidencialidad de la información* pueden ser:

a) Datos que no afectan la sensibilidad de las personas: se trata de aquella información irrelevante o anodina que por las características que tiene no permiten herir los sentimientos más íntimos de la persona relevada ni afectar su derecho a la privacidad. Es el dato rutinario, el que se ofrece sin complicaciones o se obtiene de fuentes fácilmente accesibles.

Sin embargo, hay que tener mucho cuidado con afirmar que el dato irrelevante no afecta el derecho a la intimidad, porqué hemos visto como se puede procesar la información y lograr de ella perfiles y costumbres cambiando las reglas de la colección (v.gr.: caso de los directorios telefónicos).

> Esto pone de manifiesto –según Orozco Pardo- que un dato es inocuo o sensible, no ya por su contenido, sino por el uso que de él se haga, pues como señala Castell (*La limitación informática*, en Estudios sobre la Constitución Española, editorial Cívitas, Madrid, 1991), "la interconexión de ficheros, la libre utilización de los datos, producen la teoría del mosaico, por el que datos *a priori* irrelevantes, pueden servir para una finalidad diferente y, por lo tanto, proporcionar claves insospechadas sobre una determinada persona". En tal sentido, la postura más lógica, que sostiene la jurisprudencia alemana, es la de no establecer diferencias entre los datos, atendiendo fundamentalmente al contexto y finalidad con que se utiliza. Por ello, una norma eficaz ha de atender, no al contenido en concreto del dato desligado de cualquier otro elemento, sino utilizar criterios flexibles adaptables a los supuestos y contextos concretos del caso.

b) Datos que afectan la sensibilidad de las personas: son los que de difundirse ponen en conocimiento de quien los conoce, datos de contenido privado que, salvo manifestación expresa del afectado, socavan la intimidad de las personas.

El dato sensible, como es conocido en la doctrina y legislación que lo aplica, se divide en dos campos: Uno refiere al objeto de protección, propiamente dicho; el otro, a la garantía que tutela estos datos y el nivel de protección que merecen de acuerdo al grado de sensibilidad que se le atribuye.

> Herrán Ortiz diferencia entre datos sensibles de criterio sustantivo o distinguidos por su contenido; de datos sensibles formales que tienen una garantía establecida con relación al nivel mayor o menor de protección que ampara a los mismos. En otras palabras –agrega- frente a los denominados datos especialmente sensibles, referidos a informaciones relacionadas con la libertad de ideología o creencias religiosas y que en su contenido afectan a lo que puede considerarse el "alma o interior mismo" de la persona, se reconoce la existencia de unos datos sensibles, referidos a informaciones de carácter material de la persona, que no por ello dejan de ser privados o personales, pero que afectan al comportamiento o a cuestiones más "externas" de la persona –origen racial, comportamiento sexual o salud- que sin dejar de ser privadas, y por ende sensibles, que con frecuencia se referirán a aspectos de la persona fácilmente perceptibles a los ojos de los demás, y para los cuales el tratamiento automatizado no representa un atentado tan grave a la intimidad de la persona, salvo que además de su conocimiento se proceda al tratamiento automatizado de los mismos, y constituyan elementos decisorios o de simple discernimiento en la adopción de decisiones que afectan a la persona.

El dato sensible se refiere a la salud, la condición racial y social, los pensamientos, hábitos y costumbres de la persona. Suelen establecerse categorías entre ellos con el fin de adecuar la protección al nivel de divulgación o exposición que puedan tener.

Un primer grupo se refiere a los *datos sobre ideología, religión o creencias,* que se consideran "especialmente sensibles"; ellos que no pueden hacerse públicos salvo expresa autorización del afectado. Inclusive, aun siendo obligatoria la prestación de datos, esta información está excluida por el carácter particularmente íntimo que tienen.

El segundo grupo se vincula con los *datos sobre el origen racial, la salud y la vida sexual*, que como en el caso anterior no se pueden registrar salvo que el individuo lo permita.

El tercero se relaciona con la historia personal de la persona en su vida social, destacando los *datos sobre infracciones administrativas o antecedentes penales* que tienen reglamentos especiales como veremos de inmediato (v.gr.: Registro de antecedentes personales; Registro o fichero de morosos; deudores fiscales, etc.).

> El art. 7° inciso 1° de la Ley 25.326 efectúa esa diferencia:
> "1- *Con la salvedad que se establece en el inciso siguiente, queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles, como así también el tratamiento de dichos datos y de cualquiera otro que revele ideología, raza, religión, hábitos personales y comportamiento sexual.*
>
> *No se considerarán comprendidos, a los fines de la presente ley, en la expresión "hábitos personales" los que se refieran a hábitos de consumo de bienes y servicios, siempre que dichos hábitos no revelen directamente o indirectamente, los comprendidos en la definición de datos sensibles.*
>
> *2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.*
>
> *3. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas".*

En conjunto estos datos constituyen el objeto material a proteger, pero la garantía suele variar por la naturaleza del perjuicio, obligando, en consecuencia, a una labor de interpretación del órgano –judicial o administrativo- encargado de aplicar el reglamento establecido.

> Toniatti hace una distinción partiendo de unos "datos personales irrelevantes o de rutina", sustraídos a éste régimen normativo especial. Posteriormente, desde un punto de vista material entiende por *datos sensibles* "aquellos que más directamente se refieren sea a la esfera personal e íntima, sea a la titularidad de los derechos fundamentales de la libertad", en tal sentido, cabe citar e las creencias religiosas, opiniones políticas, salud, antecedentes penales, origen racial, vida sexual, etc. Por último, habla de unos *datos supersensibles o sensibilísimos*, para atender a una categoría especial en la que el ordenamiento excluye incluso al propio interesado y el ejercicio de sus medios de control para el acceso, corrección, etc. Se trata esencialmente de datos personales clasificables desde el punto de vista material como ordinarios y sensibles que se cualifican ulteriormente por su presencia en archivos destinados a finalidades de orden particular y de valor preeminente, entre los que destacan, en primer lugar, la protección del orden público y de la seguridad nacional y, en segundo lugar, la intimidad en materia sanitaria.

- *Por la mayor o menor complejidad para lograr el dato* se clasifican en:

a) *Datos públicos o fácilmente conocidos*

La información personal que se encuentra disponible para cualquier interesado por encontrarse en registros o lugares de fácil acceso al público, no tiene derecho al reclamo de protección a través de la ley reglamentaria o del proceso constitucional específico (hábeas data).

La limitación se da cuando estos datos no sufren restricción alguna para su conocimiento y difusión, por ejemplo, resultados de censos, anuarios, bases de datos de registros oficiales, repertorios de jurisprudencia, archivos de prensa, directorio de teléfonos, y todo otro dato de similar registro.

Sin embargo la afirmación no puede ser rotunda, porqué existe información contenida en esos archivos que aun siendo expuestas y como tales divulgadas, necesitan mantener la actualidad del archivo y la proporcionalidad de sus fines.

Es decir, cualquier afectado puede reclamar la puesta al día de esa información si ella le produce un menoscabo en sus derechos subjetivos; los que deberá probar para acceder a la sentencia favorable.

Mientras que otros registros similares por su carácter público, pero restringidos por el fin al que se crean, no pueden tener la exclusión dicha con anterioridad.

En efecto, los ficheros profesionales, por ejemplo, se pueden dar a publicidad en el marco de necesidad que justifique la petición, pero nunca difundirse con fines publicitarios, por ejemplo.

> En otras palabras, dice Herrán Ortiz, la relación de miembros de grupos profesionales admite su publicación con fines y objetivos concretos propios del grupo, pero no con el propósito de utilizarlos en forma indiscriminada por terceros, fuera del ámbito profesional de que se trate.
>
> Así el dato accesible al público lo será cuando la fuente sea pública con carácter general, pero no cuando la misma tenga como fundamento un fin predeterminado y establecido entre quienes consienten la publicidad de dichos actos, ya que dicho consentimiento obedece a un interés de la propia persona de darse a conocer dentro del grupo profesional y a esos solos efectos.

¿Cuál es, entonces, la situación del dato público?

Observemos el marco legal que presta el artículo 5° respecto a cuando no se exige consentimiento del interesado:

> *Sostiene el inciso 2°:*
>
> *a) Los datos se obtengan de fuentes de acceso público irrestricto;*
>
> *b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal,*
>
> *c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio.*
>
> *d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;*
>
> *e) se trate de datos que tengan fines estadísticos a los que se les hubiera aplicado una operación de disociación.*
>
> *f) se trate de información proveniente de operaciones comerciales o financieras que realicen los socios de asociaciones empresarias de informaciones comerciales, sin fines de lucro, con la condición de que esa información se utilice exclusivamente entre los socios de tales asociaciones.*

Una respuesta posible consiste en ratificar su contenido de *res nullius* para la protección emergente de la ley y la Constitución, considerando que el dato fácilmente obtenido no puede tornar responsable al archivo que lo contiene y es abierto al público. Priva, en el caso, el derecho a la información.

Alternativa preferente nos resulta otra idea: si la fuente es pública el dato nunca, necesariamente, ha de ser público, pues persona alguna puede renunciar de manera absoluta a su derecho de privacidad.

Este es el pensamiento que inspira la mayoría de legislaciones comparadas, que defiende tanto los datos nominales directos como los de tratamiento indirecto, cuando se refieren a perfiles de la personalidad transportados desde una base de acceso facilitado.

> Lo que está en peligro no son los datos –dice Pinet- considerados como un elemento separable de la persona, sino la persona misma, para quien los datos son tan personales como una foto de la cara. De hecho, al hablar del uso de los datos personales, estamos hablando nada menos que de la libertad de la persona. Por ello, nuestra legislación sobre la protección de datos declara que el control de los datos personales es un derecho de la persona, que prevalece sobre el derecho de terceros al libre acceso de los datos personales.

b) *Datos privados, secretos y confidenciales*

La distancia entre el dato público y el privado es la misma que suele efectuarse con las relaciones humanas, es decir, los comportamientos son públicos o privados no en sí mismos, sino en atención al espacio en que se desenvuelven.

Dato privado sería aquél que la persona quiere conservar en la reserva de su intimidad. Es el dato oculto, aquél que sólo conoce la persona y que será secreto únicamente mientras esté en el reducto de lo personal, exento de toda curiosidad.

Es este un dato imposible de filtrar y por ello no cuenta en el problema de protección o defensa que merece.

El motivo es obvio. Si el dato se revela a otro, sale de la esfera de intimidad para ocupar a alguien más quien participa de la confidencialidad. Comienza así una proyección del dato privado, que es el *dato secreto* que debe custodiarse en la medida que el deber de secreto constituye una de las manifestaciones del derecho a la intimidad.

> Dice Herrán Ortiz que el secreto se caracteriza, además de por el deber de ocultamiento, por constituir un concepto fundado en las relaciones intersubjetivas. El secreto implica ocultación de "algo", pero la misma se ha de efectuar en relación a un grupo de personas, si bien éste será generalmente reducido. Por ello, no se puede conceptuar ni constituir el secreto en relación con la propia persona, ni nace de la interioridad del sujeto, más bien, se traduce en la existencia de una comunicación que se pretende preservar.

Dato confidencial es el que por su alta sensibilidad no se puede divulgar ni transmitir a terceros. Cuando el dato está en un banco o archivo la reserva es una obligación que convierte en responsable directo a quien produce la revelación.

La línea entre las tres clases de datos es muy fina, pero queda esclarecido el ámbito de protección con el derecho a la privacidad, el cual interesa al honor, la imagen, la intimidad más recóndita y aquellos sectores de la vida que sin resultar secretas, merecen sin embargo, el respeto de todos, porque el derecho que cada uno tiene a que se respete su esfera privada garantiza la inviolabilidad de la vida particular.

- *Por la subjetividad o pertenencia del dato* se clasifican en:

a) Datos personales existenciales

Se denomina así a los datos que se relacionan con definidores de la personalidad tales como el natalicio, lugar de origen, estado civil, domicilio actual y profesional, entre otros.

> Heredero Higueras es el autor de esta clasificación. Para él, *dato existencial* es el nacimiento, fallecimiento, matrimonio, divorcio, domicilio, actividad profesional, patrimonio, afiliación política o sindical, confesión religiosa, desplazamientos, enfermedades o encarcelamiento. Estos constituyen una "masa de datos" que no tienen carácter personal cuando no puedan ser asociados a personas determinadas o determinables. Asimismo es dato personal *no existencial* las informaciones referidas a condiciones personales o materiales relacionadas con cosas o bienes de las personas.

b) Datos personales no existenciales

Son aquellos vinculados con el patrimonio económico y con la pertenencia de cosas que identifican.

> La ley alemana hace esta distinción al referir a "condiciones personales y materiales" de la persona.

♦ *Por el secreto que guardan*

Los datos secretos y/o confidenciales conservan una categoría propia observada en relación con alguien que debe preservar el deber de ocultación.

El dato secreto puede ser *profesional*, al estar asentado en una base de datos que supervisa y ordena quien a recibido la información como consecuencia de su desempeño en una profesión determinada.

El caso de abogado que registra cada etapa del procedimiento que involucra a una persona o personas, anotando cuestiones que le fueron dadas en confidencia; o del médico que elabora la historia clínica; o del psicólogo que anota detalles de la personalidad del individuo, son manifestaciones del secreto profesional que no se pueden revelar.

En esta materia, el tratamiento de datos obliga a conservar el secreto a quienes hayan trabajado en las bases de datos y, por ello, tomado conocimiento de la información personal archivada.

> Por eso el artículo 10 dice que:
>
> *1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aún después de finalizada su relación con el titular del archivo de datos.*
>
> *2. EL obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.*

El *dato militar* es secreto cuando pone en riesgo operaciones de logística o compromete la seguridad del Estado al hacer público el armamento disponible, la campaña diseñada, el planeamiento estratégico, la adquisición de material, etc.

> La nueva ley de tratamiento de datos española establece en el artículo 22 sobre *Ficheros de las Fuerzas y Cuerpos de Seguridad.*

> *"1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley. 2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad. 3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales. 4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.*

El dato secreto puede estar en documentos oficiales, los que quedan restringidos del derecho de acceso con la excepción que se otorgue específicamente para ello.

20. Particularidades de los datos sensibles

La clasificación del dato sensible es ajena a la definición que del mismo se puede hacer. En efecto, los niveles observados tienden a poner énfasis a algún dato sobre otro u otros, por ejemplo, sería más importante proteger el secreto del dato sobre costumbres sexuales antes que el dato revelador de una creencia religiosa; o bien, preferir acentuar la tutela en la información que puede ocasionar discriminación de la persona en lugar de aquélla que se puede ocultar sin mayor relevancia.

En cualquier caso, los datos sensibles pertenecen a una categoría única que atiende esencialmente el derecho a la privacidad personal; son informaciones que afectan la esfera máxima de intimidad y que merecen un tratamiento particular.

> La Directiva 95/46 CE sobre Protección de datos personales establece en el artículo 8 que 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 los datos relativos a la salud o a la sexualidad.

La enumeración de cuáles son puede llevar a un *numerus clausus* peligroso, porqué no es pertinente establecer qué datos deben protegerse de acuerdo con su propia naturaleza o por el carácter secreto o confidencial que tengan, sin observar el ámbito concreto de su aplicación.

> La ley 15/99 del 13 de diciembre, prefiere establecer en España, un listado de datos sensibles a los que se asigna carácter de "*especialmente protegidos*". Ellos se refieren a la *ideología, religión o creencias.* Luego, para permitir su uso, el artículo 7 agrega que "*sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo*

> *de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado".*
>
> En cambio se prohibe expresamente la difusión de datos de *carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, que sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.* Finalmente se dice que *quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.*

Esto supone que si un dato considerado neutro o irrelevante, al ser utilizado se convierte en un elemento agresor de la intimidad o privacidad de la persona, ese dato se torna sensible por sus efectos.

> Por razones se seguridad –sostiene Sánchez Bravo- es cierto que debe procederse a la determinación legal de aquellos supuestos subsumibles bajo el ámbito de los datos sensibles. Ahora bien, será necesaria la utilización de cláusulas abiertas o generales, lo suficientemente precisas, en su vaguedad, como para determinar su ámbito de aplicación, pero, lo suficientemente amplias como para permitir la modelación en la conceptuación de los datos de acuerdo a las exigencias que demande el efectivo cumplimiento y garantía de los derechos de los ciudadanos.

20.1 Ideología y creencias

La afinidad con un partido político o la pertenencia a un sector gremial, son datos sensibles porqué se considera de riesgo para la persona denunciar tal situación.

Así lo exponen entre sus motivos las legislaciones que, mayoritariamente, los comprenden como datos de protección especial.

Entre nosotros, la sensibilidad de esta información es relativa. En primer lugar porqué los ideales políticos pueden ser manifiestos en los casos de afiliación partidaria (que son bancos de fácil acceso) o sindical (en España para considerar dato sensible se agrega el requisito de la agremiación).

En segundo término, porqué nos parece suficiente la defensa constitucional que parte del artículo 43 cuando otorga derecho de amparo contra "cualquier forma de discriminación".

Luego, porqué en un estado democrático no se puede pensar con la sospecha incorporada en cada acto, sino todo lo contrario, obrar con lealtad y buena fe, creyendo que la ideología no puede ser motivo de diferencias o de privaciones.

En todo caso, si el dato ideológico es reservado (y permanecer en el banco de datos como confidencial), el deber de mantenerlo en secreto es de la base respectiva antes que de la característica intrínseca del dato.

Lo mismo podríamos decir respecto a las creencias religiosas o cultos de fe, y sus antípodas, es decir, la ausencia de convicciones y el agnosticismo.

La filosofía moral puede ser pública en actos que se manifiestan públicos, pese a que el reducto donde se lo practique (por ejemplo, la presencia en una misa supone pertenecer al culto católico y ello puede creerlo quien con la persona se encuentra) pueda ser público o privado.

En otra variable, si la persona es famosa, o puede considerarse "pública" por su nivel de exposición, el dato que surge de sus actos cotidianos le otorga un perfil difícil de ocultar, y si a ello se suma la relevancia pública de los hechos (como la asistencia a un templo; el solicitar la bendición; confesarse; etc.), la calidad de dato sensible parece inadecuado para requerir el nivel de secreto perseguido.

20.2 Origen racial

Se considera en estos datos la pertenencia a una etnia, pueblo o lugar, al margen de la nacionalidad que le corresponda. Se incluye el color de la piel y los rasgos fisonómicos.

El rasgo racial y sus implicancias, tanto como la ideología las creencias son datos sensibles por definir una personalidad de manera directa, pero no lo serían si el ángulo de observación fuera la aplicación que del dato se haga.

Una vez más, la diferencia está en la discriminación resultante, y no en la exclusión del dato o en el secreto absoluto impuesto como deber.

¿Qué ocurriría, por ejemplo, con la política inmigratoria, que necesita conocer datos referidos al origen racial y las circunstancias derivadas de ello para el individuo y su grupo familiar?. ¿Puede excluirse un dato tan vital para una base de datos específica como es la de la Dirección Nacional de Migraciones?.

Se podrá afirmar que son archivos públicos excluidos de las previsiones reglamentarias habituales para los ordenamientos sobre tratamientos de datos, pero a nadie escapa que el dato referido no es una información de por sí privada, reservada o confidencial, porqué esta a la vista y sólo se podría proteger cuando tiene una finalidad discriminatoria.

20.3 Salud y vida sexual

La fuerte pertenencia a la esfera de la privacidad de estos datos es incuestionable y, como tales, necesitan la máxima protección. Ello determina mantenerlos secretos y confidenciales, aunque no responden a iguales significados ni merecen idéntica consideración.

En efecto, los datos del paciente han sido resguardados bajo el secreto profesional en la historia de la medicina, sin embargo en la actualidad, el tratamiento informático de la información médica permite interconectar los archivos y poner en riesgo el presunto anonimato del enfermo.

> *Art. 8º . (Datos relativos a la salud) .-*
>
> *Los hospitales y demás instituciones sanitarias públicas o privadas y los profesionales vinculados a la ciencia médica pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquellos, respetando los principios del secreto profesional.*

Esto llevó al Consejo de Europa a emitir la *"Recomendación 81/1" **, donde se insiste en que los datos médicos forman parte de la esfera de intimidad de las personas, de manera que su transmisión o divulgación, solamente puede hacerse en temas y problemas muy puntuales y restringidos.

> Debe considerarse –dice Del Peso Navarro- que el almacenamiento de determinadas informaciones relacionadas con la salud conlleva un peligro añadido, en otras palabras, no será preciso para conocer la enfermedad de un paciente registrar ésta explícitamente, porqué a través de la información relativa a determinados fármacos puede deducirse fácilmente la enfermedad que padece la persona. Por tanto, tales informaciones no deberían salvo excepciones muy especiales como la necesidad de tenerlos a los fines de una investiga salvo excepciones muy especiales como la necesidad de tenerlos a los fines de una investiga figurar en bases de datos a las que tengan acceso directo cualquier colectivo sanitario, sin restringir el acceso de alguna manera a los profesionales médicos que más directamente se relacionen con el paciente.

La privacidad del dato sobre la salud de las personas es confidencial porqué está en un reducto privado (círculo social, familiar y del médico, en particular), pero si el individuo presta conformidad para su cesión o exposición, no advertimos problemas para ello.

> A diferencia de los datos de carácter social –sostiene Jacob-, la mayoría de los datos de tipo médico no son objeto de tratamiento por autoridades públicas sino

> por entidades privadas. La mayor parte de estas entidades son consultadas por médicos que guardan en sus bases de datos la información de sus pacientes para utilizarlos en tratamientos futuros o para comunicarlos a otros médicos de manera individual. Pero no existe una red de bases de datos de carácter médico. Si el paciente así lo desea, el médico que él designe puede desempeñar una función esencial, en la medida en que se le mantiene informado de los hallazgos de otros médicos, en particular de los especialistas, y de los resultados de las pruebas clínicas. En consecuencia este médico puede disponer de un abanico de datos, más o menos completo, con el consentimiento del paciente.

El problema puede aparecer cuando los datos se transfieren sin consentimiento, lo que es habitual, por ejemplo, cuando la obra social pide información al establecimiento clínico, hospitalario o al médico de su planta profesional, sobre las atenciones prestadas a una determinada persona con el fin de reintegrar las inversiones o gastos por ella practicadas.

Para el caso, la limitación del informe a los puntos solicitados puede resolver la situación porqué, en definitiva, se trata de una relación médico-paciente que interesa a un tercero que soporta los costos necesarios del tratamiento y, para ello, debe estar tan informado como los demás interesados.

> Agrega Jacob que también hay otros contextos que muestran que ya no es válido el antiguo concepto de restringir la protección de datos de carácter médico y social a los organismos que tradicionalmente los han conservado y tratado. Esto se debe a las nuevas formas de división del trabajo, según las cuales los que prestan servicios especializados asumen funciones particulares y, en este contexto, adquieren conocimiento de datos personales. Esto es aún más cierto en el caso de la investigación moderna. La investigación social, por ejemplo, se ocupa de las causas y consecuencias de la pobreza social y la investigación epidemiológica, de la forma en la que el ambiente de trabajo o factores ambientales especiales influyen en las personas. Los investigadores no están interesados en los datos de las personas en cuanto tal, sino exclusivamente en el contexto. Sin embargo, a menudo, tienen que registrar los datos individuales y utilizar sus nombres con el fin de reconocer las relaciones objetivas. Para que la investigación sea aceptable para las personas que la realizan, es preciso no proteger los datos de carácter médico y social relacionados temporalmente para dicha investigación. De lo contrario, para proteger los intereses de las personas involucradas, tal investigación no podría realizarse.

El dato de salud puede ser actual o pasado o referir a una característica que tuvo una persona fallecida. En ningún caso existen diferencias de trato.

Se incluyen en esta categoría los informes sobre adicciones y costumbres que puedan ubicarse como inimputables.

> Habrá que tener especial cuidado –repara Sánchez Bravo- respecto a los datos referentes a la salud mental en el futuro, pues se corre el riesgo de ingresar a los afectados en una especie de “censos negros”, con el paralelo peligro para el ejercicio de sus derechos. Se puede así proceder al tratamiento de estos datos sensibles basándose en meras sospechas que no presentan ninguna constatación fáctica. Serían las verdaderas necesidades del tratamiento médico y la evolución de la enfermedad, junto a unas razonables previsiones de futuro, las que deben determinar la inclusión de estos datos.

Por su parte del dato sexual se vincula con la actividad, o las preferencias que distinguen una costumbre diferente.

En un caso, la información compila el comportamiento sexual del individuo así como la ausencia de dicha actividad, y las consecuencias derivadas.

En las preferencias se sustraen datos objetivos como las suscripciones a revistas de contenido erótico, anuncios de contacto, pertenencia a agrupaciones homosexuales o afines, etc.

Cada uno de estos datos, naturalmente, es esencialmente privado y corresponden a la intimidad personal de cada uno, circunstancia que permite sustraerlos de una base de datos o mantenerlos en estricta confidencialidad.

20.4 Las condenas penales

Esta modalidad de registro de antecedentes penales que supone archivar toda condena sufrida por la persona, suele plantearse como datos sensibles. Así los considera el artículo 7 inciso 3°.

La prohibición de almacenamiento se dirige a la creación de archivos destinados exclusivamente para ello, sin que obstaculice la acción del Estado a través de sus organismos específicos.

De todos modos, la sensibilidad del dato no llega del secreto que sobre el mismo se quiera mantener, pues las sentencias son públicas (con algunas excepciones como las condenas a menores de edad que según las *reglas de Bijing* del 29/11/95 aprobadas por "Naciones Unidas" obliga a su carácter estrictamente confidencial), sino del uso discriminatorio que se haga de él.

En tal sentido, el hábeas data no procede como vía de reparación porqué el dato no se puede excluir, al ser público. Obviamente no se pueden borrar los antecedentes carcelarios o las condenas que haya tenido una persona. Lo contrario, inutilizaría muchas reglas procesales en lo penal y seguramente provocaría una ruptura en el sistema de protección de los derechos de la sociedad.

Desde otra perspectiva, puede enfocarse el problema como deficiencias que encuentra el ex penado para reinsertarse en el medio social en que vive. El dato antecedente le impide integrarse porque se lo descalifica o segrega. En estas situaciones, no es el dato el que causa la crisis, ni la ocultación del mismo llevaría a solucionarlo.

21. Datos públicos y privados

La dualidad entre dato público (expuesto) y privado (secreto y/o confidencial) presenta la misma diatriba entre aquello que el público tiene derecho a conocer y lo que el hombre tiene derecho a conservar para sí mismo.

Derecho a la información versus derecho a la privacidad son términos aparentemente contrapuestos en esta presentación.

Por otra parte, la intimidad personal antaño considerada como "el derecho a estar en soledad", permite inferir un término donde las acciones particulares obran determinantes para esa posibilidad de aislamiento, porqué si es la misma persona quien ocasiona la publicidad de sus actitudes y comportamientos, puede existir una provocación a la exposición pública.

Al menos, la notoriedad, fama, o el reconocimiento general, significa que respecto a ese alguien la gente conoce más, lo cual no autoriza a invadir la esfera de secreto, reserva o intimidad que el hombre público quiera preservar. El problema será si lo puede conseguir.

> Es evidente que hoy –dice Concepción Rodríguez- la intimidad es el bien más amenazado y desprovisto de una enérgica tutela en todas sus facetas. El interceptar conversaciones, el revelar datos personales que constan en determinados registros para unos fines; el captar imágenes con aparatos apropiados, sin que se aperciba de ello la persona fotografiada, etc., es noticia usual. La intimidad debe ser protegida en todas las personas, sin que sea lícito discriminar, en principio, a las que gozan de fama pública o actúan en la vida pública. Sin embargo, hay que atender a la esfera que, por sus propios actos, mantenga la persona reservada.

Pongamos como ejemplo la noticia de la internación de Diego Maradona en Cuba, donde la prensa efectuó un pormenorizado relato de las adicciones padecidas y el tratamiento que se aplicaron. Evidentemente, una demanda eventual contra los medios de comunicación podría ser posible por la intromisión y divulgación de las acciones personales tomadas por el conocido futbolista, pero nunca sería

factible por difamación, porqué en los hechos que estudiamos, importa más la exposición abierta de hechos privados de la persona pública antes que la veracidad de la información ofrecida.

Ahora bien, este caso es un supuesto de invasión a la privacidad, pero ¿cómo se aplica el principio respecto a datos personales?.

Es necesario advertir que la persona pública, *lato sensu*, tiene un historial más conocido que las personas comunes. Se sabe y conocen detalles de su vida, sus actos, circunstancias caracterizadoras, etc. Es probable que cada uno de estos comportamientos se encuentren guardados en un archivo periodístico (que es, en definitiva, una base de datos).

Sobre esta base hipotética ¿qué diferencia existe entre la noticia que versa sobre aspectos clínicos del tratamiento de Maradona, respecto a otro interno por similares adicciones?.

Parece claro que la exposición de uno (la fama) trasciende más que la del ignoto, aunque le afectación sea idéntica en el grado de bochorno que produzca la invasión a información tan sensible.

> Cuando el titular del honor lesionado –dice Concepción Rodríguez- resulta ser un *personaje de proyección pública*, existen ciertas particularidades no ya porque su honor sea distinto al de cualquier persona, sino porque la esfera de protección que le dispensa el Derecho es menor, por cuanto, la opinión pública, en aras de la libertad de información, tiene derecho a conocer los datos relativos a aquéllos, facultad que cobra toda su trascendencia con relación al derecho a la intimidad.

Por eso, sostener que existe un *dato público* cuando la persona *es pública*, compromete seriamente la tutela prevista para el tratamiento de informaciones sobre la vida personal.

De igual modo, no se podría afirmar que el *dato es privado* cuando la persona es común y su grado de exposición pública sea mínimo.

En ambos casos, la defensa de la intimidad es la misma, y el derecho a proteger los datos personales no cambia.

> Observado desde otro punto de vista, suele transportarse el problema a la distinción entre información pública e información privada. En efecto, la información pública sería aquella que es de público conocimiento. La privada, por el contrario, es la que permanece constreñida a la intimidad de las personas o al conocimiento de un círculo de personas limitado. El conocimiento de la información podría ser un criterio de delimitación de la información pública, dice Sánchez de Diego, pero a su vez, establecer el grado necesario para que una información sea calificada como pública presenta innumerables dificultades…Se puede variar el enfoque y considerar que no es tan importante los indicadores cuantitativos como cualitativos. En este sentido una información sería pública cuando se tiene conocimiento de ella por personas ajenas al origen de la información o cuando es de fácil adquisición o está a disposición del público. En definitiva, establecer un nivel de conocimiento público que determine con claridad cuando una información es pública es sumamente dificultoso. Lo cierto es que cuando un hecho es de conocimiento público, más que información pública se trata de *información publicada*. Y que, sin lugar a dudas, una información puede considerarse publicada cuando ha sido difundida por los medios de comunicación social.

No obstante, una variable es considerar que existen *datos públicos* cuando la fuente de información es de fácil acceso; y *datos privados* cuando el sondeo tiene carácter confidencial o secreto.

Por ejemplo, el acceso a la información judicial es simple y difundida hacia todos, pero el lamentable archivo de abogados que llevaba la Cámara Federal de apelaciones en lo criminal y correccional (sobre comportamientos procesales que, en su caso, debieran ser considerados por el Colegio profesional) era un registro privado de circulación restringida. En el caso, existe con ese banco de datos una afectación a la esfera de intimidad, porqué los derechos fundamentales de cada uno coexisten con los llamados derechos

personalísimos que tienen una protección especial, o al menos, la merecen. Y por tanto, el honor, la privacidad, la imagen personal o el prestigio profesional son un patrimonio de la persona.

Otra proyección puede darse cuando con los datos privados que se hacen públicos se persigue lograr beneficios económicos especulativos, merced a la exposición de la persona notoria o famosa.

> Aun cuando también aquí hay que establecer diferencias, como lo hizo el Superior Tribunal de Justicia de España al tratar la afectación de un funcionario público que se sintió perturbado en su derecho a la propia imagen. Sostuvo el Alto Tribunal que "*…quien ejerce un cargo público o una profesión de notoriedad o proyección pública tiene derecho a su propia imagen y a su intimidad, cuando elude su presentación en un acto público o en lugares abiertos al mismo, pues si consta el decidido propósito de eludir la exposición al estar en una playa alejada de la gente y alejada de los núcleos de población y que, vestida sólo con una pieza inferior de su traje de baño, es fotografiada con teleobjetivo sin su consentimiento, fotografías que tomadas por un profesional son vendidas a una revista donde son publicadas, debe salvaguardarse su intimidad que tan subrepticiamente fue vulnerada".*

Identificar el dato desde la condición pública o privada de la fuente de información es el temperamento de la ley de protección de datos española que divide entre ficheros de titularidad pública y ficheros de titularidad privada. Lo característico, en esta clasificación, es el dominio del dato antes que la identidad de la persona.

> Sostiene Sánchez de Diego que este nuevo criterio explica que las informaciones divulgadas por quienes son origen de una información se convierten en informaciones públicas, desde el momento en que difunden y, por tanto, desde que pierden el dominio, la posesión. Este criterio –agrega- es también perfectamente aplicable en los casos de bases de datos, en donde la posesión de la información procede de la titularidad de los medios de almacenaje y recuperación de la misma, esto es, la titularidad de la base de datos. En principio, la titularidad de una base de datos por un particular o por una entidad pública determinaría la cualidad de la información, en cuanto pública o privada. Y todo ello con independencia del tipo de información de que se trate: datos personales de un alumno, datos estadísticos, informes de personal, movimiento de cuentas bancarias, test de eficacia de vehículos, diligencias judiciales, etc.

Bibliografía Capítulo V

Concepción Rodríguez, José Luis, *Honor, intimidad e imagen*, editorial Bosch, Barcelona, 1996.

Del Peso Navarro, Emilio, *La protección y la seguridad de los datos automatizados de carácter médico,* en "Actas del II Congreso Internacional de Informática y Derecho", Mérida, 1995.

Sánchez de Diego Fernández de la Riva, Manuel, *Criterios delimitadores de lo público y lo privado*, en "Sobre la intimidad", editorial Fundación Universitaria San Pablo C.E.U., Valencia, 1996.

Heredero Higueras, Miguel, *La Ley Orgánica 5/92 de 29 de octubre, de regulación del tratamiento automatizado de carácter personal. Introducción general,* en BIMJ nº 1669, Madrid, 1993.

Herrán Ortiz, Ana Isabel, *La violación de la intimidad en la protección de datos personales,* editorial Dykinson, Madrid, 1999.

Jacob, Joachim, *Datos objeto de protección especial: datos de carácter médico-social,* en "XX Conferencia Internacional de autoridades de protección de datos" (1998), editado por la Agencia de Protección de Datos, Madrid, 1999.

Orozco Pardo, Guillermo, *Los derechos de las personas en la Lortad,* en Revista Informática y Derecho, números 6/7, editorial UNED, Mérida, 1994.

Sánchez Bravo, Alvaro, *La regulación de los datos sensibles en la Lortad,* en Revista Informática y Derecho, números 6/7, editorial UNED, Mérida, 1994.

Toniatti, Roberto, *Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada*, en R.V.A.P. nº 29, 1991.

Uicich, Rodolfo Daniel, *Los bancos de datos y el derecho a la intimidad,* editorial Ad Hoc, Buenos Aires, 1999.

Velázquez Bautista, Rafael *Protección jurídica de datos personales automatizados*, editorial Colex, Madrid, 1993.

CAPÍTULO IX. Derechos del titular de los datos

32. ¿Quién es el titular de los datos?

La protección que a la intimidad se confiere, en miras a evitar que la intromisión informática complique la vida privada de las personas, supone pensar que estamos frente a un derecho personalísimo que sólamente le corresponde al individuo afectado por el almacenamiento, conservación y transferencia de sus datos personales.

> No es simple ocultar la facilidad como se pueden interceptar los datos en la red, ni eludir los desvíos que ellos pueden sufrir en su tránsito para ser leídos por personas no autorizadas. Por eso, interrogarse quien es el dueño de la información tiene su sentido, mucho más si quedan señalados los problemas de la seguridad en Internet, que podrían sintetizarse básicamente en dos sub categorías de conflictos:
>
> 1. los referidos a los riesgos a los que se ve expuesto un servidor Web, como por ejemplo, la exposición de documentos a terceras personas.
>
> 2. Los que se vinculan con la protección de las comunicaciones de los usuarios, ante el riesgo de la interrupción y captura de datos personales (información crítica) como tarjetas de crédito, cuentas bancarias, etc.

De este modo, se tomaría a la noción de derecho subjetivo como base de la acción y, ante una hipotética demanda, habría que demostrar la relación existente entre la titularidad de quien propone la pretensión, con el perjuicio efectivamente sufrido. Asimismo, se tendría que verificar la relación causal y el derecho a las medidas que solicita.

Sin embargo, la explicación que precede no es absolutamente cierta. En efecto, la titularidad de los datos contrae algunas dificultades de intelección, porqué una cuestión son los derechos que tiene la persona afectada por el tratamiento de sus datos personales, y otra es la legitimación procesal que se debe acreditar en el proceso constitucional de hábeas data.

Inclusive, hay quienes sostienen que una vez que los datos llegan y se incorporan a la base ocurre una suerte de legítima apropiación que le asigna la titularidad sobre ellas al responsable del archivo. La idea se basa en que existe un derecho a la información diferente al de titularidad sobre los datos.

> Dado que alguna doctrina sostiene que podría ser ejercido una suerte de derecho de propiedad sobre los datos –dice Puccinelli-, cabría entonces distinguir entre el derecho a la información y el derecho sobre la información recabada. La posición que recurre al concepto de propiedad sobre los datos plantea ciertos debates nada pacíficos en la doctrina entre quienes sostienen la propiedad colectiva de toda información con independencia de su fuente y aquellos que, por el contrario, entienden que en los supuestos en que a partir de determinados datos y por el obrar de alguien, se logra generar determinada información, a quien la generó se le debe reconocer su derecho de propiedad sobre ella, salvo en el caso de los datos personales, que pertenecerían a aquel a quien se refieren.

El siguiente paso para reconocer la pertenencia del derecho a la denominada "autodeterminación informativa", consiste en tomar los derechos que se tutelan por esta novedosa posición y advertir el alcance que ellos tienen.

> Estadella Yuste dice que la noción de datos puede conducir a falsas apariencias respecto de su contenido, ya que no va destinada a proteger los datos *per se*, sino a una parte del derecho a la intimidad individual.

De este modo, se podrá constatar que la protección dispensada no es estrictamente a los datos sino a la persona, y particularmente, a su vida privada e intimidad.

Luego, cada etapa del proceso que va desde la localización de las fuentes de información hasta la transferencia de los datos, instala exigencias diferentes que tienen mucho que ver con las propias decisiones o autodeterminación (manifestación de voluntad del interesado) impuesta por quien ofrece información personal a un archivo.

La guarda de los datos, por ejemplo, es sin duda alguna responsabilidad del archivo; como lo es también la seguridad que aplica al secreto recibido y a la efectividad de las eventuales transferencias. Aquí, los datos son de alguien a quien se conoce, informa y ha prestado autorización; mientras que el acto pleno de la información ofrecida es del titular del archivo.

Son derechos distintos, es verdad, y deben tener consideraciones diferentes. Una cosa será la protección al dueño de los datos para evitar la ofensa o lesión a su intimidad y demás derechos vinculados (identidad, honor, reputación, etc.); y otras las garantías que debe contar el titular del archivo para poder ejercer con plenitud su derecho a la información, a comerciar lícitamente, etc.

32.1 Derecho subjetivo del titular de los datos

Cuando se relaciona el derecho a tener protección de los datos personales con el derecho a la intimidad, se refleja una visión individual que asienta en un concepto civilista de la garantía. Pero cuando en la misma dimensión se cubren los derechos colectivos que persiguen evitar el abuso en el almacenamiento, recolección y procesamiento de datos personales, la intimidad queda en un segundo plano porqué el derecho garantizado adquiere alcance social.

> El Tribunal Constitucional alemán ha entendido que el principio liminar del ordenamiento jurídico establecido en su país, es el valor y la dignidad de la persona que actúa con libre autodeterminación al formar parte de una sociedad libre. De esa dignidad y libertad, entendida como libre autodeterminación, deriva la facultad de la persona de "deducir básicamente por sí misma cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida"; por lo que el Tribunal interpreta –en la deducción que hace Fappiano- que es contrario a esa facultad un orden social y un orden jurídico que hiciese posible al primero, en que el ciudadano ya no pudiera saber quién, qué, y cuándo y con qué motivo sabe algo sobre él…Esto no solo menoscabaría las oportunidades del desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos.

La dificultad de encuadrar como derecho subjetivo (propio e intransferible) a la noción de privacidad que pervive en el concepto de datos personales, está en que no se puede reparar el daño con la sola concesión de una indemnización reparatoria. La invasión a la intimidad se relaciona con las posibilidades reales que se tengan para controlarla, de manera que, los derechos emergentes de la protección de datos no pueden ser atendidos únicamente desde la visión economicista que mida el daño con la vara del resarcimiento. Es necesario que la protección del derecho se plantee como un problema social.

> La protección del derecho a la intimidad contra el uso de un tratamiento automatizado de datos personales no se plantea exclusivamente a consecuencia de problemas individuales, sino que también expresa conflictos que incluyen a todos los individuos de la comunidad internacional. Por eso –dice Estadella Yuste- la idea de que la persona titular de los datos –el afectado- tiene interés, como parte de un grupo, en controlar el tratamiento automatizado de datos es reciente, ya que no aparece así en la denominada "primera generación" de las leyes protectoras de datos, orientadas exclusivamente a la protección de la persona como entidad individual.

La socialización del derecho puede ampliar las fronteras tradicionales de la legitimación procesal, y por eso es la diferencia entre derecho subjetivo y representación del interés a defender; es evidente que la afectación de la privacidad por cualquier medio, además de lo que pertenece a los datos en sí mismos, se

puede exigir no sólo por el afectado, sino por otras personas que con iguales motivos persigan una decisión judicial al respecto.

No obstante, si la noción de autodeterminación informativa se restringe como derecho personalísimo, la defensa del honor, la imagen, o la intimidad en un amplio sentido, únicamente se podrá concretar por el afectado.

> El bien jurídico intimidad de ser tratado como un derecho exclusivamente individual puede dejar afuera del ámbito de defensa constitucional –al parecer de Perez Luño- los aspectos sociales y colectivos de las informaciones que directamente les afectan. De otro lado, dado que en la sociedad moderna la capacidad de actuación política se halla íntimamente relacionada con el acceso y control de la información, un equilibrio sociopolítico exige que se garantice a los grupos sociales formas de participación en los materiales archivados en los bancos de datos.

32.2 La protección de los datos personales como derecho humano

La perspectiva anterior puede variar si el derecho se presenta desde los intereses que tutela. Es decir, si en lugar de ver a la persona que lleva la pretensión se observa el contenido del derecho que para sí reclama.

Esta cuestión es esencial en el análisis del hábeas data, porqué la garantía constitucional se puede encontrar alterada por una caprichosa definición procesal que exija la relación directa entre quien pide y el daño producido (por ejemplo, cuando se requiere ilegalidad o ilegitimidad en el acto cuestionado y el actor únicamente solicita acceso al banco de datos); cuando en realidad, la lesión al derecho de la intimidad tiene varias manifestaciones, algunas de las cuales no reconoce un afectado directo porqué el gravamen asienta a toda la sociedad.

Muchas Constituciones del mundo han incorporado el derecho a la intimidad, el honor y la imagen como derechos del hombre; de este modo, se persigue establecer una igualdad de trato y consideración que evite diferencias escandalosas entre el significado que unos y otros puedan dar a cada uno de los intereses.

En relación estricta a los datos personales, debe aplicarse esta inteligencia porqué la intromisión a la vida privada se realiza en el preciso momento que alguien usa o conoce información personal que nos concierne, adquiriendo un conocimiento que pudo estar reservado, secreto o ser confidencial.

Esa información adquirida, cuando lo es de manera ilegítima, representa una injerencia en la vida privada, familiar o doméstica; constituye un atentado a la libertad individual cuando se usa para descalificar u ofender, o asignar conductas que lesionan el honor personal; asimismo, puede considerarse que es un hostigamiento, una vigilancia perturbadora, y en definitiva, una actitud hostil contra la reserva de los comportamientos individuales.

Cada caso es una proyección a defender, una hipótesis de cómo se afecta el derecho a través de la penetración y divulgación de los datos personales.

> Por tanto, tal como afirma Perez Luño, se trata en suma de comprobar en qué casos la *privacy* puede operar como coartada para burlar una política social avanzada, o en qué supuestos puede servir de freno ante determinadas formas de control o discriminación social o política. Pero en lo que interesa distinguir es que las cuestiones sobre las que gravita la disciplina jurídica de la intimidad han perdido su carácter exclusivo individual y privado, para asumir progresivamente una significación pública y colectiva. El problema del suministro de datos personales a la administración es evidente que atañe a los individuos, pero también a toda la sociedad, e incluso puede afirmarse que atañe a los individuos en cuanto pertenecen a un grupo social.

Enseguida veremos la dificultad de superar esta noción amplia cuando se mide el derecho al proceso desde la exigencia de arbitrariedad o ilegalidad manifiesta del acto lesivo, o cuando se toma la manifestación de voluntad como pauta legitimadora del uso de datos personales; o bien, al despojar el carácter social del derecho para centrar su tutela en la defensa exclusiva del derecho personalísimo.

Esta posición deja sin defensa a las personas jurídicas, porqué al referirse a las personas individuales se establece que el derecho a la protección de la intimidad y, en esencia, de los datos, corresponde a la persona humana; dejando en todo caso la tutela a la información de las empresas a la normativa específica que cada ordenamiento mantenga.

> El derecho a la intimidad que reconoce el artículo 18.1 de la Constitución –sostiene el Tribunal Constitucional de España- por su propio contenido se refiere a la vida privada de las personas individuales, en las que nadie debe inmiscuirse sin estar debidamente autorizado, y sin que en principio las personas jurídicas, como las sociedades mercantiles, puedan ser titulares del mismo, ya que la reserva acerca de las actividades de estas entidades quedará, en su caso, protegida por la correspondiente regulación legal, al margen de la intimidad personal y subjetiva constitucionalmente decretada; pero es que, además, y en el caso de que hipotéticamente se estimare que el derecho a la intimidad acogiera las personas jurídicas, estaría como el resto de los derechos fundamentales limitado en su total dimensión, pues su ejercicio se sometería al respeto de otros bienes jurídicos igualmente dignos y necesitados de protección, y en concreto, a exigencias derivadas de la acción de la justicia. (TC, sentencia del 17/4/85).

32.3 Disponibilidad del derecho: autodeterminación

La progresión del derecho a partir de la interpretación judicial y doctrinaria ha puesto de relieve el difícil encuadre que tiene el criterio tradicional entre derecho positivo y derecho natural. Dicho en otros términos, no siempre las cosas se presentan como polaridades entre el derecho subjetivo, individual y concreto, frente al derecho social, difuso y abstracto.

No es bueno creer que la mejor defensa parte de las garantías individuales que tenga una persona porqué desde ellas irradia la fuerza normativa hacia los demás; como tampoco lo es pensar que si la sociedad se defiende con las armas de la ley, no es posible creer en el hombre indefenso.

Una posición intermedia deja en la persona la disponibilidad de actuar con libertad y criterio, poniendo en claro que, en materia de protección de datos, nadie mejor que el afectado para promover, de acuerdo con sus propios sentimientos y convicciones, la defensa de su vida privada.

> Este planteamiento –dice Perez Luño- tiene el mérito de poner de relieve la progresiva tendencia a concebir la *privacy* como el poder de ejercer un control sobre todas las informaciones que puedan afectar a cada persona individual o colectiva…Es el derecho al control de la información sobre uno mismo.

La posición se refleja en muchas de las legislaciones sobre protección de datos, las cuales ponen énfasis en la autonomía de la voluntad individual para autorizar la guarda, almacenamiento y transferencia de información que concierne a las personas físicas o jurídicas.

> Resumiendo se puede decir –concluye Estadella Yuste- que en un primer momento los instrumentos internacionales de derechos humanos no recogían expresamente el derecho a la protección de datos o autodeterminación informativa, sino tan sólo un derecho "a la vida privada" o a la intimidad personal. Posteriormente éste se ha ido desarrollando y paulatinamente se han adoptado otros instrumentos internacionales reconociendo el derecho a la protección de datos. Ello es importante porqué, si la protección de datos sólo se hubiera plasmado en leyes de ámbito nacional, habría sido más difícil que la comunidad internacional lo considerara como un derecho individual.

La dificultad puede estar en las limitaciones que se pretendan derivar de ese acto voluntario como una proyección de la doctrina de los actos propios, que en nuestro parecer no puede ser tan inflexible porqué desnaturaliza el derecho central a proteger. De aplicar el temperamento cualquier autorización abriría una carta de crédito al archivo evitando el control externo si el afectado no efectúa una pretensión concreta.

La defensa de los datos no tiene una visión estática simplificada en el interés particular; todo lo contrario, la función dinámica que adquiere se toma del modo como actúan los archivos y registros de información personal, los que habilitan actuar en dimensiones diversas, ya sea para tutelar el interés concreto, como para descubrir el control externo que se merece.

> Esta posición ha penetrado en los últimos años en la doctrina europea y reviste una importancia prioritaria para delimitar conceptualmente el contenido del derecho a la intimidad y su alcance en la sociedad tecnológicamente avanzada. En suma, se trata de insistir –afirma Perez Luño- que en nuestra época resulta insuficiente concebir la intimidad como un derecho garantista (*status* negativo) de defensa frente a cualquier invasión indebida de la esfera privada, sin contemplarla, al propio tiempo, como un derecho activo de control (*status* positivo) sobre el flujo de informaciones que afectan a cada sujeto.

32.4 La pertenencia del dato en la ley 25.326

El capítulo VII de la ley reglamentaria habilita un procedimiento para la protección de los datos personales por el que se destaca la amplitud prevista para la legitimación activa (tema que abordaremos más adelante).

El artículo 34 (Legitimación activa) sostiene: "La acción de protección de los datos personales o de habeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.

"Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.

"En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo"

El derecho a tutelar los datos no se visualiza como un derecho subjetivo, individual y personalísimo. Pareciera plantearse al dato como un problema de propiedad a defender.

En realidad no planteamos algo novedoso al decir que la intimidad, la privacidad, la identidad personal son también "derecho de propiedad". Warren y Brandeis en su clásica obra sobre la intimidad dijeron en 1890 que *"el derecho a ser libre garantiza el ejercicio de un amplio haz de derechos subjetivos; y el término "propiedad" abarca en su significado actual, todo tipo de derechos de dominio, tanto tangibles como intangibles"* En esa *evolución "el mayor aprecio de las sensaciones...hicieron ver al hombre que sólo una parte del dolor, del placer y del disfrute de la vida reside en las cosas. Pensamientos, emociones y sensaciones exigían su reconocimiento legal"*

> Sin embargo, -agrega Loianno- estos autores encuentran alguna dificultad en asimilar la intimidad con el derecho de propiedad cuando analizan su ausencia de valor económico, que "*no reside en el derecho a obtener ganancias...sino en la tranquilidad del espíritu y en el alivio que proporciona impedir su publicación*".
>
> Por el contrario, -afirma- creemos que tanto la intimidad como la identidad personal poseen todos los atributos de la *propiedad* en la medida que constituyen bienes valiosos en sí mismos aún cuando no siempre pueda ese valor ponderarse en dinero. La evolución producida en las áreas de protección jurídica de la esfera más íntima de la persona humana justifican esta apreciación.

En todo caso las herramientas constitucionales que garantizan la propiedad son aplicables sin mayor dificultad cuando el objetivo es salvaguardar la esfera más personal del individuo.

Uno de los aspectos más importantes en este tema es distinguir por donde pasa la línea divisoria entre lo auténticamente privado y aquello que afecta los intereses de terceros.

Fundamentalmente, el problema se manifiesta respecto de la incidencia que tienen en los ámbitos reservados a lo privado, los medios de prensa y la informática.

Si en la actualidad resulta insuficiente concebir a la intimidad como un derecho de estatus negativo de defensa frente a la probable intromisión de terceros, ello se muestra con mayor exigencia frente al flujo de informaciones concernientes al sujeto, relativas a su privacidad y a la definición de su propia persona.

Es así como pueden identificarse principalmente dos fuentes de intromisión:

a) *Los bancos informáticos de datos personales*, que frecuentemente abarcan zonas que debieran ser vedadas al conocimiento público por ser reservadas a la intimidad de las personas. La protección constitucional opera aquí garantizando la veracidad de los datos así como el control de la confidencialidad en lo relativo a "*datos sensibles*".

b) *Los medios de prensa* desde la perspectiva de la ofensiva de los multimedios sobre los espectadores, lectores u oyentes considerados como consumidores.

Aquí se ubican dos aspectos diferentes de lesión a la intimidad: 1) La que se produce a través de la intromisión o divulgación de la vida privada y 2) La que provoca la información como condicionante de conductas o ideologías.

La garantía de la libertad de prensa sin censura previa, sustento esencial del estado democrático de derecho, se complementa en este aspecto para preservar el derecho a la privacidad, honor y nombre de las personas, con dos garantías constitucionales: el resarcimiento (*alterum non laedere*) y la réplica. Esta última a través de la jerarquización constitucional de la Convención Americana de Derechos Humanos.

33. Los datos de las personas jurídicas

Una de las cuestiones más debatidas en la problemática de los datos personales radica en saber si la tutela alcanza a las personas de existencia ideal.

