LA TRANSFERENCIA DE DATOS ENTRE LA UNIÓN EUROPEA Y LA ADMINISTRACIÓN PÚBLICA BRASILEÑA: ANÁLISIS DE LA "PROTECCIÓN ADECUADA" DE LOS DATOS PERSONALES EN BRASIL CONFORME A LOS PARÁMETROS DE LA DIRECTIVA 95/46/CE

CARLOS BRUNO FERREIRA DA SILVA

DIRECTOR DE TESIS:
D. JAVIER PÉREZ ROYO
DEPARTAMENTO DE DERECHO CONSTITUCIONAL
UNIVERSIDAD DE SEVILLA
AÑO DE 2013

ÍNDICE

INTRODUCCIÓN

El derecho a la protección de datos o a la autodeterminación informativa representa la respuesta que viene dando el hombre para mantener intactos los atributos de su personalidad ante los nuevos desafíos de la realidad, en este caso, el enorme desarrollo de las tecnologías informáticas de almacenamiento y comunicación de datos en escala planetaria durante los últimos 50 años.

Principalmente a partir de la década del 60 del siglo XX se observa un aumento exponencial en la capacidad de almacenamiento y tratamiento de datos por parte de los ordenadores. Con ello, las posibilidades de uso de las bases de datos también se multiplicaron. Mientras el sector privado absorbe el potencial como medio de analizar y conquistar nuevos consumidores, a través de la manipulación de las informaciones relativas a sus hábitos, la Administración Pública recibe un apoyo para administrar de manera más eficiente la provisión de las necesidades insatisfechas de las grandes poblaciones hoy existentes, usualmente aglomeradas en densos centros urbanos. Al mismo tiempo, esto representa nuevos peligros para el logro de la libertad por parte del ciudadano, ya que el manejo de dichos datos también permite fácilmente el análisis completo de su personalidad, tornándolo "transparente" a quien administra el archivo de las informaciones. Es en esa tensión de intereses discurre la regulación de la protección de datos dentro de los órganos estatales.

En el **capítulo 1** será expuesto el desarrollo histórico y los elementos que

componen el avance tecnológico y, a partir de allí, como ello afecta e influye en la acción del Estado y de los entes privados y, por último, en la realidad de cada ciudadano. Ello permitirá visualizar con mayor claridad las cuestiones que entran en conflicto cuando se pretende establecer normas en cuanto a bases de datos. En ese aspecto, el reconocimiento de las circunstancias históricas que surgen como *causa* para el discurso de un nuevo derecho a protección de datos personales ayuda a dar sentido a los elementos que en los siguientes capítulos servirán como *justificación* para su contenido y limitaciones[1].

El enorme avance de las tecnologías de almacenamiento de datos y de telecomunicaciones en el medio siglo que nos antecede provoca dos consecuencias principales sobre el Estado actual. En primer lugar, se constituye en un poderoso instrumento de organización, pero de la misma forma se le exige su protección por intermedio del derecho para evitar socavar nuestras libertades.

La consagración de un derecho subjetivo en el derecho positivo pasa, según la concepción vigente formada hace poco más de dos siglos, por su configuración por la comunidad política dentro del Estado Nacional. En el **capítulo 2**, expondremos los fallos de los Tribunales Constitucionales de España, Alemania y Brasil que identifican las principales características ya reconocidas en cada orden constitucional al individuo en la protección de la recolección y uso de sus datos personales.

[11] Nótese, como alerta RICHARD PRIMUS, que ambos, *causa* y *justificación*, sirven para explicitar las *razones* que conducen al reconocimiento por el derecho positivo que determinado derecho puede ser considerado como fundamental para el ordenamiento (PRIMUS, Richard A. *The American Language of Rights*. Cambridge University Press, 1999, p. 55).

La precedencia en el abordaje de los contornos definidos a este derecho fundamental por los Tribunales Constitucionales admite la importancia de la cuestión de la *institucionalización* en la definición de cualquier catálogo concreto de derechos del hombre[2]. Ello no significa, sin embargo, un menoscabo de la relevancia de su *fundamentación*. Al contrario, en ese mismo capítulo serán tratados los argumentos que justifican un derecho de protección de datos personales al individuo, ya que la caracterización como un derecho fundamental impone que se una, dentro del ordenamiento interno, junto a la jerarquía extrema constitucional y a la fuerza de imposición externa sobre el legislador, el contenido de carácter especialmente importante que lo exponga como derecho esencial, a la autonomía de cada ser humano[3].