La cuestión tiene diversos enfoques, pero siempre debemos partir del objeto jurídico que protege el hábeas data o los derechos que cuenta el afectado, para verificar cuando se tiene posibilidad de lograr la defensa prometida constitucionalmente.

Los datos personales afectados por la invasión informática aparecen vulnerables cuando se encuentran en una base de información que los almacena sin el consentimiento del individuo. La afectación se puede dar, también, cuando el dato es inexacto o no refleja la verdadera identidad de la persona o contiene información agraviante o discriminatoria. De igual modo, si el archivo tiene información sensible no autorizada a divulgar, se produce un agravio que la ley de protección de datos debe tener en cuenta.

Cada supuesto advierte que desde la vulnerabilidad del secreto y confidencialidad se puede llegar a lesionar la intimidad de las personas, para encontrar un acto lesivo específico en la honra agraviada, la reputación afectada, la imagen distorsionada, la humillación personal por la revelación de un dato sensible, y así, unas cuantas maneras más de lesionar la vida privada de las personas a partir de la publicidad de los datos individuales.

Ahora bien, esa información afecta por igual a personas físicas y jurídicas, porqué no existe razón para excluir del derecho a la protección de los datos a los grupos ideales que preservan, en idéntica dimensión, la reputación, imagen empresarial, seriedad institucional, confianza y seguridad, etc., para corresponderlos con las acciones dichas para las personas físicas en el párrafo anterior.

Sin embargo, la conclusión no tiene coincidencias prácticas en la doctrina y menos aun en la jurisprudencia.

No obstante, es oportuno reiterar que la ley reglamentaria esclarece el punto al sostener en el párrafo segundo del artículo 1º que:

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

33.1 El dato como derecho personalísimo

La postura clásica de los derechos derivados de la personalidad los encuentra como innatos a la persona y de fuerte contenido individual, en el sentido de ser propios e intransferibles.

> Ekmekdjian y Pizzolo apuntan que estos derechos presentan las siguientes características: a) son *innatos*, o sea, corresponden al titular desde el origen de éste; b) son *vitalicios*, en cuanto acompañan al ser humano durante toda su vida; c) son *inalienables*, en cuanto no son susceptibles de enajenación por ningún título, están fuera del comercio; d) son *imprescriptibles*, porque no son alcanzados por los efectos del tiempo que no influye en su pérdida, no obstante el abandono del titular; e) son de carácter *extrapatrimonial*, aun cuando la lesión de estos derechos pueda generar derechos patrimoniales; f) son *absolutos* en cuanto se ejercen *erga omnes.*

Cuando se establece que la protección de los datos se fundamenta, exclusivamente, en la defensa de la intimidad parece imposible encontrar este derecho en las personas jurídicas, pues no hay intimidad propiamente dicha, como sí un derecho al secreto, a la discreción, o bien a la reserva de la vida privada que bien puede tener una empresa, entidad, asociación o cualquiera otra forma de personalidad ideal.

En consecuencia, la personalización del derecho, propio de la consagración del subjetivismo jurídico, no se podría extender a quienes no tienen individualidad física, pensando que la dimensión jurídica de la persona no alcanza para atribuirle un derecho al honor, a la vida privada y, en menor medida, a la imagen.

La causa de la limitación se sostiene en el carácter de derecho humano que tiene la intimidad, condición que no poseen las personas ideales; y además, en la exigencia de tutelar un interés propio, directo y exclusivo como es la vida privada de las personas, que no son naturales en los grupos que, por su propia calidad, viven en permanente relación pública.

> El objeto del derecho radica en la intimidad, como algo que es al tiempo diferente tanto de la vida privada, como de la privacidad, como de la vida pública. Siendo como es el de intimidad un concepto jurídico indeterminado la cuestión radica en trazar siquiera sea aproximadamente sus perfiles, diferenciarle de los conceptos afines y establecer directrices para su concretización. De esta forma sostiene Martínez Sospedra que, la diferenciación entre privacidad, vida privada e intimidad dista de ser clara, al menos por lo que a los dos últimos conceptos afecta. Si la *privacy* anglosajona se corresponde parcialmente con el derecho que estudiamos, pero también con otros derechos del art. 18 CE sustantivizados por el constituyente español, como pone de relieve el antecitado informe Cutter, lo que facilita la diferenciación, es preciso reconocer que trazar el perfil de la intimidad es harto complicado, razón por la cual ha podido señalarse que el concepto mismo de intimidad es una mala herramienta de trabajo, es un cesto para recoger agua.

33.2 Intimidad y datos de la persona jurídica

Si el planteo anterior se realiza desde otra perspectiva, las respuestas podrían cambiar. En efecto, la afirmación que precede sostiene que la intimidad es un derecho personalísimo, y los datos –como una parte de ella- que se encuentran contenidos en archivos afectan de manera directa a la persona física cuando se revelan o almacenan en condiciones ilegítimas o desautorizadas por su titular.

Otra visión encuentra que la intimidad no se la vincula estrictamente con la vida privada y sí con un derecho de exclusión y reserva, desde el cual se puede construir un derecho propio para las personas jurídicas. En lugar de proteger la intimidad en sí misma, se defiende la intimidad de quien la reclama, abriendo panorámicamente los objetos y razones de la pretensión.

> Determinada persona jurídica podría interponer la acción de hábeas data, frente a los registros o bancos de datos de un organismo oficial o privado, si considera que estos datos podrían afectar su honor comercial (v.gr.: figurar como deudor de un crédito, cuando ya se ha cancelado la deuda) o su intimidad (v.gr.: datos que revelan la donación de fondos a algún partido político o credo religioso). A estos

> ejemplos de Ekmekdjian y Pizzolo, los autores agregan: “Si en situaciones iguales se les concede tal facultad a las personas físicas, ¿porqué discriminar a las jurídicas cuando las consecuencias no se discriminan? En otras palabras, si los individuos pueden ejercer un derecho de acceso a los bancos de datos personales almacenados en una entidad ¿por qué no podrían hacerlo las personas jurídicas?.

La cuestión no es pacífica si la intimidad se adquiere como derecho absoluto, pero cambia sustancialmente si la interpretación se asume confrontando la realidad del diario acontecer.

Es evidente que el criterio tradicional como se interpreta a la intimidad deja fuera de las posibilidades de reclamo a los entes ideales, por ejemplo, para el derecho al secreto de las conductas sexuales, la vida familiar, las creencias religiosas, las inclinaciones políticas, o en suma, los datos sensibles *lato sensu*. En cambio, si la visión se focaliza en los datos, exclusivamente, evidentemente la protección diferida por el hábeas data no se puede restar de las garantías que tienen las personas jurídicas.

Son varias las razones por las que se argumenta la protección de los datos aunque puedan variar los motivos. Con ello se quiere decir que no es igual la protección del honor de la persona física que la reputación de la persona jurídica; que es distinta la imagen individual respecto a la corporativa; que difiere la dignidad individual de aquella que privilegia el objeto social; y así, sucesivamente, podrán aparecer diferencias por la naturaleza de las personas, pero que a la par de los derechos encuentran simetrías posibles.

El caso del honor es una probabilidad a tener en cuenta. Este puede ser atacado por la divulgación de actos, hechos, noticias, etc., relativas a personas tanto físicas como sociales; y cuando el prestigio o la confianza de una sociedad se pone en duda a consecuencia de la revelación de datos, es indudable que ese conocimiento que los demás asumen sobre la persona ideal afecta su activo patrimonial.

> Ahora bien, dice Herrero Tejedor, distinto es el caso de las instituciones sin fines de lucro, sino de participación, opinión o defensa de ideas o creencias. Nos referimos, por ejemplo, a los partidos políticos, sindicatos, asociaciones, confesiones religiosas, fundaciones, etc. En ellas se hace indispensable la posesión de una honorabilidad clara, pues su desprestigio haría muy difícil la obtención de sus fines sociales. Por ello, el autor acepta la idea de extender la protección de datos personales hacia las personas jurídicas.

33.3 El derecho internacional

Cuando se dijo sobre la ausencia de un criterio unívoco en la protección dispensada a las personas jurídicas se tuvo en cuenta la diferencia de criterios existente en las legislaciones locales e internacionales.

La O.N.U., en sus directrices sobre la protección de grupos ideales * incorpora una cláusula optativa, por el cual sostiene que se pueden tomar disposiciones particulares, igualmente facultativas, para extender la aplicación total o parcial de los principios recogidos en el reglamento general de archivos sobre personas físicas.

> Ello significa, afirma Estadella Yuste, que los Estados pueden optar por la extensión de las disposiciones de las líneas directrices de la ONU sobre ficheros automatizados de datos personales a los ficheros de las personas jurídicas. En uno de los proyectos previos a la redacción final de este instrumento se había propuesto la inclusión incondicional de los ficheros de las personas jurídicas.

En cambio la OCDE * no incluye a las personas de existencia ideal por cuanto se considera que existen otros reglamentos que logran idéntica protección, sin interferir en derechos que son de típica raigambre individual.

> Las directrices de la OCDE, no incluyen, de forma expresa –sostiene Estadella Yuste- a las personas jurídicas en su *ratione materiae* .La doctrina permanece dividida sobre la posibilidad de que este instrumento permita o no extender su aplicación a las personas jurídicas. Pero parece que la postura que niega tal posibilidad es la más plausible por basarse en la exposición de motivos de las propias directrices. Esta exposición de motivos sostiene que las nociones de

> integridad individual y privacidad tienen características peculiares que no deben ser tratadas de la misma forma que la integridad de los grupos de personas, la seguridad y la confidencialidad empresarial. Igualmente se afirma que no sólo las necesidades para la protección de las personas físicas y jurídicas son diferentes, sino que también lo son los marcos políticos donde se deben encontrar soluciones para equilibrar los intereses existentes. Por consiguiente, se debe concluir que las personas jurídicas no quedan amparadas en el ámbito de aplicación de las directrices puesto que la exposición de motivos descarta tal posibilidad y, además, el texto legal no las incluye ni expresa ni implícitamente.

La Comunidad Económica Europea, tanto en el Convenio 108 como en la Directiva 95/46 sólo afirman la tutela de las personas físicas; temperamento que no fue receptado fielmente por los Estados partes, si observamos que Austria, Dinamarca, Islandia, Luxemburgo, Noruega y Suiza por ejemplo, admiten que las personas jurídicas tengan igual protección que los derechos humanos. Criterio que mayoritariamente han aceptado las Constituciones latinoamericanas.

> Resulta significativo, dice Herrán Ortiz, que los países nórdicos, caracterizados por su elevada y temprana conciencia en materia de protección de datos, se haya reconocido el derecho a la autodeterminación informativa a las personas jurídicas. Por el contrario, no ha sido ésta la decisión adoptada por legislaciones tales como la francesa, alemana, portuguesa o británica que niegan a la persona de existencia ideal la condición de beneficiario de los derechos y garantías que integran el derecho a la autodeterminación informativa.

En España, que ha sido fuente de inspiración de nuestros proyectos de ley, y se refleja en la actual reglamentación, se tiene como sujeto activo de la protección de datos personales, únicamente a las personas físicas; lo cual se funda en el carácter fundamental de la garantía, interpretada como un derecho humano; y en la existencia de legislación *ad hoc* que solventa con similar contundencia los fines de la autodeterminación informativa.

34. Las garantías procesales en la protección de datos

De lo que llevamos diciendo se puede deducir que la herramienta procesal destinada a proteger los datos personales es el hábeas data, el cual se fundamenta en los carriles constitucionales expresos del artículo 43 y en los implícitos del artículo 18, como reglas para un debido proceso. No se descarta la operatividad del artículo 14 que interpretado de consuno con el art. 43 abre nuevos rumbos a la legitimación procesal, ni al art. 75 inciso 22 que, con la incorporación de pactos y tratados, solidifica el derecho al proceso breve y sencillo. La reglamentación culmina un cuadro que ya estaba solidificado pero que necesitaba de los esclarecimientos aportados.

Ahora bien, esa garantía tiene una finalidad específica; no se trata de resolver con ella un impedimento para negar información personal o suprimir aquella que estuviera registrada en un banco de datos; sino de permitir que sea el propio interesado quien decida el destino de esa información y su permanencia en la base creada.

A partir de esa libertad puede, siguiendo un orden lógico en las pretensiones, *perseguir el acceso* a la fuente de información que lo concierne; y después, una vez verificado el registro personal de sus datos, disponer el control sobre ellos, ya sea para mantenerlos actualizados, reemplazarlos con los que sean exactos y veraces, solicitar la confidencialidad estricta de la información privada, o bien, plantear la supresión por alguna de las razones que enseguida se verán.

> Según Herrero Tejedor, esto constituye el “right to privacy”, es decir el derecho de acceso a los bancos de datos, el derecho de control de su exactitud, el derecho de puesta al día y rectificación, el derecho de secreto para los “datos sensibles”, y el derecho de autorización para su difusión.

34.1 Derecho de información

Hablamos aquí de un derecho distinto a la información que se le debe proporcionar al sujeto que admite incorporar sus datos a un archivo con el fin de darles un tratamiento automatizado. También difiere de aquél derecho a la exactitud que planteamos como garantías para el usuario.

El derecho a la información que se instala entre las garantías del hábeas data, no piensa en el carácter individual sino en el alcance general que tiene "toda persona" para solicitar información sobre la existencia de bancos de datos, sus finalidades y la identidad de sus responsables.

> El reglamento actual establece en el artículo 13 (Derecho a la información) que: "*Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o banco de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita*".

Tal como se orienta en el derecho comparado esa idea de amplia circulación de los datos, el derecho a la información se presenta como una garantía de la publicidad de los actos que lleven a cabo los archivos.

Quizás fuera mejor establecer como deber de los bancos de datos producir periódicamente un informe, antes que dejar en la iniciativa de las partes el control eventual de la transparencia en el tratamiento de datos personales. Así lo hacen algunas legislaciones (v.gr.: Portugal, Gran Bretaña, Suiza, Noruega, entre otros), donde se destaca la ley finlandesa que impone al responsable la elaboración de una lista de ficheros de personas que deben estar a disposición del público.

> Por otro lado, dice Herrán Ortiz, y en coherencia con la discusión que venía enfrentando a los conceptos de "tratamiento de datos" y "fichero de datos", la Directiva, al igual que habían hecho ya algunas legislaciones, opta por introducir el registro o notificación de tratamientos, como concepto más dinámico y omnicomprensivo en el sistema de protección de datos personales.

La finalidad del derecho a la información no consiste únicamente en saber quienes son los titulares ni cuantos bancos de datos existen; la garantía proyecta un control directo sobre el tratamiento que se efectúa sobre la información que a la persona le atribuyen. De este modo, cuando se pretenda deducir una calidad particular, una cualidad determinada, un perfil o personalidad de alguien, a partir de los datos que el archivo hubiere procesado, la conclusión será nula por estar ausente el derecho del afectado a conocer el informe que le concierne de manera tan directa.

Esta elaboración es común para ciertas decisiones judiciales o en algunos actos administrativos que adoptan un criterio a partir de la valoración lograda del tratamiento automatizado de datos personales; y se observa agudamente en los servicios informatizados de información crediticia que suelen elaborar un perfil de la persona a partir del cumplimiento de sus obligaciones patrimoniales.

> En nuestro país se abre un panorama similar desde la sanción de la reforma constitucional que admite la garantía del hábeas data pero acotada a la iniciativa de parte interesada. Ello no obsta a que se pueda exigir la transparencia de los archivos, sobre todo los de carácter público, que tienen una obligación inmediata con el ciudadano.
>
> Ahora bien, este derecho no debe confundirse con el derecho de acceso a la documentación administrativa; pese a que tiene una evidente vinculación con algunos derechos fundamentales como el derecho a la participación en los asuntos públicos, o el derecho a comunicar y recibir libremente información auténtica, o el más próximo que lo relaciona con el derecho a la tutela judicial efectiva. Sin perjuicio de esta vinculación, dice Peñarrubia Iza, el derecho de acceso a la documentación administrativa es un derecho constitucional, pero no un derecho fundamental, en cuanto no está ubicado sistemáticamente entre los derechos fundamentales. Para convertirse en un derecho subjetivo, basta con el reconocimiento expreso que hace la Constitución, si bien el mismo precepto que menciona este derecho se remite a las leyes, lo cual significa que hay un principio de reserva de ley para delimitar este derecho, es decir, que el modo concreto de

> ejercicio, la legitimación y cualesquiera otros aspectos, sobre todo en lo que respecta a los límites, han de ser establecidos legalmente.

En síntesis, el derecho a la información es una garantía general para la publicidad de los actos de tratamientos de datos personales que efectúen los archivos. La regla mínima es difundir el nombre y los responsables de cada banco de datos, y las extensiones radican en las consecuencias que pueda tener la información aportada sin dicho conocimiento general.

Como es bastante difícil lograr este criterio de publicidad abierta y nulidades eventuales, se han pensado mecanismos que, ejerciendo formas de control directo, obliguen a cumplir las pautas de transparencia.

> Sin embargo, apuntan Ekmekdjian y Pizzolo, este criterio inicial fue abandonado paulatinamente, entre otras razones, porque el resultado de esta actividad no garantizaba una protección mayor de los datos personales. En la actualidad se utiliza una interpretación más restrictiva y cercana al derecho de acceso, que consiste en que los titulares del registro, o banco de datos transmiten una comunicación sobre la información en su poder, previa solicitud del afectado (v.gr.: mediante la acción de hábeas data).

Finalmente, este derecho general tiene un hondo sentido práctico en el derecho de acceso de la persona afectada. Por ello, los beneficiarios del derecho a conocer –como lo denomina Estadella Yuste- son, por un lado, la sociedad en general y, por otro lado, las personas que, como entidades individuales, tienen un interés concreto sobre la información que les concierne, y que se encuentra recogida en ficheros automatizados, llegando a poder ser objeto de transmisión internacional.

> Básicamente –agrega Estadella Yuste- el derecho a conocer consiste en saber de la existencia de ficheros que contienen datos individuales, el propósito o finalidad que se persigue con la creación del archivo, la identidad y residencia del titular o responsable del fichero, y si este fichero va a entrar a formar parte de la circulación internacional de datos. Al conocimiento de estas generalidades tienen derecho los individuos en cuanto forman parte de la sociedad. No obstante, el derecho a conocer amplía este contenido cuando las personas, como entidades individuales, son las que ejercen este derecho individual.

34.2 Derecho de acceso

El derecho a solicitar y obtener información de un archivo o registro, para saber si el mismo contiene o no, información personal que a alguien concierne, constituye el fundamento esencial del hábeas data.

Es el derecho de entrada a los bancos de datos y la garantía principal que tiene la persona para conocer qué información existe sobre ella.

Resuelto el problema del acceso, el individuo puede resolver conductas posteriores. En este sentido, validará la información contenida; podrá ratificar la autorización prestada si ella se hubiese requerido; tendrá la facultad de exigir la actualización o rectificación de los datos; planteará la supresión del dato sensible, y en cada caso queda de manifiesto el poder de control de la persona sobre los archivos de datos personales.

> Falcón explica la faz procesal de este derecho, sosteniendo que comprende dos pretensiones sucesivas y secuenciales, una subsidiaria de la otra. La primera de información y la segunda de conocimiento y ejecución…Como se ve, se trata de un proceso complejo, con inversión sucesiva de pretensiones. Así la presentación, que puede ser planteada por vía de proceso sumarísimo o similar expedito, llamado en algunos ordenamientos extraordinario y aun plenario rapidísimo, debe contener una pretensión primaria destinada a que se informe al juzgado de los datos registrados por el Estado (en sí o en cualquiera de las reparticiones), instituciones o particulares referentes al actor, la finalidad de los mismos y en su caso las medidas a tomar sobre dichos datos. Dichas medidas se pueden pedir en

> ese mismo acto (de modo directo o cautelar) si se conocen o presumen, o reservar esta segunda petición para el momento en que se haya contestado el informe. No obstante los contenidos de la petición inicial, no limitan la segunda petición a la luz del informe presentado. La primera etapa del procedimiento entonces será de naturaleza informativa y voluntaria, la segunda podrá tener el carácter de contenciosa.

De alguna manera, como antes se dijo, es la libertad de requerir que "se traigan los datos", cual si fuera la acción exhibitoria propia del hábeas corpus. Aun cuando es preciso destacar que el acceso no se dirige justamente a los datos sino al archivo que los contiene, y por ello las posibilidades de lograr el control varían con la forma como se presenta el pedido.

El acceso será directo cuando la información se pueda lograr por la simple consulta al banco de datos, y éste la evacue por un medio escrito o la deje disponible en un medio electrónico por el cual se pueda lograr una rápida visualización.

En cambio, si el requerimiento necesita de la colaboración judicial, se deben adoptar los recaudos típicos de las formalidades para demandar, teniendo en cuenta que se trata de un proceso constitucional que no podrá ser anulado por el principio de legalidad instrumental.

El sistema actual sostiene que *"el titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes"*. El inciso 3 del art. 14 agrega que: *"El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto"*

La idea no es poner exigencias previas que hagan vulnerable el derecho de acceso, tales como los recaudos de legitimación o personalidad procesal, sino en su lugar, tener por suficiente la acreditación de identidad que efectúe la persona afectada o aquella que demuestre un interés legítimo para realizar el requerimiento.

> Dice Herrán Ortiz que el derecho de acceso presenta en la ley española una amplia variedad de posibilidades, que pueden ser resumidas en la siguiente idea: lo verdaderamente trascendente es que el afectado tenga constancia de la información relativa a sus datos personales registrados, de un modo claro, completo y exacto, de suerte que se procure al afectado el conocimiento de aquellos aspectos fundamentales del tratamiento automatizado de sus datos, para poder ejercitar una defensa de sus derechos con ciertas garantías jurídicas.

Es importante destacar que el derecho de acceso no le corresponde únicamente al particular afectado por la información almacenada en un banco de datos sino a toda persona que acredite un interés legítimo para actuar.

a) *¿Acceso al archivo o a la información?*

Uno de los problemas habituales en la garantía ofrecida está en resolver si el acceso supone visualizar directamente el banco de datos, con lo cual el derecho de entrada podría suponer estar en el mismo sitio donde se produce el tratamiento de los datos (y conseguir en ese acto la revelación).

Sin embargo, de esta manera se violaría la seguridad que los archivos deben preservar, razón que sugiere que el derecho de acceso se resuelva a través de la información que se debe brindar.

Nuestra ley establece en el artículo 14 inciso 2 que: *"El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley"*.

Además, es conveniente agregar que el derecho de acceso a la información no supone otro derecho similar como es acceder a la documentación del Estado.

> Nos referimos a los supuestos especiales de aquellos datos personales que se almacenan para fines administrativos, que deben ser objeto de registro permanente (v.gr.: bancos de datos de las fuerzas armadas; fuerzas de seguridad; organismos policiales; servicios de inteligencia), o bien, proporcionan estos archivos información a las autoridades administrativas o judiciales en virtud de una autorización legal precedente.

El artículo 23.2 de la ley de hábeas data argentina dispone que: "*El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad*".

b) *¿ Cómo se accede a los archivos extranjeros?*

Otra cuestión que debe ser analizada es la radicación extranjera del banco de datos, porqué las distancias pueden solapar el derecho general de información que tienen todas las personas; como también dificultar el encuentro con la base originaria de la información personal.

Cuando se desconoce de que fuente proviene el uso de los datos individuales, el derecho de acceso se puede encaminar a través de los organismos de control locales, para que sean éstos quienes asuman el derecho del afectado.

> Afirma Estadella Yuste que numerosas son las ocasiones que en la práctica los titulares de los ficheros niegan el derecho de acceso por considerar que la información personal recogida no es objeto del derecho de acceso, ya que el fichero donde está almacenado no es de carácter nominativo, sino mixto.

No se trata de una sustitución, propiamente dicha, porqué el interesado mantiene la potestad de insistencia ante quien se obliga por sus datos. Quizás el mayor problema podría surgir de aquellos países que no cuenten con ley de protección de datos, a los que puede aplicarse el principio de la "protección equivalente", y negar el acceso basados en el fundamento del trato igualitario que recoge el principio citado.

c) *¿A partir de qué momento se tiene derecho de acceso al archivo?*

También hay que aclarar que el derecho de acceso se tiene a partir del mismo momento que ingresan al archivo, sin importar si los datos personales fueron o no motivo de tratamiento automatizado.

> ¿A partir de qué momento los datos personales pueden ser objeto del derecho de acceso? Se pregunta Estadella Yuste. ¿Pueden incluirse los datos registrados provisionalmente?, o bien ¿debe ejercerse este derecho en los datos personales que ya han sido objeto de operaciones automatizadas?, ¿puede ejercitarse el derecho de acceso sobre los datos almacenados?. Entiendo –agrega- que en los dos primeros casos es posible ejercer el derecho de acceso; sin embargo, en el supuesto de información almacenada cuyos nexos de identificación ya han sido eliminados, se podría aceptar la negación del titular del fichero para el derecho de acceso, siempre que éste garantice que los datos serán borrados del sistema una vez cumplida la finalidad del fichero.

d) *Finalidades del derecho de acceso*

De acuerdo con la finalidad que la petición de acceso persiga, el derecho concreta modalidades implícitas en la garantía a preservar. Es decir, el derecho de acceder a los bancos de datos supone que se especifique para qué se quiere entrar en ellos y qué es lo que se quiere conocer.

A veces la información pretende saber el contenido de la información personal almacenada; en otras, además, se plantea inquirir el medio por donde se obtuvieron los datos; también es posible reclamar para qué y para quien se realizó el registro; y con menor intensidad, indagar los medios utilizados para alcanzar la finalidad para la cual la información ha sido recogida.

> Cada una de estas pretensiones ha llevado a Sagüés, a presentar una clasificación en el hábeas data, nominando subtipos específicos: a) *exhibitorio*, que consiste en saber qué se registró; b) *finalista*, que procura indagar además para qué y para quién se realizó el registro; c) *autoral*, cuyo propósito es inquirir acerca de quien obtuvo los datos que obran en el registro.
>
> Por su parte Puccinelli, agrega: a) aquel que tiene por objeto indagar sobre la existencia y localización de bancos y bases de datos que existe en algunos países, y que tiene como objetivo final el garantizar el ejercicio de los derechos de aquellos que se hallen potencialmente afectados, estableciendo la obligatoriedad de inscribir a las bases y bancos de datos en un registro especial que puede ser objeto de consulta; y b) aquel que puede utilizar quienes pretenden acceder a la información pública, que funciona cuando no se les permite el acceso a ella sin la debida justificación (obligación legal de reserva, motivos de seguridad del Estado, etc.), y que, aunque para nosotros es otra versión principal, denominada "hábeas data impropio", se puede englobar en la clasificación de Sagüés.

34.3 Derecho a controlar el archivo y los datos personales

La base del derecho a la protección de datos personales está en el libre consentimiento que pueda dar quien sea requerido a esos efectos, y en el control que *a posteriori* se pueda ejercer.

Esta vigilancia apunta hacia dos objetos precisos. Controlar al archivo autorizado para que cumpla la finalidad oportunamente expuesta al requerir la autorización; y verificar la actualidad de los datos para que no se ofrezca información obsoleta, equívoca o inexacta.

En ambos casos rige el principio de "calidad de los datos", que como se recordará, establece los deberes que tiene el registro en cuanto a la adecuación, pertinencia y congruencia del almacenamiento con los datos autorizados que se van compilando de la persona concernida.

> Es necesario aclarar que el deber de actualización de los datos es del archivo y no de la persona afectada, incurriendo en negligencia el responsable que no cumpla con esa obligación de veracidad. Al respecto, ha señalado Orozco Pardo que la ley impone al titular del fichero: mantener los datos exactos y al día; rectificándolos de oficio, sustituyéndolos por los correspondientes datos rectificados y completos, sin que sea necesario que ello se solicite. Los datos deben cancelarse de oficio cuando ya no sean pertinentes o necesarios para la finalidad con que se recogieron, mientras tanto, deben estar almacenados de forma que posibiliten el ejercicio de los derechos de los afectados.

La vigilancia es un poder del afectado para controlar directamente al registro, pero se debe diferenciar del control externo que los bancos de datos tienen en los organismos que cada legislación suele crear al efecto.

a) *Derecho a la rectificación del dato*

Ante la obligación del archivo de mantener actuales los datos, se instala el derecho de la persona para requerir que se rectifique la información inexacta que le concierne.

El actual reglamento, establece en el artículo 16 inciso 1º, que toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.

No estamos hablando aquí del dato falso o discriminatorio que refiere el artículo 43 de la Constitución Nacional –como veremos más adelante- sino de la información errónea, es decir, la que una vez transmitida provoca un dato incierto por ser ajeno a la realidad.

Por ejemplo, si una persona figura como deudora de un crédito que pagó con posterioridad al registro, esa información es atrasada, y el deber de corrección es del archivo –de oficio, o a requerimiento expreso del interesado-.

En doctrina suele llamarse a este tipo de actuación como *hábeas data rectificador* o *correctivo*.

> El objetivo de este tipo de hábeas data –dice Puccinelli- es el de corregir o sanear informaciones falsas, aunque también podría abarcar a las inexactas o imprecisas, respecto de las cuales es factible solicitar determinadas precisiones terminológicas, especialmente cuando los datos son registrados de manera ambigua o pueden dar lugar a más de una interpretación (v.gr.: si una información proveniente de un sistema que suministra datos acerca de la factibilidad de otorgar créditos dentro de una Cámara comercial determinada, estableciese que tal persona es un "deudor inhabilitado" y ello obedeciese a que se encuentra inhabilitado para operar con el sistema, pero que no es un inhabilitado en términos jurídicos).

b) *Derecho a la actualización.*

También es posible encontrar informaciones incompletas que dibujan un perfil insuficiente y afectan el derecho a la verdad. En este caso, se debe incorporar al archivo la información parcialmente omitida.

> Un dato puede ser incompleto cuando no tiene toda la información necesaria. Otra cuestión diferente –dice Fappiano- es que los datos de una persona estén desactualizados. Por eso una de las obligaciones que tiene el titular o responsable del registro o banco de datos es llevarlos con toda precisión, pertinencia, perfección y actualidad; para lo cual está obligado a realizar todos los esfuerzos que sean razonables.

La puesta al día trabaja sobre el dato insuficiente, llamado también, dato inexacto o incompleto. No es información real para el tiempo donde se produce y por eso la finalidad es actualizar el registro.

> Señala la jurisprudencia que quien promueve un hábeas data debe primero tener acceso a los registros del caso para luego plantear la falsedad de la información, a lo que debe añadirse que esta falsedad puede resultar tanto de una clara inexactitud como de la desactualización de los datos que se suministran (Juzgado Nacional de Primera Instancia en lo Contencioso Administrativo nº 3, noviembre 2/995, *in re* "Nallib Yabran, Alfredo c/ Ministerio de Economía, Obras y Servicios Públicos").

La actualización de los datos pretende agregar información, antes que rectificar la existente; por eso, la doctrina divide o clasifica esta modalidad como *hábeas data aditivo* segmentado en subtipos *actualizador* (que persigue renovar el dato caduco), e *inclusorio* (incorporar al registro más información).

> Enseña Puccinelli –siguiendo a Sagüés- que este tipo de hábeas data procura agregar más datos a los que figuran en el registro respectivo, y puede ser utilizado, por ejemplo, para obligar a un banco de datos comerciales a colocar que una deuda asentada ha sido refinanciada, o que se es deudor como garante de una obligación contraída por un tercero cuyo monto ha sido controvertido judicialmente. En él confluyen dos versiones distintas: se puede utilizar tanto para actualizar datos vetustos, como para incluir en un registro a quien fue omitido.

c) *Derecho a la confidencialidad de los datos*

La autorización del titular para que los datos sean utilizados con la finalidad que el archivo le informa y en la medida del consentimiento prestado para su transferencia, implica que algunos datos pueden ser restringidos en cuanto a la libre difusión y cesión.

Como regla, los datos sensibles no se pueden circular sin permiso expreso, pero hay otros datos que se pueden mantener en confidencia dentro del registro, y sólo posibles de cesión cuando el titular lo autoriza.

La reserva que estudiamos en el parágrafo 4.6 muestra algunos ejemplos de este tipo de hábeas data, que algunos de los autores más prestigiados de la ciencia procesal constitucional definen como *hábeas data reservador.*

d) *Derecho al silencio y al olvido mediante la cancelación del dato*

Una cosa es ocultar información archivada en virtud del acuerdo de confidencialidad con la persona concernida; y otra distinta, otorgarle un derecho a silenciar todo conocimiento que se tenga sobre la vida privada cuando el conocimiento de obtiene de los agentes que intervienen el proceso de tratamiento.

Esto es consecuencia del deber de secreto y confidencialidad que los registros deben preservar. La violación o amenaza que potencialmente exista, la controla el afectado a través del proceso de hábeas data.

Asimismo, cuando el dato ha cumplido la finalidad para la cual se archivó, aparecen dos consecuencias que se traducen en derechos y deberes de la persona y el banco de datos, respectivamente.

El derecho se fundamenta en la potestad de reclamar la eliminación de toda información que violente la esfera de privacidad personal cuyo almacenamiento no fuera autorizado. También, el poder de exclusión o supresión permite demandar la cancelación del dato que se ha tornado impertinente o ha devenido innecesario.

> Los derechos al silencio y al olvido se recogen de la ley de tratamiento de datos española que obliga a las personas que intervienen en cualquier fase del tratamiento de datos a mantener reservada la información que adquieren en ocasión del trabajo. Se trata por tanto –afirma Orozco Pardo- de la situación en que la existencia y contenido de los datos debe quedar dentro del ámbito funcional y finalidad del fichero para el que fueron recabados evitando el "rumor informático" (derecho al silencio) y del derecho a que, de oficio, el titular o responsable cancele o destruya los datos personales cuando se den alguno de los supuestos antes citados, sin que tenga que mediar previamente el ejercicio del derecho de cancelación (derecho al olvido).

El deber, por su parte, es del titular del archivo, quien debe eliminar la información personal compilada que ha perdido interés, actualidad o sentido para el objeto inicialmente guardado.

El afectado, si considera que los datos carecen de pertinencia o devienen inadecuados, puede ejercer el derecho de cancelación o bloqueo de transmisión, propiciando en el pedido al registro que se borren todos los datos innecesarios.

> Para Sagüés, este tipo de hábeas data se denomina *exclutorio* o *cancelatorio*, interpretando que la eliminación procede en los casos en los cuales se trate de datos sensibles, aunque no existe una regla fija acerca de verificar cuándo procede esta vía constitucional. Puccinelli, por su parte, agrega que es factible incluir en esta versión a otra clase de datos que, sin resultar sensibles, de todas formas no puede ser almacenada por cualquier registro (como ocurre, v.gr., con las fórmulas de determinadas sustancias), pues aunque alguno las podrá contener de manera reservada, en los casos en que no se trata de un registro habilitado para ello, no bastará con infidenciarla, sino que es imprescindible su eliminación.

34.4 ***Excepciones al derecho de acceso, rectificación y supresión***

En líneas generales el derecho de control sobre los archivos y los datos personales se restringe en contadas ocasiones. Las veces que así ocurre se fundamentan en cuestiones de seguridad nacional, orden público, razones morales y políticas, sin perjuicio de los derechos y acciones que a terceros les corresponde cuando están afectados sus intereses legítimos.

> El artículo 14 ("Excepciones y restricciones") del proyecto de Convención Americana sobre Protección de Datos Personales * dispone que:
>
> Sólo por ley se podrán establecer excepciones y restricciones en los principios, derechos y garantías en esta Convención enunciados y siempre que éstas sean justas y razonables en una sociedad democrática:
>
> a) Para la protección de la seguridad del Estado de la seguridad pública, para los intereses monetarios del Estado o para la represión de las infracciones penales;
>
> b) Para la protección de las personas concernidas y de los derechos y libertades de otras personas;
>
> c) Para el funcionamiento de ficheros de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existe riesgo de que las personas sean identificadas. Siempre existirá recurso para que la autoridad judicial decida si en un caso concreto estamos ante una excepción o restricción razonable.

En la ley nacional se establecen como excepciones las siguientes (art. 17):

1. *Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.*
2. *La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.*
3. *Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.*

Es importante agregar que la obstaculización al derecho de acceso es considerada falta grave del titular o usuario del archivo.

35. El ejercicio del derecho de acceso y control

Los requisitos para entrar en los bancos de datos se clasifican por el lugar, el tiempo y la forma como se debe realizar.

El *lugar* donde plantear la pretensión es ante el titular del registro o archivo que tiene los datos personales del interesado. La categoría de la información personal puede eludir el derecho de acceso, por ejemplo, en los casos de hospitales y demás instituciones sanitarias –públicas o privadas- (ver art. 8º de la ley), la recolección de datos se ampara por el secreto profesional. De similar envergadura es la prohibición de acceso a los archivos de datos sensibles que únicamente se admiten crear cuando median razones de interés general, autorizadas por la ley.

La intervención de un tercero en el tratamiento de los datos implica obligarlo solidariamente con el titular del archivo, de manera que corresponde tener en cuenta el domicilio del cesionario, a los fines de deducir el reclamo administrativo.

Si el banco de datos no informa de conformidad con lo requerido, el lugar donde presentar el hábeas data es el del órgano de control que la ley establezca, imponiendo así una suerte de procedimiento previo para entablar la demanda judicial.

El *tiempo* para formular el pedido, siguiendo el derecho comparado, oscila entre intervalos de seis a doce meses.

> El reglamento sancionado en Argentina por el Senado, establece en el art. 14 inciso 3º, que el derecho de acceso sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al afecto.

> España, por su parte, está dicho en términos similares que el derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

La periodicidad para el ejercicio del derecho de acceso es un criterio que llega de las normas europeas, especialmente del Convenio 108 y de la Directiva 95/46/CE, aunque ninguna de ellas establece un tiempo determinado sino la elasticidad del período prudente y razonable, para admitir una cobertura amplia.

La *forma* de concretar el derecho está liberada de requisitos formales. Rige el principio de libertad sin solemnidades, aunque habitualmente los órganos de control presentan formularios que facilitan la fundamentación del planteo.

35.1 Condiciones generales

España es uno de los países más avanzados en la defensa y protección de los derechos sobre los datos personales. La creación de una "Agencia de Protección de Datos" ha permitido elaborar una serie de reglas técnicas que actúan a modo de orientadores para el ejercicio de los derechos *.

La petición de acceso a los archivos, así como los de rectificación y cancelación de datos son derechos de carácter personalísimos, condición que determina que sólo puedan ser ejercidos por el afectado frente al responsable del fichero.

Este debe acreditar su identidad frente al sujeto reclamado. Podrá, no obstante, actuar a través de mandatario cuando se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos, en cuyo caso será necesario que el representante legal acredite tal condición.

La ley configura los derechos de acceso, rectificación y cancelación como derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

La pretensión deberá llevarse a cabo mediante solicitud dirigida al responsable del fichero y contendrá:

- *Nombre y apellido del interesado acreditado con la fotocopia del documento nacional de identidad y, en los casos que excepcionalmente se admita, de la persona que lo represente, así como el documento acreditativo de tal representación. La fotocopia del documento nacional de identidad podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho.*

- *Petición clara y fundada.*

- *Domicilio a efectos de notificaciones, fecha y firma del solicitante.*

- *Documentos que respalden la pretensión.*

- *El interesado deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.*

El reclamo siempre es gratuito, tanto para el derecho de acceso como para la rectificación, actualización o supresión de datos personales.

> Inclusive, en la acción judicial de hábeas data, la jurisprudencia ha señalado que se encuentra alcanzada por la exención establecida en el artículo 13 inciso b) de la ley de tasas judiciales 23.898, ya que se considera a este proceso constitucional como una especie de amparo (CNCiv., Sala F, setiembre 1/998, *in re:* "Cosentino, Ricardo C. y otro c/ Organización Veraz S.A.").

35.2 Contenido de la información

El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción.

En el caso de que la solicitud no reúna los requisitos especificados precedentemente, el requerido podrá solicitar la subsanación de los mismos.

> El proyecto de Convención Americana sobre Protección de datos personales *, establece que:
>
> 1. Toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que los ampare contra actos que violen sus derechos fundamentales reconocidos por esta Convención, la Constitución de los Estado Parte o la ley.
> 2. Toda persona tiene derecho a controlar sus datos personales existentes en los ficheros públicos o particulares, la garantía y el procedimiento judicial para ejercer tal control es el hábeas data.

La información debe ser suministrada en forma clara, exenta de codificaciones y, en su caso, acompañada de una explicación en lenguaje sencillo que permita la interpretación simple por cualquier persona.

La producción de la respuesta ha de procurar ser amplia y completa, sin acotarse a los límites de lo requerido por el afectado o interesado.

Ese informe no puede revelar datos pertenecientes a terceros, aun cuando se vinculen con el emplazamiento y la respuesta consecuente.

35.3 Derecho de acceso.

Al ejercitar el derecho de acceso, el afectado podrá optar por uno o varios de los siguientes sistemas de consulta del archivo, siempre que la configuración o implantación material del fichero lo permita:

- Visualización en pantalla.
- Escrito, copia o fotocopia remitida por correo.
- Transmisión electrónica de la respuesta.
- Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo.

El requerido resolverá sobre la solicitud de acceso en el plazo de diez días corridos, el cual surtirá los mismos efectos que los reclamos administrativos a los fines de adoptar el silencio como forma expresa de denegación. También cabe la acción de amparo por mora en el pronunciamiento.

En el caso de que los datos provengan de fuentes diversas, deberán especificarse las mismas identificando la información que proviene de cada una de ellas.

35.4 Ejercicio del derecho de rectificación y cancelación.

Los derechos de rectificación y cancelación se harán efectivos por el responsable del fichero dentro del término máximo de cinco días contados desde que se recibió el reclamo del titular de los datos. Si los datos hubieran sido cedidos previamente, el titular del archivo deberá notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su registro.

El artículo 16 dispone en cuanto aquí interesa:

Inciso 2º *El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.*

Inciso 3º *El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.*

Inciso 4º *En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.*

Inciso 5º *La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.*

Inciso 6º *Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo o consignar al proveer información relativa al mismo, la circunstancia de que se encuentra sometida a revisión.*

Inciso 7º *Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.*

La solicitud de rectificación deberá indicar el dato que es erróneo y la corrección que se requiere, acompañada de la documentación justificativa.

Cuando se reclame la cancelación, el interesado deberá manifestar si revoca el consentimiento otorgado.

En la pretensión de supresión del dato erróneo o inexacto se ha de acompañar el respaldo instrumental pertinente. Este no procederá cuando pueda causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existe una obligación de conservar los datos.

Solicitada la rectificación o cancelación, el responsable del fichero podrá estimarla y comunicar los argumentos que resulten de la decisión a adoptar.

Transcurrido el plazo de cinco días sin que de forma expresa se responda a la solicitud de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación judicial que corresponda. Obsérvese que aquí la ley otorga un plazo en días hábiles a diferencia del derecho de acceso cuya respuesta se mide en días corridos.

En el trámite administrativo incoado y mientras éste se resuelve, el titular del archivo debe bloquear la información o consignar el estado de revisión en que se encuentra, obligaciones que generan responsabilidades consecuentes cuando no se cumplen de inmediato.

> La justicia nacional tiene resuelto que en un juicio de hábeas data cuyo objeto sea la supresión de información que se aduce inexacta, es procedente el dictado de una medida cautelar tendiente a que la demandada se abstenga de brindar el dato en cuestión, pues de mantenerse la situación de hecho aparentemente irregular, la ejecución de una sentencia favorable puede convertirse en ineficaz, en tanto la difusión anterior a su dictado es susceptible de influir definitivamente, con

perjuicio al derecho que se asegura, en el ánimo de quienes sabrían del dato en cuestión (arts. 195 y 230 inciso 2º, CPr., *in re:* CNCom., sala B, agosto 8/996, "Yusin, Mauricio G. c/ Organización Veraz S.A.").

La cancelación exige el borrado físico de los datos, sin que sea suficiente a estos efectos una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las bajas producidas.

En los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización.

Se exceptúa, no obstante, el supuesto en el que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

Bibliografía Capítulo IX

Ekmekdjian, Miguél Angel – Pizzolo, Calógero, *Hábeas Data. El derecho a la intimidad frente a la revolución informática*, editorial Depalma, Buenos Aires, 1996.

Estadella Yuste, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales*, editorial Tecnos, Madrid, 1995.

Falcón, Enrique M., *Hábeas Data*, editorial Abeledo Perrot, Buenos Aires, 1996.

Fappiano, Oscar Luján, *Hábeas data: Una aproximación a su problemática y a su posible solución normativa*, en "Liber Amicorum" Héctor Fix Zamudio, volumen 1, editorial Secretaría de la Corte Interamericana de Derechos Humanos, San José, Costa Rica, 1998.

Gozaíni, Osvaldo Alfredo, *La legitimación en el proceso civil*, editorial Ediar, Buenos Aires, 1996.

Gozaíni, Osvaldo Alfredo, *Introducción al nuevo derecho procesal*, editorial Ediar, Buenos Aires, 1988.

Herrán Ortiz, Ana Isabel, *La violación de la intimidad en la protección de datos personales*, editorial Dykinson, Madrid, 1999.

Herrero Tejedor, Fernando, *Honor, intimidad y propia imagen*, editorial Colex, Madrid, 1994.

Martínez Sospedra, Manuel, *Sobre la intimidad. Derecho a la intimidad, vida privada y* privacy. *El art. 18 CE* in principio *en la jurisprudencia del Tribunal Constitucional*, en *Sobre la intimidad*, editorial Fundación Universitaria San Pablo C.E.U., Valencia, 1996.

Orozco Pardo, Guillermo, *Los derechos de las personas en la Lortad*, en Revista Informática y Derecho, números 6/7, editorial UNED, Mérida, 1994.

Peñarrubia Iza, Joaquín María, *El derecho de acceso a los archivos y a los documentos de la Administración Militar*, editorial Cívitas, Madrid, 1999.

Perez Luño, Antonio E., *Derechos Humanos, Estado de Derecho y Constitución*, editorial Tecnos, Madrid, 1991 (4ª edición).

Puccinelli, Oscar Raúl, *El Hábeas Data en Indoiberoamérica*, en *El Amparo Constitucional, perspectivas y modalidades*, editorial Depalma, Buenos Aires, 1999.

Sagüés, Néstor Pedro, *Subtipos de hábeas data*, en revista Jurisprudencia Argentina del 20/12/95. Buenos Aires.

CAPÍTULO X. El secreto de las fuentes periodísticas

36. Planteo del problema

El derecho a expresar las ideas por medio de la prensa sin censura previa constituye la base del derecho que se ha incorporado con el artículo 43 de la Constitución Nacional, en el párrafo que indica que al interponerse la acción de hábeas data "*no podrá afectarse el secreto de las fuentes periodísticas*".

Si bien con esta mención fundamental la protección dispensada es obvia y suficiente, la ley 25.326 reglamentaria del citado artículo 43, no ha querido soslayar el fin constitucional, ratificando en el párrafo final del artículo primero que *"en ningún caso se podrán afectar las bases de datos ni las fuentes de información periodísticas"*.

El derecho a la información, posiblemente amplio y extenso en las características de su actual interpretación, afirma el pensamiento constitucional, ratificando que la prensa no puede ser amenazada ni requerida para revelar la fuente de los datos que fueron aplicados en su investigación o noticia.

De las convenciones internacionales se puede extraer que el derecho a la información, género de las manifestaciones que se proyectan (libertad de prensa, libertad de opinión, censura previa, etc.), tiene tres componentes esenciales: a) la libertad de investigar; b) la libertad de edición y difusión, y c) el derecho a recibir información y reservar, como secreto profesional, la confidencialidad de la fuente.

> Al conjunto de libertades que conforman el derecho a la información –sostiene Uicich- se le incorpora el derecho a no recibir informaciones distorsionadas o abusivas…,comprende pues la faceta de quien tiene la facultad de acceder a la información cuanto la del sujeto pasivo de esa información de que no sea distorsionada o no sea revelada en tanto afecte su intimidad y no exista cuestión de orden público o de seguridad del Estado que lo justifique.

Está claro que hablamos de un derecho muy distinto al de "réplica", también llamado "derecho de rectificación o respuesta", por el cual la persona que se siente afectada o agraviada por una nota periodística, puede exigir del medio de comunicación un espacio igual al que tuvo la publicación con el fin de dar su propia versión de los hechos revelados.

Tampoco se vincula con el problema de la censura previa donde la cuestión a resolver es la crisis de la garantía de intangibilidad que tiene la libertad de manifestar opiniones y pensamientos a través de la prensa, sin que ellas sufran cortapisas o impedimentos irrazonables, abusivos o arbitrarios.

El nudo a desatar en el tratamiento de datos personales, y en la acción de hábeas data pertinente, será el que refleje los límites eventuales de la divulgación periodística, cuando revele aspectos de la vida privada o cualquier otra información sensible que, como tal, afecta el derecho a la intimidad individual.

Libertad de intimidad versus libertad de información, esa pareciera ser la problemática, aunque es exagerado presentarlo como un conflicto donde ha de existir un derrotado y un victorioso.

El justo razonamiento podría emerger del artículo 32.2 de la Convención Americana sobre Derechos Humanos:

Los derechos de cada persona están limitados por los derechos de los demás, por la seguridad de todos y por las justas exigencias del bien común en una sociedad democrática.

> Recordemos que la Corte Suprema de Justicia de la Nación, en la causa "Campillay" del año 1986 afirmó que la libertad de expresión es la libertad de dar y recibir información pero que éstas no implican un derecho absoluto y el legislador ante los posibles abusos producidos mediante su ejercicio, tipifica diversos tipos penales y establece ilícitos civiles, ya que el ejercicio del derecho de informar no puede extenderse en detrimento de la necesaria armonía con los

> restantes derechos constitucionales, entre los que se encuentran el de integridad moral y el honor de las personas (arts. 14 y 35 de la Norma Fundamental).

37. Reglas y excepciones

La potencial controversia entre intimidad e información es más aparente que real, al menos en la medida de los resultados que perseguimos alcanzar en la protección de datos personales.

El periodista y el medio de comunicación no pueden estar maniatados por una reglamentación obtusa que cancele el derecho a investigar la vida de las personas o a publicar las conclusiones de una investigación que compromete la privacidad de alguien.

Más allá de admitir que las personas públicas tienen una privacidad restringida a su propia exposición, y que el anonimato del hombre común le facilita la vida privada, no se puede modificar la perspectiva del derecho humano que a todos corresponde, es decir, la fama y notoriedad no es una excusa para invadir la intimidad, pero tampoco impide el ejercicio de informar e informarse sobre aquello que se considere de interés general.

> Urabayen sostiene que entre los derechos a la intimidad y a la información hay que encontrar un equilibrio porque ambos son de esencial y equivalente importancia pero de no ponérseles límites, cada uno tratará de anular al otro. Ahora bien, como el interés general priva sobre el particular, podría partirse de la base de que el derecho a la información es la regla y el derecho a la intimidad la excepción, debiendo analizarse cada caso independientemente.

El punto de encuentro es la verdad revelada, y el límite la prohibición de falsedad y difamación.

En ambos casos, ninguna ley de tratamiento de datos personales podría modificar esta relación tomada de los hechos tal como suceden.

Supongamos que un periodista toma conocimiento de un hecho probablemente ilegal que sucede en un organismo público y decide investigar. Pensemos que confirma la intervención bochornosa de algún funcionario y decide elaborar la nota con fines de publicidad.

El eventual conocimiento que tome el afectado podría admitir el planteo defensivo de su intimidad a través de un hábeas data reservador, por el cual el Juez tendría facultades para ordenar la confidencialidad de los datos archivados en el banco de información periodístico evitando su divulgación.

Esta hipótesis no se puede sostener.

En efecto, el principio incanjeable es la libertad de prensa y la intangibilidad del secreto de las fuentes periodísticas, de forma tal que, a lo sumo, el afectado podría deducir una demanda por derecho de rectificación; una querella por calumnia o injurias; o en menor medida, un hábeas data donde se pretenda la rectificación o supresión de aquella información que demuestre ser inexacta o desactualizada.

> Pierini ed alter, sostienen que la acción prescripta por el hábeas data, entendida como el acceso a las registraciones, veracidad, rectificación y permanencia, está limitada por el reconocimiento de otro derecho de igual importancia, como el de informar. En consecuencia, respecto de las bases de datos o registraciones periodísticas, sólo se debe limitar a la rectificación y anulación de lo publicado que sea inexacto o desactualizado. No puede realizarse con anterioridad a la publicación, por cuanto aquéllos se desconocen y porque se trataría de una cuestión de censura previa, ya que, por inexactos que fueran, no se tiene conocimiento de ellos hasta su publicación o difusión.

De suyo, tampoco podría intimarse al periodista a revelar los fundamentos donde apoya sus conclusiones, porque de esa manera se ingresaría en el secreto profesional y en la invulnerabilidad que se garantiza a las fuentes de información periodística.

38. ¿Las fuentes de información son bases de datos?

La protección constitucional a las fuentes de información periodística ubicada en el capítulo garantista de los nuevos derechos fundamentales tiene su significado.

La fuente de información es el dato reportado por otro, en cuyo caso el conocimiento logrado se toma como una confidencia. La investigación, a su vez, permita reunir otro tipo de datos, que se van almacenando en un registro particular hasta conseguir una suma razonable de información que permita elaborar la nota u opinión a publicar. Este tipo de archivo no se encuentra entre aquellos que están destinados a proveer informes a terceros.

Una interpretación diferente se puede adoptar basando la coincidencia entre fuente de información previa a la edición y banco de datos destinados a proveer información, en cuyo caso la aplicación del artículo 43 se deduce inmediatamente.

> Pierini, Lorences y Tornabene dicen que hay que diferenciar la obligación de proporcionar la fuente, del caso de los registros, bancos de datos y demás registraciones relacionadas con la actividad periodística que no implican revelación de fuentes y que se refieren a constancias concretas existentes en ellos. Esta diferenciación entre elaboración de la nota y publicidad de la información adquirida no es antojadiza, sino que responde al criterio concreto referido a la libertad de informar, la cual debe preservarse y permitirse, pudiendo acarrear responsabilidades luego de ser ejercida y no previamente. Hasta el momento de la publicación de la información, los archivos y datos tienen la entidad, las características y el resguardo similares a los de las fuentes, o sea, no están alcanzados por norma alguna y se encuentran comprendidos dentro del secreto profesional y protegidos por el artículo 43 del mismo cuerpo legal. Luego de publicada la información, nadie podrá exigir válidamente el aporte de las fuentes utilizadas, pero la noticia ha adquirido una autonomía distinta y es objeto de recursos y acciones.

Nosotros creemos que las fuentes de información periodística están protegidas por el secreto profesional y por el ejercicio libre e incondicionado para opinar y publicar las ideas por medio de la prensa.

Mientras que los bancos de información almacenada que se bosquejan como "archivos periodísticos" están excluidos de la acción de hábeas data, al no estar destinados al tratamiento de datos personales, ni para proveer información a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Ahora bien, cuando la investigación está centrada sobre una persona en particular, es evidente que el proceso de recolección de datos invadirá el reducto de la privacidad individual, pero la fuente de información se mantiene confidencial y secreta. En todo caso el problema estará en resolver si el archivo periodístico está alcanzado por la protección constitucional del artículo 43, o puede ser abierto ante el emplazamiento del afectado.

> Si bien tienen un destino diferente, conviene informar el contenido del artículo 28 de la ley sancionada: *"1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a la ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable; 2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna"*.

A veces, se ha justificado desplazar el secreto profesional del periodista cuando "intereses del Estado" lo aconsejan, haciendo ceder el derecho de libertad de prensa por un hipotético interés superior.

> En la causa "Gorriarán Merlo" (C.Fed.San Martín, Sala I, mayo 2/996) se sostuvo que "*el secreto profesional periodístico y el derecho a resguardar las fuentes de información, cede cuando razones de interés público de relevante jerarquía así lo aconsejan y cuando ello no vulnera el derecho a no autoincriminarse, ni afecta los límites previstos en el artículo 28 de la Constitución Nacional*".

En los hechos, nos parece más razonable adoptar un criterio propio y adecuado a las circunstancias y contextos en los que cada información se origina. De este modo, la reserva y confidencialidad de las fuentes es una garantía impermeable, como lo es la libertad de prensa y el derecho a la información. Pero, al mismo tiempo, proporciona un deber inexcusable a los medios de comunicación para que desde una perspectiva ética y moral no difundan aquella información que, siendo disponible, pueda afectar la sensibilidad de las personas. La diferencia entre el *poder* de contar una gran cantidad de información sobre cada individuo y el *deber* de no difundirla sería más que nunca fundamental en este terreno.

> Esta idea reproducida de Aznar Gómez, agrega que, de lo contrario, el desfase entre ambos aspectos del problema podría aumentar la sensación social de indefensión de la intimidad frente a unos medios de comunicación –y otros agentes sociales- con recursos técnicos cada vez más sofisticados a la hora de obtener datos sobre cada uno de nosotros. Pero esto tampoco significa que la prensa deba silenciar cualquier información sin más, pues es tan negativo facilitar toda la información como acallar parte de ella sin ningún otro criterio que la decisión personal de cada informador. Otros criterios deben guiar la decisión: tener presente el tipo de persona involucrada en la noticia así como la naturaleza del asunto tratado.

39. La revelación voluntaria de la fuente periodística

El art.10 de la Convención Europea sobre Derechos Humanos permite a los periodistas resolver, de acuerdo a sus convicciones, la revelación de la fuente de información con el fin de dar mayor fuerza y contundencia a la publicación que realice.

Esta decisión voluntaria se concreta en cuestiones de interés general y en la medida que los hechos sean exactos y confiables, respetando la ética periodística.

> Por ende –ha dicho el Tribunal Europeo de Derechos Humanos en la causa, Fressoz y Roire c/Francia (21 de enero de 1999), es improcedente la condena dictada respecto del director de un semanario y el periodista que publicó declaraciones de impuestos del Presidente de una importante empresa automotriz si la información sobre el monto de los ingresos anuales de dicha persona estaba autorizada. Allí se agrego que, la sentencia que condenó al director de un semanario y a un periodista a resarcir el daño moral que entendió causado al Presidente de una empresa automotriz por la publicación de sus declaraciones de impuestos, efectuada en el marco de un artículo periodístico en el que se destacaban los incrementos salariales recibidos por el directivo mientras se oponía a similar medida reclama por los trabajadores de la empresa, viola la libertad de expresión tutelada por el art.10 de la Convención Europea sobre los Derechos Humanos, pues en el caso la publicación incriminada apareció en el marco de un conflicto social largamente tratado por la prensa y su finalidad no era perjudicar al directivo, operando la comparación entre los salarios de éste y el de los reclamantes como contribución a un debate público relativo a una cuestión de interés general.

Es decir, siguiendo la línea de pensamiento de la ley comunitaria europea, una injerencia en el ejercicio de la libertad de prensa sólo podría conciliarse con el art.10 de la Convención si se justifica por un imperativo preponderante de interés público.

Entre nosotros, la revelación voluntaria de la fuente periodística es una posibilidad más entre las que dispone el profesional para dar a publicidad su nota o comentario. La protección constitucional sólo a él preserva y no se extiende al confidente (la *fuente*, propiamente dicha) quien, en todo caso, tendrá un derecho de rectificación o respuesta, o un eventual reclamo indemnizatorio derivado de la violación al secreto revelado bajo confidencialidad.

Bibliografía Capítulo X

Aznar Gómez, Hugo, *Intimidad e información en la sociedad contemporánea,* en "Sobre la intimidad", editorial Fundación Universitaria San Pablo C.E.U., Valencia, 1996.

Pierini, Alicia – Lorences, Valentín – Tornabene, María Inés, *Hábeas Data*, editorial Universidad, Buenos Aires, 1998.

Uicich, Rodolfo Daniel, *Los bancos de datos y el derecho a la intimidad*, editorial Ad Hoc, Buenos Aires, 1999.

Urabayen, Miguel, *Vida privada e información: Un conflicto permanente*, editorial Universidad de Navarra, Pamplona (España), 1977.

CAPÍTULO IX. Derechos del titular de los datos

32. ¿Quién es el titular de los datos?

La protección que a la intimidad se confiere, en miras a evitar que la intromisión informática complique la vida privada de las personas, supone pensar que estamos frente a un derecho personalísimo que solamente le corresponde al individuo afectado por el almacenamiento, conservación y transferencia de sus datos personales.

> No es simple ocultar la facilidad como se pueden interceptar los datos en la red, ni eludir los desvíos que ellos pueden sufrir en su tránsito para ser leídos por personas no autorizadas. Por eso, interrogarse quien es el dueño de la información tiene su sentido, mucho más si quedan señalados los problemas de la seguridad en Internet, que podrían sintetizarse básicamente en dos sub categorías de conflictos:
>
> 1. los referidos a los riesgos a los que se ve expuesto un servidor Web, como por ejemplo, la exposición de documentos a terceras personas.
>
> 2. Los que se vinculan con la protección de las comunicaciones de los usuarios, ante el riesgo de la interrupción y captura de datos personales (información crítica) como tarjetas de crédito, cuentas bancarias, etc.

De este modo, se tomaría a la noción de derecho subjetivo como base de la acción y, ante una hipotética demanda, habría que demostrar la relación existente entre la titularidad de quien propone la pretensión, con el perjuicio efectivamente sufrido. Asimismo, se tendría que verificar la relación causal y el derecho a las medidas que solicita.

Sin embargo, la explicación que precede no es absolutamente cierta. En efecto, la titularidad de los datos contrae algunas dificultades de intelección, porqué una cuestión son los derechos que tiene la persona afectada por el tratamiento de sus datos personales, y otra es la legitimación procesal que se debe acreditar en el proceso constitucional de habeas data.

Inclusive, hay quienes sostienen que una vez que los datos llegan y se incorporan a la base ocurre una suerte de legítima apropiación que le asigna la titularidad sobre ellas al responsable del archivo. La idea se basa en que existe un derecho a la información diferente al de titularidad sobre los datos.

> Dado que alguna doctrina sostiene que podría ser ejercido una suerte de derecho de propiedad sobre los datos –dice Puccinelli-, cabría entonces distinguir entre el derecho a la información y el derecho sobre la información recabada. La posición que recurre al concepto de propiedad sobre los datos plantea ciertos debates nada pacíficos en la doctrina entre quienes sostienen la propiedad colectiva de toda información con independencia de su fuente y aquellos que, por el contrario, entienden que en los supuestos en que a partir de determinados datos y por el obrar de alguien, se logra generar determinada información, a quien la generó se le debe reconocer su derecho de propiedad sobre ella, salvo en el caso de los datos personales, que pertenecerían a aquel a quien se refieren.

El siguiente paso para reconocer la pertenencia del derecho a la denominada "autodeterminación informativa", consiste en tomar los derechos que se tutelan por esta novedosa posición y advertir el alcance que ellos tienen.

> Estadella Yuste dice que la noción de datos puede conducir a falsas apariencias respecto de su contenido, ya que no va destinada a proteger los datos *per se*, sino a una parte del derecho a la intimidad individual.

De este modo, se podrá constatar que la protección dispensada no es estrictamente a los datos sino a la persona, y particularmente, a su vida privada e intimidad.

Luego, cada etapa del proceso que va desde la localización de las fuentes de información hasta la transferencia de los datos, instala exigencias diferentes que tienen mucho que ver con las propias decisiones o

autodeterminación (manifestación de voluntad del interesado) impuesta por quien ofrece información personal a un archivo.

La guarda de los datos, por ejemplo, es sin duda alguna responsabilidad del archivo; como lo es también la seguridad que aplica al secreto recibido y a la efectividad de las eventuales transferencias. Aquí, los datos son de alguien a quien se conoce, informa y ha prestado autorización; mientras que el acto pleno de la información ofrecida es del titular del archivo.

Son derechos distintos, es verdad, y deben tener consideraciones diferentes. Una cosa será la protección al dueño de los datos para evitar la ofensa o lesión a su intimidad y demás derechos vinculados (identidad, honor, reputación, etc.); y otras las garantías que debe contar el titular del archivo para poder ejercer con plenitud su derecho a la información, a comerciar lícitamente, etc.

32.1 Derecho subjetivo del titular de los datos

Cuando se relaciona el derecho a tener protección de los datos personales con el derecho a la intimidad, se refleja una visión individual que asienta en un concepto civilista de la garantía. Pero cuando en la misma dimensión se cubren los derechos colectivos que persiguen evitar el abuso en el almacenamiento, recolección y procesamiento de datos personales, la intimidad queda en un segundo plano porqué el derecho garantizado adquiere alcance social.

> El Tribunal Constitucional alemán ha entendido que el principio liminar del ordenamiento jurídico establecido en su país, es el valor y la dignidad de la persona que actúa con libre autodeterminación al formar parte de una sociedad libre. De esa dignidad y libertad, entendida como libre autodeterminación, deriva la facultad de la persona de "deducir básicamente por sí misma cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida"; por lo que el Tribunal interpreta –en la deducción que hace Fappiano- que es contrario a esa facultad un orden social y un orden jurídico que hiciese posible al primero, en que el ciudadano ya no pudiera saber quién, qué, y cuándo y con qué motivo sabe algo sobre él…Esto no solo menoscabaría las oportunidades del desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos.

La dificultad de encuadrar como derecho subjetivo (propio e intransferible) a la noción de privacidad que pervive en el concepto de datos personales, está en que no se puede reparar el daño con la sola concesión de una indemnización reparatoria. La invasión a la intimidad se relaciona con las posibilidades reales que se tengan para controlarla, de manera que, los derechos emergentes de la protección de datos no pueden ser atendidos únicamente desde la visión economicista que mida el daño con la vara del resarcimiento. Es necesario que la protección del derecho se plantee como un problema social.

> La protección del derecho a la intimidad contra el uso de un tratamiento automatizado de datos personales no se plantea exclusivamente a consecuencia de problemas individuales, sino que también expresa conflictos que incluyen a todos los individuos de la comunidad internacional. Por eso –dice Estadella Yuste- la idea de que la persona titular de los datos –el afectado- tiene interés, como parte de un grupo, en controlar el tratamiento automatizado de datos es reciente, ya que no aparece así en la denominada "primera generación" de las leyes protectoras de datos, orientadas exclusivamente a la protección de la persona como entidad individual.

La socialización del derecho puede ampliar las fronteras tradicionales de la legitimación procesal, y por eso es la diferencia entre derecho subjetivo y representación del interés a defender; es evidente que la afectación de la privacidad por cualquier medio, además de lo que pertenece a los datos en sí mismos, se puede exigir no sólo por el afectado, sino por otras personas que con iguales motivos persigan una decisión judicial al respecto.

No obstante, si la noción de autodeterminación informativa se restringe como derecho personalísimo, la defensa del honor, la imagen, o la intimidad en un amplio sentido, únicamente se podrá concretar por el afectado.

> El bien jurídico intimidad de ser tratado como un derecho exclusivamente individual puede dejar afuera del ámbito de defensa constitucional –al parecer de Perez Luño- los aspectos sociales y colectivos de las informaciones que directamente les afectan. De otro lado, dado que en la sociedad moderna la capacidad de actuación política se halla íntimamente relacionada con el acceso y control de la información, un equilibrio sociopolítico exige que se garantice a los grupos sociales formas de participación en los materiales archivados en los bancos de datos.

32.2 La protección de los datos personales como derecho humano

La perspectiva anterior puede variar si el derecho se presenta desde los intereses que tutela. Es decir, si en lugar de ver a la persona que lleva la pretensión se observa el contenido del derecho que para sí reclama.

Esta cuestión es esencial en el análisis del habeas data, porqué la garantía constitucional se puede encontrar alterada por una caprichosa definición procesal que exija la relación directa entre quien pide y el daño producido (por ejemplo, cuando se requiere ilegalidad o ilegitimidad en el acto cuestionado y el actor únicamente solicita acceso al banco de datos); cuando en realidad, la lesión al derecho de la intimidad tiene varias manifestaciones, algunas de las cuales no reconoce un afectado directo porqué el gravamen asienta a toda la sociedad.

Muchas Constituciones del mundo han incorporado el derecho a la intimidad, el honor y la imagen como derechos del hombre; de este modo, se persigue establecer una igualdad de trato y consideración que evite diferencias escandalosas entre el significado que unos y otros puedan dar a cada uno de los intereses.

En relación estricta a los datos personales, debe aplicarse esta inteligencia porqué la intromisión a la vida privada se realiza en el preciso momento que alguien usa o conoce información personal que nos concierne, adquiriendo un conocimiento que pudo estar reservado, secreto o ser confidencial.

Esa información adquirida, cuando lo es de manera ilegítima, representa una injerencia en la vida privada, familiar o doméstica; constituye un atentado a la libertad individual cuando se usa para descalificar u ofender, o asignar conductas que lesionan el honor personal; asimismo, puede considerarse que es un hostigamiento, una vigilancia perturbadora, y en definitiva, una actitud hostil contra la reserva de los comportamientos individuales.

Cada caso es una proyección a defender, una hipótesis de cómo se afecta el derecho a través de la penetración y divulgación de los datos personales.

> Por tanto, tal como afirma Perez Luño, se trata en suma de comprobar en qué casos la *privacy* puede operar como coartada para burlar una política social avanzada, o en qué supuestos puede servir de freno ante determinadas formas de control o discriminación social o política. Pero en lo que interesa distinguir es que las cuestiones sobre las que gravita la disciplina jurídica de la intimidad han perdido su carácter exclusivo individual y privado, para asumir progresivamente una significación pública y colectiva. El problema del suministro de datos personales a la administración es evidente que atañe a los individuos, pero también a toda la sociedad, e incluso puede afirmarse que atañe a los individuos en cuanto pertenecen a un grupo social.

Enseguida veremos la dificultad de superar esta noción amplia cuando se mide el derecho al proceso desde la exigencia de arbitrariedad o ilegalidad manifiesta del acto lesivo, o cuando se toma la manifestación de voluntad como pauta legitimadora del uso de datos personales; o bien, al despojar el carácter social del derecho para centrar su tutela en la defensa exclusiva del derecho personalísimo.

Esta posición deja sin defensa a las personas jurídicas, porqué al referirse a las personas individuales se establece que el derecho a la protección de la intimidad y, en esencia, de los datos, corresponde a la

persona humana; dejando en todo caso la tutela a la información de las empresas a la normativa específica que cada ordenamiento mantenga.

> El derecho a la intimidad que reconoce el artículo 18.1 de la Constitución –sostiene el Tribunal Constitucional de España- por su propio contenido se refiere a la vida privada de las personas individuales, en las que nadie debe inmiscuirse sin estar debidamente autorizado, y sin que en principio las personas jurídicas, como las sociedades mercantiles, puedan ser titulares del mismo, ya que la reserva acerca de las actividades de estas entidades quedará, en su caso, protegida por la correspondiente regulación legal, al margen de la intimidad personal y subjetiva constitucionalmente decretada; pero es que, además, y en el caso de que hipotéticamente se estimare que el derecho a la intimidad acogiera las personas jurídicas, estaría como el resto de los derechos fundamentales limitado en su total dimensión, pues su ejercicio se sometería al respeto de otros bienes jurídicos igualmente dignos y necesitados de protección, y en concreto, a exigencias derivadas de la acción de la justicia. (TC, sentencia del 17/4/85).

32.3 Disponibilidad del derecho: autodeterminación

La progresión del derecho a partir de la interpretación judicial y doctrinaria ha puesto de relieve el difícil encuadre que tiene el criterio tradicional entre derecho positivo y derecho natural. Dicho en otros términos, no siempre las cosas se presentan como polaridades entre el derecho subjetivo, individual y concreto, frente al derecho social, difuso y abstracto.

No es bueno creer que la mejor defensa parte de las garantías individuales que tenga una persona porqué desde ellas irradia la fuerza normativa hacia los demás; como tampoco lo es pensar que si la sociedad se defiende con las armas de la ley, no es posible creer en el hombre indefenso.

Una posición intermedia deja en la persona la disponibilidad de actuar con libertad y criterio, poniendo en claro que, en materia de protección de datos, nadie mejor que el afectado para promover, de acuerdo con sus propios sentimientos y convicciones, la defensa de su vida privada.

> Este planteamiento –dice Perez Luño- tiene el mérito de poner de relieve la progresiva tendencia a concebir la *privacy* como el poder de ejercer un control sobre todas las informaciones que puedan afectar a cada persona individual o colectiva…Es el derecho al control de la información sobre uno mismo.

La postura se refleja en muchas de las legislaciones sobre protección de datos, las cuales ponen énfasis en la autonomía de la voluntad individual para autorizar la guarda, almacenamiento y transferencia de información que concierne a las personas físicas o jurídicas.

> Resumiendo se puede decir –concluye Estadella Yuste- que en un primer momento los instrumentos internacionales de derechos humanos no recogían expresamente el derecho a la protección de datos o autodeterminación informativa, sino tan sólo un derecho "a la vida privada" o a la intimidad personal. Posteriormente éste se ha ido desarrollando y paulatinamente se han adoptado otros instrumentos internacionales reconociendo el derecho a la protección de datos. Ello es importante porqué, si la protección de datos sólo se hubiera plasmado en leyes de ámbito nacional, habría sido más difícil que la comunidad internacional lo considerara como un derecho individual.

La dificultad puede estar en las limitaciones que se pretendan derivar de ese acto voluntario como una proyección de la doctrina de los actos propios, que en nuestro parecer no puede ser tan inflexible porqué desnaturaliza el derecho central a proteger. De aplicar el temperamento cualquier autorización abriría una carta de crédito al archivo evitando el control externo si el afectado no efectúa una pretensión concreta.

La defensa de los datos no tiene una visión estática simplificada en el interés particular; todo lo contrario, la función dinámica que adquiere se toma del modo como actúan los archivos y registros de

información personal, los que habilitan actuar en dimensiones diversas, ya sea para tutelar el interés concreto, como para descubrir el control externo que se merece.

> Esta idea ha penetrado en los últimos años en la doctrina europea y reviste una importancia prioritaria para delimitar conceptualmente el contenido del derecho a la intimidad y su alcance en la sociedad tecnológicamente avanzada. En suma, se trata de insistir –afirma Perez Luño- que en nuestra época resulta insuficiente concebir la intimidad como un derecho garantista (*status* negativo) de defensa frente a cualquier invasión indebida de la esfera privada, sin contemplarla, al propio tiempo, como un derecho activo de control (*status* positivo) sobre el flujo de informaciones que afectan a cada sujeto.

32.4 La pertenencia del dato en la ley reglamentaria

El capítulo VII de la ley reglamentaria habilita un procedimiento para la protección de los datos personales por el que se destaca la amplitud prevista para la legitimación activa (tema que abordaremos más adelante).

El artículo 34 (Legitimación activa) sostiene: "La acción de protección de los datos personales o de habeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.

"Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.

"En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo"

El derecho a tutelar los datos no se visualiza como un derecho subjetivo, individual y personalísimo. Pareciera plantearse al dato como un problema de propiedad a defender.

En realidad no planteamos algo novedoso al decir que la intimidad, la privacidad, la identidad personal son también "derecho de propiedad". Warren y Brandeis en su clásica obra sobre la intimidad dijeron en 1890 que *"el derecho a ser libre garantiza el ejercicio de un amplio haz de derechos subjetivos; y el término "propiedad" abarca en su significado actual, todo tipo de derechos de dominio, tanto tangibles como intangibles"* En esa *evolución "el mayor aprecio de las sensaciones...hicieron ver al hombre que sólo una parte del dolor, del placer y del disfrute de la vida reside en las cosas. Pensamientos, emociones y sensaciones exigían su reconocimiento legal"*

> Sin embargo, -agrega Loianno- estos autores encuentran alguna dificultad en asimilar la intimidad con el derecho de propiedad cuando analizan su ausencia de valor económico, que "*no reside en el derecho a obtener ganancias...sino en la tranquilidad del espíritu y en el alivio que proporciona impedir su publicación*".
>
> Por el contrario, -afirma- creemos que tanto la intimidad como la identidad personal poseen todos los atributos de la *propiedad* en la medida que constituyen bienes valiosos en sí mismos aún cuando no siempre pueda ese valor ponderarse en dinero. La evolución producida en las áreas de protección jurídica de la esfera más íntima de la persona humana justifican esta apreciación.

En todo caso las herramientas constitucionales que garantizan la propiedad son aplicables sin mayor dificultad cuando el objetivo es salvaguardar la esfera más personal del individuo.

Uno de los aspectos más importantes en este tema es distinguir por donde pasa la línea divisoria entre lo auténticamente privado y aquello que afecta los intereses de terceros.

Fundamentalmente, el problema se manifiesta respecto de la incidencia que tienen en los ámbitos reservados a lo privado, los medios de prensa y la informática.

Si en la actualidad resulta insuficiente concebir a la intimidad como un derecho de estatus negativo de defensa frente a la probable intromisión de terceros, ello se muestra con mayor exigencia frente al flujo de informaciones concernientes al sujeto, relativas a su privacidad y a la definición de su propia persona.

Es así como pueden identificarse principalmente dos fuentes de intromisión:

a) *Los bancos informáticos de datos personales*, que frecuentemente abarcan zonas que debieran ser vedadas al conocimiento público por ser reservadas a la intimidad de las personas. La protección constitucional opera aquí garantizando la veracidad de los datos así como el control de la confidencialidad en lo relativo a "*datos sensibles*".

b) *Los medios de prensa* desde la perspectiva de la ofensiva de los multimedios sobre los espectadores, lectores u oyentes considerados como consumidores.

Aquí se ubican dos aspectos diferentes de lesión a la intimidad: 1) La que se produce a través de la intromisión o divulgación de la vida privada y 2) La que provoca la información como condicionante de conductas o ideologías.

La garantía de la libertad de prensa sin censura previa, sustento esencial del estado democrático de derecho, se complementa en este aspecto para preservar el derecho a la privacidad, honor y nombre de las personas, con dos garantías constitucionales: el resarcimiento (*alterum non laedere*) y la réplica. Esta última a través de la jerarquización constitucional de la Convención Americana de Derechos Humanos.

33. Los datos de las personas jurídicas

Una de las cuestiones más debatidas en la problemática de los datos personales radica en saber si la tutela alcanza a las personas de existencia ideal.

La cuestión tiene diversos enfoques, pero siempre debemos partir del objeto jurídico que protege el habeas data o los derechos que cuenta el afectado, para verificar cuando se tiene posibilidad de lograr la defensa prometida constitucionalmente.

Los datos personales afectados por la invasión informática aparecen vulnerables cuando se encuentran en una base de información que los almacena sin el consentimiento del individuo. La afectación se puede dar, también, cuando el dato es inexacto o no refleja la verdadera identidad de la persona o contiene información agraviante o discriminatoria. De igual modo, si el archivo tiene información sensible no autorizada a divulgar, se produce un agravio que la ley de protección de datos debe tener en cuenta.

Cada supuesto advierte que desde la vulnerabilidad del secreto y confidencialidad se puede llegar a lesionar la intimidad de las personas, para encontrar un acto lesivo específico en la honra agraviada, la reputación afectada, la imagen distorsionada, la humillación personal por la revelación de un dato sensible, y así, unas cuantas maneras más de lesionar la vida privada de las personas a partir de la publicidad de los datos individuales.

Ahora bien, esa información afecta por igual a personas físicas y jurídicas, porqué no existe razón para excluir del derecho a la protección de los datos a los grupos ideales que preservan, en idéntica dimensión, la reputación, imagen empresarial, seriedad institucional, confianza y seguridad, etc., para corresponderlos con las acciones dichas para las personas físicas en el párrafo anterior.

Sin embargo, la conclusión no tiene coincidencias prácticas en la doctrina y menos aun en la jurisprudencia.

No obstante, es oportuno reiterar que la ley reglamentaria esclarece el punto al sostener en el párrafo segundo del artículo 1º que:

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

33.1 El dato como derecho personalísimo

La postura clásica de los derechos derivados de la personalidad los encuentra como innatos a la persona y de fuerte contenido individual, en el sentido de ser propios e intransferibles.

> Ekmekdjian y Pizzolo apuntan que estos derechos presentan las siguientes características: a) son *innatos*, o sea, corresponden al titular desde el origen de éste; b) son *vitalicios*, en cuanto acompañan al ser humano durante toda su vida; c) son *inalienables*, en cuanto no son susceptibles de enajenación por ningún título, están fuera del comercio; d) son *imprescriptibles*, porque no son alcanzados por los efectos del tiempo que no influye en su pérdida, no obstante el abandono del titular; e) son de carácter *extrapatrimonial*, aun cuando la lesión de estos derechos pueda generar derechos patrimoniales; f) son *absolutos* en cuanto se ejercen *erga omnes.*

Cuando se establece que la protección de los datos se fundamenta, exclusivamente, en la defensa de la intimidad parece imposible encontrar este derecho en las personas jurídicas, pues no hay intimidad propiamente dicha, como sí un derecho al secreto, a la discreción, o bien a la reserva de la vida privada que bien puede tener una empresa, entidad, asociación o cualquiera otra forma de personalidad ideal.

En consecuencia, la personalización del derecho, propio de la consagración del subjetivismo jurídico, no se podría extender a quienes no tienen individualidad física, pensando que la dimensión jurídica de la persona no alcanza para atribuirle un derecho al honor, a la vida privada y, en menor medida, a la imagen.

La causa de la limitación se sostiene en el carácter de derecho humano que tiene la intimidad, condición que no poseen las personas ideales; y además, en la exigencia de tutelar un interés propio, directo y exclusivo como es la vida privada de las personas, que no son naturales en los grupos que, por su propia calidad, viven en permanente relación pública.

> El objeto del derecho radica en la intimidad, como algo que es al tiempo diferente tanto de la vida privada, como de la privacidad, como de la vida pública. Siendo como es el de intimidad un concepto jurídico indeterminado la cuestión radica en trazar siquiera sea aproximadamente sus perfiles, diferenciarle de los conceptos afines y establecer directrices para su concretización. De esta forma sostiene Martínez Sospedra que, la diferenciación entre privacidad, vida privada e intimidad dista de ser clara, al menos por lo que a los dos últimos conceptos afecta. Si la *privacy* anglosajona se corresponde parcialmente con el derecho que estudiamos, pero también con otros derechos del art. 18 CE sustantivizados por el constituyente español, como pone de relieve el antecitado informe Cutter, lo que facilita la diferenciación, es preciso reconocer que trazar el perfil de la intimidad es harto complicado, razón por la cual ha podido señalarse que el concepto mismo de intimidad es una mala herramienta de trabajo, es un cesto para recoger agua.

33.2 Intimidad y datos de la persona jurídica

Si el planteo anterior se realiza desde otra perspectiva, las respuestas podrían cambiar. En efecto, la afirmación que precede sostiene que la intimidad es un derecho personalísimo, y los datos –como una parte de ella- que se encuentran contenidos en archivos afectan de manera directa a la persona física cuando se revelan o almacenan en condiciones ilegítimas o desautorizadas por su titular.

Otra visión encuentra que la intimidad no se la vincula estrictamente con la vida privada y sí con un derecho de exclusión y reserva, desde el cual se puede construir un derecho propio para las personas jurídicas. En lugar de proteger la intimidad en sí misma, se defiende la intimidad de quien la reclama, abriendo panorámicamente los objetos y razones de la pretensión.

> Determinada persona jurídica podría interponer la acción de habeas data, frente a los registros o bancos de datos de un organismo oficial o privado, si considera que estos datos podrían afectar su honor comercial (v.gr.: figurar como deudor de un crédito, cuando ya se ha cancelado la deuda) o su intimidad (v.gr.: datos que revelan la donación de fondos a algún partido político o credo religioso). A estos ejemplos de Ekmekdjian y Pizzolo, los autores agregan: “Si en situaciones iguales se les concede tal facultad a las personas físicas, ¿porqué discriminar a las

> jurídicas cuando las consecuencias no se discriminan? En otras palabras, si los individuos pueden ejercer un derecho de acceso a los bancos de datos personales almacenados en una entidad ¿por qué no podrían hacerlo las personas jurídicas?.

La cuestión no es pacífica si la intimidad se adquiere como derecho absoluto, pero cambia sustancialmente si la interpretación se asume confrontando la realidad del diario acontecer.

Es evidente que el criterio tradicional como se interpreta a la intimidad deja fuera de las posibilidades de reclamo a los entes ideales, por ejemplo, para el derecho al secreto de las conductas sexuales, la vida familiar, las creencias religiosas, las inclinaciones políticas, o en suma, los datos sensibles *lato sensu*. En cambio, si la visión se focaliza en los datos, exclusivamente, evidentemente la protección diferida por el habeas data no se puede restar de las garantías que tienen las personas jurídicas.

Son varias las razones por las que se argumenta la protección de los datos aunque puedan variar los motivos. Con ello se quiere decir que no es igual la protección del honor de la persona física que la reputación de la persona jurídica; que es distinta la imagen individual respecto a la corporativa; que difiere la dignidad individual de aquella que privilegia el objeto social; y así, sucesivamente, podrán aparecer diferencias por la naturaleza de las personas, pero que a la par de los derechos encuentran simetrías posibles.

El caso del honor es una probabilidad a tener en cuenta. Este puede ser atacado por la divulgación de actos, hechos, noticias, etc., relativas a personas tanto físicas como sociales; y cuando el prestigio o la confianza de una sociedad se pone en duda a consecuencia de la revelación de datos, es indudable que ese conocimiento que los demás asumen sobre la persona ideal afecta su activo patrimonial.

> Ahora bien, dice Herrero Tejedor, distinto es el caso de las instituciones sin fines de lucro, sino de participación, opinión o defensa de ideas o creencias. Nos referimos, por ejemplo, a los partidos políticos, sindicatos, asociaciones, confesiones religiosas, fundaciones, etc. En ellas se hace indispensable la posesión de una honorabilidad clara, pues su desprestigio haría muy difícil la obtención de sus fines sociales. Por ello, el autor acepta la idea de extender la protección de datos personales hacia las personas jurídicas.

33.3 El derecho internacional

Cuando se dijo sobre la ausencia de un criterio unívoco en la protección dispensada a las personas jurídicas se tuvo en cuenta la diferencia de criterios existente en las legislaciones locales e internacionales.

La O.N.U., en sus directrices sobre la protección de grupos ideales * incorpora una cláusula optativa, por el cual sostiene que se pueden tomar disposiciones particulares, igualmente facultativas, para extender la aplicación total o parcial de los principios recogidos en el reglamento general de archivos sobre personas físicas.

> Ello significa, afirma Estadella Yuste, que los Estados pueden optar por la extensión de las disposiciones de las líneas directrices de la ONU sobre ficheros automatizados de datos personales a los ficheros de las personas jurídicas. En uno de los proyectos previos a la redacción final de este instrumento se había propuesto la inclusión incondicional de los ficheros de las personas jurídicas.

En cambio la OCDE * no incluye a las personas de existencia ideal por cuanto se considera que existen otros reglamentos que logran idéntica protección, sin interferir en derechos que son de típica raigambre individual.

> Las directrices de la OCDE, no incluyen, de forma expresa –sostiene Estadella Yuste- a las personas jurídicas en su *ratione materiae* .La doctrina permanece dividida sobre la posibilidad de que este instrumento permita o no extender su aplicación a las personas jurídicas. Pero parece que la postura que niega tal posibilidad es la más plausible por basarse en la exposición de motivos de las propias directrices. Esta exposición de motivos sostiene que las nociones de integridad individual y privacidad tienen características peculiares que no deben ser tratadas de la misma forma que la integridad de los grupos de personas, la

> seguridad y la confidencialidad empresarial. Igualmente se afirma que no sólo las necesidades para la protección de las personas físicas y jurídicas son diferentes, sino que también lo son los marcos políticos donde se deben encontrar soluciones para equilibrar los intereses existentes. Por consiguiente, se debe concluir que las personas jurídicas no quedan amparadas en el ámbito de aplicación de las directrices puesto que la exposición de motivos descarta tal posibilidad y, además, el texto legal no las incluye ni expresa ni implícitamente.

La Comunidad Económica Europea, tanto en el Convenio 108 como en la Directiva 95/46 sólo afirman la tutela de las personas físicas; temperamento que no fue receptado fielmente por los Estados partes, si observamos que Austria, Dinamarca, Islandia, Luxemburgo, Noruega y Suiza por ejemplo, admiten que las personas jurídicas tengan igual protección que los derechos humanos. Criterio que mayoritariamente han aceptado las Constituciones latinoamericanas.

> Resulta significativo, dice Herrán Ortiz, que los países nórdicos, caracterizados por su elevada y temprana conciencia en materia de protección de datos, se haya reconocido el derecho a la autodeterminación informativa a las personas jurídicas. Por el contrario, no ha sido ésta la decisión adoptada por legislaciones tales como la francesa, alemana, portuguesa o británica que niegan a la persona de existencia ideal la condición de beneficiario de los derechos y garantías que integran el derecho a la autodeterminación informativa.

En España, que ha sido fuente de inspiración de nuestros proyectos de ley, y se refleja en la actual reglamentación, se tiene como sujeto activo de la protección de datos personales, únicamente a las personas físicas; lo cual se funda en el carácter fundamental de la garantía, interpretada como un derecho humano; y en la existencia de legislación *ad hoc* que solventa con similar contundencia los fines de la autodeterminación informativa.

Las primeras lecturas tras la reforma constitucional argentino, coinciden en asignar a las personas jurídicas legitimación suficiente para entablar la acción de habeas data, criterio que compartimos y que la ley ratifica, por los fundamentos que se darán al tratar el tema de la personalidad procesal para entablar la protección constitucional que dispensa el nuevo artículo 43.

34. Las garantías procesales en la protección de datos

De lo que llevamos diciendo se puede deducir que la herramienta procesal destinada a proteger los datos personales es el habeas data, el cual se fundamenta en los carriles constitucionales expresos del artículo 43 y en los implícitos del artículo 18, como reglas para un debido proceso. No se descarta la operatividad del artículo 14 que interpretado de consuno con el art. 43 abre nuevos rumbos a la legitimación procesal, ni al art. 75 inciso 22 que, con la incorporación de pactos y tratados, solidifica el derecho al proceso breve y sencillo. La reglamentación culmina un cuadro que ya estaba solidificado pero que necesitaba de los esclarecimientos aportados.

Ahora bien, esa garantía tiene una finalidad específica; no se trata de resolver con ella un impedimento para negar información personal o suprimir aquella que estuviera registrada en un banco de datos; sino de permitir que sea el propio interesado quien decida el destino de esa información y su permanencia en la base creada.

A partir de esa libertad puede, siguiendo un orden lógico en las pretensiones, *perseguir el acceso* a la fuente de información que lo concierne; y después, una vez verificado el registro personal de sus datos, disponer el control sobre ellos, ya sea para mantenerlos actualizados, reemplazarlos con los que sean exactos y veraces, solicitar la confidencialidad estricta de la información privada, o bien, plantear la supresión por alguna de las razones que enseguida se verán.

> Según Herrero Tejedor, esto constituye el “right to privacy”, es decir el derecho de acceso a los bancos de datos, el derecho de control de su exactitud, el derecho de puesta al día y rectificación, el derecho de secreto para los “datos sensibles”, y el derecho de autorización para su difusión.

34.1 Derecho de información

Hablamos aquí de un derecho distinto a la información que se le debe proporcionar al sujeto que admite incorporar sus datos a un archivo con el fin de darles un tratamiento automatizado. También difiere de aquél derecho a la exactitud que planteamos como garantías para el usuario.

El derecho a la información que se instala entre las garantías del habeas data, no piensa en el carácter individual sino en el alcance general que tiene "toda persona" para solicitar información sobre la existencia de bancos de datos, sus finalidades y la identidad de sus responsables.

> El reglamento actual establece en el artículo 13 (Derecho a la información) que: "*Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o banco de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita*".

Tal como se orienta en el derecho comparado esa idea de amplia circulación de los datos, el derecho a la información se presenta como una garantía de la publicidad de los actos que lleven a cabo los archivos.

Quizás fuera mejor establecer como deber de los bancos de datos producir periódicamente un informe, antes que dejar en la iniciativa de las partes el control eventual de la transparencia en el tratamiento de datos personales. Así lo hacen algunas legislaciones (v.gr.: Portugal, Gran Bretaña, Suiza, Noruega, entre otros), donde se destaca la ley finlandesa que impone al responsable la elaboración de una lista de ficheros de personas que deben estar a disposición del público.

> Por otro lado, dice Herrán Ortiz, y en coherencia con la discusión que venía enfrentando a los conceptos de "tratamiento de datos" y "fichero de datos", la Directiva, al igual que habían hecho ya algunas legislaciones, opta por introducir el registro o notificación de tratamientos, como concepto más dinámico y omnicomprensivo en el sistema de protección de datos personales.

La finalidad del derecho a la información no consiste únicamente en saber quienes son los titulares ni cuantos bancos de datos existen; la garantía proyecta un control directo sobre el tratamiento que se efectúa sobre la información que a la persona le atribuyen. De este modo, cuando se pretenda deducir una calidad particular, una cualidad determinada, un perfil o personalidad de alguien, a partir de los datos que el archivo hubiere procesado, la conclusión será nula por estar ausente el derecho del afectado a conocer el informe que le concierne de manera tan directa.

Esta elaboración es común para ciertas decisiones judiciales o en algunos actos administrativos que adoptan un criterio a partir de la valoración lograda del tratamiento automatizado de datos personales; y se observa agudamente en los servicios informatizados de información crediticia que suelen elaborar un perfil de la persona a partir del cumplimiento de sus obligaciones patrimoniales.

> En nuestro país se abre un panorama similar desde la sanción de la reforma constitucional que admite la garantía del habeas data pero acotada a la iniciativa de parte interesada. Ello no obsta a que se pueda exigir la transparencia de los archivos, sobre todo los de carácter público, que tienen una obligación inmediata con el ciudadano.
>
> Ahora bien, este derecho no debe confundirse con el derecho de acceso a la documentación administrativa; pese a que tiene una evidente vinculación con algunos derechos fundamentales como el derecho a la participación en los asuntos públicos, o el derecho a comunicar y recibir libremente información auténtica, o el más próximo que lo relaciona con el derecho a la tutela judicial efectiva. Sin perjuicio de esta vinculación, dice Peñarrubia Iza, el derecho de acceso a la documentación administrativa es un derecho constitucional, pero no un derecho fundamental, en cuanto no está ubicado sistemáticamente entre los derechos fundamentales. Para convertirse en un derecho subjetivo, basta con el reconocimiento expreso que hace la Constitución, si bien el mismo precepto que

> menciona este derecho se remite a las leyes, lo cual significa que hay un principio de reserva de ley para delimitar este derecho, es decir, que el modo concreto de ejercicio, la legitimación y cualesquiera otros aspectos, sobre todo en lo que respecta a los límites, han de ser establecidos legalmente.

En síntesis, el derecho a la información es una garantía general para la publicidad de los actos de tratamientos de datos personales que efectúen los archivos. La regla mínima es difundir el nombre y los responsables de cada banco de datos, y las extensiones radican en las consecuencias que pueda tener la información aportada sin dicho conocimiento general.

Como es bastante difícil lograr este criterio de publicidad abierta y nulidades eventuales, se han pensado mecanismos que, ejerciendo formas de control directo, obliguen a cumplir las pautas de transparencia.

> Sin embargo, apuntan Ekmekdjian y Pizzolo, este criterio inicial fue abandonado paulatinamente, entre otras razones, porque el resultado de esta actividad no garantizaba una protección mayor de los datos personales. En la actualidad se utiliza una interpretación más restrictiva y cercana al derecho de acceso, que consiste en que los titulares del registro, o banco de datos transmiten una comunicación sobre la información en su poder, previa solicitud del afectado (v.gr.: mediante la acción de habeas data).

Finalmente, este derecho general tiene un hondo sentido práctico en el derecho de acceso de la persona afectada. Por ello, los beneficiarios del derecho a conocer –como lo denomina Estadella Yuste- son, por un lado, la sociedad en general y, por otro lado, las personas que, como entidades individuales, tienen un interés concreto sobre la información que les concierne, y que se encuentra recogida en ficheros automatizados, llegando a poder ser objeto de transmisión internacional.

> Básicamente –agrega Estadella Yuste- el derecho a conocer consiste en saber de la existencia de ficheros que contienen datos individuales, el propósito o finalidad que se persigue con la creación del archivo, la identidad y residencia del titular o responsable del fichero, y si este fichero va a entrar a formar parte de la circulación internacional de datos. Al conocimiento de estas generalidades tienen derecho los individuos en cuanto forman parte de la sociedad. No obstante, el derecho a conocer amplía este contenido cuando las personas, como entidades individuales, son las que ejercen este derecho individual.

34.2 Derecho de acceso

El derecho a solicitar y obtener información de un archivo o registro, para saber si el mismo contiene o no, información personal que a alguien concierne, constituye el fundamento esencial del habeas data.

Es el derecho de entrada a los bancos de datos y la garantía principal que tiene la persona para conocer qué información existe sobre ella.

Resuelto el problema del acceso, el individuo puede resolver conductas posteriores. En este sentido, validará la información contenida; podrá ratificar la autorización prestada si ella se hubiese requerido; tendrá la facultad de exigir la actualización o rectificación de los datos; planteará la supresión del dato sensible, y en cada caso queda de manifiesto el poder de control de la persona sobre los archivos de datos personales.

> Falcón explica la faz procesal de este derecho, sosteniendo que comprende dos pretensiones sucesivas y secuenciales, una subsidiaria de la otra. La primera de información y la segunda de conocimiento y ejecución…Como se ve, se trata de un proceso complejo, con inversión sucesiva de pretensiones. Así la presentación, que puede ser planteada por vía de proceso sumarísimo o similar expedito, llamado en algunos ordenamientos extraordinario y aun plenario rapidísimo, debe contener una pretensión primaria destinada a que se informe al juzgado de los datos registrados por el Estado (en sí o en cualquiera de las reparticiones),

instituciones o particulares referentes al actor, la finalidad de los mismos y en su caso las medidas a tomar sobre dichos datos. Dichas medidas se pueden pedir en ese mismo acto (de modo directo o cautelar) si se conocen o presumen, o reservar esta segunda petición para el momento en que se haya contestado el informe. No obstante los contenidos de la petición inicial, no limitan la segunda petición a la luz del informe presentado. La primera etapa del procedimiento entonces será de naturaleza informativa y voluntaria, la segunda podrá tener el carácter de contenciosa.

De alguna manera, como antes se dijo, es la libertad de requerir que "se traigan los datos", cual si fuera la acción exhibitoria propia del hábeas corpus. Aun cuando es preciso destacar que el acceso no se dirige justamente a los datos sino al archivo que los contiene, y por ello las posibilidades de lograr el control varían con la forma como se presenta el pedido.

El acceso será directo cuando la información se pueda lograr por la simple consulta al banco de datos, y éste la evacue por un medio escrito o la deje disponible en un medio electrónico por el cual se pueda lograr una rápida visualización.

En cambio, si el requerimiento necesita de la colaboración judicial, se deben adoptar los recaudos típicos de las formalidades para demandar, teniendo en cuenta que se trata de un proceso constitucional que no podrá ser anulado por el principio de legalidad instrumental.

El sistema actual sostiene que *"el titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes"*. El inciso 3 del art. 14 agrega que: *"El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto"*

La idea no es poner exigencias previas que hagan vulnerable el derecho de acceso, tales como los recaudos de legitimación o personalidad procesal, sino en su lugar, tener por suficiente la acreditación de identidad que efectúe la persona afectada o aquella que demuestre un interés legítimo para realizar el requerimiento.

Dice Herrán Ortiz que el derecho de acceso presenta en la ley española una amplia variedad de posibilidades, que pueden ser resumidas en la siguiente idea: lo verdaderamente trascendente es que el afectado tenga constancia de la información relativa a sus datos personales registrados, de un modo claro, completo y exacto, de suerte que se procure al afectado el conocimiento de aquellos aspectos fundamentales del tratamiento automatizado de sus datos, para poder ejercitar una defensa de sus derechos con ciertas garantías jurídicas.

Es importante destacar que el derecho de acceso no le corresponde únicamente al particular afectado por la información almacenada en un banco de datos sino a toda persona que acredite un interés legítimo para actuar.

d) *¿Acceso al archivo o a la información?*

Uno de los problemas habituales en la garantía ofrecida está en resolver si el acceso supone visualizar directamente el banco de datos, con lo cual el derecho de entrada podría suponer estar en el mismo sitio donde se produce el tratamiento de los datos (y conseguir en ese acto la revelación).

Sin embargo, de esta manera se violaría la seguridad que los archivos deben preservar, razón que sugiere que el derecho de acceso se resuelva a través de la información que se debe brindar.

Nuestra ley establece en el artículo 14 inciso 2 que: *"El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita*

la acción de protección de los datos personales o de habeas data prevista en esta ley".

Además, es conveniente agregar que el derecho de acceso a la información no supone otro derecho similar como es acceder a la documentación del Estado.

> Nos referimos a los supuestos especiales de aquellos datos personales que se almacenan para fines administrativos, que deben ser objeto de registro permanente (v.gr.: bancos de datos de las fuerzas armadas; fuerzas de seguridad; organismos policiales; servicios de inteligencia), o bien, proporcionan estos archivos información a las autoridades administrativas o judiciales en virtud de una autorización legal precedente.

El artículo 23.2 de la ley de habeas data argentina dispone que: "*El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad".*

e) *¿ Cómo se accede a los archivos extranjeros?*

Otra cuestión que debe ser analizada es la radicación extranjera del banco de datos, porqué las distancias pueden solapar el derecho general de información que tienen todas las personas; como también dificultar el encuentro con la base originaria de la información personal.

Cuando se desconoce de que fuente proviene el uso de los datos individuales, el derecho de acceso se puede encaminar a través de los organismos de control locales, para que sean éstos quienes asuman el derecho del afectado.

> Afirma Estadella Yuste que numerosas son las ocasiones que en la práctica los titulares de los ficheros niegan el derecho de acceso por considerar que la información personal recogida no es objeto del derecho de acceso, ya que el fichero donde está almacenado no es de carácter nominativo, sino mixto.

No se trata de una sustitución, propiamente dicha, porqué el interesado mantiene la potestad de insistencia ante quien se obliga por sus datos. Quizás el mayor problema podría surgir de aquellos países que no cuenten con ley de protección de datos, a los que puede aplicarse el principio de la "protección equivalente", y negar el acceso basados en el fundamento del trato igualitario que recoge el principio citado.

f) *¿A partir de qué momento se tiene derecho de acceso al archivo?*

También hay que aclarar que el derecho de acceso se tiene a partir del mismo momento que ingresan al archivo, sin importar si los datos personales fueron o no motivo de tratamiento automatizado.

> ¿A partir de qué momento los datos personales pueden ser objeto del derecho de acceso? Se pregunta Estadella Yuste. ¿Pueden incluirse los datos registrados provisionalmente?, o bien ¿debe ejercerse este derecho en los datos personales que ya han sido objeto de operaciones automatizadas?, ¿puede ejercitarse el derecho de acceso sobre los datos almacenados?. Entiendo –agrega- que en los dos primeros casos es posible ejercer el derecho de acceso; sin embargo, en el supuesto de información almacenada cuyos nexos de identificación ya han sido eliminados, se podría aceptar la negación del titular del fichero para el derecho de acceso, siempre que éste garantice que los datos serán borrados del sistema una vez cumplida la finalidad del fichero.

d) *Finalidades del derecho de acceso*

De acuerdo con la finalidad que la petición de acceso persiga, el derecho concreta modalidades implícitas en la garantía a preservar. Es decir, el derecho de acceder a los bancos de datos supone que se especifique para qué se quiere entrar en ellos y qué es lo que se quiere conocer.

A veces la información pretende saber el contenido de la información personal almacenada; en otras, además, se plantea inquirir el medio por donde se obtuvieron los datos; también es posible reclamar para qué y para quien se realizó el registro; y con menor intensidad, indagar los medios utilizados para alcanzar la finalidad para la cual la información ha sido recogida.

> Cada una de estas pretensiones ha llevado a Sagüés, a presentar una clasificación en el habeas data, nominando subtipos específicos: a) *exhibitorio*, que consiste en saber qué se registró; b) *finalista*, que procura indagar además para qué y para quién se realizó el registro; c) *autoral*, cuyo propósito es inquirir acerca de quien obtuvo los datos que obran en el registro.
>
> Por su parte Puccinelli, agrega: a) aquel que tiene por objeto indagar sobre la existencia y localización de bancos y bases de datos que existe en algunos países, y que tiene como objetivo final el garantizar el ejercicio de los derechos de aquellos que se hallen potencialmente afectados, estableciendo la obligatoriedad de inscribir a las bases y bancos de datos en un registro especial que puede ser objeto de consulta; y b) aquel que puede utilizar quienes pretenden acceder a la información pública, que funciona cuando no se les permite el acceso a ella sin la debida justificación (obligación legal de reserva, motivos de seguridad del Estado, etc.), y que, aunque para nosotros es otra versión principal, denominada "habeas data impropio", se puede englobar en la clasificación de Sagüés.

34.3 Derecho a controlar el archivo y los datos personales

La base del derecho a la protección de datos personales está en el libre consentimiento que pueda dar quien sea requerido a esos efectos, y en el control que *a posteriori* se pueda ejercer.

Esta vigilancia apunta hacia dos objetos precisos. Controlar al archivo autorizado para que cumpla la finalidad oportunamente expuesta al requerir la autorización; y verificar la actualidad de los datos para que no se ofrezca información obsoleta, equívoca o inexacta.

En ambos casos rige el principio de "calidad de los datos", que como se recordará, establece los deberes que tiene el registro en cuanto a la adecuación, pertinencia y congruencia del almacenamiento con los datos autorizados que se van compilando de la persona concernida.

> Es necesario aclarar que el deber de actualización de los datos es del archivo y no de la persona afectada, incurriendo en negligencia el responsable que no cumpla con esa obligación de veracidad. Al respecto, ha señalado Orozco Pardo que la ley impone al titular del fichero: mantener los datos exactos y al día; rectificándolos de oficio, sustituyéndolos por los correspondientes datos rectificados y completos, sin que sea necesario que ello se solicite. Los datos deben cancelarse de oficio cuando ya no sean pertinentes o necesarios para la finalidad con que se recogieron, mientras tanto, deben estar almacenados de forma que posibiliten el ejercicio de los derechos de los afectados.

La vigilancia es un poder del afectado para controlar directamente al registro, pero se debe diferenciar del control externo que los bancos de datos tienen en los organismos que cada legislación suele crear al efecto.

b) *Derecho a la rectificación del dato*

Ante la obligación del archivo de mantener actuales los datos, se instala el derecho de la persona para requerir que se rectifique la información inexacta que le concierne.

> El actual reglamento, establece en el artículo 16 inciso 1º, que toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.

No estamos hablando aquí del dato falso o discriminatorio que refiere el artículo 43 de la Constitución Nacional –como veremos más adelante- sino de la información errónea, es decir, la que una vez transmitida provoca un dato incierto por ser ajeno a la realidad.