El rasgo característico del *derecho fundamental a la autodeterminación informativa*, nomenclatura precisa utilizada en la importantísima decisión de 1983 sobre la "Ley del Censo" del Tribunal Constitucional Alemán, establece que se trata de un derecho que no se satisface con las facultades negativas, o sea, impeditivas de la acción de otro, sino que exige la presencia de una serie de facultades positivas, que le permitan al individuo ejercer un control efectivo sobre el uso de sus datos. Ese abordaje que se desarrolla en los Tribunales Constitucionales de Alemania y España, contrasta con la postura del Supremo Tribunal Federal brasileño de concentrarse en la función defensiva de la protección de datos, menoscabando el uso del *habeas data*.

Es importante, asimismo destacar que la elección del estudio comparado del derecho español y alemán, no fue realizada al azar, sino en función del significado que poseen para el constitucionalismo brasileño.

---

2 ALEXY, Robert. *Constitucionalismo discursivo*. Traducido por Luís Afonso Heck. Porto Alegre: Livr. do Advogado, 2008, p. 44.

3 *Ibid.*, p. 45-51.

La importancia del constitucionalismo alemán, en especial, la doctrina y jurisprudencia formada posteriormente a la Ley Fundamental de Bonn de 1949, es manifiestamente sin igual en el mundo actual. Como afirma PÉREZ ROYO, "la doctrina alemana de los derechos fundamentales ha ido calando y extendiéndose hasta convertirse en cierta medida en una doctrina europea de los derechos"[4]. Los contornos para la protección de los derechos fundamentales, que sólo encuentran rival en la peculiar experiencia estadounidense, son entonces esenciales para la realización de cualquier estudio sobre el tema en los países democratizados en los últimos 40 años, bajo la influencia de la *praxis* de la Carta alemana, como fueron prácticamente todos los países de Latinoamérica, incluido el Brasil.

Manifiestamente, en cuanto a la protección de los datos personales, esa imprescindibilidad del derecho alemán es innegable. La decisión central expuesta en la sentencia del Tribunal Constitucional Alemán de 1983 sobre la "Ley del Censo", que define la "autodeterminación informativa" como un elemento autónomo de la dignidad humana, se convirtió en un modelo que influyó a toda la literatura y legislación existente sobre el tema. No es por acaso que los autores en lengua tedesca se encuentren entre los principales doctrinadores sobre este asunto.

Por otro lado, el país ibérico es un representante central de la Segunda Fase del constitucionalismo europeo de pos guerra. El retorno tardío de la democracia en este país, permitió que su Constitución adoptase todas las fórmulas ya consagradas en otras Cartas Magnas, especialmente la alemana. Por otra parte, el constitucionalismo español

[4] PÉREZ ROYO, Javier. *Curso de derecho constitucional*. Madrid: Marcial Pons, 2007, p. 219.

renace dirigido no solo para los éxitos del pasado, sino con miras a establecer respuestas a su propio futuro. Ello concede a la Constitución de 1978 el título de pionera en el abordaje de los peligros del uso de la informática para la materia de los derechos fundamentales y un fuerte sesgo europeísta, que se refleja en su legislación ordinaria y en el respeto a las decisiones jurisprudenciales de la Corte Europea de Derechos Humanos.

El constitucionalismo brasileño, además de tener al español como fuente confesa de inspiración en la redacción de la Carta Magna de 1988, comparte con el citado país la democratización y la búsqueda por la modernización de una sociedad latina con industrialización tardía.

Existen en la "protección de datos" dos características especiales que impulsan la importancia del análisis de su *internacionalización*. Por un lado es un derecho reciente, por lo tanto, surgido a lo largo del movimiento donde, desde el final de la segunda guerra mundial, con el surgimiento de la Organización de las Naciones Unidas y sus congéneres, se busca dentro de la comunidad de países la institucionalización y reconocimiento en tratados de los derechos universales y morales debidos a hombres y mujeres, la forma de establecer parámetros al poder del Estado. A esta característica se le suma otra aún más significativa, el hecho de que la protección de datos personales represente un campo de actuación donde hay una erosión de las esperanzas de suficiente protección de los límites territoriales de los Estados.

Por ello, el **capítulo 3** de esta tesis pretende establecer el historial de las

iniciativas unificadoras, partiendo con la caracterización de las iniciativas sobre protección de datos de la OCDE y de la Comunidad Europea, hasta llegar a las características generales de la directiva 95/46/CE, que unificó el tratamiento del tema en la Unión Europea, y que se reflejó en la ampliación de la interpretación del contenido del artículo 8º del Convenio de Roma por el Tribunal Europeo de Derechos Humanos (TEDH), para finalmente mostrar los puntos de consenso sobre los lineamientos normativos del derecho de protección de datos personales.

Esta nueva estructura no descuida que la creación de normas internacionales frecuentemente no viene acompañada por mecanismos coherentes que les proporcionen los medios necesarios para su efectividad. Sin embargo, en el caso de la Comunidad Europea, el TEDH y la directiva tienen un significado que va más allá de la fuerza moral. El primero, desembocando posiblemente en un recurso la decisión en última instancia de país signatario de la Convención Europea de Derechos Humanos, ha actuado, a lo largo de su historia, como un instrumento de definición de parámetros comunes en la protección de los derechos humanos. Los tribunales nacionales se ven obligados a tener en cuenta la jurisprudencia del TEDH, si bien admite el diálogo transjudicial en la observación de las experiencias de cada país en la protección de los derechos humanos[5].

Las directivas de la Unión Europea, aunque puedan ser caracterizadas también como una forma de *cooperación* entre el orden interno y comunitario, independientemente que necesiten de un acto interno de transposición, tienen la fuerza de *obligar* a los Estados miembros destinatarios en cuanto a los resultados que

[5] MACHADO, Jónatas E. M. *Direito Internacional do Paradigma Clássico ao Pós-11 de Setembro*. Coimbra: Coimbra Editora, 2006, p. 387.

pretenden alcanzar[6]. No obstante, la libertad existente en cuanto a la forma y medios por los cuales el Estado alcanzará los resultados previstos permite que cada país adapte la norma comunitaria a sus específicas peculiaridades.

La observación de estas normas y decisiones arroja luz sobre el escenario español y alemán, evidentemente conectados con el marco de la Unión Europea y del Consejo de Europa, pero también tiene un sesgo prospectivo. A fin de cuentas, la *apertura*[7] del Estado Constitucional a la influencia del derecho internacional no es privilegio de los países de Europa, sino una formulación que se presenta en múltiples constituciones nacionales, incluyendo la brasileña. Eso justifica un abordaje conjunto del derecho constitucional y del derecho internacional, que reconoce las influencias recíprocas de las dos ramas. Existe una interacción recíproca entre los sistemas, donde el derecho constitucional, sin perder su vínculo intrínseco con la estructura nacional, recibe influencias externas al mismo tiempo que, sus soluciones, ayuda a conformar los tratados y fallos supranacionales[8].

En el caso de la protección de datos, impulsan de manera especial una tendencia unificadora de la regulación del derecho a la autodeterminación informativa de las cláusulas en tratados internacionales que estimulan la creación de parámetros similares

---

6 Además, con la superación del plazo definido para su entrada en el ordenamiento jurídico interno, pasan a tener efecto directo en este Estado infractor, sin que ello agote el deber de insertar en su propia legislación (QUADROS. Fausto de. *Direito da União Européia*. Coimbra: Almedina, 2004, p. 362).