Por ejemplo, si una persona figura como deudora de un crédito que pagó con posterioridad al registro, esa información es atrasada, y el deber de corrección es del archivo –de oficio, o a requerimiento expreso del interesado-.

En doctrina suele llamarse a este tipo de actuación como *habeas data rectificador* o *correctivo*.

> El objetivo de este tipo de habeas data –dice Puccinelli- es el de corregir o sanear informaciones falsas, aunque también podría abarcar a las inexactas o imprecisas, respecto de las cuales es factible solicitar determinadas precisiones terminológicas, especialmente cuando los datos son registrados de manera ambigua o pueden dar lugar a más de una interpretación (v.gr.: si una información proveniente de un sistema que suministra datos acerca de la factibilidad de otorgar créditos dentro de una Cámara comercial determinada, estableciese que tal persona es un "deudor inhabilitado" y ello obedeciese a que se encuentra inhabilitado para operar con el sistema, pero que no es un inhabilitado en términos jurídicos).

b) *Derecho a la actualización.*

También es posible encontrar informaciones incompletas que dibujan un perfil insuficiente y afectan el derecho a la verdad. En este caso, se debe incorporar al archivo la información parcialmente omitida.

> Un dato puede ser incompleto cuando no tiene toda la información necesaria. Otra cuestión diferente –dice Fappiano- es que los datos de una persona estén desactualizados. Por eso una de las obligaciones que tiene el titular o responsable del registro o banco de datos es llevarlos con toda precisión, pertinencia, perfección y actualidad; para lo cual está obligado a realizar todos los esfuerzos que sean razonables.

La puesta al día trabaja sobre el dato insuficiente, llamado también, dato inexacto o incompleto. No es información real para el tiempo donde se produce y por eso la finalidad es actualizar el registro.

> Señala la jurisprudencia que quien promueve un habeas data debe primero tener acceso a los registros del caso para luego plantear la falsedad de la información, a lo que debe añadirse que esta falsedad puede resultar tanto de una clara inexactitud como de la desactualización de los datos que se suministran (Juzgado Nacional de Primera Instancia en lo Contencioso Administrativo nº 3, noviembre 2/995, *in re* "Nallib Yabran, Alfredo c/ Ministerio de Economía, Obras y Servicios Públicos").

La actualización de los datos pretende agregar información, antes que rectificar la existente; por eso, la doctrina divide o clasifica esta modalidad como *habeas data aditivo* segmentado en subtipos *actualizador* (que persigue renovar el dato caduco), e *inclusorio* (incorporar al registro más información).

> Enseña Puccinelli –siguiendo a Sagüés- que este tipo de habeas data procura agregar más datos a los que figuran en el registro respectivo, y puede ser utilizado, por ejemplo, para obligar a un banco de datos comerciales a colocar que una deuda asentada ha sido refinanciada, o que se es deudor como garante de una

> obligación contraída por un tercero cuyo monto ha sido controvertido judicialmente. En él confluyen dos versiones distintas: se puede utilizar tanto para actualizar datos vetustos, como para incluir en un registro a quien fue omitido.

c) *Derecho a la confidencialidad de los datos*

La autorización del titular para que los datos sean utilizados con la finalidad que el archivo le informa y en la medida del consentimiento prestado para su transferencia, implica que algunos datos pueden ser restringidos en cuanto a la libre difusión y cesión.

Como regla, los datos sensibles no se pueden circular sin permiso expreso, pero hay otros datos que se pueden mantener en confidencia dentro del registro, y sólo posibles de cesión cuando el titular lo autoriza.

La reserva que estudiamos en el parágrafo 4.6 muestra algunos ejemplos de este tipo de habeas data, que algunos de los autores más prestigiados de la ciencia procesal constitucional definen como *habeas data reservador*.

d) *Derecho al silencio y al olvido mediante la cancelación del dato*

Una cosa es ocultar información archivada en virtud del acuerdo de confidencialidad con la persona concernida; y otra distinta, otorgarle un derecho a silenciar todo conocimiento que se tenga sobre la vida privada cuando el conocimiento de obtiene de los agentes que intervienen el proceso de tratamiento.

Esto es consecuencia del deber de secreto y confidencialidad que los registros deben preservar. La violación o amenaza que potencialmente exista, la controla el afectado a través del proceso de habeas data.

Asimismo, cuando el dato ha cumplido la finalidad para la cual se archivó, aparecen dos consecuencias que se traducen en derechos y deberes de la persona y el banco de datos, respectivamente.

El derecho se fundamenta en la potestad de reclamar la eliminación de toda información que violente la esfera de privacidad personal cuyo almacenamiento no fuera autorizado. También, el poder de exclusión o supresión permite demandar la cancelación del dato que se ha tornado impertinente o ha devenido innecesario.

> Los derechos al silencio y al olvido se recogen de la ley de tratamiento de datos española que obliga a las personas que intervienen en cualquier fase del tratamiento de datos a mantener reservada la información que adquieren en ocasión del trabajo. Se trata por tanto –afirma Orozco Pardo- de la situación en que la existencia y contenido de los datos debe quedar dentro del ámbito funcional y finalidad del fichero para el que fueron recabados evitando el "rumor informático" (derecho al silencio) y del derecho a que, de oficio, el titular o responsable cancele o destruya los datos personales cuando se den alguno de los supuestos antes citados, sin que tenga que mediar previamente el ejercicio del derecho de cancelación (derecho al olvido).

El deber, por su parte, es del titular del archivo, quien debe eliminar la información personal compilada que ha perdido interés, actualidad o sentido para el objeto inicialmente guardado.

El afectado, si considera que los datos carecen de pertinencia o devienen inadecuados, puede ejercer el derecho de cancelación o bloqueo de transmisión, propiciando en el pedido al registro que se borren todos los datos innecesarios.

> Para Sagüés, este tipo de habeas data se denomina *exclutorio* o *cancelatorio*, interpretando que la eliminación procede en los casos en los cuales se trate de datos sensibles, aunque no existe una regla fija acerca de verificar cuándo procede esta vía constitucional. Puccinelli, por su parte, agrega que es factible incluir en esta versión a otra clase de datos que, sin resultar sensibles, de todas formas no puede ser almacenada por cualquier registro (como ocurre, v.gr., con las fórmulas de determinadas sustancias), pues aunque alguno las podrá contener

de manera reservada, en los casos en que no se trata de un registro habilitado para ello, no bastará con infidenciarla, sino que es imprescindible su eliminación.

34.4 ***Excepciones al derecho de acceso, rectificación y supresión***

En líneas generales el derecho de control sobre los archivos y los datos personales se restringe en contadas ocasiones. Las veces que así ocurre se fundamentan en cuestiones de seguridad nacional, orden público, razones morales y políticas, sin perjuicio de los derechos y acciones que a terceros les corresponde cuando están afectados sus intereses legítimos.

El artículo 14 ("Excepciones y restricciones") del proyecto de Convención Americana sobre Protección de Datos Personales * dispone que:

Sólo por ley se podrán establecer excepciones y restricciones en los principios, derechos y garantías en esta Convención enunciados y siempre que éstas sean justas y razonables en una sociedad democrática:

d) Para la protección de la seguridad del Estado de la seguridad pública, para los intereses monetarios del Estado o para la represión de las infracciones penales;

e) Para la protección de las personas concernidas y de los derechos y libertades de otras personas;

f) Para el funcionamiento de ficheros de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existe riesgo de que las personas sean identificadas. Siempre existirá recurso para que la autoridad judicial decida si en un caso concreto estamos ante una excepción o restricción razonable.

En la ley nacional se establecen como excepciones las siguientes (art. 17):

4. *Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.*

5. *La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.*

6. *Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.*

Es importante agregar que la obstaculización al derecho de acceso es considerada falta grave del titular o usuario del archivo.

35. El ejercicio del derecho de acceso y control

Los requisitos para entrar en los bancos de datos se clasifican por el lugar, el tiempo y la forma como se debe realizar.

El *lugar* donde plantear la pretensión es ante el titular del registro o archivo que tiene los datos personales del interesado. La categoría de la información personal puede eludir el derecho de acceso, por ejemplo, en los casos de hospitales y demás instituciones sanitarias –públicas o privadas- (ver art. 8º de la ley), la recolección de datos se ampara por el secreto profesional. De similar envergadura es la prohibición de acceso a los archivos de datos sensibles que únicamente se admiten crear cuando median razones de interés general, autorizadas por la ley.

La intervención de un tercero en el tratamiento de los datos implica obligarlo solidariamente con el titular del archivo, de manera que corresponde tener en cuenta el domicilio del cesionario, a los fines de deducir el reclamo administrativo.

Si el banco de datos no informa de conformidad con lo requerido, el lugar donde presentar el habeas data es el del órgano de control que la ley establezca, imponiendo así una suerte de procedimiento previo para entablar la demanda judicial.

El *tiempo* para formular el pedido, siguiendo el derecho comparado, oscila entre intervalos de seis a doce meses.

> El reglamento sancionado en Argentina, establece en el art. 14 inciso 3º, que el derecho de acceso sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al afecto.

> España, por su parte, está dicho en términos similares que el derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

La periodicidad para el ejercicio del derecho de acceso es un criterio que llega de las normas europeas, especialmente del Convenio 108 y de la Directiva 95/46/CE, aunque ninguna de ellas establece un tiempo determinado sino la elasticidad del período prudente y razonable, para admitir una cobertura amplia.

La *forma* de concretar el derecho está liberada de requisitos formales. Rige el principio de libertad sin solemnidades, aunque habitualmente los órganos de control presentan formularios que facilitan la fundamentación del planteo.

35.1 Condiciones generales

España es uno de los países más avanzados en la defensa y protección de los derechos sobre los datos personales. La creación de una "Agencia de Protección de Datos" ha permitido elaborar una serie de reglas técnicas que actúan a modo de orientadores para el ejercicio de los derechos *.

La petición de acceso a los archivos, así como los de rectificación y cancelación de datos son derechos de carácter personalísimos, condición que determina que sólo puedan ser ejercidos por el afectado frente al responsable del fichero.

Este debe acreditar su identidad frente al sujeto reclamado. Podrá, no obstante, actuar a través de mandatario cuando se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos, en cuyo caso será necesario que el representante legal acredite tal condición.

La ley configura los derechos de acceso, rectificación y cancelación como derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

La pretensión deberá llevarse a cabo mediante solicitud dirigida al responsable del fichero y contendrá:

- *Nombre y apellido del interesado acreditado con la fotocopia del documento nacional de identidad y, en los casos que excepcionalmente se admita, de la persona que lo represente, así como el documento acreditativo de tal representación. La fotocopia del documento nacional de identidad podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho.*

- *Petición clara y fundada.*

- *Domicilio a efectos de notificaciones, fecha y firma del solicitante.*

- *Documentos que respalden la pretensión.*

- *El interesado deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.*

El reclamo siempre es gratuito, tanto para el derecho de acceso como para la rectificación, actualización o supresión de datos personales.

> Inclusive, en la acción judicial de habeas data, la jurisprudencia ha señalado que se encuentra alcanzada por la exención establecida en el artículo 13 inciso b) de la ley de tasas judiciales 23.898, ya que se considera a este proceso constitucional como una especie de amparo (CNCiv., Sala F, setiembre 1/998, *in re:* "Cosentino, Ricardo C. y otro c/ Organización Veraz S.A.").

35.2 Contenido de la información

El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción.

En el caso de que la solicitud no reúna los requisitos especificados precedentemente, el requerido podrá solicitar la subsanación de los mismos.

> El proyecto de Convención Americana sobre Protección de datos personales *, establece que:
>
> 3. Toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que los ampare contra actos que violen sus derechos fundamentales reconocidos por esta Convención, la Constitución de los Estado Parte o la ley.
>
> 4. Toda persona tiene derecho a controlar sus datos personales existentes en los ficheros públicos o particulares, la garantía y el procedimiento judicial para ejercer tal control es el habeas data.

La información debe ser suministrada en forma clara, exenta de codificaciones y, en su caso, acompañada de una explicación en lenguaje sencillo que permita la interpretación simple por cualquier persona.

La producción de la respuesta ha de procurar ser amplia y completa, sin acotarse a los límites de lo requerido por el afectado o interesado.

Ese informe no puede revelar datos pertenecientes a terceros, aun cuando se vinculen con el emplazamiento y la respuesta consecuente.

35.3 Derecho de acceso.

Al ejercitar el derecho de acceso, el afectado podrá optar por uno o varios de los siguientes sistemas de consulta del archivo, siempre que la configuración o implantación material del fichero lo permita:

- Visualización en pantalla.
- Escrito, copia o fotocopia remitida por correo.
- Transmisión electrónica de la respuesta.
- Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo.

El requerido resolverá sobre la solicitud de acceso en el plazo de diez días corridos, el cual surtirá los mismos efectos que los reclamos administrativos a los fines de adoptar el silencio como forma expresa de denegación. También cabe la acción de amparo por mora en el pronunciamiento.

En el caso de que los datos provengan de fuentes diversas, deberán especificarse las mismas identificando la información que proviene de cada una de ellas.

35.4 Ejercicio del derecho de rectificación y cancelación.

Los derechos de rectificación y cancelación se harán efectivos por el responsable del fichero dentro del término máximo de cinco días contados desde que se recibió el reclamo del titular de los datos. Si los datos hubieran sido cedidos previamente, el titular del archivo deberá notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su registro.

El artículo 16 dispone en cuanto aquí interesa:

Inciso 2º *El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.*

Inciso 3º *El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de habeas data prevista en la presente ley.*

Inciso 4º *En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.*

Inciso 5º *La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.*

Inciso 6º *Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo o consignar al proveer información relativa al mismo, la circunstancia de que se encuentra sometida a revisión.*

Inciso 7º *Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.*

La solicitud de rectificación deberá indicar el dato que es erróneo y la corrección que se requiere, acompañada de la documentación justificativa.

Cuando se reclame la cancelación, el interesado deberá manifestar si revoca el consentimiento otorgado.

En la pretensión de supresión del dato erróneo o inexacto se ha de acompañar el respaldo instrumental pertinente. Este no procederá cuando pueda causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existe una obligación de conservar los datos.

Solicitada la rectificación o cancelación, el responsable del fichero podrá estimarla y comunicar los argumentos que resulten de la decisión a adoptar.

Transcurrido el plazo de cinco días sin que de forma expresa se responda a la solicitud de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación judicial que corresponda. Obsérvese que aquí la ley otorga un plazo en días hábiles a diferencia del derecho de acceso cuya respuesta se mide en días corridos.

En el trámite administrativo incoado y mientras éste se resuelve, el titular del archivo debe bloquear la información o consignar el estado de revisión en que se encuentra, obligaciones que generan responsabilidades consecuentes cuando no se cumplen de inmediato.

> La justicia nacional tiene resuelto que en un juicio de habeas data cuyo objeto sea la supresión de información que se aduce inexacta, es procedente el dictado de

> una medida cautelar tendiente a que la demandada se abstenga de brindar el dato en cuestión, pues de mantenerse la situación de hecho aparentemente irregular, la ejecución de una sentencia favorable puede convertirse en ineficaz, en tanto la difusión anterior a su dictado es susceptible de influir definitivamente, con perjuicio al derecho que se asegura, en el ánimo de quienes sabrían del dato en cuestión (arts. 195 y 230 inciso 2º, CPr., *in re:* CNCom., sala B, agosto 8/996, "Yusin, Mauricio G. c/ Organización Veraz S.A.").

La cancelación exige el borrado físico de los datos, sin que sea suficiente a estos efectos una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las bajas producidas.

En los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización.

Se exceptúa, no obstante, el supuesto en el que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

Bibliografía Capítulo IX

Ekmekdjian, Miguél Angel – Pizzolo, Calógero, *Habeas data. El derecho a la intimidad frente a la revolución informática*, editorial Depalma, Buenos Aires, 1996.

Estadella Yuste, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales*, editorial Tecnos, Madrid, 1995.

Falcón, Enrique M., *Habeas data*, editorial Abeledo Perrot, Buenos Aires, 1996.

Fappiano, Oscar Luján, *Habeas data: Una aproximación a su problemática y a su posible solución normativa*, en "Liber Amicorum" Héctor Fix Zamudio, volumen 1, editorial Secretaría de la Corte Interamericana de Derechos Humanos, San José, Costa Rica, 1998.

Gozaíni, Osvaldo Alfredo, *La legitimación en el proceso civil*, editorial Ediar, Buenos Aires, 1996.

Gozaíni, Osvaldo Alfredo, *Introducción al nuevo derecho procesal*, editorial Ediar, Buenos Aires, 1988.

Herrán Ortiz, Ana Isabel, *La violación de la intimidad en la protección de datos personales*, editorial Dykinson, Madrid, 1999.

Herrero Tejedor, Fernando, *Honor, intimidad y propia imagen*, editorial Colex, Madrid, 1994.

Loianno, Adelina, *La defensa de la intimidad y de los datos personales a través del habeas data*, AA.VV., editorial Ediar, Buenos Aires, 2000.

Martínez Sospedra, Manuel, *Sobre la intimidad. Derecho a la intimidad, vida privada y* privacy. *El art. 18 CE* in principio *en la jurisprudencia del Tribunal Constitucional*, en *Sobre la intimidad*, editorial Fundación Universitaria San Pablo C.E.U., Valencia, 1996.

Orozco Pardo, Guillermo, *Los derechos de las personas en la Lortad*, en Revista Informática y Derecho, números 6/7, editorial UNED, Mérida, 1994.

Peñarrubia Iza, Joaquín María, *El derecho de acceso a los archivos y a los documentos de la Administración Militar*, editorial Cívitas, Madrid, 1999.

Perez Luño, Antonio E., *Derechos Humanos, Estado de Derecho y Constitución*, editorial Tecnos, Madrid, 1991 (4ª edición).

Puccinelli, Oscar Raúl, *El Habeas data en Indoiberoamérica*, en *El Amparo Constitucional, perspectivas y modalidades*, editorial Depalma, Buenos Aires, 1999.

Sagüés, Néstor Pedro, *Subtipos de habeas data*, en revista Jurisprudencia Argentina del 20/12/95. Buenos Aires.

CAPÍTULO X. El secreto de las fuentes periodísticas

36. Planteo del problema

El derecho a expresar las ideas por medio de la prensa sin censura previa constituye la base del derecho que se ha incorporado con el artículo 43 de la Constitución Nacional, en el párrafo que indica que al interponerse la acción de habeas data "*no podrá afectarse el secreto de las fuentes periodísticas*".

Si bien con esta mención fundamental la protección dispensada es obvia y suficiente, la ley reglamentaria no ha querido soslayar el fin constitucional, ratificando en el párrafo final del artículo primero que "*en ningún caso se podrán afectar las bases de datos ni las fuentes de información periodísticas"*.

El derecho a la información, posiblemente amplio y extenso en las características de su actual interpretación, afirma el pensamiento constitucional, ratificando que la prensa no puede ser amenazada ni requerida para revelar la fuente de los datos que fueron aplicados en su investigación o noticia.

De las convenciones internacionales se puede extraer que el derecho a la información, género de las manifestaciones que se proyectan (libertad de prensa, libertad de opinión, censura previa, etc.), tiene tres componentes esenciales: a) la libertad de investigar; b) la libertad de edición y difusión, y c) el derecho a recibir información y reservar, como secreto profesional, la confidencialidad de la fuente.

> Al conjunto de libertades que conforman el derecho a la información –sostiene Uicich- se le incorpora el derecho a no recibir informaciones distorsionadas o abusivas…,comprende pues la faceta de quien tiene la facultad de acceder a la información cuanto la del sujeto pasivo de esa información de que no sea distorsionada o no sea revelada en tanto afecte su intimidad y no exista cuestión de orden público o de seguridad del Estado que lo justifique.

Está claro que hablamos de un derecho muy distinto al de "réplica", también llamado "derecho de rectificación o respuesta", por el cual la persona que se siente afectada o agraviada por una nota periodística, puede exigir del medio de comunicación un espacio igual al que tuvo la publicación con el fin de dar su propia versión de los hechos revelados.

Tampoco se vincula con el problema de la censura previa donde la cuestión a resolver es la crisis de la garantía de intangibilidad que tiene la libertad de manifestar opiniones y pensamientos a través de la prensa, sin que ellas sufran cortapisas o impedimentos irrazonables, abusivos o arbitrarios.

El nudo a desatar en el tratamiento de datos personales, y en la acción de habeas data pertinente, será el que refleje los límites eventuales de la divulgación periodística, cuando revele aspectos de la vida privada o cualquier otra información sensible que, como tal, afecta el derecho a la intimidad individual.

Libertad de intimidad versus libertad de información, esa pareciera ser la problemática, aunque es exagerado presentarlo como un conflicto donde ha de existir un derrotado y un victorioso.

El justo razonamiento podría emerger del artículo 32.2 de la Convención Americana sobre Derechos Humanos:

Los derechos de cada persona están limitados por los derechos de los demás, por la seguridad de todos y por las justas exigencias del bien común en una sociedad democrática.

> Recordemos que la Corte Suprema de Justicia de la Nación, en la causa "Campillay" del año 1986 afirmó que la libertad de expresión es la libertad de dar y recibir información pero que éstas no implican un derecho absoluto y el legislador ante los posibles abusos producidos mediante su ejercicio, tipifica diversos tipos penales y establece ilícitos civiles, ya que el ejercicio del derecho de informar no puede extenderse en detrimento de la necesaria armonía con los restantes derechos constitucionales, entre los que se encuentran el de integridad moral y el honor de las personas (arts. 14 y 35 de la Norma Fundamental).

37. Reglas y excepciones

La potencial controversia entre intimidad e información es más aparente que real, al menos en la medida de los resultados que perseguimos alcanzar en la protección de datos personales.

El periodista y el medio de comunicación no pueden estar maniatados por una reglamentación obtusa que cancele el derecho a investigar la vida de las personas o a publicar las conclusiones de una investigación que compromete la privacidad de alguien.

Más allá de admitir que las personas públicas tienen una privacidad restringida a su propia exposición, y que el anonimato del hombre común le facilita la vida privada, no se puede modificar la perspectiva del derecho humano que a todos corresponde, es decir, la fama y notoriedad no es una excusa para invadir la intimidad, pero tampoco impide el ejercicio de informar e informarse sobre aquello que se considere de interés general.

> Urabayen sostiene que entre los derechos a la intimidad y a la información hay que encontrar un equilibrio porque ambos son de esencial y equivalente importancia pero de no ponérseles límites, cada uno tratará de anular al otro. Ahora bien, como el interés general priva sobre el particular, podría partirse de la base de que el derecho a la información es la regla y el derecho a la intimidad la excepción, debiendo analizarse cada caso independientemente.

El punto de encuentro es la verdad revelada, y el límite la prohibición de falsedad y difamación.

En ambos casos, ninguna ley de tratamiento de datos personales podría modificar esta relación tomada de los hechos tal como suceden.

Supongamos que un periodista toma conocimiento de un hecho probablemente ilegal que sucede en un organismo público y decide investigar. Pensemos que confirma la intervención bochornosa de algún funcionario y decide elaborar la nota con fines de publicidad.

El eventual conocimiento que tome el afectado podría admitir el planteo defensivo de su intimidad a través de un habeas data reservador, por el cual el Juez tendría facultades para ordenar la confidencialidad de los datos archivados en el banco de información periodístico evitando su divulgación.

Esta hipótesis no se puede sostener.

En efecto, el principio incanjeable es la libertad de prensa y la intangibilidad del secreto de las fuentes periodísticas, de forma tal que, a lo sumo, el afectado podría deducir una demanda por derecho de rectificación; una querella por calumnia o injurias; o en menor medida, un habeas data donde se pretenda la rectificación o supresión de aquella información que demuestre ser inexacta o desactualizada.

> Pierini ed alter, sostienen que la acción prescripta por el habeas data, entendida como el acceso a las registraciones, veracidad, rectificación y permanencia, está limitada por el reconocimiento de otro derecho de igual importancia, como el de informar. En consecuencia, respecto de las bases de datos o registraciones periodísticas, sólo se debe limitar a la rectificación y anulación de lo publicado que sea inexacto o desactualizado. No puede realizarse con anterioridad a la publicación, por cuanto aquéllos se desconocen y porque se trataría de una cuestión de censura previa, ya que, por inexactos que fueran, no se tiene conocimiento de ellos hasta su publicación o difusión.

De suyo, tampoco podría intimarse al periodista a revelar los fundamentos donde apoya sus conclusiones, porque de esa manera se ingresaría en el secreto profesional y en la invulnerabilidad que se garantiza a las fuentes de información periodística.

38. ¿Las fuentes de información son bases de datos?

La protección constitucional a las fuentes de información periodística ubicada en el capítulo garantista de los nuevos derechos fundamentales tiene su significado.

La fuente de información es el dato reportado por otro, en cuyo caso el conocimiento logrado se toma como una confidencia. La investigación, a su vez, permita reunir otro tipo de datos, que se van almacenando en un registro particular hasta conseguir una suma razonable de información que permita elaborar la nota u opinión a publicar. Este tipo de archivo no se encuentra entre aquellos que están destinados a proveer informes a terceros.

Una interpretación diferente se puede adoptar basando la coincidencia entre fuente de información previa a la edición y banco de datos destinados a proveer información, en cuyo caso la aplicación del artículo 43 se deduce inmediatamente.

> Pierini, Lorences y Tornabene dicen que hay que diferenciar la obligación de proporcionar la fuente, del caso de los registros, bancos de datos y demás registraciones relacionadas con la actividad periodística que no implican revelación de fuentes y que se refieren a constancias concretas existentes en ellos. Esta diferenciación entre elaboración de la nota y publicidad de la información adquirida no es antojadiza, sino que responde al criterio concreto referido a la libertad de informar, la cual debe preservarse y permitirse, pudiendo acarrear responsabilidades luego de ser ejercida y no previamente. Hasta el momento de la publicación de la información, los archivos y datos tienen la entidad, las características y el resguardo similares a los de las fuentes, o sea, no están alcanzados por norma alguna y se encuentran comprendidos dentro del secreto profesional y protegidos por el artículo 43 del mismo cuerpo legal. Luego de publicada la información, nadie podrá exigir válidamente el aporte de las fuentes utilizadas, pero la noticia ha adquirido una autonomía distinta y es objeto de recursos y acciones.

Nosotros creemos que las fuentes de información periodística están protegidas por el secreto profesional y por el ejercicio libre e incondicionado para opinar y publicar las ideas por medio de la prensa.

Mientras que los bancos de información almacenada que se bosquejan como "archivos periodísticos" están excluidos de la acción de habeas data, al no estar destinados al tratamiento de datos personales, ni para proveer información a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Ahora bien, cuando la investigación está centrada sobre una persona en particular, es evidente que el proceso de recolección de datos invadirá el reducto de la privacidad individual, pero la fuente de información se mantiene confidencial y secreta. En todo caso el problema estará en resolver si el archivo periodístico está alcanzado por la protección constitucional del artículo 43, o puede ser abierto ante el emplazamiento del afectado.

Si bien tienen un destino diferente, conviene informar el contenido del artículo 28 de la ley sancionada: *"1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a la ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable; 2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna"*.

A veces, se ha justificado desplazar el secreto profesional del periodista cuando "intereses del Estado" lo aconsejan, haciendo ceder el derecho de libertad de prensa por un hipotético interés superior.

> En la causa "Gorriarán Merlo" (C.Fed.San Martín, Sala I, mayo 2/996) se sostuvo que *"el secreto profesional periodístico y el derecho a resguardar las fuentes de información, cede cuando razones de interés público de relevante jerarquía así lo aconsejan y cuando ello no vulnera el derecho a no autoincriminarse, ni afecta los límites previstos en el artículo 28 de la Constitución Nacional"*.

En los hechos, nos parece más razonable adoptar un criterio propio y adecuado a las circunstancias y contextos en los que cada información se origina. De este modo, la reserva y confidencialidad de las fuentes

es una garantía impermeable, como lo es la libertad de prensa y el derecho a la información. Pero, al mismo tiempo, proporciona un deber inexcusable a los medios de comunicación para que desde una perspectiva ética y moral no difundan aquella información que, siendo disponible, pueda afectar la sensibilidad de las personas. La diferencia entre el *poder* de contar una gran cantidad de información sobre cada individuo y el *deber* de no difundirla sería más que nunca fundamental en este terreno.

> Esta idea reproducida de Aznar Gómez, agrega que, de lo contrario, el desfase entre ambos aspectos del problema podría aumentar la sensación social de indefensión de la intimidad frente a unos medios de comunicación –y otros agentes sociales- con recursos técnicos cada vez más sofisticados a la hora de obtener datos sobre cada uno de nosotros. Pero esto tampoco significa que la prensa deba silenciar cualquier información sin más, pues es tan negativo facilitar toda la información como acallar parte de ella sin ningún otro criterio que la decisión personal de cada informador. Otros criterios deben guiar la decisión: tener presente el tipo de persona involucrada en la noticia así como la naturaleza del asunto tratado.

39. La revelación voluntaria de la fuente periodística

El art.10 de la Convención Europea sobre Derechos Humanos permite a los periodistas resolver, de acuerdo a sus convicciones, la revelación de la fuente de información con el fin de dar mayor fuerza y contundencia a la publicación que realice.

Esta decisión voluntaria se concreta en cuestiones de interés general y en la medida que los hechos sean exactos y confiables, respetando la ética periodística.

> Por ende –ha dicho el Tribunal Europeo de Derechos Humanos en la causa, Fressoz y Roire c/Francia (21 de enero de 1999), es improcedente la condena dictada respecto del director de un semanario y el periodista que publicó declaraciones de impuestos del Presidente de una importante empresa automotriz si la información sobre el monto de los ingresos anuales de dicha persona estaba autorizada. Allí se agrego que, la sentencia que condenó al director de un semanario y a un periodista a resarcir el daño moral que entendió causado al Presidente de una empresa automotriz por la publicación de sus declaraciones de impuestos, efectuada en el marco de un artículo periodístico en el que se destacaban los incrementos salariales recibidos por el directivo mientras se oponía a similar medida reclama por los trabajadores de la empresa, viola la libertad de expresión tutelada por el art.10 de la Convención Europea sobre los Derechos Humanos, pues en el caso la publicación incriminada apareció en el marco de un conflicto social largamente tratado por la prensa y su finalidad no era perjudicar al directivo, operando la comparación entre los salarios de éste y el de los reclamantes como contribución a un debate público relativo a una cuestión de interés general.

Es decir, siguiendo la línea de pensamiento de la ley comunitaria europea, una injerencia en el ejercicio de la libertad de prensa sólo podría conciliarse con el art.10 de la Convención si se justifica por un imperativo preponderante de interés público.

Entre nosotros, la revelación voluntaria de la fuente periodística es una posibilidad más entre las que dispone el profesional para dar a publicidad su nota o comentario. La protección constitucional sólo a él preserva y no se extiende al confidente (la *fuente*, propiamente dicha) quien, en todo caso, tendrá un derecho de rectificación o respuesta, o un eventual reclamo indemnizatorio derivado de la violación al secreto revelado bajo confidencialidad.

Bibliografía Capítulo X

Aznar Gómez, Hugo, *Intimidad e información en la sociedad contemporánea*, en “Sobre la intimidad”, editorial Fundación Universitaria San Pablo C.E.U., Valencia, 1996.

Pierini, Alicia – Lorences, Valentín – Tornabene, María Inés, *Habeas data*, editorial Universidad, Buenos Aires, 1998.

Uicich, Rodolfo Daniel, *Los bancos de datos y el derecho a la intimidad*, editorial Ad Hoc, Buenos Aires, 1999.

Urabayen, Miguel, *Vida privada e información: Un conflicto permanente*, editorial Universidad de Navarra, Pamplona (España), 1977.

CAPÍTULO XI. El proceso constitucional de habeas data

40. Naturaleza jurídica

La calidad de proceso constitucional del habeas data resulta discutible cuando la configuración normativa de origen no es la Norma Fundamental.

Se debe recordar que la consagración de esta garantía puede ser *autónoma* como en la Constitución de Brasil; derivada como *especie* tal como resulta en Argentina donde se cataloga como sub tipo de amparo; o *subsidiaria* de otros procesos menos específicos pero de mayor cobertura como el recurso de protección chileno, la tutela colombiana o el amparo del Perú.

> En la explicación de García Belaúnde, Brasil fue el primero en introducir el habeas data en su Carta Constitucional, y otros lo han seguido. Y lo han hecho como figura autónoma. Pero en otros casos, como lo es la reforma argentina de 1994, existe como un sub tipo de amparo. Es decir, en la Argentina no existe el habeas data, sino el amparo en su vertiente protectora del dato. Pero pese a no existir, la doctrina de manera dominante y cierta jurisprudencia aceptando este hecho, tiende a denominarlo como *habeas data*, ya que de esta forma es más específico y más preciso en su protección.

En cada caso la originalidad latinoamericana muestra paralelos en la condición constitucional que tiene la figura, pues casi todos los países coinciden en darle un lugar al proceso dentro del capítulo de garantías procesales.

La diferencia con Europa es evidente; aquí la protección sobre los datos personales se toma de la tutela fundamental al derecho de intimidad, donde los Tribunales Constitucionales y los jueces comunitarios tienen una cobertura normativa amplia y completa desde las directivas de la Unión y la legislación específica de cada nación (donde se destaca España entre todos los demás).

Por su parte, Estados Unidos sigue la línea de sus enmiendas en materia de derechos subjetivos y colectivos prefiriendo las acciones individuales cubiertas por una ley que defiende la privacidad de los hogares y las personas.

La posición legal donde el habeas data se instala no es una cuestión menor. Siguiendo el esquema enumerado se podría afirmar que América ha creado un "proceso constitucional" propio (autónomo) o derivado (como modalidad del amparo); Europa tiene derechos y deberes a partir de las leyes de tratamiento de datos personales y Estados Unidos una acción especial que difiere en poco de las pretensiones destinadas a la defensa de la intimidad.

Ahora bien, esta línea de presentación no es simétrica con la eficacia que cada uno acredita. América no tiene hasta ahora una experiencia valiosa para mostrar; Estados Unidos ha evolucionado en la tutela de la privacidad sobre los datos pero es regresiva en otros aspectos; mientras Europa orienta desde la comunidad económica una potencia arrolladora de normas y resoluciones que persiguen más ideales que protecciones concretas o particulares.

Si basamos la naturaleza jurídica del habeas data en estas características, no cabe duda que Argentina tiene un proceso constitucional propio logrado desde la interpretación amplia del artículo 43 de la Constitución. Pero además, el capítulo VII de la ley sancionada incorpora una "acción de protección de datos personales" que se aleja del modelo amparista, pese a que el artículo 37 declara aplicable el procedimiento de este proceso constitucional.

> La amplitud teleológica es necesaria para evitar el restriccionismo tradicional en la jurisprudencia del amparo, que sigue atendido como un proceso excepcional y contingente. Tampoco hay que olvidar que el "Núcleo de coincidencias básicas" obligó a localizar el habeas data dentro del capítulo que se le asignó al derecho de

> amparo, pero que puede ampliar su lectura con los derechos que al afectado se le acuerdan a través de la ley reglamentaria para el tratamiento de datos personales.

La conclusión interesa reafirmarla para evitar disquisiciones sobre la jerarquía que tiene, toda vez que es diferente la ubicación y el rango de garantía según se interprete nacida desde la Constitución, legislada por una ley procesal o reglamentada con independencia de su ubicación normativa.

> La explicación de García Belaúnde, al respecto, es ineludible por su claridad y precisión. El prestigioso autor peruano sostiene que si el habeas data no está expresamente consagrado en la Constitución no es un instituto procesal constitucional, ya que para que existan figuras procesales es necesario que la institución no sólo se destine a la defensa constitucional, sino que tenga una ubicación constitucional expresa…., pero puede ser que el derecho sea defendido por un habeas data que no es creación constitucional, sino creación de una ley procesal cualquiera, de naturaleza mas bien civil. Pues simplemente estaremos al frente de una institución de naturaleza civil que protegerá derechos fundamentales…, nada impide que una institución como es el habeas data, nazca al margen de la Constitución y por ley expresa, si bien es cierto que estará destinada a la defensa de determinados derechos con rango constitucional. Existe otro problema y es el relacionado con la reglamentación del habeas data, que interesa con independencia a su ubicación normativa. Esto es, aún cuando el habeas data nazca directamente en la Constitución, cabe la pregunta de cómo tiene que regularse. Y al respecto caben cuatro posibilidades: a) que el habeas data sea regulado dentro de un código procesal cualquiera; b) …que sea regulado dentro de una ley cualquiera; c)… que sea regulado por una ley especial, y d)… que sea regulado por un código especial sobre procesos constitucionales.

40.1 El habeas data es un proceso constitucional

El derecho a la intimidad como género que caracteriza la defensa de la privacidad, del honor, la imagen, la reputación, la identidad, entre otros de los derechos que mencionamos en los capítulos iniciales, es el fundamento de la garantía que tutela el habeas data.

Al ser *garantía*, es la herramienta procesal que la Constitución dispone para afianzar el cumplimiento de los derechos fundamentales; por eso, a partir del derecho de amparo creado por la Constitución Nacional, se perfila este proceso constitucional específico de protección a la persona agredida o amenazada por los bancos de datos que aprovechan la información personal que le concierne.

> El habeas data no es un derecho fundamental *stricto sensu* –dice de Slavin-, sino que se trata de un proceso constitucional. Nos hallamos frente a un instrumento procesal destinado a garantizar la defensa de la libertad personal en la era informática.

La calidad de los derechos a proteger le otorga esa base constitucional que torna al habeas data como un instrumento procesal irremplazable e incondicionado.

En América, la fortaleza del proceso constitucional se mide por la finalidad a cumplir como un derecho fundamental que a todos corresponde. Es decir, la libertad de controlar los archivos que contienen datos personales y disponer sobre ellos el destino de la información que utilizan, permite extender la figura a personas físicas e ideales, sin acotar la tutela al derecho consagrado en Europa como "autodeterminación informativa" que sólo se interpreta como un derecho humano.

40.2 Es un proceso constitucional "autónomo"

La autonomía del habeas data como proceso diferente al amparo se sostiene por la identidad propia que tiene el objeto a demandar. Se tiende a proteger los datos personales de la persona que se han ingresado en un archivo, registro o banco de datos.

Es verdad que la definición del modelo amparista de cada lugar determina el perfil que puede revestir al proceso de protección de datos personales, y a su vez, ocupar más o menos espacios que la tradicional herramienta enumera como derechos de acceso, actualización, rectificación, exclusión y confidencialidad de los datos.

> Es el caso, entre otros, de Perú que desde la perspectiva de su habeas data incluye el derecho de acceso a la información pública y el derecho de rectificación o respuesta. En Paraguay también comprende, además de los consabidos derechos personales como privacidad, no discriminación, reserva sobre convicciones políticas o religiosas, otros derechos personales de índole patrimonial, referidos a información sobre bienes o datos sobre bienes.

En nuestro país, la inclusión del "habeas data" entre los contenidos del derecho de amparo, no puede llevar a confundir la naturaleza jurídica del mismo.

Actualmente, el nuevo artículo 43 de la Constitución Nacional significa un cambio fundamental en el tratamiento del tradicional proceso de amparo. Ha dejado de ser una figura procesal para constituirse en un "derecho" o "garantía" específico, cuya principal concreción es instalar el derecho al amparo.

Por ello, el criterio que observa al amparo como juicio está abandonado, para convertirse en la garantía por antonomasia; la única herramienta disponible para actuar los derechos fundamentales de inmediato, sin mediateces ni postergaciones.

De este modo, el artículo 43 promete, en realidad, una tutela judicial rápida y expedita, y con varias finalidades que seguidamente enumera:

a) Amparo contra actos u omisiones de autoridades públicas.

b) Amparo contra actos u omisiones de particulares.

c) Amparo contra la inconstitucionalidad de las leyes.

d) Amparos especiales según se trate de "cualquier forma de discriminación", "protección del ambiente", "derechos de la competencia", "derechos del usuario y consumidor".

e) Amparo colectivo, para los derechos de incidencia general que se encuentren afectados (derechos de pertenencia difusa).

f) Habeas data

g) Hábeas Corpus.

Cada uno tiene una finalidad específica e inconfundible, y no pueden tramitar por carriles comunes porqué ellos son independientes. La comunión que los encuentra está en la "tutela judicial efectiva" que cada derecho establece, y las reglamentaciones deberán señalar los procedimientos pertinentes.

Adoptar al habeas data como un tipo o modalidad del amparo no nos parece equivocado –sin compartirlo-, si este se toma como el género común donde reposar la garantía procesal única y permanente que es, en definitiva, el proceso judicial.

Si observamos la ley sancionada, una interpretación rápida puede llevar a confusiones, porqué el artículo 37 dice:

La acción de habeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común, y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo.

¿Cuál es el error?. En que si es un amparo común, requiere acreditar la arbitrariedad o ilegalidad manifiesta; actualmente no hay ley de amparo y la 16.986 se encuentra derogada –virtualmente- en buena parte de sus disposiciones. Lo mismo sucede con el derecho a un proceso rápido y expedito sujeto, únicamente, a la preferencia de otra vía judicial más idónea; de modo tal que si es un amparo, sería inconstitucional el reclamo administrativo previo que establecen los artículos 13 a 15, los que si bien es cierto refieren al derecho de los titulares de los datos como facultativos (*Toda persona puede…*), el artículo 41 establece que al contestarse la demanda, el banco de datos, archivo o registro debe señalar las razones por las

cuales no evacuó el pedido efectuado por el interesado (dando como supuesto que el actor dedujo un reclamo administrativo anterior).

En cambio, si tomamos al habeas data como proceso constitucional autónomo, sería suficiente tener en la ley sancionada el marco reglamentario, sin encontrar fricciones con el proceso de amparo o con el procedimiento sumarísimo que es absolutamente incompatible con las características que tiene el sistema de protección de datos personales.

40.3 No es el habeas data un amparo sobre los datos personales

En razón de lo expuesto no existe, en nuestro país, el amparo contra los actos arbitrarios o ilegítimos que en forma actual o inminente afecten la libertad por el uso de datos personales.

La vía pertinente es el habeas data como actual mecanismo para lograr el acceso a los archivos y otras pretensiones como la actualización, rectificación, supresión o confidencialidad de la información personal almacenada. Inclusive, con la ley se puede responder a otras lesiones derivadas del tratamiento de datos personales (v.gr.: lesiones al honor, la imagen, la identidad, etc.).

La única explicación posible que tiene la confusión reinante en la jurisprudencia, la cual concibe al habeas data como una modalidad del amparo, y que en los términos de la reglamentación puede consolidarse, llega de la ubicación constitucional donde está inserta la garantía, que como se recuerda, proviene del marco restrictivo que tuvo la reforma constitucional; sin perjuicio de la mencionada alegación del artículo 37 reglamentario.

> Bien lo dicen Dalla Via y Basterra cuando piensan que cada párrafo del artículo 43 tiene autonomía y se refiere a acciones diferentes. Esto es muy claro –afirman- en el caso del hábeas corpus, que es anterior al amparo y que, inclusive, le dio razón de ser. Su ubicación constitucional debería haber sido el artículo 18, donde está su base en la enumeración que garantiza que nadie será arrestado sino en virtud de orden escrita emanada de juez competente; pero la prohibición establecida por la ley 24.309, de modificar la primera parte nos privó de esa posibilidad, consagrando expresamente la garantía en el artículo 43; razones históricas de la Argentina reciente justificaban dar rango constitucional a los principios ya consagrados en la denominada "Ley De la Rua" de hábeas corpus. Otro tanto podría decirse del habeas data, una acción cuyos basamentos originarios se rastrean más bien en el hábeas corpus que en el amparo; y no sólo por razones de denominación sino, principalmente, por las características de un procedimiento destinado a averiguar y, eventualmente, modificar una situación determinada. En el caso del habeas data, no sólo ocurrió que estaba vedado introducir modificaciones en la primera parte del texto constitucional, sino que además su inclusión no fue expresamente prevista en la ley 24.309 declarativa de la reforma constitucional, de manera que el constituyente recurrió al ardid de incluirla en el artículo sobre amparo, como un párrafo dentro de esa especie de garantía.

41. Reclamo administrativo previo

La acción judicial de habeas data no se puede plantear directamente al Juez sin antes haber requerido el acceso a los archivos y deducidos los reclamos que contra el mismo se tuviere.

La afirmación no se puede llevar al extremo de negar la acción basándose en la necesidad de transitar por vías previas o paralelas, pero es preciso diferenciar a la garantía constitucional, propiamente dicha, del reclamo administrativo previo que constituye la etapa prejudicial.

> El agotamiento de la vía administrativa para generar el acto que cause estado susceptible de revisión contencioso-administrativa no resulta de necesaria producción como paso previo al habeas data, ya que tal proceder no se concilia

> con lo normado por la Constitución, al considerarlo como un supuesto de amparo (C.Cont.administ. Córdoba, Sala 1ª , 29/3/95, en Rev. La Ley Córdoba 1995-948).
>
> Sin embargo, el mismo fallo aclara que esta conclusión no impide sostener la conveniencia que el peticionante solicite a la Administración tanto el suministro de la información necesaria y de su finalidad, cuanto su rectificación, debiendo ello ser tomado en cuenta al momento de imponer las costas.

En efecto, la tutela sobre los datos personales persigue afianzar el control sobre los bancos de datos desde una doble perspectiva: a) la del acceso libre y sin restricciones de la persona interesada y, b) del órgano especialmente creado para esos fines de vigilancia y fiscalización.

En primer término se ha previsto que el derecho de acceso se deduzca directamente al archivo que almacenó la información personal, para que una vez conocido se resuelva las acciones a seguir.

En segundo lugar, el órgano de control –art. 29- (por ejemplo, la Agencia de Protección de Datos) tiene la función de velar por el cumplimiento de la ley específica e informar a las personas afectadas en sus derechos para asumir la representación de ellas o adoptar decisiones particulares con poderes suficientes derivados del poder que acreditan.

> En Argentina la ley diferencia el derecho de acceso, otorgando al titular de los datos, previa acreditación de su identidad, la posibilidad de obtener información directa de los archivos públicos o privados destinados a proveer informes; respecto al habeas data que asume como demanda judicial cuando se quiera tomar conocimiento de los datos personales almacenados o se pretenda la rectificación, supresión, confidencialidad o actualización. En caso alguno se establece la subsidiariedad y, por ello, no hay reclamo administrativo obligatorio expreso, aunque ello se desprende del art. 41 párrafo final.

Por su parte el proceso constitucional de habeas data es la etapa judicial ineludible, al menos en alguna de estas situaciones: a) cuando el derecho de acceso o las acciones consecuentes se niegan en la vía prejudicial o, b) cuando es necesario obrar con urgencia acordando al habeas data un sentido eminentemente cautelar.

> En opinión de Dalla Vía y Basterra existen dos etapas bien diferenciadas: una prejudicial y otra judicial. Primeramente, si la persona interesada en tomar conocimiento de sus datos, de la finalidad o utilización, o aún teniendo conocimiento de ellos desea la supresión, actualización, rectificación o confidencialidad de los mismos, debería solicitar a través de notificación suficiente, tal el caso de carta-documento, por ejemplo, su necesidad de conocimiento o corrección de datos al titular del registro o banco de datos. Si el requerido cumple con la solicitud, o no hubiera nada que rectificar o suprimir, no es necesario pasar a la etapa judicial, pero si el titular del registro, banco o archivo se niega a exhibir los datos o proceder según el requerimiento del interesado, o directamente no contesta dicho requerimiento, se pasará a la acción judicial.

Actualmente, los bancos de datos de información crediticia admiten el acceso en forma gratuita, comunicando a interesados o representantes sobre la base de datos informatizada.

Sin embargo, llevar las conclusiones que preceden al ámbito de las circunstancias que transitamos, puede poner en riesgo la libertad de intimidad que el artículo 43 constitucional ha querido consagrar.

La razón de ello está en que, de ser obligada la etapa prejudicial, la posibilidad del derecho de acceso establecida en el artículo 14 de la ley, depende absolutamente de la voluntad del titular del registro. En tanto que, afianzando el criterio cautelar del habeas data, se puede prevenir el mal uso de los datos y conseguir otras proyecciones defensivas que el derecho a la intimidad promete (v.gr.: honor, reputación, identidad, etc.).

Este temperamento ha orientado a calificados autores a sostener antes que fuera sancionada la ley que, frente a la ausencia de normas reglamentarias, se deben considerar dos pretensiones, secuenciales y sucesivas, una subsidiaria de la otra. La primera de información y la siguiente de ejecución.

> Sostiene Falcón que para la primera etapa, de información, se han de aplicar los trámites previstos en el artículo 6 de la Ley 16.986 cuando los archivos sean públicos, y el trámite sumarísimo si el banco de datos es privado destinado a proveer información. Por su parte De Slavin agrega que, sea que se lo considere como amparo específico o como amparo especializado, hay acuerdo sobre su carácter de acción tutelar de una garantía constitucional, y que la acción de habeas data se halla comprendida por la figura genérica del amparo.

En conclusión, pensamos que el reclamo administrativo establecido como "Derecho de los titulares de los datos", en los artículos 13, 14 y 16 actúa como vía concurrente al habeas data; determinando a partir de lo dispuesto en el Capítulo VII de la ley dos alternativas:

a) El planteo directo al órgano de control (art. 13)

Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita.

b) La petición concreta, antes de plantear una demanda judicial, al titular o responsable del archivo, base o banco de datos. El artículo 14 dice:

1. *El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.*
2. *El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de habeas data prevista en esta ley.*
3. *El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.*
4. *El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.*

Por su parte, si el planteo fuera de rectificación, actualización o supresión de datos, opera en la especie el artículo 16 con las excepciones del artículo 17 ya mencionados.

c) Deducir directamente la demanda judicial conforme los presupuestos establecidos en el artículo 33:

1. La acción de protección de los datos personales o de habeas data procederá:

- *Para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos.*
- *En los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.*

Queda en claro que cada pretensión puede abrir requerimientos incorporados en el derecho reconocido, es decir, desde el acceso se puede peticionar el conocimiento del destino y finalidad del archivo; y con el ejercicio del derecho de control se consigue individualizar la responsabilidad del titular o usuario, así como indagar sobre la existencia y localización de otros archivos o bancos de datos donde se hubieran transferido los datos personales.

> Es importante destacar –dicen Dalla Vía y Basterra- que el habeas data tiene un sentido preventivo o cautelar, pero puede suceder asimismo que el daño se produzca con motivo y en ocasión del uso de datos personales que se encuentren en archivos, bancos o registros de datos. En el primer caso, acción preventiva o cautelar, estaríamos ante la presencia de la garantía constitucional de habeas data. En el segundo caso no, puesto que una vez cometida la violación de la reserva de

la información se deberá recurrir al procedimiento tendiente a lograr una sanción penal, y la correspondiente indemnización de daños y perjuicios. El habeas datas solo servirá para evitar una nueva o futura violación de la información.

41.1 ¿Mediación previa?

En el régimen establecido por la ley 24.573 el artículo 2º apartado 5 excluye al amparo, hábeas corpus e interdictos de la instancia previa de mediación, obligatoria para acceder a la justicia.

La claridad de la norma impide opiniones dispares. Sin embargo, al sólo y único efecto de polemizar con el carácter procesal de "juicio de amparo" que se le asigna al habeas data, se puede plantear una calidad diferente para el procedimiento y, si bien es cierto continuaría su condición de proceso constitucional, el trámite sumarísimo o especial que se acuerde puede establecer la necesidad de un trámite previo de conciliación.

Cuando observamos la exigencia del reclamo administrativo previo, algunos coinciden en apuntar el sentido condicionante que la instancia supone; frente a ello existen opciones como la conciliación procesal (intra procesal o extra procesal).

De este modo se persigue pacificar sobre la cuestión litigiosa. La mediación no está en la órbita de estos condicionamientos. Parte del principio de voluntariedad para el modismo y sigue todo su curso atendiendo la manifestación de deseos original; el mediador no es absolutamente neutral, o al menos, lo es desde una posición diferente.

En esta corriente, el resultado es lo que menos interesa por estar elevado el sentido humanista del encuentro que pretende quebrar rigideces para acercar puntos de reflexión coincidentes. Por eso es correcto ver al mediador como un negociador espiritual que busca despejar la crisis elocuente entre las partes.

Puesta las cosas en estos términos, la alternativa de esquivar el reclamo administrativo previo con la intervención de un mediador, presenta la cuestión de nuevas metodologías para resolver controversias (v. gr.: mediación, conciliación prejudicial, arbitraje, etc.), y así tener una visión diferente, aunque polémica.

> Hemos dicho en otro lugar que, cuando se aprisionan los objetivos de una reforma legislativa sin tener en cuenta a la política procesal, o cuando se diseñan objetivos, se practican modificaciones judiciales o se planifica sobre la base de normas adjetivas de cambio, sin atender las facetas de la sociología procesal, queda latente el conflicto, pervive la insatisfacción y poco consigue el sistema creado sino cuenta con la confianza de la gente, que es justamente, el destino final de nuestras intenciones.

41.2 Tasa de Justicia

La etapa prejudicial en el derecho a la protección de datos personales se garantiza con el acceso gratuito y a intervalos que oscilan entre seis y doce meses para repetir el interés en lograr la información.

> Dice el artículo 19 (Gratuidad) que, *la rectificación, actualización o supresión de datos personales inexactos o incompletos se efectuará sin cargo alguno para el interesado*.

Respecto a la contribución fiscal por las actuaciones judiciales, el habeas data está exento de pagar tasa de justicia siempre y cuando proceda y consiga sentencia estimatoria. En caso contrario, la denegación confirmada (firme y consentida) obliga al peticionante a oblar el tributo.