7 CRUZ VILLALÓN, Pedro. *La constitución inédita*. Madrid: Editorial Trotta, D. l., 2004, p. 28.

8 En ese sentido CANÇADO TRINDADE, Antônio A.. *El Derecho Internacional de los Derechos Humanos en el siglo XXI*. Organizado por Máximo Pacheco Gómez. Santiago de Chile: Editorial Jurídica de Chile, 2001, p. 274, NEVES, Marcelo. *Transconstitucionalismo*. São Paulo: Martins Fontes, 2009, p. 166 y BOGDANDY, Armin von. *Hacia un nuevo derecho público. Estudios de Derecho Público Comparado, Supranacional e Internacional*. México, D. F.: Universidad Nacional Autónoma de México, 2011, p. 431. KLAUS STERN, aun antes de la caída del muro de Berlín, ya se refería a una *internacionalización del Estado Constitucional*, aunque todavía resaltando su limitación al espacio constitucional atlántico europeo (STERN, Klaus. *Derecho del Estado de la República Federal Alemana*. Traducido por Javier Pérez Royo y Pedro Cruz Villalón. Madrid: Centro de Estudios Constitucionales, 1987, p. 817).

con miras a la transferencia internacional de datos. En este orden de ideas, la norma comunitaria que buscó unificar la garantía de la autodeterminación informativa dentro de la Unión Europea, en el artículo 25.1 de la Directiva 95/46/CE, estableció la prohibición de transmisión de datos a países que no posean un "nivel de protección adecuado". Es evidente que dicha verificación es prescindible para otros países miembros, que ya están sujetos a las reglas de la citada Directiva. El artículo 25.2, define los parámetros para la medición de la condición de protección "adecuada", las cuales involucran el estudio de las normas de derecho interno e internacional que obligan al país destinatario. Aunque no se requiere una "protección equivalente", conforme sugería antes el Convenio 108 del Consejo de Europa, está claro que el parámetro para la investigación es el alto nivel de protección en la UE[9].

Se plantea la validez de tomar como parámetro de análisis para la legislación brasileña la regulación europea, pues la significativa menor protección al individuo del modelo estadounidense de protección de datos, basado en un abordaje mercadológico del tema y en diversos reglamentos sectoriales con limitaciones de los derechos de los individuos, con relación al modelo europeo de visión del asunto dentro de la temática de los derechos fundamentales, desembocan en el establecimiento del "Acuerdo de *Safe Harbor*", en que se concertó que las compañías estadounidenses deberían adherirse voluntariamente a los principios referentes a la protección de datos, bajo la fiscalización de la *Federal Trade Comission* (FTC – Comisión Federal del Comercio) y del *Department of Transportation* (Ministerio de Transportes) del gobierno de los Estados Unidos. Por tanto, se suman a las razones morales y políticas de ver un país actuando en pro de una ampliación de los derechos humanos, los elementos de naturaleza de

[9] Considerando 10 de la Directiva 95/46/CE.

competitividad comercial en el sentido de reforzar la posibilidad de la recepción de estructuras de servicio que manipulen datos personales. Por tanto, podemos expresar que el establecimiento supranacional de un derecho a la protección de datos posee un estímulo que es típico al derecho internacional económico, pero poco común al derecho internacional de los derechos humanos[10].

El criterio de la "protección adecuada" para la transferencia internacional de datos demuestra incluso que hay diferentes formas de garantizar una protección efectiva de la autodeterminación informativa del individuo, condecentes con la realidad social de cada país, sin que ello niegue las características básicas del derecho fundamental. Esto es una verdad incluso dentro de la propia Unión Europea, ya que las directivas europeas, como la de la protección de datos, no exigen una reproducción literal e idéntica en todos los países.

El análisis del constitucionalismo democrático en un Estado Social, de dos países como Alemania y España, garantiza que podamos verificar como las características propias de cada sociedad afectan el formato del derecho interno y la configuración de contenidos y garantías que, incluso con distinciones, preserven en ambos, la protección suficiente a los datos de sus ciudadanos y las necesidades de ambas sociedades. Con ello, se puede cotejar, en este **capítulo 4**, dichas legislaciones europeas con lo existente actualmente en Brasil en cuanto a la doctrina del "habeas data" y de la preservación del "derecho fundamental a la intimidad y a la vida privada" en los datos personales, a partir de la Constitución de la República de 1988.

[10] MACHADO, Jónatas E. M. *Direito Internacional... cit.*,p. 381.

Entender los derechos fundamentales significa entender su doble sentido, de expresión de las facetas indiscutibles de la dignidad humana, pero también de definición de bases para la acción de los Poderes constituidos y, por consiguiente, de límites al objeto de la decisión democrática. Al mismo tiempo que protegen a sus titulares, los derechos deben servir para reforzar la vida en sociedad. Evidentemente en la coexistencia en comunidad existen innumerables momentos en que las posiciones individuales se enfrentan y el Estado debe tener los medios necesarios para garantizar que todos sus ciudadanos preserven sus libertades.