> En efecto, si se pondera que el artículo 43 de la Constitución Nacional programa una subespecie de amparo, o amparo específico conocido en el derecho comparado como amparo informático o informativo, o por otros como una variable de esta acción, es por demás evidente que se encuentra alcanzado por la particular exención prevista por el artículo 13 inciso b) de la ley 23.898, (Cfr.

CNCiv., Sala F, setiembre 1/998, *in re:* Cosentino, Ricardo C. y otro c/ Organización Veraz S.A.).

42. Competencia

La diferencia que suelen establecer las normas reglamentarias, entre archivos públicos y privados, lleva también a distinguir la jurisdicción interviniente y la actuación de un fuero en particular.

Cuando el habeas data se plantea ante un banco de datos oficial la competencia es federal por estar comprometido el interés del Estado y corresponderle a éste la defensa de la Nación y sus dependencias.

> No obstante, en el estado actual de nuestra jurisprudencia, la Corte Nacional ha dicho que, "dado que las acciones de amparo y habeas data iniciadas contra una empresa de televisión por cable con el fin de conocer los datos personales y antecedentes que dicha entidad tiene del actor, no pone en tela de juicio ninguna materia relativa a cuestiones regidas por la ley 19.798 de telecomunicaciones, ni comprometen la responsabilidad del Estado, no resulta competente para entender en las mismas la justicia federal.
>
> De todos modos, el criterio mayoritariamente seguido es aquél por el cual se sostiene que, cuando la situación a tutelar por el habeas data se relaciona con el ejercicio de la función administrativa y los registros o bases de datos pertenecen a la autoridad pública, el fuero competente debe ser el contencioso administrativo (Cfr. C.Cont. Administ. Córdoba, Sala 1, marzo 23/995 *in re "*García de Llanos, Isabel c/ Caja de Jubilaciones, Pensiones y Retiros de Córdoba").

Es también la justicia federal la que debe actuar cuando los archivos de datos se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales.

En cambio, cuando la pretensión se formula ante archivos privados, rigen las disposiciones del código procesal civil, dando oportunidad al actor para deducir la demanda ante el juez del lugar donde debe cumplirse la obligación, o en su defecto, podrá elegir entre el domicilio del archivo, el del domicilio donde firmó el eventual acuerdo para el tratamiento de los datos, o donde se produzcan los efectos del uso de la información que le concierne.

El artículo 36 de la ley sostiene que: *"Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en que el hecho o acto se exteriorice o pudiere tener efecto, a elección del actor. Procederá la competencia federal: a) Cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y b) Cuando los archivos de datos se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales"*.

La jurisprudencia local afirma que, tratándose el habeas data de un proceso vinculado con la defensa de la intimidad personal, le corresponde intervenir a la justicia nacional en lo civil; criterio que se basa en relacionar las situaciones reguladas por el derecho privado y la pertenencia particular (privada) de la base de datos.

> Si la acción de habeas data se relaciona con situaciones reguladas por el derecho privado y el registro o base de datos pertenece a un particular, corresponde que la jurisdicción ordinaria sea la competente para juzgar el tema (Cfr. C.Cont. Administ. Córdoba, Sala 1, marzo 29/995, La Ley 1995-C, 948).

En cambio, si el registro demandado se dedica comercialmente a difundir información del contenido de su banco privado de datos, ello lo instala en la calidad de comerciante y, como tal, debe intervenir ante la justicia del fuero.

> Atento la manifestación del accionante referida a la inexistencia de antecedentes comerciales o bancarios perjudiciales, en razón de la cual se cuestionan los datos base de la información prestada, información que se vincula con el giro comercial de la empresa accionada, entiendo que la situación encuadra *prima facie* dentro

del ámbito mercantil (Cfr. CNCom., Sala A, noviembre 30/994, *in re* "Rossetti Serra, Salvador y otro c/ Organización Veraz S.A.")

43. Derecho de acceso y diligencias preliminares

El habeas data reconocido en el artículo 43 constitucional vincula el *conocimiento* o derecho de acceso, con la *finalidad* del archivo, circunstancia que demuestra la necesidad de acreditar algo más que un interés informativo.

El derecho de entrada al banco de datos se debe fundar en la presunción que se tiene respecto a la hipótesis de estar concernido y, en su caso, plantear la necesidad de conocer que datos se registraron, con qué finalidades y para cuáles propósitos.

Tal como surge de la norma fundamental, la subsidiariedad del reclamo es posible, de modo tal que se podría solicitar el acceso y la información para que, una vez confirmada la presencia individual en el registro, se concreten las pretensiones consecuentes de actualización, rectificación, supresión o confidencialidad.

Pero ello no es así; al menos no resulta más que una hipótesis probable para formalizar la demanda.

La doble vía de ingreso a los archivos públicos o privados que contienen datos personales se puede concretar directamente al titular del registro, como requerimiento extrajudicial; o a través de la acción de habeas data.

Sin embargo, el conocimiento también se puede lograr con diligencias preliminares, y particularmente por la medida que permite proponer al futuro demandado que *preste declaración jurada sobre algún hecho relativo a su personalidad sin cuya comprobación no pueda entrarse a juicio* (en cuyo caso, debería informar si es titular del archivo y si tiene registrado en el mismo al requirente).

Por otra parte, *el juez accederá a las pretensiones si estimare justas las causas en que se fundan, repeliéndolas de oficio en caso contrario.*

44. Sujetos procesales

¿Quién puede reclamar por sus datos personales?, ¿ante quién?, ¿se puede plantear en nombre de otro?, ¿tienen igual derecho las personas jurídicas?, ¿existe el derecho de representación del interés por familiares o allegados?

Todas son cuestiones que se vinculan con el derecho de acceso y control sobre los archivos. En cada caso se debe resolver quienes tienen posibilidades reales de actuar, así como saber quienes son las justas partes o legitimados que pueden responder por los derechos y obligaciones emergentes.

Inicialmente, reconocer los sujetos procesales del habeas data lleva la necesidad de asegurar la plenitud constitucional de protección a la intimidad o privacidad para quienes sean legítimos portadores del derecho que reclaman y frente a quienes deben asegurar el cumplimiento del mandato superior emitido por el artículo 43.

Sin embargo, no es suficiente partir del concepto que sirve de portada a esta norma constitucional. En efecto, la afirmación que "*toda persona*" pueda interponer la acción de habeas data respecto a los datos que a ella se refieren, no aclara la extensión ni el alcance que asigna a la legitimación activa; tampoco esclarece si los únicos obligados son *los titulares de archivos públicos, o privados destinados a proveer información*, y está ausente un criterio central sobre los derechos esenciales que tutela el habeas data. Se sabe que son los datos personales, pero falta indicar cómo pueden ellos provocar una lesión en otros derechos sensibles de la persona (v.gr: honor, imagen, reputación, etc.) y perseguir su restitución desde el proceso constitucional.

> El tema –dice Puccinelli-, de por sí es opinable, por cuanto en el primer párrafo aparece claro que el habeas data funciona respecto de los datos propios de quien lo articula. Sin desconocer los problemas que la ampliación de la legitimación activa en estos casos podría acarrear, cabe considerar que en el segundo párrafo

se lo faculta al Defensor del Pueblo a articular amparos y también a determinadas asociaciones, teniendo en cuenta la gran cantidad de violaciones a los derechos humanos que se producen porque cuando la actividad dañosa involucra a cientos o miles de personas, una importante cantidad de afectados no accionan por mero desconocimiento, por temor, por el costo, etc.

Por tanto, es preciso comenzar desde una base cierta que evite confusiones ulteriores. Con ello queremos expresar que la calidad del trámite a desarrollar, así como las condiciones y presupuestos del mismo, no pueden ser analizadas desde la tradición normativa y jurisprudencial del juicio de amparo, porqué el habeas data es un proceso constitucional diferente.

El marco general lo propicia el artículo 34 (Legitimación activa) que sostiene:" *La acción de protección de los datos personales o de habeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado. Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto. En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo"*.

44.1 Legitimación activa

La legitimación para obrar no es común para todos los casos, pues depende del objeto que se pretenda.

Diferentes son los requisitos si uno persigue el "derecho de acceso" a las fuentes de información; o se quiere un "control sobre la base de datos", o es otra la intención.

a) Si el caso fuera *conocer la información*, los probables intereses serían: 1) saber sobre la formación y existencia de los bancos de datos; b) tomar conocimiento del acopio informativo personal que se tenga, y c) la finalidad o destino que tienen esos registros.

La norma constitucional, como se dijo, vincula el conocimiento con la finalidad de ellos, circunstancia que demuestra la necesidad de acreditar algo más que un interés sobre los archivos, debiendo el demandante fundamentar las razones que entiende lo habilitan para ser informado de las fuentes y los objetivos que con los datos levantados se persigue.

El derecho a saber su incorporación en una base de datos, ocupa también al anoticiamiento permanente sobre la permanencia.

La forma como se conocen los datos puede ser voluntaria, en cuyo caso estamos fuera del marco que precisa el habeas data; o provocada, a través de las acciones judiciales pertinentes que al efecto se encaminen.

La información directa se brinda a través de la consulta en los ficheros, o visualizándolos si estos fueran telemáticos o informáticos. En cambio, es indirecta cuando se obtiene mediante escrito, copias, fotocopias u otro medio similar que no requiera el uso de dispositivos mecánicos específicos.

Para Velázquez Bautista, la ejecución del derecho de acceso conlleva una serie de exigencias o deberes, que realizan tanto el titular de la base de datos como el del derecho. Es la obligación de comunicar los datos encontrados al titular del derecho de acceso, comunicación que, según especifican las leyes de protección de datos, deber realizarse en forma comprensible, es decir, de manera que pueda entenderse.

El libre ingreso a los archivos informáticos o manuales puede limitarse cuando existan situaciones de reserva o secreto, o la difusión provoque inseguridad en las instituciones o, el mismo Estado atraviese por circunstancias de excepción (estado de sitio, por ejemplo).

b) Si la pretensión fuera de *control sobre las bases de datos*, la cuestión reconoce variantes.

Desde la óptica de las acciones tendientes a dar eficacia al control, las pretensiones se desglosan.

La necesidad de saber sobre datos personales que se ingresan en bancos de información públicos o privados constituye un aspecto del derecho a la información que no puede ser contrariado sin dar excepciones válidas o razonables.

Es el derecho de acceso que señalamos en el punto anterior, el cual se puede incoar ante el archivo, es decir, directamente al registro que lo contiene, y facultativamente, a través del habeas data, ante la renuencia de los organismos a suministrar la información que se pide, o por intentar el reclamo como acción directa.

En algunas legislaciones, el impedimento o la obstaculización del ejercicio al derecho de acceso o la negativa a facilitar los datos que se solicitan, son causales graves que pueden llevar a la sanción de los funcionarios, o a cancelar la autorización para tener sistemas informáticos de almacenamiento.

c) La facultad de requerir la *cancelación o la corrección* de los datos inexactos, otorga el denominado derecho al olvido, esto es, el principio a tenor del cual ciertas infomaciones (v.gr.: antecedentes penales prescriptos) deben ser eliminadas de los archivos transcurrido un determinado espacio de tiempo desde el momento en que acaeció el hecho a que se refieren, para evitar que el individuo quede prisionero de su pasado.

La corrección de los archivos puede efectuarse por el mismo sistema que los contiene, sea ya por la aclaración que formule el individuo, o por la información corroborada por la base de datos.

Estos organismos de registración, públicos o privados, generalmente pueden oponerse a las rectificaciones cuando ellas se promueven por quienes no son directamente interesados; excepción hecha de las pretensiones sostenidas por personas que invoquen un legítimo interés y la conservación de los datos les provocare riesgos o daños inminentes.

d) En cambio, si la idea es *actualizar los datos registrados*, debe acreditarse la inutilidad de los trámites administrativos dirigidos a obtener el pedido. De otro modo se llevan a la justicia cuestiones de naturaleza administrativa que harían de la función jurisdiccional un auténtico notariado.

e) Un supuesto más a considerar es el *derecho de rectificación o respuesta* con relación al habeas data.

El derecho a réplica, también conocido como derecho de rectificación y respuesta, que no se encuentra aun legislado en el ordenamiento positivo, tiene no obstante, plena captación a través del "bloque de constitucionalidad" que significan los tratados incorporados en el artículo 75 inciso 22. Particularmente, la Convención Americana sobre Derechos Humanos norma en el art. 14 que:

"*Toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley*".

La dimensión del problema se vincula con la difusión que pueden hacer los medios de prensa, de datos que conozcan sobre ciertas personas y los reproduzcan en una nota periodística, causándoles perjuicios.

El artículo 43 de la Constitución Nacional, y el agregado final que tiene el artículo 1º de la ley, disponen que "no podrá afectarse el secreto de las fuentes de información periodística", dejando en claro que el habeas data no se puede utilizar como remedio alternativo para el derecho de réplica.

En los hechos la norma le otorga a la prensa, *lato sensu*, la posibilidad de escudarse tras este derecho al secreto profesional, evitando revelar las fuentes donde obtuvo los datos que publica o difunde.

Pero el sujeto interesado debe tener, entonces, una vía útil y efectiva para conocer los registros que de él se tienen, así como para rectificarlos, actualizarlos o pedir su anulación.

Si no los tiene, existe una omisión inconstitucional.

> El derecho público provincial ejemplifica la preocupación del constituyente por esta situación. En Río Negro, la carta superior establece el "amparo informativo", reglamentado en la ley 2384.
>
> Ella dispone la procedencia de "*la acción de amparo informativo en favor de toda persona física o jurídica que temiera ver perjudicados su privacidad, su honor o el goce completo de sus derechos, según el caso, ante informaciones agraviantes o inexactas vertidas a través de cualquier medio de difusión*".

La coincidencia entre las disposiciones aparece en la "información inexacta", pero la diferencia estriba en los motivos que acuden para fundar una u otra pretensión.

Mientras el derecho a réplica supone obtener un medio equivalente al que difunde o reproduce un dato equívoco que nos agravia para perseguir su correcta exposición; el derecho de rectificación presente en el habeas data concierne al derecho de acceso a los bancos de datos para lograr cualquiera de las pretensiones a que ya hicimos referencia.

> De esta manera, dice Velázquez Bautista, se configura el derecho de rectificación aplicado a los servicios de información electrónica como una garantía más, un plus, que coadyuvar a proteger los bienes involucrados en un tratamiento automatizado de datos de carácter personal, que pueden lesionarse con la difusión de datos inexactos a través de los servicios de información periodística, situación que ya se ha dado en la práctica.

En líneas generales podemos decir que, a pesar de la amplitud que profesa el término "*toda persona*" que empieza el párrafo tercero del art. 43 citado, la acción sólo es posible para quien acredite un interés directo y un daño potencial o cierto que lo habilite al reclamo, tal como expone el artículo 38 inciso 2º de la ley.

> Cierto sector doctrinario (Falcón, Ekmekdjian), inspirados en el carácter constitucional de la medida, admiten que la legitimación sea amplia e irrestricta, encolumnando tras las personas físicas (quienes pueden actuar por sí o por medio de representaciones convencionales), los casos de ausencia (la legitimaciones el Defensor oficial), de herederos o sucesores universales (en resguardo del honor u otros derechos del difunto), las personas jurídicas y el Defensor del Pueblo.
>
> Palazzi, inclusive, sostiene la posibilidad de realizar un habeas data colectivo en los casos de discriminación.
>
> Cifuentes, entre otros autores, mantienen el "carácter personalísimo" de la garantía, agregando que, en ciertos supuestos, "es una variable del derecho a la intimidad consagrado en el art. 19 de la Constitución Nacional".

Para nosotros es preciso reconocer en el que peticiona algún derecho o interés vinculado con lo que está reclamando.

Por ejemplo, existe información totalmente privada que pertenece a la esfera de la intimidad y constituye un auténtico derecho al secreto absoluto. Esta, no puede ser difundida, aunque pudiera estar registrada (v.gr.: enfermedades psicosociales que informa una historia clínica). Mientras que otro tipo de registraciones eluden la condición de privacidad y se instalan en la dimensión de informaciones públicas que procuran una mejor administración del Estado (v.gr.: Registro Civil, Registros de la propiedad inmobiliaria o automotor, Policía Federal, Colegios, Universidades, Obras Sociales, Clubes, Compañías de Seguros, etc.), o el cumplimiento adecuado de ciertas obligaciones constitucionales (v.gr.: los registros en padrones).

Esta división pone de manifiesto que hay una esencial distinción entre el "titular" de los datos, y quienes los administran.

> Bianchi explica que titular es el individuo porqué a él le corresponden y pertenecen; en tanto que los administradores son quienes poseen los bancos o registros que recopilan y ordenan tales datos. "Estos últimos tienen cuatro

> obligaciones básicas: a) estar legitimados para haberlos obtenido; b) llevar un correcto registro, sin incurrir en falsedades, lo que incluye también su actualización; c) asegurar su confidencialidad y no proveer de información sino mediante autorización del titular o a requerimiento de autoridad competente; d) evitar su destrucción o deterioro".

La distinción entre sujetos con legitimación activa y sujetos legitimados pasivamente es naturalmente obvia e imprescindible.

Conclusiones:

- En el "habeas data" destinado a *conocer la información* que se tiene registrada, la legitimación para obrar le corresponde a "toda persona", "todos los habitantes", "todos los ciudadanos", o cualquiera otra persona física o jurídica (para utilizar algunas de las expresiones usadas en textos constitucionales o leyes reglamentarias) que proponga a un Juez el proceso.

Es un derecho a la información que no puede ser restringido por el "derecho subjetivo vulnerado" o el "interés legítimo a tutelar".

Esta libertad irrestricta proviene del carácter público que tiene la fuente informativa y de la condición expuesta de los datos (que en el caso se denominan "vacantes").

Ahora bien, como la norma constitucional relaciona el conocimiento con la finalidad del registro, es preciso que la persona que deduce la acción indique el motivo por el cual los solicita, para que una vez conocido, pueda concretar la supresión, rectificación, actualización o requerir la confidencialidad o reserva de aquellos.

> Altmark y Molina Quiroga señalan que la norma constitucional debió habilitar a toda persona a “tomar conocimiento de los datos a ella referidos y de su finalidad”, y como consecuencia de este derecho establecer la vía procesal para hacerlo efectivo. Esperamos –agregan- que esta interpretación correctora sea en definitiva la que se imponga, ya que resultaría contradictorio que debiera acreditarse la existencia de “ilegalidad o arbitrariedad manifiesta” por parte del titular u operador del banco de datos para que se pueda ejercer los derechos de acceso a los datos de carácter personal.

Elocuentemente se muestra de que manera la pretensión es compleja al fraccionar el objeto en dos motivos esenciales aunque dependiente el segundo del primero: a) conocer los datos o registros y, b) solicitar, en caso de información falsa o discriminatoria, alguna de las causas que posibilitan el habeas data.

No existirían problemas de intentar acciones independientes, pero como dijimos anteriormente, el Código procesal tiene otras vías para la pretensión, de modo que al proponer el habeas data como garantía subsidiaria, estaría postergada si el remedio propuesto en paralelo es más idóneo.

- Si la intención fuese interponer *habeas data correctivo*, en cualquiera de sus posibilidades (rectificación o actualización), va de suyo que sólo quienes tengan el "interés" específico de la demanda tendrán legitimación procesal.

La noción de "interesado" expresa la idea según la cual, toda persona -física o jurídica- tiene un derecho subjetivo sobre la información relativa a sí misma, aun cuando tal información haya sido reunida por otras personas.

Desde luego, un habeas data puede ser mixto, en el sentido de comprender un objetivo simplemente exhibitorio, o pretender también actualizar, rectificar, reservar o excluir datos, concernientes a la información que obre en un registro.

En este cuadro se puede aceptar la legitimación para actuar de aquellos que continúen el interés procesal de la persona registrada, tales como los herederos forzosos (v.gr.: ascendientes y descendientes, los colaterales hasta un grado determinado, los afines y el cónyuge -salvo que estuviese divorciado).

- En el supuesto del *habeas data tendiente a lograr la confidencialidad*, reserva o directa exclusión de los datos registrados, se acentúa el carácter personalísimo y, por tanto, la necesidad de acreditar la relación procesal que se invoca.

Para iniciar la protección solicitada basta cumplir con los recaudos indicados en el párrafo anterior; pero lograr la sentencia favorable depende del tipo de registro que los contiene y del uso que de ellos se haga.

La finalidad del habeas data es impedir que en bancos o registro de datos se recopile información respecto de la persona titular del derecho que interpone el "amparo", cuando dicha información está referida a aspectos de su personalidad que estén directamente vinculados con su intimidad, no correspondiendo encontrarse a disposición del público o ser utilizados en su perjuicio por órganos públicos o entes privados, sin derecho alguno que sustente dicho uso.

Se trata, particularmente, de información relativa con la filiación política, las creencias religiosas, la militancia gremial, el desempeño en el ámbito laboral o académico, entre muchos otros objetivos.

La diferencia entre el secreto y la intimidad está presente en este capítulo. Obsérvese que quien deduce la demanda no es titular ni dueño del secreto que está registrado. Es el legitimado pasivo -el que opera el archivo- quien tiene el secreto, que al ponerlo en contacto con otros medios evita la ocultación y los expone ante otras personas, provocando, con ese acto de circulación, el perjuicio que habilita el habeas data.

También la amenaza de difusión permite la vía.

Por eso la intimidad le pertenece a un sujeto preciso y queda en él la reserva de sus derechos. En cambio, el secreto está proyectado a terceros que lo conocen y que se convierten en garantes de la confidencialidad.

> A este respecto, dice Quintano que la simple indiscreción no puede ser objeto de protección jurídica ni menos jurídico-penal, porque la criminalización de tal comportamiento daría al traste o dificultaría no pocos aspectos de la vida social. Lo que sí es claro es que no reviste tanta importancia saber si un secreto, para su titular, constituye realmente una materia digna de reserva, como saber si, efectivamente, ese secreto es digno de protegerse jurídicamente porque sea merecedor de tal protección. Naturalmente, siempre será digno de protección un secreto que, para la persona titular, sea digno de ella, habida cuenta de que la lesión produciría un perjuicio en la intimidad de dicha persona, si bien esta protección ya no alcanzaría la vía penal, sino la civil.

44.2 Legitimación pasiva

Frente al derecho de las personas a conocer su inclusión en bancos de datos o cualquier archivo, se encuentra el derecho de los administradores o titulares de ellos, sean públicos o privados.

> Palazzi diferencia según se trate uno u otro registro, responsabilizando al funcionario que está a cargo del mismo cuando sea público; y al representante legal cuando sea privado. Puede suceder que el mantenimiento del registro o base de datos esté a cargo de un tercero especializado -caso de empresas de computación-, que puede llevar a integrar la litis con éste para que la resolución final le sea válidamente oponible, sobre todo en el caso de registros desactualizados o erróneos que hayan causado algún perjuicio económico o moral".

Cada modalidad de habeas data reconoce variables en los legitimados pasivos correspondientes.

La ley ha establecido en el artículo 35 (Legitimación pasiva): *"La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes"*

La jurisprudencia reunida al presente nos muestra que no existe un "derecho del titular de bs registros", salvo en lo referente a empresas periodísticas que están amparadas por la exclusión expresa del art. 43 Constitucional.

Hay un claro derecho de los registrados, pero está ausente en la legislación los problemas emergentes de la acumulación, tratamiento y distribución de los datos.

> Apuntan Altmark y Molina Quiroga que es muy factible que siguiendo una inveterada tradición de ocultismo, la administración pública esterilice este derecho de acceso y resista al "habeas data" invocando la necesidad de un actuar "manifiestamente" ilegal o arbitrario, que derivará a la apreciación discrecional del magistrado materias tan subjetivas como la "seguridad nacional", la "salud pública", etc. Nuestra opinión en este aspecto –concluyen- es que el derecho de acceso no puede ser retaceado bajo ningún concepto, ya que la norma constitucional no hace excepciones.

De este modo, liminarmente, podemos sostener que tienen legitimación pasiva todas las entidades públicas o privadas que compilen datos personales aunque no tengan finalidad comercial, pero siempre y cuando estén destinados a producir informes (aunque después no los circulen).

La condición para adquirir la calidad de sujeto pasivo depende de los datos almacenados y de la forma como se compilan. Una cosa es el archivo común que no tiene finalidades informativas, y otra muy distinta el registro ordenado y sistemático que tienen los bancos de datos.

La diferencia que la norma constitucional establece entre "registros públicos y privados destinados a proveer información" es simplista, aunque efectiva a los efectos de lograr alguna precisión respecto a saber a quienes se puede demandar.

Pero en los hechos, los registros públicos reconocen supuestos especiales, tales como los que menciona el artículo 23.

1. *Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquéllos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.*
2. *El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función del grado de fiabilidad.*
3. *Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.*

Inclusive, todos los ordenamientos jurídicos admiten la necesidad de establecer un cierto orden para clasificar los tipos de bancos de datos de acuerdo a la información que manejen y el destino que para ellos esté previsto.

Por ejemplo, la información sensible no se puede recolectar ni ser objeto de tratamiento, pero la iglesia católica, las asociaciones religiosas o las organizaciones políticas y sindicales pueden llevar un registro de sus miembros (art. 7 inciso 3º párr. final).

Lo mismo cabe decir de los hospitales y demás instituciones sanitarias, públicas o privadas, y los profesionales vinculados a la ciencia médica que pueden recolectar y tratar los datos personales relativos a la

salud física y mental de los pacientes que acudan a los mismos, o que estén o hubieren estado bajo tratamiento de aquéllos (art. 8).

Los archivos privados, que no sean de estricto uso particular, tienen el mismo problema de adaptación a las reglas constitucionales. Así se observa en aquellos servicios destinados a la información crediticia, los que tienen fines publicitarios o estadísticos, entre otros.

Por ejemplo, se ha dicho que *"los libros de comercio que posee un banco o entidad financiera no constituyen el supuesto constitucional de registros privados destinados a proveer informes"* (Cfr. CNCom., Sala D, mayo 13/996 *in re* "Figueroa Hnos S.A. c/ Banco de la provincia de Santiago del Estero". Sin embargo, otros fallos opinan que *"la vía del amparo informativo es el camino para ejercer la acción de habeas data a fin de que el Banco demandado corrija o suprima datos de sus registros y rectifique informes falsos que pudieran haberse proporcionado en su virtud"* (Superior Tribunal de Justicia de Entre Ríos, sala 1ª penal, setiembre 8/994, *in re* ".R.R.J.E., c/ Banco Francés del Río de la Plata, en El Derecho, 164-413).

La información crediticia también juega la misma incertidumbre, porqué siendo bancos destinados a proveer información, algunos requieren para la procedencia del habeas data que los datos circulados sean falsos, erróneos, inexactos o discriminatorios, pues de otro modo, el archivo sólo cumple con la finalidad para la cual ha sido creado.

> Entre muchos más que se desarrollan en capítulos siguientes, la jurisprudencia ha sostenido que "no vulnera principios de intimidad el informe dado por una organización que proporciona información a las entidades que lo requieran sobre posibles clientes, en tanto éstos se limitan a datos personales y juicios pendientes, no siendo ellos datos secretos ni confidenciales" (Cfr. C.Civ. y Com. San Isidro, Sala 1ª , junio 21/996, *in re* "Depaolini, Angela M. c/ Organización Veraz S.A., en Rev. La Ley Buenos Aires, 1996-1082)

Ahora bien, la jurisprudencia de la Corte Suprema de Justicia de la nación argentina ha sido más generosa al permitir extender la acción de habeas data a los archivos obrantes en organismos o fuerzas de seguridad, tal como ocurrió en los casos "Urteaga" y "Ganora".

En síntesis, la calidad de sujeto pasivo del habeas data, con legitimación suficiente para actuar, solamente se obtiene del tipo de información que almacenan y del destino previsto para ellos.

Cuando la información no tiene fines informativos, la calidad procesal se difumina, aunque en todos los casos se deben resguardar el derecho de acceso para tomar conocimiento de los datos que a las personas interesadas concierne.

44.3 Los herederos y causahabientes

El problema de admitir la posibilidad de transmisión del derecho a proteger los datos personales de la persona fallecida, depende del criterio que se adopte para interpretar la vida privada tras la muerte de alguien.

De igual modo, si la tutela sobre la intimidad se establece como un derecho personalísimo, existirá la misma dificultad para admitir la demanda a través de una persona causahabiente.

> Para Estadella Yuste, *a priori* la respuesta debe ser negativa ya que no existe un derecho a la vida privada después de la muerte. Sin embargo, el caso es importante respecto a datos de carácter médico relativos a enfermedades hereditarias. Aunque en estos casos el argumento a favor del acceso por terceras personas es conveniente, porque el uso incorrecto de la información podría perjudicar la memoria o buen nombre del difunto.

El caso es que la protección reglamentaria admite la representación del derecho a través de los sucesores universales (v.gr.: arts. 14 inciso 4º y 34), lo cual no obsta a que se plantee la legitimidad de tal reconocimiento.

En realidad, el problema de la legitimación activa en los herederos no se puede analizar como si fuera una cuestión de resguardo a la vida privada del difunto, sino para observar cuales son los derechos *intuito personae* que tienen los sucesores universales.

> Bidart Campos explica que los muertos no prolongan los derechos que titularizaron en vida, ni siquiera como subsistentes en la memoria de sus deudos; los derechos de éstos podrán estar concatenados a los que fueron de la persona fallecida, pero serán derechos de quienes siguen viviendo, que se les reconocen en virtud del vínculo parental con el difunto.

En efecto, el derecho de acceso es un derecho a estar informado. Es una garantía que no se puede limitar, pues para establecer presupuestos y condiciones están las modalidades que el habeas data plantea.

De todas maneras, cada pretensión de control sobre los bancos de datos (actualización, corrección, supresión o confidencialidad) permite extender la petición respectiva hacia otros campos de tutela, sin que ello signifique afectar el derecho subjetivo de quien fuera titular. Es decir, si los herederos plantean el acceso a los archivos y practicado verifican que los datos contenidos afectan la dignidad, el honor o la imagen del difunto, la pretensión que ellos deduzcan se podrá encarrilar por el habeas data si es la vía idónea. Mientras que una demanda indemnizatoria, una reparación moral, un desagravio a la reputación o fama de la persona fallecida no se fundamenta en este proceso constitucional.

En este sentido, nuestra ley sustancial divide los caminos para la defensa de la intimidad, el honor y la imagen, evitando que se transite por el habeas data. Este, por su parte se rige por los cánones que marca el artículo 43 constitucional (acceso y control sobre los archivos) y la jurisprudencia que lo interpreta, merced a la omisión legal incurrida al respecto.

> Por eso en la causa Urteaga se permitió que los parientes de un desaparecido, presuntamente muerto en las acciones militares sucedidas después de la revolución del 24 de marzo de 1976, pudieran demandar desde el habeas data, el conocimiento y la información que dispusieran los archivos militares sobre la citada persona.
>
> Comparte Bazán el fallo, agregando que el mismo resulta totalmente compatible con el derecho a la autodeterminación informativa que postula como bien protegible por medio del habeas data, pues el espectro de cobertura de aquel derecho incluye la posibilidad de conocer qué tipo de información (en este caso, perteneciente al hermano presuntamente fallecido del peticionario) existe en los archivos o bancos de datos (estatales, en este caso), para luego decidir someterla a un manto de confidencialidad o, a la inversa, hacerla pública.

44.4 La representación y el mandato

La cuestión no es baladí porqué hay que recordar que la protección de los datos personales se concreta por etapas: una extrajudicial y otra, eventual e hipotética, judicial (habeas data, propiamente dicho).

Si la idea que pervive es tutelar la intimidad y evitar intromisiones indeseadas en la vida privada de las personas, la delegación hacia otros para conocer la información concernida puede resultar en sí misma contradictorio, al habilitar un acceso más a lo que se pretende conservar secreto o confidencial.

En nuestro parecer, el primer reclamo debe ser hecho por la persona afectada o que ostente un interés legítimo para ingresar al registro informativo, pudiendo discernir, en situaciones excepcionales –caso de incapacidad física o legal, impedimentos manifiestos, minoría de edad- la representación a un tercero. Este, a su vez, consigue legitimación por mandato, pero el acceso sólo podrá acordarse cuando actúe en interés y beneficio del afectado, y no para la satisfacción de intereses de terceros –padres, tutor, entre otros-.

> Esta es la conclusión de Estadella Yuste, quien agrega otro supuesto relacionado con la transferibilidad del título cuando un tercero pretende acceder al fichero en favor de una persona que jurídica y físicamente es capaz, pero que por circunstancias especiales no puede ejercerlo. En este caso tampoco parecen existir disposiciones normativas que impidan el derecho de acceso a través de mandatario autorizado; no obstante siempre habrá que considerar lo previsto en las jurisdicciones nacionales, las cuales pueden determinar ciertas excepciones.

En cambio, el acceso a la justicia requiere y exige patrocinio letrado, circunstancia que no cambia en los procesos constitucionales. Por eso, el planteo de habeas data supone, necesariamente, la deducción por abogado, calidad que cubre el recaudo de la representación legal.

> Dice Velázquez Bautista que una situación diferente es aquella en la que el ordenamiento jurídico admite la posibilidad de actuar en nombre de otro, y ejercer el derecho de acceso mediante mandato, es decir, en nombre y por cuenta su titular. Ocasión en la que no se plantea que el titular se desprenda del derecho, sino, como tal, autoriza a otro para que acceda en su nombre. Esta opción debe establecerse con especial cuidado, especificando siempre quiénes son los que pueden actuar en este sentido. La primera cuestión que habría que plantear con respecto a lo anterior es en qué casos se podría proponer, así como quien, apoderado por el titular, en su nombre, accedería de forma efectiva a los datos. Esto podría contemplarse con ocasión de una enfermedad que conlleve la inmovilización permanente del paciente, una declaración de incapacidad, la desaparición del sujeto mientras transcurre el plazo legal que permite se proceda a la declaración de fallecimiento, etc. Estarán legitimados para acceder, según los casos, el calificado como tutor, el profesional del derecho al que se otorga el correspondiente poder, el padre, madre, cónyuge o hijos del desaparecido.

44.5 El Defensor del Pueblo

El artículo 43 de la Constitución Nacional ha consagrado un sistema abierto para la legitimación en los procesos constitucionales. El marco dispuesto en el capítulo del derecho de amparo afirma desde el comienzo que "toda persona tiene derecho" y marca seguidamente las condiciones que reviste la amenaza o el acto lesivo para que dicha potestad pueda ser ejercida por el afectado, las entidades que propenden a la defensa de los derechos de incidencia colectiva y el Defensor del Pueblo.

El mismo temperamento inicia el párrafo correspondiente al "habeas data", *toda persona podrá interponer esta acción* dice la norma constitucional.

Ambos indicativos plantea la necesidad de esclarecer el alcance que tienen y determinar si guardan relación con el derecho que para el Ombudsman establece el artículo 86 del mismo orden fundamental cuando sostiene que *el Defensor del Pueblo tiene legitimación procesal.*

En otra publicación hemos dicho que este artículo 86 es un *mandato preventivo*, por el cual se propicia que los jueces, en el análisis de admisión de una demanda, priorice por sobre la acreditación del derecho subjetivo, la esencia fundamental de la tutela que se solicita.

> Agregamos que este enunciado, lejos de ser genérico, apunta a aspectos muy particulares que lleva a cabo el *ombudsman*, que se completa en el párrafo final del apartado, cuando menciona que tiene también en su cometido, *el control del ejercicio de las actividades administrativas públicas*

Con esta prevención, el Juez podría antes de dar trámite formal al acceso a la información contenida en el banco de datos, analizar el fundamento de la petición y medir la trascendencia que tiene, para resolver en el mérito que advierta la posibilidad de admitir el habeas data por persona distinta a quien tiene el derecho subjetivo.

También, es posible afirmar la legitimación del Defensor del Pueblo por su carácter representativo de los derechos del hombre, aun cuando no sea una acción popular en términos estrictos.

> Sostiene Quiroga Lavié que la facultad de accionar en representación de aquellas personas del pueblo cuyos derechos hubieran sido lesionados por actos u omisiones de la administración y de las empresas privadas prestadoras de servicios públicos, proviene de la triple categoría de actos por los cuales se llega a la instancia judicial, es decir, el acto u omisión ilegítimo, el acto discriminatorio o el que sea propio de la protección del usuario o consumidor.

La ley argentina dispone la intervención del Defensor del Pueblo “en forma coadyuvante”, de manera que la figura procesal es la del tercero adhesivo simple, porque carece de legitimación propia pero tiene y justifica plenamente un interés para la intervención.

La ley española ha previsto que la intervención del Defensor del Pueblo sea factible en el marco de sus facultades reglamentarias, aun cuando la Agencia de Protección de Datos debe comunicarle las actuaciones que promueva en defensa de la persona afectada por el tratamiento de sus datos.

Ahora bien, ¿es posible que el Defensor del Pueblo demande por habeas data el acceso a un banco de datos, y en su caso, la actualización, corrección, supresión o confidencialidad de aquella información que tiene un profundo contenido personal? La vida privada de las personas afectada por las agresiones informáticas ¿puede ser resuelta por un organismo que, en líneas generales, asume la representación de la colectividad cuando el derecho individual es débil o indefenso? ¿No es acaso el habeas data un proceso constitucional autónomo que se nutre de la autonomía de la voluntad particular de quien se considera afectado? Finalmente, la tutela de los datos personales ¿puede ser ejercida como un amparo colectivo?.

Cada uno de estos interrogantes considera el problema de la representatividad del derecho, pero no atiende la compleja situación que produce la amenaza tecnológica, el impacto informático en la vida privada y la necesidad de prevenir el riesgo y resolver el daño, a partir de una acción decidida por quien debe restablecer el equilibrio de fuerzas entre el hombre y su circunstancia.

Teniendo en cuenta ello, el oficio del Defensor del Pueblo, antes que reparador ha de ser preventivo, sin que una acción impida la otra, pero dando preferencia a la primera.

> Un ejemplo de nuestra situación se puede confrontar con España antes de tener una ley de tratamiento de datos. Allí el Defensor del Pueblo señaló en sus informes de 1990 y 1992, la especial importancia del control efectivo de las bases de datos en lo que se refiere al ámbito jurídico, por cuanto en el de las Administraciones Públicas directamente y organismos o entes de ellos dependientes, tiene yá prevista la intervención del ombudsman. Agregando tiempo después que los datos de carácter personal utilizados por las Fuerzas y Cuerpos de Seguridad del Estado deben estar controlados, tanto como aquellos que mantienen las empresas de seguridad privada.

El derecho de autodeterminación informativa puede resultar contradictorio si se interpreta en sus términos, pues daría a entender que sólo la persona afectada por el tratamiento de sus datos puede decidir la protección de ellos en cualquiera de las acciones disponibles.

Pero es posible colegir en este derecho, la necesidad de mantener permanentemente vigilados los archivos públicos y privados que trabajan sobre datos individuales de las personas, lo cual se puede hacer por un organismo especialmente creado al efecto, y en conjunto con el Defensor del Pueblo.

Europa advierte la necesidad de consagrar la defensa efectiva de la intimidad y de la denominada libertad informática creando para ello un “Defensor del Pueblo de los Datos Personales” *, que se argumenta y sostiene en los artículos 21 y 195 del Tratado constitutivo de la Comunidad Europea, el artículo 20 D del Tratado de la Comunidad Europea del Carbón y del Acero, el artículo 107 D del Tratado formativo de la Comunidad Europea de la Energía Atómica y en el artículo 286 del Tratado constitutivo de la Comunidad Europea, en el que se establece que los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el Tratado o sobre la base del mismo.

De igual modo, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre 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 abunda en los fundamentos de su creación.

> El 30 de noviembre de 1999, se estableció como considerandos de la resolución, que el nombramiento de un funcionario encargado de la protección de datos en el seno de la Oficina del Defensor del Pueblo europeo puede contribuir a la promoción de los derechos y las libertades de los interesados objeto de operaciones de tratamiento de datos efectuadas por el Defensor del Pueblo

europeo; indicando el artículo segundo las funciones del encargado de la protección de datos:

- Crear y mantener un registro público de las actividades en materia de tratamiento de datos llevadas a cabo en la Oficina del Defensor del Pueblo europeo.
- Supervisar las actividades en materia de tratamiento de datos llevadas a cabo en la Oficina del Defensor del Pueblo europeo.
- Presentar al Defensor del Pueblo europeo una declaración de garantía anual relativa al cumplimiento por parte de la Oficina de las disposiciones comunitarias relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

La presente Decisión entró en vigor el 1º de enero de 2000.

44.6 Las personas jurídicas

La calidad de sujeto activo en el habeas data no resulta exclusivo de las personas físicas; el mismo derecho acreditan las personas jurídicas.

La conclusión no se basa únicamente en cuestiones normativas que, por sí mismas, son contradictorias y ambivalentes; mientras algunas –como la ley argentina- receptan la protección a los entes ideales, otras –especialmente las leyes europeas- esquivan la tutela argumentando que se trata de un derecho personalísimo que no pueden sostener las empresas o corporaciones.

Cualquiera de los derechos emergentes del artículo 43 pueden entablarse por las personas jurídicas, no sólo por la captación que se pueda hacer desde quienes interpretan al habeas data como un modismo de amparo, en cuyo caso, sería indiscutible que la amenaza o la lesión constitucional atiende al derecho conculcado antes que al tipo de persona que reclama (salvando la calidad de afectado); sino también, por las particularidades que tiene el derecho a la información (acceso a los bancos de datos) y el derecho a efectuar un control activo sobre quienes registran datos personales con la finalidad de producir informes a terceros.

> En España se ha dicho que, aunque es cierto que el derecho al honor reconocido como fundamental en el art. 18.1 de la Constitución Española, deriva de la dignidad humana del art. 10.1 y consecuentemente presenta, en su concepción estricta, un innegable carácter personalista, ello no excluye la extensión de su garantía constitucional a las personas jurídicas y, en concreto, a las sociedades mercantiles…Agrega después que, admitido que el prestigio profesional de la persona física es objeto de protección, no existe razón para excluir de la misma el prestigio de la sociedad mercantil en el desenvolvimiento de sus actividades pues, si bien en cuanto al honor afecta a la propia estimación de la persona de carácter inmanente, sería difícil atribuirlo a la persona jurídica societaria, no ofrece grave inconveniencia entender que, en su aspecto trascendente o exterior, que se identifica con el reconocimiento por los demás de la propia dignidad, es igualmente propio de aquellas personas jurídicas que pueden gozar de una consideración pública protegible (TS, sentencia del 23 de marzo de 1987, en La Ley, 1992-3, 666).

En cuanto a lo primero, el acceso se garantiza a toda persona física o moral interesada, a quien el dato concreto registrado por un archivo público o privado, afecta en sus derechos subjetivos, intereses legítimos o de pertenencia colectiva.

La norma constitucional es clara: "*Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad…*", disposición que no excluye la aplicación de otros artículos de la ley fundamental que abarca en el concepto de *personas* a las entidades ideales (arts. 15, 22 y 23).

> Bidart Campos, refiriéndose a la legitimación activa en el habeas data sostiene que debe quedar en claro que la promoción del proceso queda reservada, en forma estrictamente personal, al sujeto a quien se refieren los datos archivados en el banco de que se trate, siendo el único investido de legitimación procesal activa. Con esta severa restricción, creemos –agrega- que la legitimación pertenece no sólo a las personas físicas, sino también a las entidades colectivas, asociaciones, organizaciones, etc., en la medida en que, por igualdad con aquellas, tengan datos registrados en los bancos públicos o privados.

En consecuencia, quien promueve un habeas data, primero debe lograr el acceso a los registros del caso, para después plantear las acciones de control efectivo que contra el mismo quiera deducir.

Estas pretensiones son objetivas y el grado de afectación perturba por igual a personas físicas y morales. Si el registro es inexacto, la fidelidad de la información altera la identidad y la verdad objetiva que trasciende al dato almacenado. Si la información está desactualizada, cualquier afectado tiene derecho a que los datos transferidos que le conciernen sean actuales y concretos, y no especulaciones ni perfiles logrados tras el tratamiento. Si el archivo conserva datos secretos o confidenciales de la persona, ésta –sin importar su cualidad física o jurídica- tiene derecho a plantear la reserva o supresión.

En suma, el tratamiento de datos personales es el control efectivo que la norma constitucional quiere asegurar y, por ello, cuando se informa que *toda persona tiene derecho*, se está diciendo que cualquiera sea el afectado existe un derecho a conocer y rechazar las informaciones y los razonamientos usados en los sistemas de almacenamiento cuyos resultados la perjudiquen; como para lograr una vía directa para rectificar, completar, esclarecer, poner al día, eliminar o requerir la confidencialidad y secreto de los datos que han sido recolectados.

La única duda posible se puede centrar en los llamados "*datos sensibles*", en la medida que éstos se acoten a la reserva íntima de la persona física por representar la vida privada, o sus ideas políticas, religiosas o gremiales.

En este caso, la condición de "derechos personalísimos" puede fundamentar la exclusión y así debiera ser; pero el caso es que alguna jurisprudencia tiende a instalar en este espacio a la información de carácter comercial, oponiéndola a la "información sensible" y resolver, entonces, cuál puede circular y cual no lo puede hacer.

> "La información de carácter comercial o financiero, al contrario de lo que sucede con la *información sensible*, está destinada a divulgarse entre todas las entidades financieras del país, tal como lo prevé la Circular OPASI 2 del Banco Central de la República Argentina" (CNContencioso-administrativa, Sala 4ª, setiembre 5/995, *in re* "Farrel Desmond A. c/ B.C.R.A. y otros s/ amparo", en Jurisprudencia Argentina 1995-IV, 350).

Bibliografía Capítulo XI

Altmark, Daniel R. – Molina Quiroga, Eduardo, *Régimen jurídico de los bancos de datos*, en Informática y Derecho, volumen 6, editorial Depalma, Buenos Aires, 2.000.

Bazán, Víctor, *El habeas data y sus particularidades frente al amparo*, en Revista de Derecho Procesal nº 4, editorial Rubinzal Culzoni, Buenos Aires, 2.000.

Bianchi, Alberto B., *Habeas data y derecho a la privacidad*, publicado en El Derecho, tomo 161 págs. 866 y ss.

Bidart Campos, Germán J., *Tratado elemental de derecho constitucional argentino*, tomo VI, editorial Ediar, Buenos Aires, 1995.

Bidart Campos, Germán J., *¿Habeas data o qué? ¿Derecho a la verdad o qué?*, en suplemento de Derecho Constitucional, Revista La Ley, del 15 de febrero de 1.999, págs. 21 y ss.

Cifuentes, Santos, *Protección inmediata de los datos privados de la persona. Habeas data operativo*. Revista La Ley del 15/11/95.

Dalla Vía, Alberto R., - Basterra, Marcela Izascum, *Habeas data y otras garantías constitucionales*, editorial Némesis, Buenos Aires, 1999.

De Slavin, Diana, *Mercosur: La protección de los datos personales*, editorial Depalma, Buenos Aires, 1999.

Ekmekdjian, Miguél Angel – Pizzolo, Calógero, *Habeas data. El derecho a la intimidad frente a la revolución informática*, editorial Depalma, Buenos Aires, 1996.

Estadella Yuste, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales*, editorial Tecnos, Madrid, 1995.

Falcón, Enrique M., *Habeas data*, editorial Abeledo Perrot, Buenos Aires, 1996.

García Belaúnde, Domingo, *El Habeas data y su configuración normativa (con algunas referencias a la Constitución peruana de 1993)*, en Liber Amicorun Héctor Fix Zamudio, volumen I, editorial Secretaría de la Corte Interamericana de Derechos Humanos, San José de Costa Rica, 1998.

Gozaíni, Osvaldo Alfredo, *Derecho de Amparo, 2ª edición*, editorial Depalma, Buenos Aires, 1998.

Gozaíni, Osvaldo Alfredo, *Formas alternativas para la resolución de conflictos*, editorial Depalma, Buenos Aires, 1995.

Gozaíni, Osvaldo Alfredo, *La legitimación en el proceso civil*, editorial Ediar, Buenos Aires, 1996.

Gozaíni, Osvaldo Alfredo, *Mediación y reforma procesal*, editorial Ediar, Buenos Aires, 1996.

Palazzi, Pablo, *El habeas data en la Constitución Nacional (La protección de la privacidad en la "era de la información")*, en Jurisprudencia Argentina del 20 de diciembre de 1995.

Puccinelli, Oscar Raúl, *El Habeas data en Indoiberoamérica*, en *El Amparo Constitucional, perspectivas y modalidades*, editorial Depalma, Buenos Aires, 1999.

Quintano Ripollés, Antonio, *Tratado de la parte especial de derecho penal*, editorial Madrid, 1972.

Quiroga Lavié, Humberto, *El amparo colectivo*, editorial Rubinzal Culzoni, Buenos Aires, 1998.

Romero Coloma, Aurelia María, *Los derechos al honor y a la intimidad frente a la libertad de expresión e información. Problemática procesal*, editorial Serlipost, Barcelona, 1991.

Velázquez Bautista, Rafael, *Protección jurídica de datos personales automatizados*, editorial Colex, Madrid, 1993.

CAPÍTULO XII. El procedimiento en el habeas data

45. Pretensiones posibles

El esquema siguiente se analiza de acuerdo con la experiencia aportada por el derecho comparado y la ley que reglamenta el artículo 43 constitucional en la parte que al habeas data corresponde.

Para confrontar el encuadre con las dificultades actuales será necesario ir al capítulo siguiente, toda vez que la configuración jurisprudencial reconocida al presente sostiene la misma incertidumbre que tuvo el amparo, de modo tal que se confunde la naturaleza del acto lesivo, el concepto de "acto discriminatorio", la condición de vía directa o subsidiaria, entre muchos conflictos más que después se analizarán.

45.1 Petición extracontenciosa [*]

Las leyes de tratamiento de datos personales suelen diferenciar las peticiones de quienes se encuentran alertados (es decir, previamente informados del almacenamiento) sobre el registro que los archivos practican y el destino que acuerdan a la información que recaban; respecto a otros que persiguen acceder a los bancos de datos para saber si están en ellos y, en su caso, obrar en alguna de las direcciones posibles de control.

El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes (cfr. Art. 14.1).

Esta primera presentación se sostiene en el derecho de información que tiene "toda persona", con la amplitud que admite la Constitución Nacional en materia de legitimación. La consulta es gratuita e informal (art. 13).

La etapa extracontenciosa tiene modalidades distintas para hacerla efectiva. Puede ser a través del *acceso directo* a las fuentes de información almacenada, sin que resulte necesaria la intervención del titular o usuario del archivo; o *indirecta*, cuando se intima por medio fehaciente para que se produzca la información.

> "*Vencido el plazo* –10 días corridos desde la intimación- *sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de habeas data prevista en la ley*" (art. 14.2).

La petición se concreta con la simple presentación al organismo consultado (público o privado), y completando un formulario de acceso a la información se cumple con la formalidad mínima prevista para autorizar el ingreso.

> En ocasiones, se admite agregar documentación que respalda otras peticiones conexas con los datos archivados, en miras a su actualización o rectificación.

Cuando la pretensión sea de rectificación, actualización, confidencialidad o planteo de supresión fundado, el acceso al registro de datos personales debe ser igualmente facilitado por los prestadores del servicio, y en su caso, como indica la norma antes mencionada: *"..el responsable o usuario del banco de datos debe proceder a {ello}, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido del error o falsedad"*.

Una vez más, el incumplimiento o la denegatoria, habilitan la instancia judicial inmediatamente.

El procedimiento, en todos los supuestos, es breve y sencillo: se concreta la pretensión ante el archivo y el titular o usuario responsable debe responder con la mayor brevedad. La negativa o la

[*] Ver parágrafo 34.3 y subsiguientes, para complementar esta información.

insuficiencia habilitan la instancia judicial sin que ello suponga un trámite condicional, aunque resulte conveniente y aconsejable.

> "El presupuesto fáctico y jurídico del habeas data debe ser la sencilla acreditación objetiva, pues la hipotética complejidad de las cuestiones a interpretar podría atentar contra la *ratio juris* del instituto" (C.Contencioso-administrativa Córdoba, Sala 1ª, marzo 29/995 *in re* García de Llanos, Isabel c/ Caja de Jubilaciones, Pensiones y Retiros de Córdoba, en Rev. La Ley Córdoba, 1995-948 con nota de Oscar A. Bayo).
>
> Asimismo se ha dicho que "si el objeto de la acción de habeas data es tener acceso a la información relativa al peticionante, no es imprescindible el reclamo administrativo previo" (C.Fed. Bahía Blanca, Sala 1ª, diciembre 30/994, *in re* Gutierrez Héctor c/ Casino Militar del Personal Superior de la Base Naval Puerto Belgrano, en Rev. La Ley 1996-A, 314).

45.2 Demanda judicial. Daño moral

La etapa informativa o extrajudicial no condiciona la vía jurisdiccional. Tampoco la congruencia entre lo pedido fuera del proceso y la demanda en el proceso se vinculan necesariamente. El hilo conductor está entre aquello que debió ser propuesto al archivo para reconocer la información que concierne a una persona, y los datos que se advierten inexactos o sensibles y, por tanto, son posibles de plantear directamente como acción contenciosa. En el primer caso, el reclamo administrativo parece más recomendable que argüir una demanda; mientras que ésta es la pretensión precisa cuando no hubo instancias previas de acuerdo o solución.

> Dice Falcón que, no obstante los contenidos de la petición inicial no limitan la segunda petición a la luz del informe presentado; la primera etapa del procedimiento entonces será de naturaleza informativa y voluntaria, la segunda podrá tener el carácter de contenciosa. En el procedimiento nacional y los que siguen su línea, resultan debidamente adecuados para la primera parte los trámites previstos en la ley 16.986 para el informe y los del Código Procesal Civil y Comercial del proceso sumarísimo (art. 498), para la etapa de conocimiento y ejecución, aplicándose la combinación de ambos tanto al requerimiento al Estado como a los particulares.

Las formas a seguir se guían por los principios generales que sostiene la "legalidad instrumental", el cual se puede adaptar en las categorías o tipos de procedimiento que se establezcan para el habeas data. No olvidemos que hay legislaciones que liberalizan las solemnidades en los procesos constitucionales, dando un tipo abierto donde basta con enunciar el objeto material que se peticiona y la relación procesal que con ella se tiene (interés jurídico); hasta los que pretenden encontrar una auténtica demanda contenciosa y encolumnan la fisonomía en las reglas tradicionales de la demanda (requisitos objetivos y subjetivos). En el medio se encuentran aquellos que apegan las formas a un proceso similar, como es el caso de las reglas del "habeas corpus" aplicadas al "habeas data", o los que regulan el sistema de admisión por el Código de procedimientos en lo penal, como es el caso de algunas provincias argentinas.

> El Código Procesal Constitucional de la provincia de Tucumán aplica las reglas del amparo (porqué considera al habeas data como un amparo especial) y dice: "*La acción de amparo se interpone por cualquier medio de comunicación escrito, por telegrama o carta documento y debe contener: 1. El nombre, apellido, nacionalidad y domicilio real y constituido y, en su caso, del accionante o personería invocada suficientemente justificada; 2. La individualización, en lo posible, del autor del acto u omisión impugnados o de quien hubiere ordenado la restricción; 3. La relación circunstanciada, con la mayor claridad posible, de los hechos, actos u omisiones que han producido o que estén en vías de producir la lesión que motiva el amparo; 4. La petición formulada en términos claros y precisos.*

La demanda debe interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario. En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen (cfr. Art. 38.1).

Cada pretensión exige un fundamento distinto, porqué haber denegado el acceso supone no conocer los datos personales que eventualmente se han almacenado en el archivo demandado; mientras que la inexactitud requiere prueba del error; la falsedad informativa debe indicar en qué consiste y cómo se quiere demostrar; el dato cuya supresión se formula plantea la verificación de su procedencia (teniendo en cuenta que *"la supresión no procede cuando pudiese causar perjuicios a derechos e intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos"* –art. 16.5 ley reglamentaria) y la confidencialidad debe ser justificada.

Asimismo, encontrándose prevista la posibilidad de plantear el daño moral por el archivo infidente que perturba la intimidad o la vida privada personal, también la motivación debe ser desenvuelta suficientemente.

En este sentido el marco procesal puede seguir la fisonomía de la acción privada específica tutelada por el Código Civil (o penal, en su caso), o plantearla ante el organismo de control de los archivos de datos personales.

El derecho de indemnización en el marco del proceso constitucional parece desajustado con las características de la pretensión y la necesidad de asegurar un debate amplio sin restricciones para el conocimiento judicial.

Una cosa puede ser el derecho a lograr un resarcimiento porqué el archivo o banco de datos produce informaciones inexactas o hace públicos datos que pertenecen a la esfera de la intimidad personal o a la vida privada del afectado, supuestos donde se puede aceptar la acumulación de pretensiones en el habeas data; respecto al daño moral planteado como daño derivado del hecho ilícito.

La demanda, en síntesis, debe reunir mínimamente: a) nombre, apellido y domicilio –real y constituido- de la persona que reclama; b) individualización del archivo público o privado, indicando su domicilio; c) la relación circunstanciada de los hechos que fundan la pretensión, de acuerdo con el motivo que motiva el planteo (acceso o control); d) la pretensión claramente expuesta (acceso, actualización, supresión, confidencialidad, etc.); e) la petición términos claros y positivos.

a) *¿Se puede reclamar daño moral?*

La posibilidad de demandar el daño moral en los carriles del habeas data es motivo de planteos disímiles; mientras algunos sostienen que es inadmisible por la especificidad que supone, además del carácter objetivo y reparador de la pretensión; otros argumentan que el daño emergente por la intromisión indebida en la privacidad de las personas se puede incluir entre las cuestiones que el proceso constitucional debe tutelar.

> Según Herrán Ortiz, una primera consideración, ante el constatable silencio legal, podría conducir a la negación de esta posibilidad, y ello precisamente porque el legislador nada ha dispuesto y de haberlo querido lo hubiera previsto. Lo cierto es que parece ser el único argumento en que puede ampararse la denegación de la indemnización del daño moral no necesita de norma alguna que lo establezca expresamente. Además, si se excluyera el daño moral, poco sería lo que deba indemnizarse en el ámbito de esta ley, cuando la norma se orienta a la protección de los derechos y libertades fundamentales, porque entonces lo que habrá que indemnizar será el lucro o beneficio económico obtenido por quienes han utilizado los datos ilícitamente, circunstancia ésta que no siempre existirá.

El código civil argentino adopta como criterio rector el de reparar económicamente los perjuicios sufridos a consecuencia del incumplimiento contractual y extracontractual.

Los bancos de datos tienen deberes y obligaciones hacia las personas que concierne en el proceso de almacenamiento con fines diversos. Especialmente, el deber de confidencialidad hace incurrir en responsabilidad a quien difunde un dato secreto. Esta responsabilidad tiene origen contractual.

Pero existe otra perspectiva para la cuestión de responsabilizar por el uso de los datos personales. Se trata de analizar si la actividad de las bases de datos es una actividad riesgosa, lo que implica una aptitud especial para generar en sus actos daños de índole diversa (contractuales, extracontractuales, a bienes, a personas, etc.).

> En la doctrina italiana –apuntan Altmark y Molina Quiroga-, refiriéndose a la actividad vinculada con el software, y al art. 2050 del código italiano, se ha señalado que la jurisprudencia es bastante cauta en la aplicación de dicha regla, aun cuando ya es principio pacífico que actividades peligrosas no son sólo aquellas previstas como tales en el texto ordenado de leyes de seguridad pública o en otras leyes especiales. Existen actividades que si bien no presentan como característica típica el requisito de peligrosidad, pueden volverse peligrosas si se las desarrolla de cierto modo, mientras que no lo son cuando se las ejerce en forma o modo distinto.

De este modo, la tarea de almacenar datos no es peligrosa en sí misma, pero sí lo es cuando en esos archivos se almacenan datos pertenecientes a otros, consentido o no el proceso de guarda y recolección, y con ello se difunde a terceros una información que afecta la vida privada y otros valores sensibles de las personas.

> Para Altmark y Molina Quiroga esa tarea de compilación no es peligrosa por su naturaleza, pero se convierte en tal por la forma de su realización, cuando se utiliza tecnología informática. La natural propensión a producir daños, propia de la actividad en cuestión, es tal que los lleva a afirmar en su calificación en términos de peligrosidad.
>
> Asimismo, concluyen, en materia extracontractual, el fundamento de la responsabilidad reside en la circunstancia de considerar a la actividad informática destinada a la recolección, almacenamiento y recuperación de datos personales como una *actividad peligrosa* en sí misma, por el riesgo creado, consistente en el potencial uso indiscriminado de la información personal registrada en un banco de datos informatizado. La responsabilidad existe tanto cuando el daño (uso o difusión indebida de los datos personales contenidos en la base de datos) tiene origen en el hecho propio del gestor del banco de datos, como en el hecho de sus dependientes. Existe responsabilidad objetiva tanto cuando el banco de datos es de carácter público, como cuando es privado. El titular del banco para eximirse de responsabilidad, deberá probar el hecho de un tercero por quien no deba responder, o el hecho de un tercero por quien no deba responder, o el hecho de la misma víctima o el caso fortuito o fuerza mayor.

45.3 La demanda en la ley nacional

El artículo 38 de la ley, divide la pretensión en etapas ofreciendo un modelo anómalo que puede tener varias dificultades.

Dice la norma, en el inciso 2º: "*El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley*".

Sobre esta línea de actuación, en consecuencia, el actor debe: 1) solicitar el acceso a los bancos de datos, archivos o registros, indicando las causas por las cuales presume que en ellos se encuentra; 2) debe demostrar que ha cumplido la etapa de requerimiento extrajudicial; 3) ha de motivar adecuadamente sus consideraciones sobre la calidad de información falsa, inexacta o discriminatoria que alega contra los datos almacenados, y 4) en su caso, podrá plantear en forma subsidiaria o posterior, las pretensiones de supresión, rectificación, confidencialidad o actualización de sus datos personales.

El artículo 42 (ampliación de la demanda) establece que: *"Contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación,*

confidencialidad o actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el misma acto la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días".

En los términos presentados, la ley propone dividir las etapas procesales: a) una instancia administrativa, donde plantear el derecho de acceso y, en su caso, el reclamo de actualización, rectificación, supresión o confidencialidad; b) negado el acceso o estimado insuficiente la cobertura otorgada, se deduce la demanda ante el juez competente persiguiendo tomar conocimiento de los datos que a él se refieren y lograr saber la finalidad que tienen como destino; c) una vez que se ha evacuado el informe por el titular o usuario del archivo, se puede ampliar la demanda, concretando la pretensión (actualización, rectificación, supresión o confidencialidad).

46. Resolución judicial de admisibilidad. Medidas provisionales

Al quedar propuesta la demanda, el juez competente debe estudiar la procedencia formal y objetiva para resolver. Esto es, decidir si la acción es admisible en los carriles comenzados, rechazar *in limine* por carecer de fundamento o razonable proposición, o bien, ordenar medidas de saneamiento destinadas a expurgar vicios del acto de pedir que, hacia adelante, podrían llevar a nulidades del procedimiento.

> Indica Falcón que el juez debe examinar primeramente si la acción es admisible, pues puede rechazarla *in limine*. Si la considera admisible, el juez requerirá a la autoridad que corresponda o al particular, en su caso, un informe sobre la existencia y objeto del archivo, registro o banco de datos; todos los datos que tengan del actor; si le han sido requerido o emitido datos del mismo y, en su caso, a quién.

La pertinencia de la vía se confronta con el objeto solicitado y los medios procesales disponibles. Por ejemplo, se ha dicho que "*el habeas data no es el proceso apto para obtener una historia clínica por parte del sanatorio demandado que se niega a entregarla*" (cfr. CNCiv., Sala F, julio 6/995, en Rev. La Ley 1996-C, 473). O cuando se persigue obtener a través de este proceso constitucional el conocimiento de las causas judiciales criminales que pudiera tener una persona a fin de regularizar la situación de las mismas, que también es improcedente como se dijo en algún fallo local (cfr. Juzg. Nac. 1ª Instancia 19 secretaría 159, firme, del 23 de enero de 1995, en Jurisprudencia Argentina del 26/3/97 pág. 57). También es improcedente cuando se dirige contra un banco comercial que registra en sus libros de comercio información crediticia de sus clientes, toda vez que éstos no constituyen bancos de datos ni archivos personales destinados a proveer información a terceros (cfr. CNCom., Sala D, mayo 13/996, en Jurisprudencia Argentina del 26/3/97 pág. 51). Con simolar inteligencia se ha agregado que *"es improcedente la acción de habeas data intentada para corregir los asientos contables de un banco, pues éstos no constituyen registros o bancos de datos públicos de la entidad, aunque ésta sea de carácter público, sino que se trata de meros datos jurídicos y contables referidos a un contrato de derecho privado, en el que es parte la entidad y que no están destinados a su divulgación"* (cfr. CNCom., Sala A, octubre 4/996, *in re* Automotores Santa María c/ Banco de la Provincia de Santiago del Estero, en Jurisprudencia Argentina del 26/3/97 pág. 56).

El artículo 38.3 establece que: *"El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial"*, consiguiendo de este modo, alertar sobre el conflicto que produce la información almacenada en cuanto a la verdad o certeza de lo que ellos transmiten.

Seguidamente el inciso 4 dispone que: "*El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate"*, supuestos que aun establecidos legalmente guardan algunas dudas respecto a su probable decisión.

En efecto, cuando la medida provisional coincide con el objeto pretendido, la sentencia anticipatoria puede vulnerar el punto de equilibrio que el Juez debe resguardar en todo momento, aun en los procesos constitucionales, donde la bilateralidad no es estricta.

En alguna causa judicial, se ha recordado la jurisprudencia que establece la prohibición de establecer medidas cautelares coincidentes con el objeto del litigio, en la medida que con ellas se desvirtúa el instituto cautelar al convertírselo en un medio para arribar precozmente al resultado buscado por medio de la sentencia definitiva. En el caso objeto de la demanda, era suprimir información inexacta de un banco de datos, donde se dijo que *"el dictado de la medida innovativa tendiente a que se elimine cautelarmente de los registros la información tildada de inexacta no haría más que colocar a la actora en análoga situación a la que resultaría de una eventual sentencia favorable, obteniéndose así en los hechos una satisfacción anticipada de la pretensión de fondo, por lo que corresponde rechazar la medida cautelar*" (cfr. CNCom., Sala C, abril 24/996, *in re* Yusin S.A. c/ Organización Veraz S.A, en Jurisprudencia Argentina del 26/3/97 pág. 53).

De todos modos pareciera ineludible mantener la prohibición de innovar mientras dure la instancia judicial, como una forma de evitar la transferencia de los datos en controversia.

46.1 Resoluciones en caso de solicitar acceso *a los bancos de datos*

La pretensión de acceso o de conocimiento para lograr información sobre datos personales es el vehículo de más sencillo alcance y con menores limitaciones.

Uno de los primeros fallos tras la reforma constitucional aseguró que *"dentro de las garantías constitucionales introducidas por la reforma de 1994 se halla el habeas data como una variable del derecho a la intimidad, consagrado tradicionalmente en el artículo 19 de la Constitución Nacional, que otorga a toda persona el derecho de interponer acción de amparo para tomar conocimientos de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes y, en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos*" (cfr. CNCiv., Sala A, mayo 19/995 *in re* Rossetti Serra, Salvador c/ Dun & Bradstreet SRL, en Jurisprudencia Argentina, 1995-IV, 355).

Dado que la protección de los derechos individuales en el sistema previsto para la defensa de los datos personales comprende la preservación de la vida privada y el derecho a ser informado de los datos registrados acerca de las personas, quedó establecido que entre los derechos del acceso a la justicia sin restricciones que modela el sistema garantista introducido se encuentra el habeas data infomativo.

Por ello, este derecho se divide en una etapa abierta que no tiene requisitos formales o sustanciales absolutos, y en otra de control donde se debe acreditar la relación jurídica y el derecho a la pretensión planteada.

Es decir, conforme a lo dispuesto en el artículo 43, el objeto del habeas data es que la persona afectada tome conocimiento de los datos a ella referidos, y de su finalidad, que consten en los registros o bancos de datos públicos o privados, y en caso de falsedad o discriminación, exigir la supresión, rectificación, confidencialidad o actualización (cfr. C.Civ. y Comer. San Isidro, Sala 1ª, junio 21/996 *in re* Depaolini, Angela M. c/ Organización Veraz S.A., en Rev. La Ley Buenos Aires, 1996-1082).

> La legislación europea ha sido reacia a dar este derecho a las personas jurídicas porque la comunidad empresarial argumentaba que el derecho de acceso otorgaría la oportunidad a la competencia de tener información sobre otras entidades. Esta crítica estaba basada en la suposición de que el derecho de acceso se ejercía por la persona (física o moral) *in situ* donde se encontraba el fichero. Esta concepción sobre el contenido del derecho de acceso no sólo es errónea –dice Estadella Yuste-, sino también aventurada, ya que pone en peligro el derecho a la intimidad de terceras personas.

Por eso, simplificando la cuestión, el deber de resolver en el derecho de acceso ha de ser inmediato aunque se debe sustanciar el pedido, porque para el progreso del habeas data informativo no parece necesario que quien lo deduzca alegue la existencia de un gravamen o perjuicio, ya que la verdad integra el mundo jurídico y el peticionante puede promoverlo en resguardo de la simple verdad (cfr. CNCiv., Sala F, julio 7/995, *in re* Bianchi de Saenz, Delia A. c/ Sanatorio Greyton S.A., en ED, 165-255).

Por otra parte, el derecho de acceso a la información constituye una premisa para asegurar que los datos personales que se incorporan a un archivo respondan a los deberes y principios que los bancos de datos

deben asegurar, esto es: la justificación social, el consentimiento del afectado, la confidencialidad de ciertos datos, etc.

> Dice Molina Quiroga que la recolección de información de carácter personal debe estar sujeta a ciertos principios tales como la justificación social, información y limitación, que no funcionan necesariamente en relación a la falsedad o inexactitud. Este aspecto es contemplado por el principio de calidad o fidelidad de la información.

46.2 Resoluciones en caso de solicitar actualización *de los datos*

La actualización es una forma de control sobre los archivos. La Corte afirma que "*en la era de las computadoras el derecho a la intimidad ya no se puede reducir a excluir a los terceros de la zona de reserva, sino que se traduce en la facultad del sujeto de controlar la información personal que de él figura en los registros, archivos y bancos de datos…El derecho a la intimidad o privacidad, que se halla consagrado en forma genérica por el art. 19 de la Constitución Nacional y especificado respecto de alguno de sus aspectos en los arts. 18, 43 y 75 inciso 22 (los dos últimos según la reforma de 1994) de la Constitución, ha sido definido por la Corte como aquél que protege jurídicamente un ámbito de autonomía individual constituida por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física y, en suma, las acciones, hechos o datos que teniendo en cuenta las formas de vida aceptadas por la comunidad, están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significa un peligro real o potencial para la intimidad"* (cfr. CS, febrero 13/996, D.G.I. c/ Colegio Público de Abogados de la Capital Federal, en Jurisprudencia Argentina, 1996-II, 295).

Actualizar es poner al día un dato que de mantenerse en la base con la información lograda anteriormente se torna inexacto.

De suyo, cabe pensar que la promoción ante la justicia obedece a que el archivo público o privado ha denegado la puesta al día de la información, y que a consecuencia de ello, el interesado se considera afectado y amenazado en su derecho a la verdad.

Es este un derecho diferente a la rectificación o supresión que se refieren a datos equivocados, en la medida que el dato anterior es auténtico pero ha perdido actualidad.

> Se ha sostenido que "*si la acción entablada no es el habeas data consagrado en el párrafo tercero del artículo 43 de la Constitución Nacional, sino la vía más genérica del amparo, contemplada en el párrafo primero de dicho artículo, cabe considerar que no media el requisito de que el dato obrante en los registros de la demandada sea falso; sino que es suficiente que la información sea verdadera, pero se presente en forma incompleta o le falte la necesaria exactitud para evitar que cause perjuicio a la persona a la que se refiere" (*CNCom., Sala A, agosto 27/999, *in re* Vicari, Clemente s/ amparo)

Por eso, la petición debe acreditar los hechos nuevos y, eventualmente, demostrar la denegatoria del banco de datos a obrar en la actualización planteada.

Esta pretensión debe tener un interés jurídico suficiente, porqué la justicia no está para corregir errores formales que se basen, únicamente, en el deseo de estar registrado con datos actuales. Hay que recordar que es deber de los archivos mantener actualizada la información compilada y que la caducidad de ellos admite pretensiones por las cuales el actor indique los motivos por los que considera que la información le resulta discriminatoria, falsa o inexacta.

Ahora bien, ¿qué ocurre cuando el dato pierde actualidad en informaciones que no son determinantes para la transmisión de ellos a terceros?. El caso sería, por ejemplo, cuando una persona cambia su domicilio, obtiene una profesión, o modifica algún aspecto de su personalidad que, para los fines que se tomaron sus datos personales, no incide ni afecta el destino de la transmisión a cumplir. En estos casos suponemos que la acción judicial es improcedente por resultar improponible aquellas pretensiones que no tienen gravamen alguno.

La Corte Nacional en la causa "Matimport S.A."* (marzo 9/999, en Doctrina Judicial, 2000-1, 25) declaró improcedente la acción de habeas data deducido con la única finalidad de suprimir del Registro de Juicios Universales datos atinentes al pedido de quiebra rechazado por el tribunal comercial, en razón de haber admitido ésta que tales datos se corresponden con las constancias del expediente judicial, pues no se cumple el presupuesto fáctico de la falsedad previsto en el art. 43 de la Constitución Nacional.

> Asimismo se sostuvo que "el asiento en el registro de juicios universales de la existencia de un pedido de quiebra, con la especificación de que fue rechazado por el tribunal comercial, no es discriminatorio por sí mismo, pues no implica juicio de valor alguno ni permite derivar de él la conclusión racional acerca de la situación patrimonial de la empresa requerida, no siendo la vía intentada la vía idónea para proporcionar protección (del voto del Dr. Petracchi)"

No obstante, existe otra variable que admite actualizar la información de la base de datos cuando existe un límite legal establecido para la conservación de la información y ella se encuentra vencida.

> "A los fines de establecer el límite temporal de conservación en los registros de un banco de datos de la información referida a una sanción administrativa de inhabilitación bancaria, cabe aplicar analógicamente el plazo de cinco años previsto en el artículo 51 inciso 3º del Código Penal, que es la norma que tiene mayor afinidad con la situación, pues se trata del límite para la conservación de los registros de condenas a penas de multa o inhabilitación" (CNCom., Sala A, agosto 27/999, *in re* Vicari, Clemente s/ amparo).

46.3 Resoluciones en caso de supresión de los datos

La cancelación del dato registrado se puede plantear por distintos motivos: a) cuando la información compilada oportunamente ha perdido la finalidad prevista; b) si los datos archivados son excesivos con relación al destino que portan; c) cuando la información es caduca u obsoleta y d) cuando contiene revelaciones que hieren la sensibilidad personal del concernido.

> Sostiene Herrán Ortiz que no parece coherente establecer la gratuidad del trámite cuando se pide la corrección del dato inexacto y no preverlo para la supresión. Esta idea no concilia con el principio de calidad de los datos, ni en general con el sistema de protección de datos personales, si la rectificación representa en sentido amplio una modificación de los datos, bien para ponerlos al día o completarlos, bien para corregirlos no puede interpretarse en sentido tan restrictivo dicho precepto, y además en perjuicio del afectado; por inexactos o incorrectos debe entenderse, por tanto aquellos datos obsoletos, erróneos o incompletos. Debe insistirse, quien se beneficia con la utilización de un fichero automatizado de datos personales penetra en una esfera privada del individuo, en la que serán constantes los roces con los derechos fundamentales de la persona, ahora bien, el ordenamiento jurídico permite dicha invasión siempre que se encuentren garantizados los derechos de la persona.

La cancelación pretende que no se aproveche el uso de datos portadores de una verdad que se debe mantener reservada en algunos casos o suprimida cuando no responde con la finalidad para la cual fueron archivados.

La anulación del dato requiere demostrar efectivamente el derecho a la cancelación, sin embargo ésta no procede cuando de ello pudieran derivar perjuicios a terceros interesados, o la información guardada se deba conservar por razones suficientemente fundadas. En uno u otro caso, es el juez quien deberá resolver interpretando cada hecho alegado.

El problema puede estar en la distinción que la Constitución establece entre archivos públicos y bancos de datos privados destinados a proveer informes. Mientras los primeros están sujetos a un deber permanente de actualización, a velar por la confidencia y asegurar el secreto de los datos sensibles, así como suprimir los datos que devienen innecesarios; los otros no tienen un control adecuado ni un régimen que los obligue a actuar por sí mismos.

Observemos cuál es la complejidad:

Los *bancos públicos* de datos exigen, para conocer la información que ellos mantienen, la acreditación de un interés legítimo o la orden judicial que disponga producir el informe respectivo.

> Un trabajo muy interesante de Antik y Ramunno muestra de que manera los registros públicos resultan abiertos facilitando el acceso, mientras los privados lo limitan. Por ejemplo, el decreto 2080/80 * establece que *"se presume que tienen interés legítimo, en conocer los asientos registrales, además de sus titulares: a) Los organismos del Estado Nacional, provincial y de las municipalidades; b) El poder judicial de la Nación y de las provincias; c) Los que ejerzan las profesiones de abogado, escribano, procurador, ingeniero o agrimensor; d) Los martilleros públicos, los gestores de asuntos judiciales y administrativos reconocidos como tales ante el Registro y las personas debidamente autorizadas por los profesionales mencionados en el inciso anterior"*

En cambio los *bancos privados destinados a proveer informes* se apegan a la función que realizan, evitando modificar sus archivos cuando quien lo plantea no demuestra la razón y fundamento de su pretensión.

El cuadro de Antik y Ramunno pone en evidencia las distancias:

	BANCOS PUBLICOS	/ BANCOS PRIVADOS
En relación al acceso a la información	Hay que acreditar un interés legítimo	No existe regulación, pero actualmente acceden tanto el titular del dato, como todos los interesados en una transacción o negocio con objeto lícito.
En relación a la vigencia o caducidad de los datos contenidos en sus bases	Los términos se encuentran expresamente establecidos (vgr.art. 86 y ss. dec. 2080 /80, regl. De la ley 17.801	No existe regulación, pero las empresas se han autoimpuesto el límite de diez años desde la finalización de los efectos del hecho originario.
En relación a la regulación	Todas tienen regulación específica.	No existe regulación específica.
En relación al control	Existe control jerárquico o de tutela según como se encuentre constituido el banco de datos.	No existe control de ningún tipo.
En relación a la responsabilidad	Existe responsabilidad extracontractual objetiva del Estado, del que se presume la solvencia.	A pesar de encontrarse inmersos, en caso de cometer errores que causen daños, en la teoría general de la responsabilidad, no se les exige para operar la constitución de fianza alguna que acredite solvencia.

Por ejemplo, la jurisprudencia sostiene que "si la información difundida por el banco de datos privado no es falsa sino que se trató de un hecho verdadero –la promoción de un juicio ejecutivo-, corresponde rechazar el pedido de supresión realizado con fundamento en el artículo 43 de la Constitución Nacional" (cfr. CNCom., Sala C, setiembre 6/996 *in re* Rodriguez, Rafael c/ Organización Veraz S.A.).

La hipótesis de falsedad o discriminación alegada no resulta viable cuando el dato que el registro transmite no es otro que el que recibe o toma de fuentes de información pública, como la "Central de Información Crediticia del Banco Central de la República Argentina", o del Poder Judicial de la Nación, o de los registros oficiales de bienes muebles o inmuebles. Además, si dicha comunicación no se divulga indiscriminadamente, o fuera del marco de confidencialidad que impone este tipo de información, no existen reparos que efectuar, sencillamente porque el banco de datos sólo está cumpliendo con su función de proveer informes.

> "Si no han existido informes contrarios al peticionante de la acción de habeas data que justifiquen un pedido de rectificación o modificación de dichos datos, la finalidad del instituto debe considerarse cumplida –en el caso, de los informes recabados a distintos organismos fue negativa la respuesta respecto de condenas penales o correccionales, así como causas penales, fiscales, previsionales, aduaneras, postales, administrativas o de otra índole contra el peticionante de la acción-" (Juzgado Nacional de 1ª instancia en lo contencioso administrativo nº 3, noviembre 2/995 *in re* Nallib Yabrán, Alfredo c/ Estado Nacional).

El *quid* de la información crediticia está en que no se califica como discriminatoria la actividad de suministrar información comercial, si son los terceros que hacen uso de ella los que en definitiva diferencian al informado que posea antecedentes negativos. Por eso, se ha dicho que "no existiendo disposición legal que fije un límite temporal para la actividad de brindar información comercial y crediticia, no puede admitirse la pretensión de que por vía judicial se limite el tiempo de almacenamiento y distribución de información que la empresa brinda por el servicio que se ha fijado" (cfr. CNCiv., Sala M, noviembre 28/995 *in re* Groppa c/ Organización Veraz S.A.).

En este aspecto, ya observamos porqué las pretensiones de supresión o confidencialidad en materia de información crediticia son más restringidas que en otros datos particulares.

El derecho que otorga la Constitución para exigir el secreto de los datos no se puede extender a todo tipo de información, en particular a aquélla de alcances comerciales o financieros, siempre y cuando ésta sea correcta.

Ahora bien, si el archivo registra datos obsoletos, la persona afectada puede plantear la supresión demostrando la causa de pedir.

> "El sujeto afectado tiene el derecho a lograr la supresión del dato obrante en un registro informatizado, cuando el dato sea impertinente para la finalidad perseguida por la base de datos o en el supuesto en que en función del transcurso del tiempo no resulte necesario mantener el dato en el registro. En virtud del tiempo transcurrido, los datos sobre inhabilitaciones para operar en cuenta corriente, producidos hace más de diez años se encuentran caducos y el accionante del habeas data tiene derecho a obtener su cancelación. La subsistencia del dato caduco indefinidamente en la base de datos de la demandada impide el derecho al olvido. El dato caduco es el dato que por efecto del transcurso del tiempo ha perdido virtualidad, ha devenido intrascendente a los efectos de cualquier efecto jurídico relativo a la ejecutabilidad" (cfr. Juzgado Nacional de 1ª instancia en lo civil nº 91, marzo 5/996 *in re* Falcionelli, Esteban c/ Organización Veraz S.A., ratificado por la CNCiv., Sala G, mayo 10/996)).

En esta hipótesis la calidad del dato archivado deviene inadecuada con el derecho al olvido que tiene toda persona para no mantenerse presa de su pasado.

Frente al conflicto, es razonable establecer un bloqueo provisorio de los datos evitando que ellos circulen mientras perdure la situación de incertidumbre sobre la permanencia en el archivo.

El art. 38.4 de la ley, ya comentado dice: *"El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate"*

> "En un juicio de habeas data cuyo objeto es la supresión de cierta información que se aduce ser inexacta, es procedente el dictado de una medida cautelar tendiente a que la demandada se abstenga de informar el dato en cuestión, pues de mantenerse la situación de hecho aparentemente irregular, la ejecución de una sentencia favorable puede convertirse en ineficaz, en tanto la difusión anterior a su dictado es susceptible de influir definitivamente, con perjuicio al derecho que se asegura, en el ánimo de quienes sabrían del dato en cuestión" (CNCom., Sala B, agosto 9/996, *in re* Yusin, Mauricio G. c/ Organización Veraz S.A.).
>
> Agrega Herrán Ortiz que el bloqueo de datos en el ámbito de la protección de datos personales en España, debe considerarse una modalidad o sistema de cancelación para aquellos supuestos en que siendo procedente ésta, no puede efectuarse por problemas de índole técnico o material. Sucede, sin embargo, que cuando se demuestre que los datos se recabaron o registraron de forma ilícita, desleal o fraudulenta la cancelación supondrá la destrucción de los mismos, y no su conservación en forma ilegible o inutilizable. Una diferencia que los separa de los otros derechos reconocidos a las personas es que en este supuesto quien decide o solicita el bloqueo no es el propio afectado, sino el responsable de los datos, y las garantías para el afectado se reducen incomprensiblemente, porque la decisión entre destruir o bloquear corresponde al responsable del fichero.

46.4 Resoluciones en caso de solicitar la **confidencialidad** *de los datos*

La prohibición de divulgar información personal, alcanza a los denominados "datos sensibles", porque éstos refieren a la vida íntima de las personas.

> Es este un criterio aceptado por la jurisprudencia, que entre otros fallos han dicho: *"Las tristes experiencias de persecución ideológica vividas en el país justifican plenamente la tutela –a través de la acción de habeas data- de la información relativa a la filiación política, las creencias religiosas, la militancia gremial, o el desempeño en el ámbito laboral o académico, entre muchos otros datos referidos a la persona titular del derecho, que no corresponde que se encuentren a disposición del público o de ser utilizados por órganos públicos o entes privados, sin derecho alguno que sustente su uso"* (Cfr. CNCiv., Sala H, mayo 19/995, *in re* Rossetti Serra, Salvador c/ Dun & Brandstreet SRL, en ED, 164-300; La Ley 1995-E, 294).

La calidad del dato refiere a ese deber de secreto y confidencialidad que los archivos, cualquiera sea su naturaleza, están obligados a resguardar.

Este deber, no obstante, tiene dos criterios que la distinguen: por un lado el llamado *sentido formal* de la obligación, que involucra la información especialmente secreta como son las creencias o la ideología política; frente al *sentido sustancial* que determina la necesidad de no revelar datos que, por su propia calidad, están más expuestos pero que, aun así, deben mantenerse reservados (v.gr.: origen racial, comportamiento o preferencias sexuales, salud, etc.).

En esta categoría se incorporan los datos médicos y los archivos de antecedentes penales, sobre los cuales ya nos hemos referido, pero que en el caso conviene agregar su indisponibilidad cuando se propicia la acción de habeas data como vía correctora de información sobre ella.

> "Corresponde rechazar el habeas data (art. 43, CN) que tiene por objeto conocer las causas judiciales criminales que pudiera tener el actor a fin de regularizar su situación en las mismas, si existe otro medio judicial más idóneo para tal finalidad cual es la solicitud de exención de prisión (art. 316, C.Pr.Cr.)" (Juzgado Nacional de Instrucción nº 19, *in re* Celesia, Horacio).

Por eso, el art. 7 inciso 4 de la ley establece que *"los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas"*.

La demanda constitucional requiriendo la confidencialidad supone mantener los datos en la base pero sin autorizar su difusión. No es un supuesto de cancelación o supresión informativa, sino la exigencia para que se lleve a cabo el deber impuesto a través de las normas.

Es sabido que este tipo de relevamiento personal es indisponible, de modo tal que la acción de habeas data pretende asegurar la garantía de confidencialidad y prevenir que las eventuales transferencias sean efectuadas a las personas autorizadas al efecto.

La reparación por el incumplimiento de este mandato sólo es posible como acción sumaria por los perjuicios causados, acumulando pretensiones punitivas contra el responsable del archivo.

47. Medidas cautelares

Las medidas cautelares que acompañan la deducción del habeas data corresponden a cada modalidad de petición. Así como ante el requerimiento de conocer la información archivada no resulta necesario articular una acción preventiva; en las pretensiones de control sobre los archivos es preciso adecuar cada providencia precautoria.

Vimos antes de ahora el caso del "bloqueo de información", o el deber de anunciar la calidad controvertida de la información que se facilita a terceros mientras se sustancia el derecho de rectificación, actualización o supresión del dato.

La medida está presente también en el artículo 27.3 del reglamento, según el cual en los archivos, registros o bancos de datos con fines de publicidad, *el titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos.* Pero no se aplica a las encuestas de opinión, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable.

> Según Falcón las medidas cautelares a tomar en este tipo de procedimientos, tienen sus propios alcances. En principio corresponderá la medida de no innovar, específicamente de no informar, como una medida cautelar genérica y subsidiaria de las previstas en el Código Procesal Civil y Comercial nacional en los artículos 232 y 233. La particularidad del pedido deberá ser contemplado por el juez con amplitud, debido a que los datos sobre los que se pide la medida cautelar son obviamente del propio peticionario.

La prohibición de innovar parece la medida más adecuada para mantener el estado actual de la controversia, pero tiene la dificultad de sostener inalterable aquello que, justamente, debe ser alterado. Es decir, si la pretensión es evitar que se difunda el dato, lo que se debe lograr es una medida innovativa, porqué al registro debe impedírsele la transferencia informativa que es su función habitual.

La ausencia de una precautoria expresa se resuelve a través de la medida cautelar genérica.

El marco del proceso constitucional, rápido y expedito, elimina la necesidad de prestar contracautela, salvo en caso de que se requiera un embargo o inhibición general de bienes sobre el archivo o sus responsables y usuarios por demandar una indemnización restitutiva.

> Sostiene Leguisamón que el habeas data tolera las denominadas medidas autosatisfactivas; opinión receptada en las conclusiones del XX Congreso Nacional de Derecho Procesal (San Martín de los Andes, octubre/1999) al recomendar que la acción de habeas data, tanto contra una persona pública como privada, sea reglamentada, sin sujeción a ninguna vía administrativa previa y de manera autosuficiente, reglando los aspectos procesales necesarios, con la estructura de un proceso monitorio que contemple la implementación de medidas autosatisfactivas.

En la etapa prejudicial que se sustancia ante el órgano de control, o bien directamente requiriendo al banco de datos, archivo o registro, la medida provisional es la "suspensión provisional" de los actos que cumplan la cesión terceros de los datos personales de la persona concernida que formula la petición de acceso o revisión.

> En el derecho comparado se discute la posibilidad de entablar medidas cautelares en el desarrollo de un planteo sobre autodeterminación informativa. En Perú, por el caso, el Tribunal Constitucional ha dicho que el proceso de habeas data no tiene por objeto constituirse en un mecanismo procesal a través del cual se pueda desvirtuar o vaciar de contenido a las libertades informativas reconocidas en el art. 2º inciso 4 de la carta constitucional. Esta salvedad la hace no porque considere que el ejercicio de tales libertades esta exento de cualquier tipo de control sino porque, precisamente, el habeas data como medio de control no actúa con carácter preventivo sino como mecanismo reparador (TC, abril 2/998, *in re* Tavara Martin, Luis c/ Carrascal Segundo Alejandro).

47.1 El acceso a los documentos públicos

Todos los actos de la administración son públicos. Los interesados tienen derecho a obtener, en cualquier tiempo, informes, copias, reproducciones y certificaciones que soliciten y la exhibición de los expedientes que deseen consultar, salvo que se trate de asuntos militares, o diplomáticos de seguridad nacional o de datos suministrados por particulares bajo garantía de confidencia.

La *Constitución de la República del Paraguay de 1992* en su artículo 28 trata del Derecho de Informarse y, al respecto, en sus incisos pertinentes establece: *Se reconoce el derecho de las personas a recibir información veraz, responsable y ecuánime. Las fuentes públicas de información son libres para todos. La ley regulará las modalidades, plazos y sanciones correspondientes a las mismas, a fin de que este derecho sea efectivo*.

Más específica la *Constitución Política de Colombia de 1991*, norma en su artículo 74: *Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley*.

Y la *Constitución del Brasil de 1988*, en su artículo 5, numeral XXXIV garantiza: b) *la obtención de certificaciones en oficinas públicas para la defensa de derechos y el esclarecimiento de situaciones de interés personal*.

No resulta ocioso recordar por su amplitud la correspondiente norma *Constitucional Española de 1978*, la cual garantiza en el artículo 105-B: *El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.*

Estos párrafos que corresponden a Gutiérrez Castro, y que reproducimos, agrega que:

> Visto con detenimiento este derecho, tal como aparece en la legislación de los Estados Unidos y Canadá, como en las constituciones latinoamericanas que lo acogen, tratan del derecho universal de recibir información, sino de un derecho público subjetivo concreto y determinado de acceder directamente a los archivos, documentos y reuniones del gobierno y, en su caso, de obtener reproducciones de los documentos.
>
> Si marcamos diferencias de este derecho con el derecho a la información, veremos en primer lugar que éste último, al menos en su aspecto esencial de derechos del público a recibir información, o sea una especie de derecho social que no contiene un derecho subjetivo concreto que se puede hacer valer contra el Estados o contra los medios, aunque en el llamado genéricamente derecho a la información si se dan situaciones en las que se reconocen derechos subjetivos como en el caso del Derecho de Rectificación o Respuesta.

Por su lado el derecho a obtener información se puede exigir Estado mediante el requerimiento a una conducta determinada; derecho por otro lado plenamente tutelado mediante acción judicial.

Profundizando un tanto en este derecho a la publicidad administrativa o mejor dicho a la administración –continúa Gutierrez-, es un derecho de defensa del sistema democrático y republicano, pues nos permite estar informados de la conducta pública para controlarla y tomar decisiones; es un derecho que debe ejercitarse mediante un actuar del ciudadano o sea, o sea requiere una petición.

Procede en relación con informaciones personales del peticionario como en relación con cualquier información de actos públicos o del gobierno que tengan un interés general. Sólo es viable en relación con información en manos del gobierno, por consiguiente no es ejercitable contra particulares o contra grupos de poder.

La información o documentación que se obtenga en principio no produce efectos probatorios, salvo que en casos específicos las leyes se lo concedan, como es el caso de la obtención de certificaciones.

Por último, los intereses en juego y por consiguiente a ser armonizados son: el encontrar un ecuánime balance entre la necesidad de confidencialidad del gobierno y el de la información del público y la prensa, amén de la promoción de la democracia.

Esta finalidad que determina el marco de la institución que nos ocupa ha marcado sus límites en los cuales al ser el Estado, por así decirlo, el sujeto pasivo de la relación jurídica que se entabla son diferentes de los trazados al derecho a la información, en relación con la vida privada y el derecho de acceso a la información personal. Sus límites están fijados por razones de interés estatal: seguridad, defensa, secretos diplomáticos, de interés social: averiguación de delitos: o de interés de terceros: protección de la intimidad de terceros, datos suministrados por particulares bajo garantía de confidencia.

En nuestra opinión, el derecho de acceso previsto en el artículo 43 constitucional, como un derecho a la información, no se puede confundir con el derecho de entrada o conocimiento de las actuaciones administrativas, documentos o archivos de carácter público.

Si la inteligencia que se acuerde a la norma fundamental es demasiado amplia, podría llegarse a vulnerar aspectos importantes del secreto y confidencialidad que tiene el Estado y los mismos particulares para que no revele información que es naturalmente confidencial.

> Dice Diaz Sieiro que el tema es aún más conflictivo cuando el contribuyente pretende ejercer el derecho de acceso, no ya a un expediente administrativo generado como consecuencia de una actuación vinculada a su persona, sino a un expediente administrativo generado como consecuencia de un procedimiento iniciado con la exclusiva intervención de un tercero o, peor aún, cuando pretende ejercer el derecho de acceso a los datos de terceros que obran en registros o bases de datos de la administración fiscal. Lo cual no le impide concluir que, en su opinión, no existe violación alguna al derecho a la intimidad y/o privacidad, y mucho menos a las disposiciones que consagran el secreto fiscal en la legislación tributaria, si se aportan los datos requeridos en este supuesto, porque lo que el derecho a la intimidad implica es una garantía contra toda intromisión arbitraria o abusiva en la vida privada de los afectados, arbitrariedad que no puede existir cuando existe un interés prioritario que justifique dicha intromisión.

47.2 La obtención de seguridad cuando se tratan datos personales

Si bien en este último límite encontramos cierto paralelismo con el derecho de acceso a la información personal -continúa Gutiérrez, es por así decirlo, sólo en el límite del respeto a la privacidad ante la información, pues en éste el caso de la publicidad administrativa, el límite nace cuando tratamos de obtener información de particulares en manos del gobierno, pues si se trata de información personal no se nos podría oponer como privado lo que es privativo nuestro, sino que tendría en su caso que acudirse a razones de seguridad estatal o social.

Por otro lado, cuando se trata de información de interés personal en el cual se trabajo sobre la hipótesis de documentos e informaciones personales, el derecho se agota en solicitarlo y, en su caso, obtener la información o su certificación, pero no comprende toda la gama de controles sobre nuestra información

personal que reconocen las leyes de protección de datos personales y en concreto que se tutela judicialmente por el habeas data.

De lo hasta aquí expuesto, podemos sacar las siguientes conclusiones respecto a la problemática de resolver por las leyes de protección de datos personales:

- Se trata de una legislación cautelar tendiente a dar una protección específica al honor, a la vida privada y a los demás derechos y libertades de las personas.
- Esta protección se da contra el procesamiento de datos de carácter personal por medios informáticos generalmente, pero sin excluir otros medios mecánicos e incluso manuales.
- Tratándose de datos personales la acción de protección le corresponde al titular de los mismos porque los datos le pertenecen, son lo más mío de lo mío; o lo más tuyo de lo tuyo.
- Este derecho entra o puede entrar en conflicto con otros derechos aunque como vimos se trata de una cuestión de legitimidad, pero su limitación y lo que vuelve necesaria su institucionalización, más por razones de interés nacional relacionados con el progreso y con intereses económicos y de desarrollo del correspondiente Estado y de competitividad e integración internacional por la comunicación de los datos. Es en el fondo en esta armonización de intereses que el legislador cede ante la realidad de la tecnología informática, pero para mantenerse el equilibrio refuerza, por así decirlo, la protección a la vida privada, principalmente.
- Aunque estas leyes se encuentran dentro del campo del derecho objetivo de la información, se distinguen de otros derechos subjetivos como son el derecho a la información y el derecho a informarse de los actos públicos de gobierno, tanto en sus fines, en los conflictos de intereses a resolver, en su contenido y en los medios tecnológicos usados.
- A diferencia del derecho a la información o libertad de prensa que están plenamente constitucionalizados, y del derecho a acceder a los actos de gobierno que también lo están, siendo ambos derechos, además inherentes al Estado democrático de derecho. El derecho a la información personal o mejor dicho el derecho a recabar información personal sea por computadoras u otros medios, no lo está, por lo que en ningún caso puede hablarse de superioridad jurídica desde el punto de vista del derecho objetivo o de un derecho a recabar información sobre otros con fines a condenarles al efecto de obtener criterios y conclusiones, muy por el contrario cuando se constitucionalizan y se hace referencia a datos personales o a principios informáticos es para limitarlos en su recolección, almacenamiento y distribución y para proteger la vida privada y otros derechos, incluso la libertad e implícitamente el sistema democrático en contra de los abusos que puedan provenir del indebido uso de los bancos o bases de datos.

Véase al respecto el Convenio Europeo, la Constitución española, la portuguesa y en latinoamericanos del Brasil, Paraguay, Guatemala, Colombia, Argentina, Perú, Bolivia y Ecuador.

Consecuencia de lo anterior es que en este campo los derechos individuales ceden menos para mantener la armonía y, si la prensa tiene por límite lo justo y razonable ante la vida privada, lo que usualmente se califica a posteriori; la transparencia administrativa tiene por límites la seguridad nacional y estatal, el interés público e incluso el respeto a la privacidad cuando la información en manos del Estado es concernida a terceros; tratándose del acceso de terceros a datos personales con el fin de difundirlos, el umbral de la intimidad se mantiene prácticamente incólume y su gran principio rector es el consentimiento de la persona identificada o identificable, o lo que se ha denominado el principio de autodeterminación informativa.

48. Contestación del informe. Defensas

Una de las polémicas tradicionales en los procesos constitucionales, y el habeas data es uno de ellos, consiste en asignar el carácter de procesos contradictorios o controversiales; frente a otra corriente que establece como deber jurisdiccional afianzar la supremacía constitucional, a cuyo fin el Juez ha de realizar estricto control sobre los actos y hechos que juzga, sin necesidad de seguir la versión de una u otra de las partes que confrontan.

La primera de las ideas se encuentra en algunas constituciones provinciales que requieren de la autoridad pública o del sujeto privado que se denuncia como autor del acto lesivo, que *conteste* la demanda instaurada y ofrezca la prueba que sostiene como fundamento de sus derechos.

De esta forma se consagra un proceso contradictorio, con posiciones probablemente ambivalentes, hechos controvertidos que deben probarse y todo ello en el marco del principio de bilateralidad y congruencia que obligará al Juez a resolver en el marco de lo alegado y probado.

> El Código Procesal Constitucional de la provincia de Tucumán es un buen ejemplo de esta corriente, porqué aun previendo la intervención activa del juez en el proceso de amparo, señala que de la demanda se debe dar *traslado* al accionado, y si el informe *niega los hechos* o existe prueba a producir la misma debe producirse siguiendo el principio de la carga probatoria aplicable en el proceso civil o común.

Desde otra perspectiva, pero sin perder de vista la necesaria bilateralidad del proceso, se propicia tramitar a los procesos constitucionales sin la gravedad de la controversia con intereses opuestos y disímiles.

Más que un demandado, la observación se fija en el objeto que se reclama, de forma tal que el control de legalidad y constitucionalidad deviene inmediato, sin apegarse el juez a los escritos postulatorios.

> El habeas data busca la protección –dicen Slaibe y Gabot- de manera inmediata, de una diversidad de derechos (a la verdad, a la autodeterminación informativa, a la intimidad, a la privacidad, a la voz, a la imagen, a los valores familiares, al honor, al patrimonio, entre otros). Sin perjuicio de ello, debe encuadrársele en un marco protector de la libertad y de la dignidad humana, coherente con la norma constitucional y comprensiva de registros informáticos y ficheros manuales.

Este es el sentido que tiene la ley nacional, cuando en el artículo 39 dice: "*1. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente; 2. El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez*".

De esta manera se persigue observar si los datos archivados son falsos, inexactos o establecen una orientación discriminatoria en el proceso de tratamiento que ellos tienen.

La primera obligación del titular del registro será responder al planteo del requirente sobre el consentimiento obtenido para el tratamiento de datos personales y, en su caso, indicar el destino que ellos tienen previsto.

Inmediatamente, tendrá que informar los mecanismos técnicos y de seguridad que funcionan en el archivo, y acompañar la documentación que respalde sus explicaciones.

Entre los artículos 39.1 y 41 de la ley, existe alguna inconsistencia pues parte del supuesto que el actor ha reclamado el acceso a la información o efectuado algún planteo de revisión sobre los archivos que le conciernen. Por eso, el art. 41 dice que *"al contestar el informe, el archivo, registro o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquéllas por las que no evacuó el pedido efectuado por el interesado, de conformidad a lo establecido en los artículos 13 a 15 de la ley"*.

Las únicas defensas admisibles provienen de la calidad del dato registrado, de modo tal que los responsables o usuarios de bancos de datos públicos pueden, mediante decisión, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y seguridad públicos, o de la protección de los derechos e intereses de terceros.

El artículo 17.2 agrega que "*la información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso, vinculadas a la investigación sobre el cumplimiento de*

obligaciones tributarias o previsionales, el desarrollo de funciones de control de salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado".

En cambio se veda la excepción de confidencialidad, salvo que para hacerlo se revelen fuentes de información periodística.

Las defensas articuladas actúan como impeditivas y deben tratarse como de previo y especial pronunciamiento, procurando acumular actos procesales en la providencia resolutiva, de modo tal que el proceso cumpla la condición de rápido y expedito que la Constitución nacional establece.

48.1 Excepciones admisibles

Más allá de lo dispuesto en la ley reglamentaria, debemos confrontar si las excepciones o defensas que habitualmente traen las leyes de amparo, son aplicables al habeas data, en la medida que se tome a este proceso como una modalidad o *sub tipo* del proceso constitucional por antonomasia.

En particular estimamos que el habeas data es un proceso autónomo que no se adscribe el modelo excepcional del amparo, pero que puede admitir en su trámite los siguientes planteos:

a) Reclamo administrativo previo

Si el habeas data fuera interpretado como continuador de la línea procesal del amparo, hay que observar que el actual artículo 43 constitucional elimina las vías previas, calidad que llevaría a sostener la operatividad directa sin necesidad de articular un reclamo al archivo en forma anterior a la demanda judicial.

No obstante, y pese a este eventual encuadre, la misma ley fundamental condiciona la vía amparista cuando existe "un medio judicial más idóneo". Quizás, basados en esta inteligencia, la Corte Nacional ha dicho que *"la acción de habeas data puede hacerse valer por cualquier vía procesal razonable: amparo, hábeas corpus y aún la incidental, hasta tanto una ley reglamente su ejercicio"* (cfr. Voto del Dr. Boggiano en Ganora, Mario F. y otro, sentencia del 16 de setiembre de 1999).

Nosotros creemos que la especialidad que trae el tratamiento de datos personales requiere dos etapas bien precisas: a) una *extraprocesal* que le permite al afectado tomar conocimiento directo de los datos almacenados por una archivo sin necesidad de contar con una orden judicial que lo autorice; y b) otra *procesal* o *jurisdiccional* que supone la actuación judicial oportuna cuando se han negado por el banco de datos las posibilidades de acceso y control consecuente.

Pero el tránsito previo por la instancia administrativa, si bien recomendable y adecuado, no puede surtir las veces de un obstáculo para acceder a la justicia, de modo tal que si el interesado prefiere recurrir a la acción de habeas data, el archivo podrá alegar que no ha tenido posibilidad de ser oído y, en tal caso, la instancia jurisdiccional podrá ser de encuentro y conciliación antes que de controversia pura.

> Recordemos que la jurisprudencia ha dicho que *"los jueces pueden rechazar* in limine *la acción de habeas data con criterio restrictivo y la mayor prudencia y cautela, ya que de lo contrario podría interpretarse como una negación de justicia"* (cfr. Cfed. Bahía Blanca, Sala 1ª, diciembre 30/994, *in re* Gutierrez, Héctor R. c/ Casino Militar del Personal Superior de la Base Naval Puerto Belgrano).
>
> Asimismo se ha señalado que *"el promoviente del habeas data debe acreditar haber realizado las gestiones o tramitaciones para acceder a los registros u obtener la información requerida o bien la inutilidad de los trámites administrativos"* (CNCom., Sala D, mayo 13/996, *in re* Figueroa Hnos c/ Banco de la Provincia de Santiago del Estero).
>
> Finalmente, se puede agregar que *"si bien el reclamo administrativo previo no resulta necesario para la interposición de la acción de habeas data, resulta conveniente que el peticionario solicite a la Administración tanto el suministro*

de la información necesaria y de su finalidad, cuanto de su rectificación, debiendo ello ser tomado en cuenta al momento de imponer las costas" (C.Contencioso administrativa, Córdoba Sala 1ª , marzo 29/995, *in re* García de Llanos, Isabel c/ Caja de Jubilaciones, Pensiones y Retiros de Córdoba, en La Ley Córdoba, 1995-948).

c) *Competencia*

Las características de proceso que tutela derechos constitucionales y, particularmente, la intimidad de las personas y la vida privada que se perturba por el tratamiento de datos individuales, permite afrontar la cuestión de competencia en la dimensión que tiene la tradición legal y jurisprudencial del juicio de amparo.