La definición de una "protección adecuada" para el individuo no significa señalar límites intraspasables a la necesaria acción del Estado en pro de toda la sociedad. La protección del hombre se concilia con el mantenimiento de medios para que el Estado alcance el ideal hobbesiano de garantizar nuestra defensa de los males de la sociedad alejada del derecho. Como afirma HANS PETER SCHNEIDER:

> "(..) en el moderno Estado de las prestaciones sociales la realización de determinadas tareas por el Estado y la esfera de vida individual están entrelazadas de muchas maneras, de modo que la libertad personal debe organizarse disponiendo de formas adecuadas de actuación estatal, así como la creación de condiciones iguales de vida debe organizarse como una política de prestaciones"

La realidad brasileña a día de hoy, al no existir una legislación y jurisprudencia claramente comprometida con la protección de los datos personales provoca una doble afectación sobre el individuo, que percibe su personalidad amenazada por la insuficiencia de medios que le son puestos a su disposición para controlar la íntegra utilización de los datos que coloca bajo el control de otros en diversos momentos de la vida moderna e inhibe la acción administrativa por el no establecimiento de pautas firmes de cuándo y cómo actuar eficazmente en sus funciones a través del uso de las informaciones sobre cada individuo.

De esta forma, la jurisprudencia vacila entre negar a los datos personales el status de la protección constitucional, lo que se verifica notoriamente en los datos de registro en posesión de las operadoras de telefonía y otras empresas privadas, así como en la imposición de graves limitaciones a la divulgación de informaciones de los individuos donde haya efectos patrimoniales claros, como en los datos bancarios y fiscales. Estos casos serán estudiados separadamente para mostrar su propia regulación.

Como bien se verá a lo largo del desarrollo de la presente tesis, la intención es puntualizar entre los aspectos comunes y dispares de las legislaciones europea y brasileña aplicables al sector público. A través de ello se observará si existe el requisito de "adecuación" para la remesa de datos de la Unión Europea a la Administración Pública brasileña.

La metodología a ser utilizada en este trabajo es el de una investigación comparativa del tratamiento del derecho sobre la protección de datos en la Unión Europea y en el Brasil. En el escenario comunitario, no obstante la intención unificadora de la Directiva 95/46/CE, serán analizadas, como hemos señalado, las especificidades del ordenamiento interno de España y de Alemania. Esta verificación auxiliará en la crítica referente a los ajustes necesarios para el mejoramiento de la protección del derecho en el Brasil, ya que permitirá que expongamos como estos países atienden sus requisitos sociales propios. Además, ese abordaje del derecho interno de los tres países remite a la significación de la importancia de las normas y decisiones internacionales sobre la protección de datos. Porque en estas iniciativas se encuentran los marcos para la efectividad de la protección de datos.

El material será recogido con un abordaje cualitativo de manera que abarque las principales decisiones judiciales y bibliográficas relativas a la protección de datos personales en España, Alemania y Brasil. En la Unión Europea, además de los principales tribunales de los países citados, será relevante la investigación de los precedentes existentes en la Corte Europea de Derechos Humanos, en su condición de "auxilio interpretativo para la determinación del contenido y alcance de los derechos fundamentales en las Constituciones Nacionales[11].

El raciocinio elaborado privilegiará el método hipotético deductivo, con un método auxiliar histórico y comparativo, siendo el carácter descriptivo general añadido de un análisis crítico de la jurisprudencia y ordenamiento brasileño en función del concepto de "protección adecuada" presentado.

[11] Conforme BVerfGE 74, 358 (370) e 74, 102 (128).

1 Los efectos de las tecnologías de información y comunicación

1.1 Desarrollo de las tecnologías de almacenamiento y transmisión a partir de la segunda mitad del siglo XX

A partir de la segunda mitad del siglo XX ocurre un continuo avance de la tecnología de información, ya sea en su obtención o transmisión, que permitió el auge del "medio masivo" (*mass media*) y del conjunto de informaciones personales dominadas por el Gobierno y por las empresas comerciales. Sin embargo, como en muchos otros momentos en la historia, la evolución de las tecnologías de información a lo largo de ese período no progresó en una escala constante, siendo al principio bastante tímida y, repentinamente, avanzando simultáneamente en diversas áreas.