El art. 4º de la Ley 16.986 –aplicable por analogía al habeas data-, declara juez competente al de la jurisdicción del lugar en que el acto se exteriorice o pudiere tener efecto, observándose asimismo en lo pertinente, las normas sobre competencia por razón de la materia, salvo que aquellas engendraran dudas razonables al respecto, en cuyo caso el juez requerido debe asumir la jurisdicción (cfr. CNContencioso administrativa Federal, Sala 3ª , diciembre 15/994, *in re* Basualdo, Pedro, en Jurisprudencia Argentina, 1995-IV, 349).

Si la demanda se articula como defensa de la intimidad contra empresas privadas destinadas a proveer informes, la jurisdicción interviniente corresponde a los tribunales civiles por razón de la materia. Empero, también se ha dicho que si la demandada se dedica comercialmente a la difusión de información contenida en sus bancos de datos, en cuyo caso, evidentemente desarrolla una actividad mercantil (art. 43 bis, decreto/ley 1285/58, t.o. ley 23.637), la justicia comercial es competente por así asignarlo la calidad de las personas (cfr. Dictamen del Fiscal de 1ª Instancia en la causa Benseñor, S. c/ Organización Veraz S.A., del 15 de agosto de 1995).

El artículo 36 ya enunciado dice: *"Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho se exteriorice o pudiera tener efecto, a elección del actor.*

"Procederá la competencia federal:

a) Cuando se interponga en contra de archivos de datos públicos de organismos nacionales; y

b) Cuando los archivos de datos se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales".

c) Legitimación para obrar

Sin perjuicio de lo dicho en el parágrafo 44 y subtítulos, conviene agregar que la norma constitucional es abierta y, en principio, no limita el acceso a la información contenida en los bancos de datos.

Claro está que existen recaudos para admitir las acciones provenientes del control, pues como estas se fundan en decisiones personales, sólo al afectado, su representante o las personas que tengan un interés legítimo se les permite articular las pretensiones de rectificación, actualización, supresión o confidencialidad.

En la causa Ganora, la Corte sostiene que sólo puede ser ejercida por el titular del derecho la acción de habeas data, pues ella tiene por objeto defender aspectos de su personalidad que no pueden encontrarse a disposición del público ni ser utilizados sin derecho, garantizando a toda persona que su filiación política, sus creencias religiosas, su militancia gremial, sus antecedentes laborales o académicos, no puedan ser divulgados ni utilizados en su perjuicio por órganos públicos o entes privados (voto del Dr. Fayt,setiembre 16/999).

La jurisprudencia señala también que la admisibilidad del habeas data contra particulares debe ser juzgado con un criterio menos estricto, habida cuenta que no existe la presunción de legitimidad de los actos provenientes de autoridades en los casos de archivos privados.

Por tanto, se estima conveniente habilitar la instancia judicial aunque más no sea para escuchar al que pretende acceder a la justicia (cfr. CNCiv., Sala F, Julio 6/995, *in re re* Bianchi de Saenz, Delia A. c/ Sanatorio Greyton S.A., en ED, 165-255).

Vale reiterar lo dispuesto en el artículo 34 (Legitimación activa) cuando sostiene: *"La acción de protección de los datos personales o de habeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.*

"Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.

"En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo"

d) *La negativa a suministrar datos*

Los registros, archivos o bancos de datos privados no pueden valerse de la confidencialidad de los datos para negar el acceso que la justicia le notifica.

Por su parte, los bancos de datos públicos, al producir el informe siguiente a la demanda deducida, pueden oponerse al requerimiento invocando que la revelación de los datos o el control sobre ellos que se plantea, provoca una lesión a sus derechos, lo cual ha de acreditar con sujeción a los términos que las excepciones legales establecen.

> Dice Falcón que en la contestación al informe puede jugar el secreto profesional y el de las fuentes de información. Si el informe no es contestado, además de las sanciones previstas para los informes en general, el accionado puede ser sancionado con apercibimiento, multa y arresto de hasta cinco días (art. 18, dec-ley 1285/58, ref. Ley 24.289, art. 2º). Algunas Constituciones han previsto expresamente la sanción ante el incumplimiento de una orden judicial en este sentido (v.gr. Chaco, art. 19 *in fine*).

En uno u otro caso, el Juez puede requerir que "le traigan los datos" para tomar él mismo conocimiento directo bajo promesa de confidencialidad.

> Sostiene Mercedes Serra, coincidiendo con Sagüés, que en principio el Estado no puede invocar razones de seguridad para negarse a suministrar los datos que se requieren. Empero –agrega, por la analogía que guarda el instituto del habeas data con el del amparo, si el acto lesivo que se intenta atacar mediante el amparo debe padecer de arbitrariedad o ilegalidad manifiesta, la negativa de la autoridad pública a suministrar determinada información frente a la promoción de un habeas data deberá ser evaluada por el juzgador en orden a su razonabilidad.
>
> Sobre el particular, la jurisprudencia rechazó un habeas data sosteniendo que *"a los efectos de la acción de habeas data, la Constitución Nacional prevé que las informaciones deben constar en registros o bancos de datos públicos, es decir, que la información debe ser pública o al alcance de los particulares. De esta forma, no procede la acción en relación a la información obrante en los registros de las fuerzas y organismos de seguridad, pues no reviste tal carácter público por obvias razones de seguridad pública"* (CNCrim. y Correccional, sala de Feria, agosto 3/997 *in re* Ganora, Mario y otra; fallo posteriormente revocado por la Corte Suprema).

El artículo 40 (Confidencialidad de la información) dice: "1. *Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo en caso en que se afecten las fuentes de información periodística; 2. Cuando un archivo, registro o banco de dato*

público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad"

49. Prueba

La prueba en el habeas data se fracciona según se demande el acceso a las bases de datos, o se requiera una pretensión expresa de cancelación, actualización, supresión o confidencialidad.

En la petición dirigida para *tomar conocimiento* de la información que sospecha se encuentra en una base de datos, la presunción es la fuente donde recurrir.

A su vez, si la demanda solicita la *exhibición* únicamente, el fundamento se razona en el interés que el afectado plantea. Si con la acción se persigue conocer la *finalidad* del archivo, es decir, para qué se tomaron los datos y para quien se realizó el registro, la cuestión no requiere de refuerzos argumentales porqué la garantía se respalda en el derecho a la información. Mientras que en el habeas data deducido con la intención de conocer al autor del registro que capturó información que le concierne, se debe satisfacer el requisito del interés suficiente.

En los casos de acceso a la información, más que probar el presupuesto de derecho que vincula con los hechos denunciados, se debe acreditar la insuficiencia de las peticiones precedentes.

> "*Resulta inadmisible denegar la presente acción de habeas data interpuesta a fin de efectuar una actualización de datos a un legajo de la CONADEP, sobre la base de no haber el accionante acreditado la negativa del Estado Nacional –v.gr. la Subsecretaría de Derechos Humanos y Sociales- a tal petición, pues, por el contrario, de la clara conducta de la autoridad administrativa se evidencia la ineficacia cierta que tendría tal procedimiento, lo cual transformaría al reclamo previo en un ritualismo inútil"* (CNContenciosoadministrativo Federal, Sala V, diciembre 1/999).

En cambio, si las modalidades responden al control del archivo, cada pretensión se debe demostrar.

En efecto, en el habeas data destinado a *actualizar* la información, se deben aportar los documentos necesarios para producir ese acto innovador para la base de datos. También procede la prueba testimonial cuando se debe demostrar el cambio efectuado en la información que se encuentra almacenada.

> Se ha dicho que "*si la actualización de la información constituye la finalidad de la acción de habeas data, cabe considerar que la acción impetrada resulta idónea para efectuar la actualización de datos a un legajo de la CONADEP, completando la ya realizada por la Subsecretaría de Derechos Humanos y Sociales, mediante el agregado de una declaración testimonial prestada en sede penal"* (CNContenciosoadministrativo Federal, Sala V, diciembre 1/999).

En la *rectificación* por informaciones inexactas, de igual modo, ha de aportarse la prueba documental pertinente, siendo subsidiaria y eventual la prueba de testigos.

> El artículo 56 del Código Procesal Constitucional de la provincia de Tucumán, que rige para el habeas data local, dispone que: "*Con el escrito de demanda, debe ofrecerse toda la prueba y acompañarse la documental que se disponga. En caso contrario, se la individualizará expresando su contenido y el lugar donde se encuentre. El número de testigos no puede exceder de cinco (5) por cada parte, siendo carga de ésta hacerlos comparecer a su costa a declarar, sin perjuicio de requerir el uso de la fuerza pública en caso de necesidad. Sólo se admite la prueba de absolución de posiciones cuando la acción se promueva contra particulares, en cuyo caso debe acompañarse el pliego con el escrito de demanda".*

50. Sentencia

Lo expresado en el punto anterior deja en claro que en la mayor parte de las veces el proceso de habeas data se resolverá sin necesidad de producir prueba, toda vez que la misma está preconstituida.

Por eso, el artículo 43 establece lo siguiente:

"1. Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo 42 (ampliación de la demanda), *luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia.*

"2. En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo el plazo para su cumplimiento.

"3. El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante.

"4. En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto".

Ahora bien, al considerar al habeas data como un típico proceso constitucional, le llegan a él los mismos problemas que contrae la sentencia en los sistemas donde los jueces deben aplicar la ley, controlar la supremacía constitucional o, simplemente, derivar el conflicto a un órgano especializado (Tribunal Constitucional).

En líneas muy amplias y a los fines de presentar el meollo del problema podemos destacar que la sentencia debe resolver estos planteos:

Cuando el modelo previsto para el control de constitucionalidad es concentrado (Tribunales Constitucionales) el debate se sostiene acerca de si es jurisdiccional o no el pronunciamiento. Como tal, los alcances objetivos y subjetivos dependen de la consideración que reciba el carácter de la sentencia, pues si fuera interpretada como resolución que permita aplicar o inaplicar una norma, los efectos se reducen a la validez misma de la ley.

En otros términos, no existiría una decisión para las partes sino para toda la sociedad respecto a la validez o ilegitimidad de una norma jurídica.

> La incertidumbre que rodea a este instituto –dice Blasco Soto- tiene una de sus causas en que la sentencia constitucional se ha reducido en su concepto al hecho jurídico material (resultado del legislador negativo), sin advertir que el régimen de las decisiones procesales y su naturaleza varía según se trate el tema desde el punto de vista sustancial o procesal. Si el estudio del alcance cronológico se resuelve desde el derecho sustancial, su virtualidad se desplegará desde el momento en que se verifica el hecho constitutivo (la sentencia); eficacia que, en modo alguno, se considera consecuencia jurídica de la naturaleza de la decisión. Desde esta posición las categorías jurídico-materiales (nulidad/anulabilidad) son las que definen la eficacia temporal de la sentencia constitucional. La concepción dogmática dominante que considera la sentencia más como acto normativo que procesal determinó que sus efectos se delimitaran en atención al vicio de la ley (acto nulo o acto anulable) sin establecer diferencias entre el objeto del control (la ley) y la naturaleza del resultado (la sentencia).

En los sistemas difusos, el tema de la bilateralidad del proceso lleva a posiciones opuestas. O se justifica la sentencia en los términos como se expide en un proceso común, haciendo verdad el precepto que el Juez debe fallar según lo alegado y probado por las partes; o se permite al Juez resolver la cuestión de constitucionalidad sin mediar petición expresa de las partes, con el fundamento que los procesos constitucionales llevan implícita esta misión jurisdiccional.

En uno u otro caso, vemos que el habeas data es un proceso constitucional de ribetes muy particulares; con un objeto muy preciso y una libertad a custodiar que le facilita incursionar más allá de los límites que la pretensión y la resistencia (demanda y contestación) pueden acotar.

En definitiva, el juez deberá resolver si hubo o no afectación a la persona cuando se tomaron y procesaron sus datos personales; y en su caso, seguir –o no- las peticiones consecuentes respecto a actualizar, renovar, suprimir o guardar la información compilada en estricta reserva y confidencialidad.

Bibliografía Capítulo XII

Altmark, Daniel R. – Molina Quiroga, Eduardo, *Régimen jurídico de los bancos de datos,* en Informática y Derecho, volumen 6, editorial Depalma, Buenos Aires, 2.000.

Antik, Analía – Ramunno, Luis A., *Habeas data (Comentarios sobre los bancos de datos privados destinados a proveer informes),* en Rev. La Ley del 14/4/2.000.

Blasco Soto, María del Carmen, *La sentencia en la cuestión de constitucionalidad,* editorial Bosch, Barcelona, 1995.

Díaz Sieiro, Horacio D., *El derecho de acceso a los datos en poder de la administración tributaria. La necesidad de su expresa consagración en nuestro ordenamiento jurídico,* en Doctrina Tributaria nº 241, editorial Errepar, Buenos Aires, 2000.

Estadella Yuste, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales,* editorial Tecnos, Madrid, 1995.

Falcón, Enrique M., *Habeas data,* editorial Abeledo Perrot, Buenos Aires, 1996.

Gozaíni, Osvaldo Alfredo, *Derecho Procesal Constitucional,* tomo 1, editorial de Belgrano, Buenos Aires, 1999.

Gozaíni, Osvaldo Alfredo (coordinador), *La defensa de la intimidad y de los datos personales a través del Habeas Data,* editorial Ediar, Buenos Aires, 2000.

Gutierrez Castro, Mauricio, *Derecho de la información (acceso y protección de la información)* 51º Período Ordinario de Sesiones OEA/Ser. Q; 4 a 29 de agosto de 1997 CJI/SO/I/doc.9/96 rev.2; Rio de Janeiro, RJ, Brasil 19 agosto 1997.

Herrán Ortiz, Ana Isabel, *La violación de la intimidad en la protección de datos personales,* editorial Dykinson, Madrid, 1999.

Leguisamón, Héctor Eduardo, *Procedimiento y aspectos procesales del habeas data,* en Revista de Derecho Procesal, nº 4, editorial Rubinzal Culzoni, Buenos Aires, 2.000.

Molina Quiroga, Eduardo, *Autodeterminación informativa y habeas data,* en Jurisprudencia Argentina, suplemento especial de "Informática Jurídica" del 2 de abril de 1997, págs. 30 y ss.

Serra, Mercedes, *Habeas data: problemas que plantea su implementación,* comunicación presentada al XX Congreso Nacional de Derecho Procesal (San Martín de los Andes, octubre 1999).

Sagüés, Néstor Pedro, *Subtipos de habeas data,* en revista Jurisprudencia Argentina del 20/12/95. Buenos Aires.

Slaibe, María Eugenia – Gabot, Claudio, *Habeas data: su alcance en la legislación comparada y en nuestra jurisprudencia,* en Rev. La Ley, suplemento de Derecho Constitucional, del 17 de marzo de 2.000.

CAPÍTULO XIII. Problemas particulares del habeas data argentino

51. Tipo de proceso

Los procedimientos conservan generalmente una estructura simétrica que varía con el grado de conocimiento que el Juez consiga sobre los hechos que se debaten.

En los procesos constitucionales, se ilumina la cuestión constitucional que provoca la amenaza o el gravamen en los derechos de la persona, obligando al órgano jurisdiccional a resolver sobre el acto lesivo.

En esta tónica es procedente el *rechazo in limine* ya que dentro de las facultades jurisdiccionales de los jueces se encuentra la calificación jurídica de las pretensiones esgrimidas por los litigantes, sin estar obligado a sujetarse a los esquemas jurídicos que las partes le proporcionan, decidiendo en su caso, aplicar al proceso reglas diferentes a las invocadas.

En el habeas data argentino la polémica se ha centrado por el lugar donde la institución se origina, llevando a sostener a buena parte de la doctrina que se trata de una modalidad del juicio de amparo, a cuyo fin el juez debe encontrar la ilegalidad o la arbitrariedad manifiesta en los actos de registro de información personal.

Otros, en cambio, observan que la ubicación constitucional no es suficiente para encontrar la naturaleza procesal porqué cada párrafo del artículo 43 es un tipo diferente de tutela judicial efectiva (que es el sentido que supone dar al concepto "amparo" dentro de la carta fundamental). Entre estas modalidades de protección se encuentra el habeas data.

> El último Congreso Nacional de Derecho Procesal (San Martín de los Andes, octubre de 1999) expuso en sus conclusiones estas dos corrientes, que tampoco puede ser vistas como antagónicas.
>
> La primera sostuvo que el habeas data no es una modalidad del amparo, sino que tiene perfiles propios que lo definen como un proceso constitucional autónomo y con carriles propios que se apartan del restriccionismo tradicional que al amparo se le ha acordado.
>
> La segunda consideró que es un sub tipo de amparo con características propias, sin que sea aplicable la idea básica de encontrar ilegalidad o arbitrariedad en el acto lesivo.
>
> En la jurisprudencia, algunos sostienen que *"la acción de habeas data es una variable del género amparo, como tutela de los derechos consagrados en la legislación nacional" (*cfr. Rossetti c/ Dun & Bradstreet SRL, citado, en Rev. La Ley 1995-E, 294). Mientras que otros afirman que *"para la procedencia del habeas data no se requiere en principio, arbitrariedad o ilegalidad manifiestas, dado que procede ante la mera falsedad en el contenido de los datos o discriminación que de ellos pudiera resultar, y aún sólo para conocer dichos datos, sin que sea necesario que ellos vulneren inmediatamente derechos o garantías constitucionales*" (cfr. CNContenciosoadministrativo, Sala 4ª , octubre 4/995, *in re* Gaziglia, Carlos R. y otro c/ Banco Central de la República Argentina).

Nosotros ya hemos afirmado el carácter autónomo e independiente de las reglas del amparo, aun reconociendo la condición de proceso rápido y expedito que debe tener ineludiblemente.

Otra calidad insoslayable es la naturaleza preventiva que debe sumar el habeas data, antes que obrar como proceso reparatorio de las lesiones constitucionales que, en el caso, serían las pretensiones que contra el archivo se hagan en miras a lograr la rectificación o la supresión de la información personal almacenada.

51.1 ¿Trámite especial, amparo o sumarísimo?

La confusión reinante lleva a que en los tribunales se ordene tramitar el proceso de habeas data siguiendo las reglas clásicas del amparo; algunos establecen cierta flexibilidad en las cuestiones de acceso (legitimación y plazos), otros aplican la ley 16.986, los menos utilizan el sistema procesal penal por la similitud con el hábeas corpus y, con sentido conciliador, se suele decir que *"la vigencia del artículo 43 párrafo tercero de la Constitución Nacional debe ser asegurada por los jueces a pesar de la ausencia de reglamentación legislativa*" (cfr. Voto del Petracchi en la causa "Urteaga", cit.).

> "En ausencia de ley específica en la materia, la vía del amparo genérico (art. 43, primer párrafo) reglamentada por las normas pertinentes resulta el camino adecuado para ejercer el habeas data, ya que no es otra la solución que emerge de la Constitución Nacional, art. 43, tercer párrafo" (Superior Tribunal de Justicia de Entre Ríos, Sala 1ª , noviembre 8/994, en Zeus del 14/7/95).
>
> Afirma Serra que, sin embargo, y si bien es cierto que se admite la aplicación supletoria de las normas relativas al amparo en todo aquello que no se oponga a expresas directivas de la Constitución Nacional, no lo es menos que dicha aplicación no puede hacerse sin restricciones, en razón de que el objeto perseguido procesalmente difiere en ambos casos. En todo caso, se acepta que en el derecho público local, las provincias gozan de amplia autonomía en cuanto a trámite y competencia en materia de habeas data, pero sujeto claro está, a que la implementación del instituto federal en esos ámbitos no los desnaturalice, perjudique o retacee, respetándose las reglas del debido proceso, tanto para el promotor de la acción como para el sujeto pasivo contra el cual se promueve.

El problema de aplicar el artículo 43 cuál si fuera el reconocimiento constitucional al juicio de amparo, es un equívoco palmario, porqué en realidad la ley fundamental crea el derecho a la tutela judicial efectiva (derecho de amparo) a través de distintos tipos o fisonomías de amparo sobre actos especialmente previstos. (Debe perdonar el lector esta insistencia temática, que la ley repite en su texto –ver art. 37-, pero estamos en las conclusiones y es mejor recordar esta cuestión).

> Afirmamos en otra parte que actualmente, el nuevo artículo 43 de la Constitución Nacional significa un cambio fundamental en el tratamiento del tradicional proceso de amparo. Ha dejado de ser una figura procesal para constituirse en un "derecho" o "garantía" específico, cuya principal concreción es instalar el derecho al amparo.
>
> Por ello, el amparo no es una vía subsidiaria o indirecta, sino la garantía por antonomasia; la única herramienta disponible para actuar los derechos fundamentales de inmediato.
>
> Son varios los fundamentos que tiene esta lectura constitucional del fenómeno que manifiesta el amparo. Uno de ellos proviene de la interpretación transnacional. En efecto, el derecho a la celeridad en los procesos se pide a través de numerosas declaraciones internacionales, tales como el Pacto Internacional de Derechos Civiles y Políticos (Nueva York, 1966), la Convención Americana sobre Derechos Humanos, el Convenio Europeo para la protección de los Derechos Humanos, entre muchos más. Por tanto, el registro constitucional que reclama la "acción rápida y expedita" no puede tomarse sin referencia con este cuadro de aptitudes y posibilidades.

El obrar como derecho modifica el emplazamiento del proceso tradicional, pues además de reconocer en la letra expresa del texto fundamental ese cambio trascendente, requiere que la garantía se consolide en un proceso "rápido y expedito".

Ahora bien, si se aplica la Ley 16.986 debe tenerse en cuenta que esta se opone en varias de sus disposiciones al nuevo sentido constitucional, sobre todo, en la cobertura de actos provenientes de autoridades públicas o de particulares que, ahora, se encuentran unificados en la Constitución nacional.

Esta sutil pero importante diferencia no puede dejarse de lado, porque con la ley de amparo (virtualmente derogada) los procesos contra el acto ilegal o arbitrario de la autoridad pública se regían por las reglas especiales, no contenciosas, de la ley federal; mientras que las acciones entabladas contra los actos de particulares, tramitaban como proceso sumarísimo –controvertido- según lo dispuesto en el código procesal civil y comercial de la nación.

Si advertimos la protección que tiene como destino el habeas data, podrá constatarse que existe una gran complejidad en asignar uno u otro procedimiento.

En efecto, el artículo 43 párrafo tercero de la Constitución puede tener otra lectura que no sea estrictamente procesal, es decir, que lleve necesariamente a encontrar un cauce a la protección de los datos frente al tratamiento informatizado de la información que concierne a las personas.

Se podría afirmar, como lo dijo el Dr. Boggiano en la mencionada causa "Urteaga" que el habeas data puede hacerse valer por cualquier vía procesal razonable, aun la incidental, hasta tanto una ley reglamente su ejercicio. De este modo, lo importante es la protección efectiva antes que el sistema formal de enjuiciamiento.

A la hora de elegir un procedimiento adecuado, rápido y expedito, que cumpla con las finalidades preventivas (acceso a los bancos de datos, archivos o registros) y de control (actualización, rectificación, supresión y confidencialidad), es evidente que no hay trámite actualmente vigente que reconozca ser la vía procesal más idónea.

> Impacta la información que proporciona Leguisamón cuando relata que, en un caso recientemente fallado, la demanda contra una empresa dedicada al suministro de informes comerciales fue promovida el 15 de diciembre de 1997. Sustanciado el proceso mediante las reglas del proceso sumarísimo, el juez de primera instancia dictó sentencia el 29 de octubre de 1998 y el tribunal de alzada, apelación de la demandada mediante, pronunció la definitiva el 23 de marzo de 1999, y posteriormente, el 13 de mayo de 1999, denegó el recurso extraordinario interpuesto por la accionada, resolución contra la cual la empresa de informes comerciales interpuso recurso de queja ante la Corte Suprema, recurso éste que al tiempo de ser terminado este trabajo (marzo/2000) aún no ha sido resuelto (*in re* Lascano Quintana, Guillermo V. c/ Organización Veraz S.A.).

Tal ausencia tampoco permite sostener la vía del hábeas corpus, pese a que en definitiva, en el sistema garantista siempre están en juego libertades, en el caso, la libertad informática o "autodeterminación informativa".

> La Corte Suprema de Justicia de la provincia de Mendoza, aplicó este criterio en razón de que el código de procedimientos en materia penal regla un sistema rápido y urgente que facilitó el camino para el habeas data (causa *Costa Esquivel, Oscar c/ CO.DE.MA.*, sentencia del 17 de noviembre de 1997); pero la Corte Nacional lo ha refutado en la ya citada causa "Urteaga" al decir que la aparición del habeas data no puede entenderse como una sustitución del hábeas corpus, cuya función para la defensa de la libertad física sigue siendo plenamente vigente, sino que se trata de una garantía para nuevas agresiones a otras facetas de la libertad. No resultaría extravagante pensar, como alternativa, que la justicia penal es la más idónea para la realización de una investigación tendiente a encontrar a una persona desaparecida en las circunstancias denunciadas. Pero, más allá de la posible existencia de impedimentos que obstaculizarían esta vía, de todos modos, ella sólo cobraría sentido en tanto el accionante pretendiera activar la persecución penal y arribar a la imposición de una pena. En cambio, si su objetivo inmediato es "conocer los datos" y decidir luego sobre ellos, parece claro que, sin sustituir sus propósitos, no es el proceso penal el que la pretensión de que se trata, la que sólo puede ser acogida en el marco del habeas data (cfr. Voto del Dr. Petracchi).

51.2 Vía directa o subsidiaria. ¿Existe la vía judicial más idónea?

El punto anterior sirve de pórtico al presente porqué reitera similares dificultades. Es decir, si el habeas data se adopta como una modalidad del amparo-proceso, habrá que confrontar con las vías judiciales paralelas o concurrentes para deducir cuál es la más idónea.

Mientras que excluirlo de este encuadre permite identificar un proceso autónomo pero sin reglas precisas ni conocidas, en cuyo caso, merced a esta incertidumbre podríamos interrogarnos si es factible tramitar al habeas data como acción declarativa.

La operatividad directa no es punto a debatir toda vez que se reconoce el mandato constitucional expedito sin necesidad de tener la ley o el reglamento de esta.

> En "Urteaga" la Corte dijo que, como principio, la falta de reglamentación legislativa no obsta a la vigencia de ciertos derechos que, por su índole, pueden ser invocados, ejercidos y amparados sin el complemento de disposición legislativa alguna. Calidad coincidente con las conclusiones del XX Congreso Nacional de Derecho Procesal cuando sostuvo que *el habeas data es una garantía constitucional operativa de carácter federal que beneficia y tutela a toda persona; ello sin perjuicio de los regímenes provinciales que tendrán como base o mínimo las modalidades protectoras previstas en el artículo 43, párrafo 3º de la Constitución Nacional*.

El problema está en las condiciones o presupuestos que como requisitos de admisión se interponen como vallas para el progreso inmediato de la acción.

El amparo tradicional siempre se encolumnó tras el carácter excepcional y contingente de los procesos constitucionales, pensando que las vías ordinarias o comunes debían ser bastantes para resolver los conflictos con la ley fundamental.

> "No hallándose aún reglamentado el trámite de la acción de habeas data regida en el art. 43 de la Constitución, cabe estar por analogía a las reglas de competencia y procedimiento fijadas por la acción de amparo en la ley 16.986" (CNContenciosoadministrativo, Sala 3ª , diciembre 15/994, *in re* Basualdo, Pedro s/ amparo).

La idea del proceso concurrente con el amparo, eliminó en reiteradas ocasiones la puesta en marcha de éste, en razón de sostener la habilidad del primero para defender los conflictos con la ley fundamental (v.gr: admisión del juicio contencioso administrativo en lugar del amparo).

> "Si cabe la posibilidad de ejercer una acción reparadora contra la divulgación de un dato falso por parte de una entidad financiera, no cabe hacer lugar al habeas data planteado por existir otras vías idóneas" (CNCom., Sala D, mayo 13/996, *in re* Figueroa Hnos S.A. c/ Banco de la provincia de Santiago del Estero).

Igual sucedió con las vías previas, que suponían transitar por el reclamo administrativo previo para habilitar la instancia jurisdiccional.

> "Corresponde rechazar la acción de habeas data intentada tendiente a actualizar los sobreseimientos dictados a favor del accionante si éste no ha agotado los recursos o remedios administrativos que permitan dar satisfacción a sus pretensiones (art. 2 inciso a ley 16.986 y 43 CN)" Juzgado Nacional de Instrucción nº 12, secretaría nº 137, agosto 29/995, *in re* Rossetti Serra, Salvador s/ habeas data).

La redacción del actual artículo 43 modificó este cuadro de situación, porque sólo establece como condición para el juicio de amparo que no exista una *vía judicial más idónea*.

No se trata de decir que el amparo se ha convertido en un remedio ordinario, sino que, a pesar de mantener su condición excepcional y, por ende, extraordinario, ahora debe confrontar fuerzas con las vías procesales comunes para resolver cuál de ellas es más rápida y expedita y constituye la acción idónea que requiere el hábitat constitucional.

Ahora bien, si hemos afirmado que el habeas data no es una modalidad del amparo, va de suyo que también sostenemos la imposibilidad de establecer un paralelo con el requisito de la vía judicial más útil y efectiva.

Ya se ha dicho que el problema está en que nuestro país no tiene control ni recursos o herramientas en manos de los particulares para poder articular defensas contra las desviaciones del poder en el uso de medios informáticos del Estado o de particulares; y si a consecuencia de ello se difunden datos que perturban o penetran la vida personal, afectando la intimidad de las personas, el perjuicio material es evidente, sin perjuicio de la honda lesión generada en los derechos de la personalidad.

> "El presupuesto fáctico y jurídico del habeas data debe ser la sencilla acreditación objetiva, pues la hipotética complejidad de las cuestiones a interpretar podría atentar contra la *ratio juris* del instituto" (C.1ª Contenciosoadministrativa, Córdoba, marzo 29/995, *in re* García de Llanos, Isabel c/ Caja de Jubilaciones, Pensiones y Retiros de Córdoba).

Por todo ello, el habeas data no sólo es, sino debe ser, una acción directa, especial, autónoma e independiente de las reglas vigentes o previstas para el amparo. La finalidad perseguida es impedir que en bancos, archivos o registros de datos se recopile información respecto de la personas físicas o jurídicas, cuando dicha información esté referida a aspectos de su personalidad vinculados directamente con la intimidad.

La reglamentación prevista por el artículo 37 de la ley simplifica la cuestión:

Primero: se aplica la ley (en sus dos vertientes: o se reclama administrativamente y tras ello se deduce la demanda de protección de datos personales o habeas data; o se plantea directamente esta acción).

Segundo: A falta de reglas previstas, se aplica la acción de amparo común (tanto para archivos públicos, como privados destinados a proporcionar información a terceros).

Tercero: Si las reglas no son suficientes, se remite a las normas procesales que regulan el proceso sumarísimo.

52. Arbitrariedad e ilegalidad del acto.

El objeto que persigue el habeas data pone en dudas la aplicación de los requisitos de arbitrariedad o ilegalidad en el acto que se cuestiona porqué la preocupación procesal que trae esta nueva garantía constitucional consiste en darle a las personas una herramienta útil, rápida y efectiva, para que sin otra condición que ser la vía judicialmente más idónea, se responda al simple requerimiento de entrar a los archivos como un derecho a la información que tiene toda persona, y una vez conocido el contenido de ellos, resolver sobre los datos que la afectan o conciernen.

Teniendo en cuenta esta afirmación, el habeas data procede para dar suficiencia al derecho a la información que tiene toda persona, y para ejercer un control sobre los bancos de datos que almacenan datos individuales que le conciernen. En definitiva, el derecho a la libertad informática y a la autodeterminación informativa.

> El habeas data tiene cinco objetivos principales: a) que una persona pueda acceder a la información que sobre ella conste en un registro o banco de datos; b) que se actualicen datos atrasados; c) que se rectifiquen los datos inexactos; d) que se asegure la confidencialidad de cierta información legalmente obtenida para evitar su conocimiento por terceros; y e) supresión del registro de la llamada "información sensible" (vida íntima, ideas políticas, religiosas o gremiales) (CNContenciosoadministrativa, Sala 4ª , setiembre 5/995, *in re* Farrel, Desmond A. c/ Banco Central de la República Argentina).

La información que proporciona una base de datos, archivo, registro o banco *destinado a proveer informes*, no resulta en sí mismo arbitraria, porqué este concepto supone ejercer con abuso o exceso de autoridad la función para la cual está autorizado a ejercer.

Un dato que se facilita al medio social o privado, es decir, que se transfiere desde el archivo al público por su calidad de dato abierto o de fácil obtención (por ejemplo, información sobre bienes muebles registrables o inmuebles), o aquél que se conoce por adquisición o compra al particular (v.gr.: información crediticia), no es arbitrario sino, en todo caso, la aplicación que de él se haga.

Asimismo, un dato no es arbitrario por salir de su base para constituirse en fuente de información; en todo caso, la arbitrariedad puede ocultar algunas cuestiones de responsabilidad del titular o usuario del archivo para mantener actualizada la base, rectificar ante el pedido del las personas los datos que sean erróneos o produzcan información equivocada, o se niegue la supresión de datos sensibles, etc.

Es decir, *la arbitrariedad no es del dato, propiamente dicho, sino de los actos que el archivo resuelva frente a un expreso pedido del titular de la información* (afectado, en sentido estricto).

> Por eso la jurisprudencia, aun vacilante, establece que el presupuesto fáctico que habilita el ejercicio de la acción de habeas data se constituye cuando los registros públicos o los privados incluyen información inexacta, desactualizada o discriminatoria. La protección que dispensa el art. 43 párrafo tercero, es improcedente si no se demuestra el motivo descalificante o discriminatorio del dato en cuestión, ni que su origen sea la anotación en registros o bases de datos propios o de terceros, ya sean públicos o privados destinados a suministrar información (Cfed. Bahía Blanca, Sala 1ª , enero 18/995, *in re* Gutierrez, Héctor c/ Casino Militar del Personal Superior de la Base Naval de Puerto Belgrano).

Obsérvese que no hay arbitrariedad en el acto de difundir un dato verdadero; tampoco es arbitraria la acción de producir informes personales de quienes están concernidos en las bases o archivos; siendo absurdo privar a estas empresas privadas o a los registros públicos de emitir información que constituye la actividad central prevista y que cumple con el destino para el cual se crearon.

> Se ha dicho que "si el objeto del giro comercial de la empresa accionada se centra en el suministro de información objetiva sobre la actividad comercial y crediticia de las personas, pero no de datos de otra índole, a los que cabe sumar la ausencia de un juicio de valor sobre el sujeto de que se trate, su patrimonio o solvencia, no puede tildarse de parcial, discriminatorio e incompleto (y por ende falso) al informe que se brinda. En tales condiciones no puede obligarse a la empresa a que integre su negocio con un plexo normativo que permita formarse un juicio integral o que suprima la información que a criterio del propio interesado es incompleta, por cuanto es a éste a quien le cabe suministrar estos elementos a las personas que hayan requerido la información sobre él" (CNCiv., Sala M, noviembre 28/995, *in re* Groppa c/ Organización Veraz S.A.).

Si existe arbitrariedad ella se constata en las actitudes que tome el archivo frente al reclamo administrativo tendiente a tomar información que concierne a la persona o que pretenda acceder al mismo, y la negativa a facilitar la información sea irrazonable.

De igual modo, si la base contiene verdades que no son tales o están desactualizadas, y se niega al titular la posibilidad de rectificar o actualizar, sin dar fundamentos atendibles, es también una conducta reprochable que se puede denunciar por la acción de habeas data.

Esta última posibilidad roza con la *ilegalidad* de las conductas que se pueden atacar, porqué si entre los principios que debe cumplir el registro se encuentra el de finalidad, que supone almacenar información para un destino establecido que el afectado conoce, la negativa al derecho de acceso es también un acto ilegítimo o ilegal. Lo mismo se afirma respecto a la congruencia de la información acumulada, esto es, cuando existe abuso potencial por el exceso de datos recopilados para un fin que, en los hechos, requiere de menor información.

> El sujeto afectado tiene el derecho a lograr la supresión del dato obrante en un registro informatizado, cuando el dato sea impertinente para la finalidad perseguida por la base de datos o en el supuesto en que en función del transcurso del tiempo no resulte necesario mantener el dato en el registro. En virtud del tiempo transcurrido, los datos sobre inhabilitaciones para operar en cuenta

> corriente, producidos hace más de diez años se encuentran caducos y el accionante del habeas data tiene derecho a obtener su cancelación. La subsistencia del dato caduco indefinidamente en la base de datos de la demandada impide el derecho al olvido. El dato caduco es el dato que por efecto del transcurso del tiempo ha perdido virtualidad, ha devenido intrascendente a los efectos de cualquier efecto jurídico relativo a la ejecutabilidad (Juzgado Nacional de 1ª Instancia nº 91, marzo 5/996, Falcionelli, Esteban P./ Organización Veraz SA).

La *ilegalidad* del dato es posible cuando la información capturada se transfiere sin consentimiento del afectado, o sin que éste tenga conocimiento de la guarda efectuada.

> Dicen Altmark y Molina Quiroga que un dato personal puede ser correcto y verdadero, pero si se ha recolectado con una finalidad y se emplea con otra, o directamente se almacena con un fin ilícito o socialmente reprochable, debe ser suprimido por cuanto afecta la esfera de reserva del individuo, con independencia de su potencialidad discriminatoria.

De lo expuesto se colige que el acto lesivo que el habeas data controla no proviene de la acción arbitraria o ilegítima que genera el autor del hecho, sino por el contrario, la lesividad proviene de la agresividad que potencialmente manifieste para el afectado los datos que se hubieren registrado.

> "En virtud de la redacción del artículo 43 CN, se desprende que no se ha impuesto limitación alguna respecto de los bienes tutelados, con excepción de las que surgen del párrafo primero referido al amparo genérico, y la que deviene del hecho de que la agresión se produzca mediante datos o informaciones inexactas existentes en el registro" (CNCiv., Sala F, Julio 6/995, *in re* Bianchi de Saenz, Delia c/ Sanatorio Greyton S.A.).

De este modo, el gravamen que habilita la revisión puede ser clasificado de la siguiente manera:

a) *Arbitrariedad derivada de la conducta del titular, usuario o responsable de la base de datos* (por ejemplo, cuando deniega el acceso sin dar fundamentos para ello; rechaza la documentación que demuestra la inexactitud del registro, o se niega a dar información).

b) *Ilegalidad deducida del contenido del archivo, registro o banco de datos*, como resulta la colección de información lograda por medios intrusivos o invasivos de la intimidad personal, sin conocimiento de la persona afectada.

c) *Ilegalidad del archivo por violación de los deberes de información*, que ocurren cuando se pone en circulación datos personales no autorizados; o se los destina a efectos diferentes a los comunicados al titular; o se les cambia la finalidad.

d) *Ilegalidad del archivo, en sí mismo*, caso donde no se trata de recuperar el derecho a la autodeterminación informativa sino de resolver la legitimidad del banco de datos que presta información o produce informes sin tener autorización legal para obrar en esa dirección.

53. La discriminación como argumento para el habeas data

El artículo 43 establece que la acción de amparo (en el supuesto de admitir que la norma se refiere a esta garantía) procede "contra cualquier forma de discriminación", concepto que encierra múltiples posibilidades de interpretación.

En el caso de los datos personales, *prima facie*, se pueden encontrar dos inteligencias previas: a) que el archivo no discrimine o distinga sus registros estableciendo diferencias irritantes para las personas, y b) que el registro informativo no sea fuente para violar el principio de igualdad entre los hombres.

> Explica Falcón que la voz "discriminación" significa dar trato de inferioridad a una persona o colectividad por motivos raciales, religiosos, políticos, gremiales,

> ideológicos, sexuales, sociales, etc. En algunos casos existe una zona gris donde la discriminación de este último tipo se realiza a través de sutiles maniobras y desplazamientos. La discriminación se ha desarrollado del modo más grave para la especie humana usando distintos grados, pero siempre fundada en prejuicio, ignorancia y temor.

El primer caso supone la formación de perfiles distintivos que provocan una directa afectación de las personas concernidas, al establecer entre ellas diferencias provenientes de datos sensibles que las clasifica. Por ejemplo, ordenar y procesar los datos según las preferencias, costumbres o ideologías (datos sensibles) de las personas.

En este grupo se pueden establecer como discriminatorios los registros individuales de tipo médico o científico que transmiten a terceros esta información con el fin de reconocer el riesgo de vida de cada uno (v.gr.: para la venta de pólizas de seguros); o la formación de perfiles de acuerdo con las convicciones políticas registradas; entre otras bases similares.

El segundo grupo es aquél que al circular el dato permite diferenciar a las personas y establecer entre ellas diferencias perjudiciales o perturbadoras para su vida personal.

Indicar en un informe las creencias políticas o religiosas de alguien, sin que ese dato sea necesario para el fin que se pide, es una muestra de lo dicho.

> Se ha dicho que la finalidad del habeas data es impedir que en bancos o registros de datos se recopile información respecto de la persona titular del derecho que interpone la acción, cuando dicha información esté referida a aspectos de su personalidad que se hallan directamente vinculados con su intimidad (CNCiv., Sala H, mayo 19/995, *in re* Rossetti Serra, Salvador c/ Dun & Bradstreet).

La discriminación no solamente se alega; también debe ser demostrada la descalificación sufrida a consecuencia del dato proporcionado.

> Si no se encuentra verosímilmente demostrado el motivo descalificante o discriminatorio, y que su origen sea la anotación en registro o base de datos propios o de terceros, ya sean públicos o privados destinados a suministrar información, la acción de habeas data resulta improcedente (C.Fed. Bahía Blanca, Sala 1ª , enero 18/995, *in re* Gutiérrez, Héctor R. c/ Casino Militar del Personal Superior de la Base Naval Puerto Belgrano).

La ley fundamental es confusa al respecto porqué al señalar la procedencia del habeas data para tomar conocimiento de los datos referidos a una persona y permitir que ésta, en caso de falsedad o discriminación, exija las acciones correctivas pertinentes, no esclarece el alcance de ambos conceptos. Tampoco lo ha resuelto la ley reglamentaria.

En particular, algunos sostienen que no se puede calificar de discriminatoria la acción de suministrar información comercial y crediticia si son los terceros que hacen uso de ella los que en definitiva discriminan al informado que posee antecedentes negativos.

> La información que proporciona la empresa de datos comerciales no es de por sí sola discriminatoria. Ello por cuanto contiene datos objetivos relativos a la actividad crediticia del accionante, obtenidos de medios oficiales. Las opiniones que transcribe el recurrente sobre el valor que se le asigna a la información crediticia que brindan empresas como la de la demandada, resultan irrelevantes a los fines de decidir la presente causa. Asimismo, no pude calificarse de discriminatoria la actividad de suministrar dichos informes, si –como el propio recurrente lo reconoce- son los terceros que hacen uso de ella los que en definitiva discriminan al informado con antecedentes negativos (CNCiv., Sala M, noviembre 28/995, *in re* Groppa c/ Organización Veraz S.A.).

La falsedad se distingue de la discriminación. Falso es aquello que disimula lo verdadero, oculta la realidad o esconde las intenciones mostrando una actitud aparente.

Si observamos estas condiciones en los informes de uso comercial o financiero, se puede extraer que no existe falsedad propiamente dicha, aunque haya inexactitud o falta de actualidad. Mientras la falsedad se corrige suprimiendo de la base de datos la información almacenada; la inexactitud o falta de actualización se rectifica con las acciones consecuentes que el habeas data permite. No se borra el dato, simplemente se lo conserva en el registro o archivo pero puesto al día.

> Sostiene Palazzi que debe distinguirse la falsedad de la discriminación en cuanto a sus efectos. En el primero sólo tendrá sentido pedir supresión, rectificación o actualización, pero no la confidencialidad. En el segundo caso, el paso más lógico parece pedir la supresión del acto lesivo…Una vez que se ha tomado conocimiento del dato y de su finalidad, se deberá probar que existe una falsedad o una discriminación para poder acceder a los otros derechos. En cuanto a la falsedad, será necesario demostrar que el dato no está de acuerdo con la realidad…La supresión busca eliminar el dato erróneo –falso o discriminatorio-, que afecta la verdad o la igualdad…Frente a esta premisa, el borrado del dato enfrenta el derecho de propiedad del operador del banco de datos con la privacidad del individuo registrado. Creemos –concluye- que la solución adecuada –que contemple ambos valores-, consistirá en eliminar el dato si se logra probar que el mismo es falso o erróeno o que causa algún perjuicio. En este sentido la tipología que adopta nuestro habeas data, al permitir suprimir el dato sólo si hay discriminación o falsedad parece haber querido conciliar ambos valores.

En conclusión, el habeas data nacional tiene varias puertas de entrada, a saber:

a) Por la arbitrariedad de los actos del titular, usuario o administrador responsable del archivo.

b) Por la ilegalidad interna del archivo, registro o banco de datos.

c) Por la ilegalidad del archivo por informar datos sensibles.

d) Por la ilegalidad del archivo que niega los derechos de entrada y control sobre el mismo.

e) Por la discriminación que tenga la base de datos al formar y procesar los datos personales.

f) Por la discriminación que provoque la información circulada a terceros.

g) Por la falsedad que porte la información adquirida, y

h) Por los derechos que en particular se persiga proteger a partir de la acción constitucional.

54. Bilateralidad o contradicción atenuada

En varios pasajes de esta obra se ha destacado el carácter de proceso constitucional que tiene el habeas data, y la consecuencia que esta figura tiene en torno a la condición que asume el procedimiento.

Si la función del Juez será controlar efectivamente el cumplimiento de los mandatos constitucionales, respetar el principio de la supremacía constitucional, fiscalizar la legalidad del comportamiento administrativo y, en su caso, asegurar a las partes el equilibrio e igualdad en el desarrollo de sus posiciones y para la decisión final que proceda; si esta es la función jurisdiccional en los procesos constitucionales, queda en claro que el principio dispositivo, por el cual el proceso es cosa entre partes, queda difuminado y obliga a una inteligencia diferente.

El artículo 37, recordemos, aplica el trámite del amparo al proceso de habeas data, y supletoriamente, las normas del código procesal civil y comercial en lo atinente al juicio sumarísimo.

Este cauce otorgado no es contencioso, tampoco supone entablar una controversia entre partes con posiciones distintas. Se trata, únicamente, de encontrar si el archivo, registro o banco de datos denunciado ha incluido en su base a la persona afectada y, en su caso, le ha brindado la totalidad de derechos que la Constitución Nacional le dispone conforme al artículo 43.

Por eso, el artículo 39 señala que "*admitida la acción el Juez requerirá al archivo…la remisión de la información concerniente al accionante…";* pudiendo inclusive solicitar informes sobre el soporte técnico de datos, y documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa.

El archivo debe producir el informe que el Juez le requiere; no está obligado a contestar la demanda en las reglas tradicionales de la *litis contestatio*, esto es, respondiendo uno a uno los hechos por el reconocimiento, la admisión o la negación de ellos.

El banco de datos debe informar cómo actuó frente al derecho de acceso planteado, o en su caso, con las pretensiones de control sobre el archivo que se le hubieran planteado.

Si la demanda o el requerimiento judicial fuera la primera oportunidad para hacerse oír podría actuar en los términos desarrollados en el punto 48 y apartados; pero siempre debe quedar en claro, que la bilateralidad no es estricta, apenas se trata de una contradicción atenuada con una firme intervención judicial.

Bibliografía Capítulo XIII

Altmark, Daniel R. – Molina Quiroga, Eduardo, *Habeas data*, en Revista La Ley, 1996-A, 1565.

Falcón, Enrique M., *Habeas data*, editorial Abeledo Perrot, Buenos Aires, 1996.

Gozaíni, Osvaldo Alfredo, *Derecho Procesal Constitucional*, tomo 1, editorial de Belgrano, Buenos Aires, 1999.

Gozaíni, Osvaldo Alfredo, *La justicia constitucional*, editorial Depalma, Buenos Aires, 1994.

Leguisamón, Héctor Eduardo, *Procedimiento y aspectos procesales del habeas data*, en Revista de Derecho Procesal, nº 4, editorial Rubinzal Culzoni, Buenos Aires, 2.000.

Palazzi, Pablo, *El habeas data en la Constitución Nacional (La protección de la privacidad en la "era de la información")*, en Jurisprudencia Argentina del 20 de diciembre de 1995.

Serra, Mercedes, *Habeas data: problemas que plantea su implementación*, comunicación presentada al XX Congreso Nacional de Derecho Procesal (San Martín de los Andes, octubre 1999).

CAPÍTULO XIV. Jurisprudencia local

55. Derechos protegidos. Subtipo de amparo. Competencia.

Autos: Rossetti Serra, Salvador c/ Dun y Brandstreet SRL. (CNCiv., sala H, mayo 19-995).

1) *El habeas data, garantia constitucional introducida por la reforma, es una variable del derecho a la intimidad consagrado en el art. 19 CN.*
2) *El objeto tutelado por el habeas data es un derecho individual personalísimo: el derecho a la intimidad definido como el derecho a decidir por sí mismo en que medio se compartirán con los demás los pensamientos, sentimientos y los hechos de la vida personal.*
3) *La finalidad del habeas data es impedir que en bancos o registros de datos se recopile información respecto de la persona titular del derecho que interpone la acción, cuando dicha información esta referida a aspectos de su personalidad directamente vinculados con su intimidad, que no puede encontrarse a disposición del publico o ser utilizados en su perjuicio por órganos publicos o entes privados. Se trata, particularmente, de información referida a la filiación politica, las creencias religiosas, la militancia gremial, el desempeño en el ámbito laboral o académico, etc.*
4) *El habeas data es una variable del género amparo, como tutela de los derechos consagrados en la legislación nacional*
5) *Como el habeas data es una acción iniciada por un particular para que se tutele su derecho a la intimidad, son competentes los tribunales civiles.*

Hechos: Un particular (legitimado activo), inicia una acción de habeas data contra una empresa privada (legitimado pasivo) a fin de que se tutele su derecho a la intimidad. La Cámara decide que nada impide que sea un tribunal con competencia civil quien entienda en la causa, precisando en la providencia el círculo de derechos que la garantía constitucional consagra.

55.1 ***Derechos protegidos. Legitimación para actuar.***

Autos: Urteaga, Facundo R. C/ Estado Mayor Conjunto de las Fuerzas Armadas, CSJN, octubre 15/998, La Ley, 1998-F, 237 y ss.

1) *La ausencia de normas regulatorias de los aspectos instrumentales de la acción de habeas data no es óbice para su ejercicio, incumbiendo a los órganos jurisdiccionales determinar provisoriamente -hasta tanto el Congreso de la Nación proceda a su reglamentación-, las características con que tal derecho habrá de desarrollarse en los casos concretos.*
2) *Debe admitirse la legitimación invocada por quien reviste la calidad de hermano de quien se supone fallecido, toda vez que la habilitación para accionar de un familiar directo con sustento en el derecho de que se proporcione información, configura una de las alternativas de reglamentación posibles de la acción de habeas data.*

3) *Las garantías individuales existen y protegen a los individuos por el sólo hecho de estar consagradas en la Constitución, e independientemente de las leyes reglamentarias.*

4) *La pretensión del actor-destinada a tener acceso a los datos obrantes en los registros estatales, militares o civiles, de donde pudiera resultar el destino de su hermano desaparecido durante las luctuosas circunstancias que vivió el país-, no debe ser apreciada en el marco jurídico del específico amparo informativo-habeas data-, sino en el amparo en general (Del voto de los Dres. Belluscio y López).*

5) *Si bien el art. 43, cuarto párrafo, de la Constitución Nacional, contempla la acción de hábeas corpus en los supuestos de desaparición forzada de personas, no es razonable -atento el tiempo transcurrido-, imponer a quien reclama información sobre una persona desaparecida, hacerlo a través del hábeas corpus, pues ello conduciría a la frustración de su derecho a conocer la verdad de los hechos, en la medida en que pueda constar en registros o bancos de datos públicos (Del voto de los doctores Belluscio y López).*

6) *La garantía del habeas data -dirigida a que el particular interesado tenga la posibilidad de controlar la veracidad de la información y el uso que de ella se haga-, forma parte de la vida privada y se trata, como el honor y la propia imagen, de uno de los bienes que integran la personalidad. (Del voto del doctor Fayt).*

7) *El control sobre los datos acumulados y procesados en registros o bancos de datos públicos y privados-derecho individual reconocido únicamente al afectado, tiene tres dimensiones: la de conocer, la de acceder y la de rectificar. (Del voto del doctor Fayt).*

8) *El habeas data -en tanto garantía de un derecho individual, personalísimo-, sólo puede ser ejercido por el titular del derecho a interponer la acción, en defensa de aspectos de su personalidad, vinculados con su intimidad, que no pueden encontrarse a disposición del público ni ser utilizados sin derecho. (Del voto del Dr. Fayt).*

9) *La aparición del habeas data no puede aparecer como una sustitución del hábeas corpus, cuya función para la defensa de la libertad física sigue siendo plenamente vigente, sino que se trata de una garantía para nuevas agresiones a otras facetas de la libertad. (Del voto del Dr. Petracchi).*

10) *Proteger el derecho a conocer todo lo relativo a la muerte de un familiar cercano -ocurrida en las luctuosas circunstancias que vivió el país- significa reconocer el derecho a la identidad y a reconstruir la propia historia, los cuales se encuentran estrechamente ligados a la dignidad del hombre. (Del voto del doctor Petracchi).*

11) *El derecho del habeas data puede hacerse valer por cualquier vía procesal razonable, aun la incidental, hasta tanto una ley reglamente su ejercicio (art. 28 Constitución Nacional). (Del voto del Dr. Boggiano).*

12) *Entre los atributos de la persona humana se encuentra el derecho a conocer el destino de aquellas personas con las que existen vínculos familiares. (Del voto del Dr. Bossert).*

13) *Los derechos de los hombres que nacen de su propia naturaleza, no pueden ser enumerados de manera precisa. No obstante dicha deficiencia de la letra de la ley, ellos forman el derecho natural de los individuos y de las sociedades, porque fluyen de la razón del género humano, del objeto mismo de la reunión de los hombres en una comunión política y del fin que cada individuo tiene derecho a alcanzar (Del voto del Dr. Bossert).*

14) *Los vínculos familiares, que determinan el estado de la familia integran la identidad de la persona. (Del voto del Dr. Bossert).*

15) *Aunque el párrafo tercero del art. 43 del la Constitución Nacional organiza la acción de habeas data con requisitos propios y determinados objetivos, se trata de una forma específica de la acción de amparo -establecida en términos genéricos en el párrafo primero-, por lo que no excluye otra forma de indagación de datos asentados en registros públicos o privados a través de dicha acción. (Del voto del doctor Bossert).*

16) *La interpretación de las leyes debe hacerse armónicamente teniendo en cuenta la totalidad del ordenamiento jurídico y los principios y garantías de raigambre constitucional, para obtener un resultado adecuado, pues la admisión de soluciones notoriamente disvaliosas no resulta compatible con el fin común, tanto de la tarea legislativa como de la judicial. (Del voto del Dr. Bossert).*

Hechos: Facundo R. Urtega dedujo acción de habeas data contra el Estado Nacional y/o el Estado Mayor Conjunto de las Fuerzas Armadas y/o el Gobierno de la Provincia de Buenos Aires con el objeto de obtener información que exista en los Bancos de Datos de la Secretaría de Informaciones del Estado, Servicio de Inteligencia del Ejército, Servicio de Informaciones de la Armada, Servicio de Informaciones de Aeronáutica, Servicio de Inteligencia de la Policía Federal, Servicio de Informaciones de la Policía de la Provincia de Buenos Aires y Servicio de Inteligencia de la Provincia de Buenos Aires y/o cualquier otro del Estado Nacional, de las Fuerzas Armadas y del Gobierno de la Provincia de Buenos Aires, sobre su hermano Benito Jorge Urteaga, supuestamente abatido el día 19 de julio de 1976 en un departamento ubicado en la localidad de Villa Martelli, Partido de Vicente López, Provincia de Buenos Aires.

El juez de primera instancia rechazó in límine la pretensión examinando el art. 43 de la Constitución Nacional, y concluyó que la acción de habeas data sólo podía ser interpuesta por la persona a quien se refieren los datos que consten en los registros públicos o privados. Destacó asimismo que la vía apta para el caso era el hábeas corpus, ya que puede ser interpuesto por cualquier persona a favor del afectado y se encuentra específicamente establecida para el caso de desaparición forzada de personas. El otro argumento fue que la finalidad que se pretendía con la interposición de esta acción no se compadece con la que surge del texto constitucional.

La Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal confirma la decisión de primera instancia, por lo cual el actor deduce recurso extraordinario federal ante la Corte Suprema de Justicia de la Nación, el cual resultó formalmente procedente pues se encuentra en tela de juicio la interpretación de la garantía constitucional consagrada por el art. 43 CN y el alcance que le ha sido asignado resultó contrario a las pretensiones del recurrente.

La Corte Suprema establece que la interpretación del a quo importa un excesivo rigor formal que deja sin protección el derecho invocado por el recurrente que no resulta ajeno al bien jurídico tutelado ni al propósito del constituyente.

También establece que lo afirmado por la alzada en cuanto a que la finalidad perseguida en la presente acción no se compadece con el texto constitucional, se aparta de las constancias de la causa. Ello es así en la medida en que la presentación inicial incluia la de obtener la información existente en registros o bancos de datos públicos que permita al recurrente establecer el fallecimiento de la persona desaparecida y, en su caso, conocer el destino de sus restos, es decir, acceder a datos cuyo conocimiento hace al objeto de la garantía que se trata.

Por consiguiente la Corte Suprema declara procedente el recurso extraordinario interpuesto, y dispone el libramiento de oficios a fin de que los organismos requeridos den cuenta de si en sus registros obra constancia del fallecimiento de Benito Jorge Urteaga y, en su caso, la localización de sus restos.

55.2 . ***Procedencia. Diligencias preliminares. Prueba anticipada***

Autos: Bianchi de Sáenz, Delia A. c/ Sanatorio Greyton S.A., CNCiv., sala F, julio 6-995.

1. *El habeas data se explica en virtud del desarrollo del llamado "poder informático". Es una acción que tiende a proteger los derechos de los "registrados" en los archivos o bancos de datos, que pueden contener información equivocada, antigua, falsa o con potenciales fines discriminatorios, o lesiva del derecho a la intimidad de las personas. De ahí que el promotor del habeas data tendrá que alegar, para tener buen resultado, que los registros del caso incluyen informacion que es inexacta, o que puede provocarle discriminación.*
2. *El habeas data no es la via apta para obtener una historia clínica por parte del sanatorio demandado que se niega a entregarla.*

3. *Si bien el habeas data deducido por la actora para lograr que el sanatorio demandado le entregue su historia clínica es improcedente para tal fin, el principio "iura novit curia" autoriza a los jueces a efectuar la calificacion juridica de las pretensiones de las partes. En consecuencia puede encuadrarse la cuestion en las disposiciones contenidas en el art. 323 CPCC.*

4. *Las diligencias preliminares no necesariamente deben ser el antecedente de una demanda. Su promoción se limita a la exhibición de una cosa mueble, un título, documentos, elementos útiles al interesado en un proceso posterior, cuya iniciación y modalidades pueden depender del resultado de la diligencia.*

Hechos: La actora fue internada en el Sanatorio Greyton para ser operada de una fractura de cadera. Al día siguiente de la operación, y por razones que desconoce, su estado de salud comenzó a agravarse. Ante la pasividad del personal del sanatorio que retaceaba explicaciones acerca de las complicaciones, su hija recurrió al asesoramiento de un médico que evaluó que debía ser internada inmediatamente en terapia intensiva. Para ello, la hija solicitó el traslado de su madre al Hospital Británico culpando de negligentes al personal del Sanatorio. Previo a autorizar el retiro, las autoridades del Sanatorio exigieron a la hija firmar una declaración asumiendo la responsabilidad del traslado, conocer el estado de salud de la enferma y "prestar conformidad" con la historia clínica, documento del cual no se le permitía sacar fotocopias

Una vez internada en el Hospital Británico en terapia intensiva y con diagnóstico, el nuevo médico solicitó al Sanatorio la historia clínica pero le fue denegada.

Con este fin promueve acción de amparo (habeas data).

En principio, la decisión del juez a quo de rechazar el amparo es irreprochable en cuanto a que no es dudoso concluir que la actora no ha escogido el camino adecuado.

Pero por aplicación de la regla "iura novit curia", el juzgado puede decidir el proceso aplicando distintas normas a las invocadas.

Se habló de una actuación negligente de la damandada, por lo que bien podrían traerse a este caso las disposiciones contenidas en el art. 323 CPCC., y asi obtener la información requerida, a pesar de ser utilizada para un fin distinto que el común. Es que si bien las diligencias preliminares son el antecedente de una demanda, de ello no se sigue que necesariamente tenga que ser asi.

De este modo, se confirma el rechazo "in limine" del amparo (habeas data), pero se ordena el secuestro de la historia clínica.

55.3 Medidas cautelares

Autos: Yusin, Mauricio G. c/ Organización Veraz S.A. S/ Sumarísimo s/ Incidente de apelación, CNCom, Sala B, agosto 9/996, ED, 173-15 y ss.

Hechos: El actor procura que la demandada suprima de sus registros cierta información que se aduce ser inexacta. Requirió además una medida cautelar tendiente a que se produzca la supresión de los datos mientras tramite el pleito.

Juzgóse insuficientemente acreditado el peligro en la demora y la verosimilitud del derecho invocado, por lo cual se desestimó el pedido. El actor apeló esta resolución. La Sala, para mejor proveer, requirió el aporte de datos atinentes a los extremos denunciados y luego, como consecuencia, apareció objetivamente verosímil la indicación de que se informa con inexactitud sobre la situación patrimonial del denunciante, en el sentido de que se informa a terceros que el actor regularizó una operación de préstamo supuestamente celebrada con el Banco Galicia y Buenos Aires S.A., pero ocurre que dicha institución parece no tener registrados con respecto al negocio mismo.

El peligro en la demora se acredita de la siguiente manera: de mantenerse la situación de hecho aparentemente irregular, la ejecución de una sentencia favorable puede convertirse en ineficaz, en tanto que la difusión anterior a su dictado es susceptible de influir definitivamente en el ánimo de quienes sabrían del dato en cuestión.

Se concede el recurso y se manda que la demandada se abstenga de brindar el dato referido, hasta tanto concluya el proceso principal.

56. Necesidad de mayor debate y prueba. Arbitrariedad e ilegalidad manifiesta.

Autos: Automotores Santa María S.A. c/ Banco de la Provincia de Santiago del Estero s/ Sumarísimo, CNCom., Sala A, octubre 4/996, ED, 173-13 y ss.

1) El amparo es un remedio excepcional que sólo resulta utilizable en delicadas y extremas situaciones en las que, por carencia de otras vías aptas, peligra la salvaguarda de derechos fundamentales.

2) En los casos en que se discute la inteligencia de un convenio regido por el derecho privado, la existencia de una vía legal para la protección de los derechos que se dicen lesionados excluye, como regla, la admisibilidad del amparo, ya que esta vía no resulta apta para alterar el juego de la instituciones vigentes, ni para justificar la extensión de jurisdicción legal y constitucional de los jueces.

3) El amparo no debe ser admitido cuando la dilucidación de las cuestiones planteadas adquiere un grado de complejidad tal que excede de este remedio sumarísimo.

4) Para la procedencia de la acción de amparo, debe acreditarse el daño grave e irreparable que se produciría remitiendo el examen de la cuestión a las vías del procedimiento ordinario.

5) Habiendo adoptado la reforma constitucional el modelo de la ley 16.986, ha dejado librado a apreciación del juez la viabilidad del amparo sólo para aquellos supuestos en los que la arbitrariedad e ilegitimidad sea manifiesta.

6) La acción tendiente a que se declare la inexistencia de saldo deudor en una cuenta bancaria, es un conflicto entre dos derechos privados que no corresponde dilucidar a través de la instancia sumarísima del amparo.

7) El remedio excepcional del amparo no puede ser utilizado cada vez que los contratantes discutan el alcance de un contrato y pretendan mantener provisoriamente una cierta situación de hecho existente hasta ese momento.

8) Puesto que, en el caso, no se está en presencia de un supuesto de arbitrariedad o ilegitimidad manifiesta en el proceder del banco accionado que torne procedente la acción de amparo, la eventual inexistencia de saldo deudor en cuenta corriente que subyace en el planteo de la recurrente sólo puede ser determinada a través de un mayor debate o prueba, impropios del recurso de amparo.

9) El hecho de que la recurrente no haya acreditado no contar con otros procedimientos idóneos que puedan remediar sus agravios, es una circunstancia obstativa a la procedencia de la vía del amparo.

10) Los asientos contables de una entidad bancaria, aunque ésta sea de carácter público, no constituyen registros o bancos de datos públicos en los términos del art. 43 de la Constitución Nacional ya que se trata de meros datos jurídicos y contables referidos a un contrato de derecho privado en el que es parte la entidad y que no están destinados a su divulgación.

Hechos: Automotores Santa María S.A. y el Banco de la Provincia de Santiago del Estero se hallaban vinculados por un contrato de cuenta corriente bancaria. La institución bancaria demandada establece que existe un saldo deudor a cargo de la actora, motivo por lo cuál ésta última interpone una acción de habeas data tendiente a que el demandado informe si en sus registros existe constancia de alguna deuda de aquélla hacia éste último y, en su caso, que elimine los datos falsos o erróneos que pudiera tener registrados. La sentencia rechaza la demanda, y es por esta razón que se recurre.

De acuerdo con los antecedentes, el carácter de la institución bancaria no fue motivo de atención en el caso, cuando debió serlo para caracterizar si es una entidad destinada a proveer informes o, en todo caso, el registro de clientes es un archivo público.

Se prefirió destacar la complejidad del caso y la necesidad de un mayor debate y prueba.

La importancia del precedente está en que se adopta el carril del amparo para tramitar la litis, y se elimina la procedencia sobre el presupuesto de la arbitrariedad o ilegalidad manifiesta que se dice está ausente.

56.1 Necesidad de mayor debate y prueba. Costas

Autos: Diaz Cisneros, Adriano c. B.C.R.A. y otro, CNFed. Contenciosoadministrativo, sala I, abril 29/997.

1. *Las cuestiones atinentes a la responsabilidad que les cabria a las demandadas por la incorrecta información que contiene en sus bases de datos no puede ser tratada en la acción de habeas data sino que debe ser ponderada en juicio de conocimiento posterior.*
2. *En las acciones de habeas data no resulta procedente la eximición de costas del art.68, parr.2º del Cod. Procesal fundado en el argumento de que la falsa o incorrecta información que brindo la demandada fue suministrada por otra entidad.*

Considerando: Que a fs. 90/104 la juez a cargo del Juzgado Nº 7 del fuero hizo lugar a la acción interpuesta por el actor, y ordenó al Banco Central de la República Argentina a rectificar los datos que pudieran constar en sus archivos relativos a Adriano Diaz Cisneros en el plazo de 10 dias. Tambien condenó a la codemandada Organización Veraz S.A. a rectificar los mismos datos en igual plazo, debiendo hacer saber a los clientes de la rectificación operada. Las costas del pleito las impuso a la demandadas vencidas, por mitades.

Que contra la forma en que fueron impuestas las costas, Organización Veraz S.A. interpuso recurso de apelación.

Sostiene que se la debe eximir de las costas ya que no es responsable de los errores registrados en las bases de datos por la errónea información proporcionada por el Banco de Galicia y Buenos Aires, que no fue demandado en este juicio.

Lo relativo a la responsabilidad de las codemandadas respecto a su conducta excede el marco de la presente acción y deberá ser ponderado, eventualmente, en un proceso de conocimiento posterior.

Se resuelve: confirmar la sentencia apelada en cuanto haya sido materia de agravios, con costas por no haber motivo para su dispensa.

El fallo tiene varias cuestiones que atender:

Un primer tema se da con la intervención que probablemente plantea contra el Banco, al cual considera responsable por la errónea información.

En rigor, casi es mayor la responsabilidad del que copia, sin control, información falsa proveniente de terceros, y la hace propia, que el que se equivoca la primera vez. Obviamente, le cabe a quien elabora una base de datos sobre terceras personas asegurarse de que sus fuentes sean fidedignas y sus datos, correctos; si no lo logra, le corresponde como mínimo las costas del juicio que su error en la fuente y su deficiente control han hecho necesario, sin perjuicio del derecho que le pudiere asistir contra el proveedor originario de la información falsa. Es decir que el actor puede optar por demandar también al que primero originó la información falsa.

56.1 Arbitrariedad e ilegalidad manifiesta

Autos: Basigaluz Saez, Laura Ema c/ Banco Central de la República Argentina s/ habeas data (art. 43 CN). CNCiv. y Com.Fed., Sala III, mayo 21/998.

1. *El habeas data, que puede ser calificado como un " amparo informativo" o "amparo informático", prevé en nuestro derecho cinco metas fundamentales: acceder a la información, rectificarla, actualizarla, suprimirla y asegurar su "confidencialidad", sin embargo, como requisito de admisión formal de su trámite, el promotor de dicho remedio deberá alegar que los registros del caso incluyen información que es inexacta o que puede provocarle discriminación, debiéndose además, tenerse presente que, como variable que es de la acción del amparo, el habeas data está sometido a las previsiones constitucionales de aquélla, entre las cuales se encuentra la necesidad de que el acto lesivo padezca de una "arbitrariedad o ilegalidad manifiesta".*
2. *No cuadra emplear el camino de habeas data como vehículo de cualquier pedido de informes.*

Una vez más se ratifica el criterio jurisprudencial que exige para la procedencia del habeas data la arbitrariedad o ilegalidad manifiesta del acto.

56.3 Tipo de amparo. Información falsa o errónea.

Autos: Pochini, Oscar y otro c. Organización Veraz S.A., CNCiv., sala A, septiembre 8/997.

1- *El art.43, parr.3º de la Constitución Nacional establece una subespecie de amparo o amparo específico, conocido en el derecho comparado como habeas data, que algunos califican como "amparo informativo" o "amparo informático".*
2- *El habeas data prevé cinco metas fundamentales: acceder a la información, rectificarla, actualizarla, suprimirla y asegurar su "confidencialidad". Sin embargo, como requisito de la admisión formal de su trámite, el promotor de dicho remedio, deberá alegar que los registros del caso incluyen información que es inexacta o que puede provocarle discriminación. Además, como variable de la acción de amparo, el habeas data esta sometido a las previsiones constitucionales de aquella, entre ellas, la necesidad de que el acto lesivo padezca de una arbitrariedad o ilegalidad manifiesta.*
3- *La información brindada por la demandada no puede incursionar en el terreno del honor e intimidad de los actores y con ello resultar discriminatoria en su vida de relación por orientarse a actividades de índole estrictamente comercial y crediticia.*
4- *Dado que no se acreditó, ni se invocó que la información brindada por la demandada sea falsa o errónea, y que aun no ha transcurrido el plazo de diez años desde el vencimiento de la inhabilitación que pesaba sobre los actores, no es arbitraria o producto de un excesivo rigor informático. La conservación de ese dato en los archivos de la demandada, y su información a*

quienes se encontraren legitimados para ello, en concordancia con la obligación mercantil del art.67 del Cód. de Comercio, según la cual ese es el periodo de conservación de los libros y documentación, a su vez exigida por el art.44 de ese cuerpo legal.

Hechos: Se agravian los accionantes contra la resolución de fs. 85/89 en cuanto allí el *a quo* rechaza el "habeas data" promovido por su parte.

En el caso, la alzada insiste en el temperamento del habeas data como modalidad o tipo de amparo, y como tal, le asigna los mismos requisitos de admisibilidad. Por ello dice que no se advierte en los términos en que ha sido propuesta la pretensión, la concurrencia de los recaudos mínimos necesarios que la tornen procedente. Los interesados no han cumplido con la carga de justificar la manifiesta arbitrariedad que debe animar el grave y excepcional remedio que se intenta.

56.4 Falsedad. Desactualización de los datos.

Autos: Rodriguez, Rafael Jacinto c/ Organización Veraz S.A. s/ Sumarísimo, CNCom., Sala C, septiembre 6/996, ED,173- 88 y ss.

1) *Dado que las disposiciones constitucionales regulatorias del habeas data exigen como presupuesto de admisibilidad del mismo que se haya configurado una hipótesis de falsedad o desactualización de cierta información concerniente al actor, dicha acción deberá ser desestimada si, como en el caso, los datos en los cuales se fundó la misma, han resultado ser ciertos y subsistentes.*
2) *Si no ha quedado acreditado que los datos concernientes al estado patrimonial del amparista hubiesen sido divulgados indiscriminadamente o fuera del marco de confidencialidad que impone este tipo de información-ya que la empresa demandada sólo la transmitió a empresas crediticias, sin exorbitar su función dirigida al saneamiento del crédito-, cabe concluir que no se observan en autos reparos constitucionales o legales en punto a eventuales molestias que tal proceder pudiera haber suscitado, que hagan procedente la vía prevista por el art. 43 del la Constitución Nacional.*

Hechos: La Organización Veraz S.A. informó que el Banco de Boston había entablado una demanda ejecutiva contra el Sr. Rafael Jacinto Rodriguez, en 1991, por el cobro de cierta suma de dinero devengada en una cuenta corriente. También dio a conocer que la cónyuge del actor había sido igualmente demandada, aunque luego se desistió de la acción ejecutiva contra ella. Para el actor, esta información, le provocaba serios perjuicios por cuanto le dificultaba el acceso al crédito. Solicita que una vez comprobada la falsedad de los datos difundidos, se ordene su rectificación.

La demandada contesta estableciendo los fundamentos de su constitución como sociedad los cuales son lícitos y útiles a los fines de promover el acceso al crédito. Pone de resalto que tuvo acceso a los datos del juicio ejecutivo de la publicación periódica que realiza la Cámara, y que dicha información la dio a conocer solamente a la entidad interesada, la cual quedó comprometida a guardar su confidencialidad.

La jueza de primera instancia rechazó la demanda, considerando, mediante un informe del Juzgado en donde tramitó dicho proceso de ejecución, que los datos publicados por la demandada no eran falsos.

Planteada apelación, la alzada interpreta que, el recurrente no cuestiona la cuestión principal de la sentencia de primera instancia, que es la autenticidad del dato publicado. Es más, al tiempo de presentar el Juzgado su informe, la ejecución continuaba adelante, sin que el se hubiera saldado y con los autos provedido el auto de subasta.

Por lo que parece subsistir el dato dado a conocer por la demandada. Con estos hechos, el habeas data no tendría fin, por que ni siquiera hay desatualización en los datos.

El recurrente no ha especificado el daño sufrido. Por todos estos fundamentos se confirma la sentencia de primera instancia.

56.5 Falsedad o discriminación.

Autos: Lapilover, Hugo Daniel c/ Organización Veraz S.A. s/ Sumarísimo, CNCom., Sala E, marzo 20/1997, ED,173-20 y ss.

1) La acción de habeas data tendiente a obtener que la demandada suprima de sus registros y boletines periódicos los datos relativos a cierta inhabilitación como cuenta correntista impuesta al actor por el Banco Central de la República Argentina, debe ser desestimada, dado que dicha información no puede ser considerada falsa o discriminatoria, tal como lo exige el art. 43 de la Constitución Nacional. En efecto, más allá de que, en el caso, la mentada inhabilitación efectivamente existió, los antecedentes comerciales o bancarios no son datos inherentes a la personalidad que se hallen amparados por el principio de confidencialidad; por el contrario, el suministro de los mismos no sólo no está vedado, sino que resulta acorde con la protección y saneamiento del crédito.

2) Cabe desestimar la acción de habeas data tendiente a hacer desaparecer de los registros de la demandada un antecedente comercial del actor, pues tal información no se encuentra desactualizada en los términos del art. 43 de la Constitución Nacional, ya que, la misma incluye una expresa referencia al cese de la mencionada inhabilitación.

3) Puesto que la acción de habeas data se encuentra aún pendiente de reglamentación legal, resulta improcedente pretender, ante la falta de normativa al respecto, que se suprima un antecedente comercial del actor de la base de datos de la sociedad accionada con fundamento en el transcurso de un término de prescripción en particular, en desmedro del autoimpuesto por ésta última a tal fin.

4) Aun cuando, en el caso, la información relativa a los antecedentes comerciales del actor contenidos en la sociedad accionada podría considerarse incompleta –por omisión de indicar la fecha concreta de vencimiento del plazo de inhabilitación para operar como cuentacorrentista que pesaba sobre aquél-, este extremo no puede servir de fundamento para la acción de habeas data deducida. En efecto, por un lado, dicho dato podría haber sido obtenido por cualquier interesado mediante la consulta del pertinente Boletín del BCRA, y por otro, la pretensión entablada no tuvo por objeto la integración del dato faltante, sino la supresión de tal información de los registros de la demandada; con lo cual, de admitirse la acción intentada, se produciría una violación al principio de congruencia contemplado por el art. 163 inc. 6 del CPCC.

5) Puesto que la pretensión deducida en autos -hacer desaparecer de los registros del demandado un antecedente comercial del actor- carece de contenido patrimonial directamente ponderable, cabe concluir que el pleito carece de monto en los términos del art. 6 inc. a) de la ley 21.839, t.o. ley 24.432. Por lo cual el emolumento debe calcularse con arreglo a las pautas previstas en los inc. b) y ss. De la citada norma, sin desatender, asimismo, la trascendencia económica del juicio para las partes en la particular cuestión planteada.

Hechos: Organización Veraz S.A. publica en su boletín una inhabilitación como cuenta correntista impuesta por el BCRA contra el actor. Este interpone demanda de habeas data para que la accionada suprima de sus registros y boletines dicho dato. El juez de grado hizo lugar a la demanda, estableciendo que la información suministrada era parcial, incompleta e incluida en una acepción amplia del concepto falsedad, y además que no se hacía referencia a la fecha de vencimiento de dicha inhabilitación, que la indicación de tal circunstancia era revelada como un dato incidental y que la misma no podía ser suministrada más allá de un plazo razonable. La accionada recurre el fallo.

La Cámara establece que el propio promotor de las actuaciones denunció haber sufrido el cierre de una cuenta corriente bancaria abierta a su nombre en el Banco de la Provincia de Neuquén, logrando posteriormente su rehabilitación, y del informe agregado por la demandada surge que dicha inhabilitación fue dispuesta por el BCRA en mayo den 1987, y que la misma se encuentra vencida. Ninguno de los datos emergentes de este informe resultan falsos o inexactos ya que le inhabilitación efectivamente existió y se deja constancia de su vencimiento.

Tampoco esta información puede ser considerada discriminatoria, ya que el suministro de antecedentes comerciales o bancarios resulta acorde con la protección del crédito, que ha merecido tutela jurisdiccional en muchos pronunciamientos de la Cámara. Tampoco se puede decir que la información resulte desactualizada, ya que la misma contiene la fecha de vencimiento de la inhabilitación.

Y como la acción de habeas data no está reglamentada, no existe normativa que sustente la pretensión de que se suprima un antecedente de la base de datos de la accionada por el mero transcurso de un plazo determinado. Lo único que se podía cuestionar es que no se indicaba la fecha concreta de vencimiento del plazo para operar como cuentacorrentista, pero se podía llegar a la misma respuesta de dos maneras: o bien consultando el boletín del BCRA, o inferido de la fecha en que se dispuso la inhabilitación, también suministrada en el informe cuestionado.

57. Derecho a la información. Acreditación del perjuicio

Autos: Tassotti, Luis G. c. Organización Veraz S.A., CNCom., sala B, julio 4/997.

1. *El "habeas data" está previsto para obtener el acceso a información almacenada en bancos de datos a efectos de verificar su aptitud y, eventualmente, obtener su rectificación o cuando se trate de datos sensibles o en supuestos de falsedad o discriminación, su supresión, confidencialidad o actualización. Se trata de datos relativos al afectado que consten en registros o bancos de datos públicos o privados destinados a proveer informes.*
2. *Es improcedente la acción de amparo iniciada para que la demandada, empresa dedicada a brindar informes sobre antecedentes comerciales, se abstenga de proporcionar información, pues el actor no menciono las consecuencias dañosas que pretende evitar.*
3. *Es improcedente la acción de amparo iniciada para que la demandada, empresa dedicada a brindar informes sobre antecedentes comerciales, se abstenga de proporcionar información pues a tal fin es insuficiente la genérica manifestación del actor de verse impedido de tomar crédito, sin aportar elementos que permitan apreciar la seriedad de esa información. Además, el hecho de no haber invocado la realización de gestiones previas y, en su caso, la inutilidad de estas, impide también el acceso a la via intentada.*

Hechos: Luis G. Tassotti incoa acción de amparo (art.43, Constitución Nacional) contra la Organización Veraz S.A. Invoca el "habeas data" y que se disponga que la demandada se abstenga de proporcionar información (cuya arbitrariedad prometió demostrar) que le impediría obtener créditos bancarios y/o comerciales.

El juez de grado desestimó la pretensión en base a dos argumentos: autocontradicción emergente de atribuir arbitrariedad a una información desconocida y ausencia de acreditación de haber realizado gestiones privadas y su inutilidad.

Es decir, sostiene el rechazo en la falta de acreditación del perjuicio sufrido y en la ausencia de reclamos previos que le hubieran permirido conocer mejor la situación personal en el archivo.

57.1 Rechazo in limine

Autos: Adecua - Asociacion de Defensa de Consumidores y Usuarios de la Republica Argentina c/ Estado Nacional, CNFed. Contenciosoadministrativo, sala I, abril 29/997.

1. *El mero hecho de disentir con interpretación dada por el juez, sin dar las bases jurídicas del distinto punto de vista, no es suficiente para sustentar un recurso de apelación, por tanto la sola manifestación del accionante de que el rechazo "in limine" del habeas data limitaría arbitraria e injustificadamente los alcances del instituto no configuran un agravio en los términos del art.265 del Código de Proced. Civil y Comercial de la Nación.*

Considerando: Que a fs. 45/49 la juez a cargo del Juzgado Nº 3 rechazó parcialmente "in limine" la pretensión para que se ordene a la Secretaría de Obras Públicas y Transporte que provea a las asociaciones de consumidores legalmente constituidas y debidamente inscriptas, los antecedentes de la apertura de la renegociación del contrato con Aguas Argentinas, la información que se produzca a medida que avancen las tratativas y las conclusiones a las que se arribe todo con fundamento en el art.43, parr.3º de la Constitución Nacional.

Para así decidir, estimo que dicha pretensión es extraña al remedio intentado.

Que contra dicha resolución interpuso recurso de apelación la parte actora que fundó a fs. 47/48.

Que no es suficiente para sustentar el recurso de apelación el mero hecho de disentir con la interpretación dada por el juez sin dar las bases jurídicas del distinto punto de vista.

Se resuelve: declarar desierto el recurso de apelación deducido por la parte actora, con costas por su orden.

57.2 Reclamo administrativo. Rechazo in limine

Autos: Gutierrez, Hector R. C/ Casino Militar del Personal Superior de la Base Naval Puerto Belgrano. C. Fed., Bahia Blanca, Sala I, dic. 30/994).

1- *Los jueces pueden rechazar "in limine" la acción de amparo –en el caso, "habeas data"- con criterio restrictivo y la mayor prudencia y cautela, pues lo contrario podría interpretarse como una negación de justicia.*

2- *No es imprescindible el reclamo administrativo previo si el objeto de la acción de habeas data es tener acceso a la información relativa al actor.*

Hechos: El actor, oficial retirado de la Armada Argentina, interpuso acción de habeas data contra el Jefe del Casino Militar del Personal Superior de la Base Naval Puerto Belgrano por haberle retirado la credencial que lo autorizaba a ingresar a dicho Casino. Para ello alegó el "desprestigio" que le provocaba la actitud del oficial quien al ser requerido sobre las causas por las cuales se lo excluia de la entidad, se las negó con amparo en la confidencialidad de las fuentes. Asi las cosas planteó habeas data para que se le exhiban los datos o informes que se refieren a su persona.

El juez a quo rechazo "in limine" la demanda considerando que debe agotarse la vía del reclamo administrativo aun no finalizada y que a la fecha de presentación de la demanda habia transcurrido el plazo del art. 2, inc. e) de la ley de amparo.

El actor apeló y la Cámara, teniendo en cuenta lo mencionado en el sumario, y en lo tocante al plazo legal para deducir la acción sostuvo que la fecha tomada como base de su razonamiento por el *a quo* resulta ajena a los términos y objeto de la acción, resolviendo asi revocar la resolución de 1ª Instancia.

Pero todo ello en cuanto a la admisibilidad de la acción. Una vez analizada esta por la Camara, se resuelve que:

La acción de "habeas data" es improcedente si no se demuestra el motivo descalificante o discriminatorio del dato en cuestión, ni que su origen sea la anotación en registros o bases de datos propios o de terceros, ya sean públicos o privados, destinados a suministrar información.

La acción de "habeas data" tiene por objeto tomar conocimiento, actualizar, exigir la supresión, rectificación y/o confidencialidad de datos o información del sujeto, tanto existentes en bancos de datos públicos como privados, siempre y cuando éstos últimos estén destinados a proveer informes.

La denegatoria de la admisión como socio en un club –en el caso Casino Militar- no esta incluida dentro de los presupuestos de procedencia de la acción de habeas data, salvo que para tal negativa se haya tenido en cuenta algún dato descalificante o discriminatorio que conste en sus propios archivos, categoría que no alcanzan ni el listado de socios ni el registro de pago de cuotas.

57.3 Rechazo in limine

Autos: Figueroa Hnos. S.A. c/Banco de la Provincia de Santiago del Estero S/Sumarísimo", CNCom., Sala D, mayo 13/996, E D, 173-17 y ss.

1) *Puesto que la apelante solamente criticó a la sentencia recurrida en cuanto fundó la desestimación de una acción de habeas data deducida contra un banco en el hecho de que las entidades bancarias no son organismos destinados a brindar datos, pero no cuestionó que en dicha resolución se hubiese considerado que el habeas data debe utilizarse sólo cuando no existen otras vías aptas para cuestionar la tutela de derechos fundamentales, cabe concluir que tal omisión crítica erige en verdad legal, en este caso, que la accionante debió haber efectuado previas gestiones privadas y acreditado la inutilidad de ellas para que fuera viable la acción interpuesta.*

2) *Puesto que la acción prevista en el tercer párrafo del art. 43 de la Constitución Nacional procede sólo en ausencia de otras idóneas para reparar el derecho que se dice vulnerado, cabe desestimar in límine su ejercicio en caso de que haya quedado establecida la existencia de un trámite ordinario conducente para lograr lo que se persigue en esta vía.*

3) *Cabe rechazar in límine la pretensión de ejercer la acción de habeas data si el apelante no mencionó las consecuencias dañosas concretas y actuales que sólo se hubiesen podido evitar mediante esta vía, argumentando al respecto simples eventualidades.*

4) *El contenido de la teneduría de libros de un banco no parece constituir un supuesto de registro o banco de datos públicos o privado destinado a proveer informes previsto en el art. 43 de la Constitución Nacional, ya que los bancos no prestan profesionalmente servicios al público como informantes, por lo cual resulta dudosa la habilitación de una entidad bancaria para ser emplazada como sujeto pasivo de una acción de habeas data.*

Hechos: Figueroa Hnos. S.A. trabajaba en cuenta corriente con autorización para girar en descubierto con el Banco de la Provincia de Santiago del Estero. A partir del mes de octubre de 1986 dejó de operar con dicho banco, y el saldo deudor de esa cuenta fue totalmente cancelado mediante la dación en pago de varios inmuebles.. A partir de entonces, y durante nueve años, no hubo reclamos por parte del Banco demandado, pero luego sobrevinieron declaraciones de un intendente de la municipalidad santiagueña, del presidente de un partido político y del presidente del Banco de la Provincia de Santiago del Estero según las cuales la sociedad actora adeudaba al Banco la suma de $10.000.000.

Luego estas declaraciones tomaron estado público, pasando a declaraciones periodísticas y publicaciones en revistas.

La postura del demandante es que es el Banco de la Provincia de Santiago del Estero quien, a través de su representante legal, informa a la opinión pública de la existencia de una deuda. Por lo tanto ello debe surgir de sus registros, y por ello habilita la vía del habeas data.

En primera instancia la pretensión fue desestimada *in límine* debido a que: una entidad bancaria no es un organismo que se encuentre destinado a brindar datos; el habeas data debe utilizarse en situaciones extremas y delicadas y cuando no existan otras vías aptas para resguardar la tutela de los derechos fundamentales; el amparo procede únicamente ante la ineficacia de procesos ordinarios y ante la existencia de un daño concreto y grave que sólo sea reparable por esta acción urgente y expeditiva.

El actor apela dicha resolución, criticando solamente el aspecto de la sentencia que establece que una entidad bancaria no es considerada organismo destinado a brindar datos o proveer información. Como establece la Cámara, las normas del Código Procesal, con respecto al recurso de apelación, exigen del apelante la crítica concreta y razonable de las partes del fallo que el impugnante considere equivocadas, y en el presente caso el recurrente no cumplió con dichos preceptos legales. No critica el fallo de primera instancia en cuanto establece que el habeas data debe intentarse cuando no existan otras vías aptas para resguardar la tutela de los derechos fundamentales, sino que el apelante reconoce que, cuando menos, podría ejercerse una acción de daños y perjuicios que causa el dato falso que se ha divulgado, pero implicaría relegar a los trámites ordinarios la protección del buen nombre de su sociedad. Por otro lado, el art. 505 C. Civil atribuye a quien hubiere cumplido su obligación, derecho para obtener la liberación correspondiente, cosa que tampoco hizo el recurrente. Así como también omitió mencionar las consecuencias dañosas concretas y actuales que habrían derivado de los hechos relatados. Indica un perjuicio pero en forma eventual y potencial. Se confirma la decidido en primera instancia.

58. Hábeas corpus. Amenaza a la libertad ambulatoria. Información registrada por archivos de seguridad

Autos: Ganora, Mario F. y otra. CNCrim. y Correc., sala de feria, agosto 3 – 997.

1- *Dado que la ley 23098 prevé la aplicación del procedimiento de "hábeas corpus" cuando se denuncie una amenaza o limitación actual de la libertad ambulatoria sin orden escrita de autoridad competente, si nadie ha intentado la detención del actor, ni existen elementos que permitan sospecharlo, pues solo se ha denunciado que personas no identificadas han efectuado averiguaciones sobre su vida personal, no existe tal amenaza o limitación actual de dicha libertad.*

2- *A los efectos de la acción de "habeas data", la Constitución Nacional prevé que las informaciones deben constar en registros o bancos de datos públicos, es decir que la información debe ser pública o al alcance de los particulares. De esta forma, no procede la acción en relación a la información obrante en los registros de las fuerzas y organismos de seguridad, pues no revista tal carácter público por obvias razones de seguridad pública.*

1ª Instancia. – Buenos Aires, agosto 1 de 1997.

Considerando: Que Mario F. Ganora interpone acción de "hábeas corpus" y de "habeas data" en su favor y el de Rosalía L. Magrini.

Ganora manifiesta en su presentación y en la ratificación que ambos son letrados defensores de Adolfo F. Scilingo, quien está efectuando diversas denuncias relativas a hechos ilícitos cometidos durante el régimen militar de gobierno, en especial relativas al grupo de tareas que prestaba funciones en la Escuela de Mecánica de la Armada.

Que relaciona directamente con esta actividad ciertos hechos que puntualiza en su presentación. Personas que no se identificaron han hecho averiguaciones sobre la vida personal de los beneficiarios.

El 17 de julio una persona interrogó al portero del edificio donde funciona el estudio jurídico del presentante sobre la actividad de los beneficiarios, si eran propietarios o inquilinos, si pagaban expensas o no; todo era para un informe en un banco en el que habrían solicitado un crédito, hecho que el denunciante afirma que es falso.

El 26 de julio se presentó una persona en un domicilio vecino al de la doctora Rosalia Magrini preguntando por sus hábitos, horarios y actividades en virtud de una supuesta solicitud de empleo que había efectuado la nombrada.

Finalmente, el 29 de julio se presentó una persona en el edificio donde vive Ganora solicitando datos sobre su persona.

Deja por si radicada la denuncia por intimidación publica y amenazas (arts.211 y 149 bis, Cod. Penal).

Asi planteadas las cosas, se rechazó la acción de "hábeas corpus" y de "habeas data" planteada con costas, auto que fue revocado por el superior en la fecha al solo efecto que el suscripto requiera a los organismos respectivos si los beneficiarios tenían alguna medida restrictiva de su libertad.

Las conductas denunciadas no encuadran en las previsiones de la ley 23.098 que regula la acción de "hábeas corpus". El procedimiento de "hábeas corpus" se aplicara cuando se denuncie una amenaza o limitación actual de la libertad ambulatoria sin orden escrita de autoridad competente (art.3º inc.1º). Estas circunstancias de hecho no existen porque nadie ha intentado detenerlos ni existen elementos que permitan sospechar esto.

A mas de ello, los informes emanados por Policía Federal, Gendarmería Nacional, Prefectura Naval Argentina y la Secretaria de Inteligencia del Estado dan cuenta que respecto de los beneficiarios no existe orden restrictiva de su libertad.

Por lo tanto, tampoco es procedente la acción de "habeas data" ya que las informaciones deben constar en registros o bancos de datos publicos. Es decir que la información que se pide debe ser pública o al alcance de los particulares. La obrante en las fuerzas y organismos de seguridad no reviste tal carácter por obvias razones de seguridad pública.

Se resuelve: Rechazar la presente acción de "hábeas corpus" y de "habeas data" interpuesta a favor de Mario F. Ganora y de Rosalia L. Magrini.

2ª Instancia. – Buenos Aires, agosto 3 de 1997

Considerando: Por encontrarse ajustado a derecho y a las constancias de autos se convalidara lo resuelto por el juez, sin costas, por entender que el presentante pudo considerarse con derecho a accionar. Ello sin perjuicio de señalar la improcedencia del pedido de "habeas data" en función del relato de hechos realizados por el doctor Mario F. Ganora.

Se resuelve: Confirmar: la presente acción de "hábeas corpus" y de "habeas data" interpuesta a favor de Mario F. Ganora y de Rosalía L. Magrini.

59. Falsedad o desactualización. Confidencialidad del informe crediticio.

Autos: Rodriguez, Rafael Jacinto c. Organización Veraz, S.A. s/ sumarísimo, CNCom, sala C, septiembre 6/996.

1. *Dado que las disposiciones constitucionales regulatorias del habeas data exigen como presupuesto de admisibilidad del mismo que se haya configurado una hipótesis de falsedad o desactualización de cierta información concerniente al actor, dicha acción deberá ser desestimada si, como el caso, los datos en los cuales se fundo la misma, han resultado ser ciertos y subsistentes.*

2. *Si no ha quedado acreditado que los datos concernientes al estado patrimonial del amparista hubiesen sido divulgados indiscriminadamente o fuera del marco de confidencialidad que impone este tipo de información – ya que la empresa demandada solo los transmitió a entidades crediticias, sin exorbitar su función dirigida al saneamiento del crédito -, cabe concluir que no se observan en autos reparos constitucionales o legales en punto a eventuales molestias que tal proceder pudiera haber suscitado, que hagan procedente la vía prevista por el art.43 de la Constitución Nacional.*

Hechos: El señor juez de Cámara doctor José Luis Monti dice: la demanda fue fundada en la circunstancia de que la firma demandada habría dado a conocer indebidamente determinada información concerniente al estado patrimonial del actor. Concretamente, lo que Organización Veraz, S.A. informó en plaza era que una entidad bancaria – el Banco de Boston – había entablado contra Rafael Jacinto Rodriguez en agosto de 1991 un juicio ejecutivo ante un juzgado de este fuero por el cobro de cierta suma dineraria devengada en una cuenta corriente.

Y he aquí que, para el actor, la información en la que el se hallaba involucrado le provocaba serios perjuicios, por cuanto le dificultaba el acceso al crédito.

Rodriguez solicitó que Organización Veraz S.A. se abstuviera de brindar informes perjudiciales de su capacidad económica, y que, una vez comprobada la falsedad de los datos difundidos, se ordenara la pertinente rectificación. Rodriguez postuló como sustento jurídico el art.43 de la Constitución Nacional.

La actividad de la demandada resulta completamente lícita y útil a los fines de promover el acceso al crédito. En tal sentido, Organización Veraz S.A. puso de resalto que obtuvo los datos del juicio ejecutivo de la publicación periódica que realiza esta Cámara, con base en el art.52, inc.j , del Reglamento del Fuero. Asimismo, la demandada expresó que la información que por esa vía obtuvo la dio a conocer solo a la entidad interesada, la cual quedó comprometida a guardar la confidencialidad y la reserva del caso.

Se especificó, también, que son dadas a conocer las modificaciones que se producen en sus registros.

La Jueza de primera instancia rechazó la demanda, considerando que la información difundida por Organización Veraz, S.A. no era falsa y teniendo en cuenta un informe proveniente del Juzgado interviniente en la ejecución seguida por el Banco de Boston contra Rodriguez, el que daba cuenta de la efectiva promoción y existencia de tal causa.

Apeló el actor. Rodriguez pone su acento recursivo reiterando objeciones fundadas en su supuesta ilicitud. No cuestiona concreta y razonadamente el argumento basal de la sentencia de la sentencia de 1ª instancia, que fue la autenticidad del dato objeto de la información dada a conocer por la demandada. Esto es, que el proceso ejecutivo del Banco de Boston contra Rodriguez efectivamente habia sido iniciado. No se puede, en esas condiciones, predicar la falsedad del dato.

Asi las cosas, la pretensión contenida en la demanda no resulta viable en el marco de las disposiciones constitucionales regulatorias de la medida requerida por el actor, las que precisamente exigen, como presupuesto para su admisibilidad, la configuración de una hipótesis de falsedad o desactualización.

También es pertinente señalar que no surge de autos que los datos en cuestión hubieran sido divulgados indiscriminadamente, ya que la demandada los habría transmitido a entidades crediticias.

Por los motivos expuestos, si mi criterio fuera compartido, deberá confirmarse la sentencia apelada, con costas de Alzada al recurrente (art.68 1ª parte, código procesal).

Por los fundamentos del Acuerdo que antecede, se confirma la sentencia apelada, con costas de Alzada al recurrente. – *J.L. Monti.- Bindo B. Caviglione Fraga.- Hector M. Di Tella.*

DOCUMENTOS AGREGADOS EN EL CD

☑ **Indice normativo general**

1. Indice de normas sobre protección de datos
2. Indice de leyes varias
3. Legislación mundial sobre habeas data
4. Resúmenes de artículos constitucionales argentinos sobre habeas data

☑ **Tratados internacionales sobre Derechos Humanos**

5. Declaración Universal de los Derechos Humanos
6. Declaración Americana sobre Derechos y Deberes del Hombre
7. Convención Americana sobre Derechos Humanos
8. Pacto Internacional de Derechos Civiles y Políticos
    - *Protocolo facultativo del Pacto Internacional de Derechos Civiles y Políticos*
    - *2do. Protocolo facultativo del Pacto Internacional de Derechos Civiles y Políticos*
9. Pacto Internacional de Derechos económicos, sociales y culturales
10. Declaración Americana contra la Tortura y otros tratos o penas infamantes
11. Convención Americana contra la Tortura y otros tratos o penas infamantes
12. Convención sobre el derecho internacional de rectificación

☑ **Constituciones Americanas, Europeas y locales**

1. Comparación de Constituciones sobre el tema garantías jurídicas (amparo, habeas data y hábeas corpus). *Fuente:* www.georgetown.edu/plba/comp/derechos *(base de datos políticos de las Américas)*
2. Comparación de Constituciones sobre el tema privacidad familiar y personal. *Fuente anterior*.
3. Comparación de Constituciones sobre el tema libertad de pensamiento y expresión. *Fuente anterior*.
4. Constituciones provinciales de la República Argentina
5. Constitución Nacional Argentina
6. Constitución de Estados Unidos de América
7. Constituciones de América. Artículos vinculados

☑ **Normativa Europea y americana**

1. A Framework for global electronic comerce
2. Acuerdo del CEE (12-03-99) sobre transmisión a terceros de datos personales
3. Anteproyecto de Convención Americana sobre autodeterminación informativa

4. Carta de la OEA
5. Código Etico de protección de datos en Internet (28/01/99)
6. Directiva 91/250/CE sobre protección jurídica de programas de ordenador (14/5/91). *Fuente:* www.onnet.es
7. Directiva 95/46/CE Protección de las personas físicas en el tratamiento de datos personales y libre circulación de datos (24/10/95).
8. Directiva 96/9/CE del Parlamento Europeo y del Consejo de Europa (11/03/96) sobre protección jurídica de las bases de datos.
9. Directiva 97/66 (31/10/98) sobre intimidad en las telecomunicaciones
10. Directiva 98/84/CE de protección jurídica de servicios de acceso condicional
11. Directiva europea cobre protección de datos personales (Convenio 108 del Consejo de Europa). *En francés.*
12. Directiva sobre tratamiento de datos en el sector de telecomunicaciones
13. Documento del Parlamento Europeo y del CEE sobre protección de datos (31-01-2000)
14. Electronic Communications Privacy (USA)
15. Ley 78/17 del 6/1/78 (Francia)
16. Ley de Habeas data del Perú.
17. Ley de Protección de Datos de Canadá
18. Ley reglamentaria del Habeas data en Brasil
19. P3P Architecture working group (22/10/97)
20. Privacy Act (1974). Versión texto y documento electrónico.
21. Proyecto de ley de Habeas data de Costa Rica
22. Proyecto de ley de Habeas data de Venezuela
23. Reglamento 1588/90 sobre secreto estadístico
24. Resolución 44/132 de la ONU sobre regulación de datos (15/12/89)
25. Seguridad en los sistemas de información (Directivas OCDE)
26. Utilización de video cámaras para la prevención del delito

☑ **Recomendaciones emitidas en la Unión Europea**

1. Recomendación sobre protección de datos del Consejo de Europa (97/5 del 13/02/97).
2. Recomendación del CEE sobre datos con finalidad científica (23-09-83)
3. Recomendación 81/679 del 29-07-81
4. Recomendación del CEE sobre comercio electrónico
5. Protección de los consumidores en el comercio electrónico
6. Protección jurídica de programas en ordenadores
7. Defensor de los Datos en la Unión Europea
8. Recomendación 97 sobre datos médicos

☑ **Resoluciones de la Organización de las Naciones Unidas**

1. Resolución 45/95
2. Resolución 44/132 (15-12-89) sobre regulación de datos
3. Documento A 44/606 (24/10/89) sobre regulación de ficheros computarizados de carácter personal

☑ **Normativa Española**

1. Ley Orgánica regulatoria del tratamiento de datos personales (Lortad) 5/92
2. Real Decreto 1332/94 sobre reglamentación de la Lortad (20/06/94)
3. Ley Orgánica 15/1999 sobre protección de datos de carácter personal (15/12/99)
4. Ley de incorporación al derecho español de la Directiva 96/9/CE
5. Instructivo 1/95 de la Agencia de Protección de Datos de España sobre solvencia patrimonial y crédito
6. Instructivo 1/98 de la APD para el ejercicio de los derechos de acceso, rectificación y cancelación.
7. Real Decreto 994/1999 sobre medidas de seguridad de los ficheros

☑ **Normativa Nacional**

1. Ley 11.683
2. Decreto 165/94
3. Ley 24144
4. Ley 24745
5. Decreto 1616/96
6. Decreto 606/99
7. Ley 24.766
8. Ley 25.036
9. Ley 25.200
10. LEY….DE PROTECCIÓN DE LOS DATOS PERSONALES
11. Decreto 2080/80
12. Sistema OSIRIS para la confidencialidad de datos en las declaraciones juradas impositivas
13. Comunicación A/2729 del Banco Central de la República Argentina (Clasificación de deudores)
14. Base de datos de riesgo crediticio (Proyecto de ley)
15. Consulta al Banco Central sobre deudores

☑ **Proyectos de ley sobre habeas data y amparo en Argentina**

1. Proyecto Menem
2. Proyecto Menem sobre habeas data

3. Proyecto elevado por el Senado
4. Proyecto de Diputados
5. Proyecto Del Piero
6. Proyecto Lopez
7. Proyecto Lopez Alcides
8. Proyecto Berhongaray

☑ **Políticas de privacidad**

1. Declaración de Infosel sobre políticas de privacidad
2. Declaración de Hotmail sobre política de privacidad

☑ **Jurisprudencia internacional**

1. American Civil Liberties Union vs. Reno Janet (USA)
2. Hotmail vs. Van Money Pie inc.
3. Jurisprudencia de Brasil (cuatro fallos)
4. Jurisprudencia de Colombia (dos fallos)
5. Síntesis de jurisprudencia local

INDICE GENERAL

Capítulo VIII: La transferencia de los datos

28. Distinción inicial: Transmisión local e internacional
    28.1 *Protección local de los datos personales*
    28.2 *Protección internacional de los datos personales*
29. El principio de la protección adecuada o equivalente
    29.1 *Las normas de la ONU*
    29.2 *La situación en Europa*
    29.3 *Principios básicos de la "protección adecuada"*
    29.4 *Excepciones al principio de "protección adecuada"*
    29.5 *El control de equivalencia*
30. La transferencia de datos en América Latina
31. La transferencia de datos personales a través del correo.

Capítulo IX: Derechos del titular de los datos

32. ¿Quién es el titular de los datos?
    32.1 *Derecho subjetivo del titular de los datos*
    32.2 *La protección de los datos como derecho humano*
    32.3 *Disponibilidad del derecho: autodeterminación*
    32.4 *La pertenencia del derecho en la ley reglamentaria*
33. Los datos de las personas jurídicas
    33.1 *El dato como derecho personalísimo*
    33.2 *Intimidad y datos de la persona jurídica*
    33.3 *El derecho internacional*
34. Las garantías procesales en la protección de datos
    34.1 *Derecho de información*
    34.2 *Derecho de acceso*
        a) ¿Acceso al archivo o a la información?
        b) ¿Cómo se accede a los archivos extranjeros?
        c) ¿A partir de qué momento se tiene derecho de acceso al archivo?
        d) Finalidad del derecho de acceso
    34.3 Derecho a controlar el archivo y los datos personales
        a) *Derecho a la rectificación del dato*
        b) *Derecho a la actualización*
        c) *Derecho a la confidencialidad de los datos*
        d) *Derecho al silencio y al olvido mediante la cancelación del dato*
    34.4 Excepciones al derecho de acceso, rectificación y supresión

57. Derecho a la información. Acreditación del perjuicio

    57.1 Rechazo in limine

    57.2 Reclamo administrativo previo. Rechazo in limine

    57.3 Rechazo in limine

58. Hábeas corpus. Amenaza a la libertad ambulatoria. Información registrada por archivos de seguridad

59. Falsedad. o desactualización. Confidencialidad del informe crediticio