Podemos dividir las tecnologías importantes para este estudio en dos grandes campos: las que facilitan la recolección de datos y las que mejoran su distribución. Por tanto, de un lado la creciente capacidad de almacenamiento permite que sea recogida una gran cantidad de datos, sin grandes filtros previos. Asimismo, el aumento de la velocidad de los procesadores garantiza la utilidad de uso, permitiendo que sean realizadas casi de forma automática conexiones lógicas en el material recogido. Por otro lado, la mejora de la comunicación planetaria implica que sepamos cosas de personas con las que nunca tendremos contacto.

Esos cambios en esas tres áreas del conocimiento humano se inician después del 45, pero tienen amplia difusión solamente a partir de la década del 60[12]. El primero de esos campos es la c*omputación*, que avanza con la utilización de la electrónica para la realización de cálculos. El primer ordenador que utilizó válvulas es el famoso *Eletronic Numeric Integrator and Calculator* (ENIAC), capaz de realizar quinientas multiplicaciones por segundo y que pesaba treinta toneladas y ocupaba todo un gimnasio deportivo. Es a través de este modelo primitivo, que John Von Neumann establece la arquitectura hasta hoy usada en esas máquinas, fundada en un lenguaje compuesto de 0 y 1 y cuyas instrucciones para el cumplimiento de las funciones quedaban almacenadas en una memoria interna y no en tarjetas perforadas.

Pero es la microelectrónica la que provoca la "revolución dentro de la revolución"[13].

El *transistor* (***trans****fer resi****stor***), creado en 1947 por los físicos John Bardeen, Walter Houser Brattain y William Bradford Shocley (que ganaron por ello el premio Nobel de Física en 1956) para reemplazar las válvulas, fue imaginado, inicialmente, como un amplificador/interruptor de señales eléctricas, para ser usado en los micrófonos y radios. Sin embargo, fue en 1958 cuando Jack Kilby, ingeniero de Texas Instruments, lo aplicó en su principal función, al imaginar y patentar el *circuito integrado* (también llamado *chip)*, mostrando su capacidad para transmitir señales de forma binaria en una pieza formada por transistores interconectados, y, con ello, permitir la comunicación entre máquinas. La mejora del *design* y el uso perfeccionado del silicio en la fabricación

[12] WESTIN, Alan F. "Social and Political Dimensions of Privacy." Journal of Social Issues, 2003, p. 436.

[13] CASTELLS, Manuel. *A Sociedade Em Rede:* a era da informação: economía, sociedade e cultura. São Paulo: Paz e Terra, 2007, p. 79.

de los *chips*, produjo una significativa caída en su precio, de un 85% entre 1959 y 1962, y después de aproximadamente US$ 50 en 1962 a US$ 1 en 1971 (para comparar el precio del algodón en la Inglaterra de la Revolución Industrial cae 85%. en 70 años, entre 1780 y 1850).

Esa desvalorización permite que la computación modifique su enfoque. Se observa a lo largo de la década del 60 que las organizaciones pasan a ver el ordenador ya no sólo como un medio de automatización del procesamiento de informaciones, sino que también pasan a utilizarlo como centrales de bases de datos. El uso de registros unificado de datos permite compartir informaciones divididas entre diversos departamentos y organizaciones permitiendo de esta forma la unión de esfuerzos tanto en la recolección como en la obtención de resultados[14].

Los peligros de la recolección de nuestros datos personales por parte de otros se inician en este momento histórico, pues se encuentran configuradas las condiciones tecnológicas para una catalogación del individuo, cambiando los medios de tomas de decisiones y las propias relaciones privadas. Los efectos todavía eran limitados en la práctica, pero el deseado continuo avance de la técnica ya preveía la necesidad del debate[15].

La realidad confirmó las previsiones. En 1971, Intel crea el primer *microprocesador*, que es la esencia de los ordenadores personales, capaz de funciones de cálculo y ser programado para tomas de decisiones. El denominado *i4004*, verdadero padre de todas las microcomputadoras, fue creado originalmente para cumplimentar un

[14] WESTIN, Alan F., e BAKER, Michael A.. *Databanks in a free society*. New York: Quadrangle, 1972, p. 230.
[15] WESTIN, Alan F. "Social and Political Dimensions of Privacy... *cit.*, p. 436.

pedido de una fábrica de calculadoras japonesa, era un sencillo circuito integrado programable que trabajaba con registradores de 4 bits, 46 instrucciones, *clock* de 740Khz y contaba con cerca de 2300 transistores. En la secuencia, viendo los potenciales del invento, Intel desarrolla, en 1972, el primer procesador de 8 bits, el 8008, que tenía como características trabajar a una velocidad de 0,2 megahertz (Mhz) y poseer 3500 transistores separados por líneas de conducción de 10000 nanómetros (millonésimos de un milímetro – nm). A modo de comparación de la gigantesca evolución, el chip 80286, también de Intel, diez años más tarde trabaja a 12 Mhz, con 134.000 transistores a 1500 nm y el procesador Cell de la consola Playstation 3 de 2008 funciona a 3000 Mhz, con 234 millones de transistores a 45 nm. O sea, hay un aumento exponencial de la velocidad de procesamiento y del número de funciones procesadas en el tamaño equivalente.

Los ordenadores personales permiten la multiplicación del número de dueños de bases de datos, pero nótese que hasta la década de los 90 los ordenadores en general no tenían conexión entre sí[16]. Por último, y con un impacto profundo en cuanto a las perspectivas transnacionales de la utilización del poder de la información, hay un espectacular avance en las *telecomunicaciones*, apoyado principalmente en el progreso de la optoelectrónica (fibra óptica y láser) potencializada por un conexión en "nodos" (uso en escala mundial de enrutador y conmutadores electrónicos) y un patrón único de comunicación (TCP/IP).

Internet, cuyos orígenes están en la red de ordenadores de una agencia del Departamento de Defensa estadounidense (ARPANET), cuya creación ocurrió en 1969,

[16] WESTIN, Alan F. "Social and Political Dimensions of Privacy... *cit.*, p. 439.

no sería lo que es hoy sin las citadas tecnologías (y tampoco, claro, sin el entusiasmo de individuos en todos los rincones del planeta por intercambiar contenidos a través de ellas). Ella funciona como una potente facilitadora del acceso y disposición de la información, ya que sus direcciones en red (ya sea por medio de e-mail o páginas web) son accesibles a través de pocos caracteres digitados por los usuarios[17].

La conexión entre los ordenadores que era fundamentalmente intra-institucional en los años 80 pasa a ser a escala mundial entre los años 90 y 2000. Podemos achacar ese desarrollo a algunos elementos, que son conjugados e impulsan la espectacular expansión de la interconexión global, como la popularización de nuevos medios de comunicación entre individuos, como los foros de chat y correos electrónicos y la transición a la telefonía inalámbrica, que impone la creación de una potente infraestructura de antenas a escala planetaria para soportar las redes de celulares[18].

Acaeció, por tanto, una coincidente convergencia de tres estupendos avances de la ciencia en la década del 70 que modelan una parte significativa de la realidad social del presente, casi cincuenta años después. La microelectrónica y sus microprocesadores permitieron que los ordenadores aumentasen sus capacidades y se vuelvan accesibles para una buena parte de los individuos, empresas y órganos públicos. Paralelamente hubo pasos que tornaron posible la interconexión comunicacional entre todos los rincones del planeta, una búsqueda de siglos del hombre, que, como una de las principales consecuencias, hizo posible que esta masa de ordenadores en cada espacio territorial aunará esfuerzos con todos los demás, de manera *sinérgica*, demostrando las

[17] TINNEFELD, Marie-Therese, EHMANN, Eugen, , y GERLING, Rainer W. *Einführung in das Datenschutzrecht : Datenschutz und Informationsfreiheit in europäischer Sicht*. München ; Wien: Oldenbourg, 2005, p. 7 y 32.

[18] WESTIN, Alan F. "Social and Political Dimensions of Privacy... *cit.*, p. 441.

ventajas de productividad de una actuación en *red*.

Mientras el beneficio de producción de la Revolución Industrial se puede sintetizar en el uso de máquinas impulsadas por el abaratamiento de los insumos de energía, el paradigma actual se concentra en la producción de riqueza por la brutal reducción de los costos de procesamiento y transmisión de información. Ese modelo económico de la Sociedad de Información posee cinco características básicas: tiene como materia prima *datos* producidos y recogidos por el hombre; actúa sobre un elemento inherente al ser humano, que es su capacidad comunicacional, o sea, tiene accesibilidad directa sobre la experiencia humana; es basada en una *lógica de redes*, las líneas de relación se interrelacionan así como se combinan las líneas producidas por unaaraña, con inherente *complejidad*; al contrario de esta, sin embargo, pueden ser desconectadas o realineadas fácilmente, por tanto, son naturalmente *flexibles*; y, como ya vimos, son creadas por la unión de la microelectrónica, de la lógica computacional y del uso de la electrónica óptica en las telecomunicaciones condensadas en los llamados *sistemas de información*[19].

1.2. La denominada Sociedad de Información

El avance de la circulación de la información en el mundo actual hace que no se torne fuera de lugar el apodo de que vivimos hoy en una "sociedad de la información". Cuando nos referimos aquí a la "Sociedad de Información" como elemento caracterizador del momento actual de la experiencia humana, lo hacemos admitiendo

[19] CASTELLS, Manuel. *A Sociedade Em Rede... cit.,* p. 109.

que podemos caracterizar el *modo de desarrollo* actual como cimentado en la *información*, asumiéndolo como núcleo de importantes transformaciones en la esfera económica, de poder y cultural. Ese "*Informacionismo*" no destruye el capitalismo como *modo de producción* hegemónico, aunque le provoque importantes adaptaciones, pero reemplaza, gradualmente, a la "Industrialización" surgida del siglo XVIII. Por ello, mientras la Revolución Industrial definió bases económicas que buscaban eminentemente el aumento de la producción a través de máquinas alimentadas por nuevas fuentes generadoras y de distribución de energía, actualmente, aunque no se haya abandonado ese ideal, existe una centralidad en la búsqueda de procedimientos que permitan la progresiva evolución de las tecnologías de procesamiento, información y comunicación, impulsados por el reconocimiento que esas técnicas componen hoy el eje de la riqueza y poder mundial [20].

Podemos decir que la terminología *sociedad de información* "representa una forma de *economía* y un tipo de *sociedad postindustrial* en la que el protagonismo de la producción y de la distribución de bienes parece desplazarse hacia una sociedad de servicios en cuyo centro se sitúa la obtención, procesamiento y distribución de *información*"[21].

Ello no significa menospreciar la importancia de la información en épocas pasadas, ni el impacto en el desarrollo como el invento del papel o el perfeccionamiento en las técnicas de impresión y tipografía realizadas por Johannes Gutenberg, sino, asumir que actualmente existe la posibilidad que ofrecen los medios para aprovecharla

[20] CASTELLS, Manuel. *A Sociedade Em Rede... cit.,* p. 61.
[21] BARNES VÁZQUEZ, Javier. "Sobre el procedimiento administrativo: evolución y perspectivas." In *Innovación y reforma en el derecho administrativo / coord. por Javier Barnes Vázquez.* Sevilla: Derecho Global, 2006, p. 301.

integralmente, a través de la potencialidad incomparable que la informática y el texto electrónico aporta para el almacenamiento de datos y la consecuente acumulación de conocimiento, aun más cuando combinados con un estadio comunicacional permite un acceso instantáneo desde cualquier punto del planeta, evidentemente modificando nuestra relación con el espacio y el tiempo. Tenemos entonces dos grandes modificaciones en la sociedad y en la economía que son dignas de destaque; por un lado, hubo un notable incremento en la potencia de alcance de la producción eminentemente intelectual y por el otro, la interconexión generó un mercado de trabajo absolutamente ininterrumpido y cuya cooperación puede ocurrir sin limitaciones de simultaneidad o proximidad física.[22].

Desde el punto de vista de amplitud y velocidad, podemos trazar igualmente una distinción significativa entre la Revolución Industrial y la revolución causada por las nuevas "tecnologías de la información". Mientras que la primera ocurrió de manera gradual y selectiva, primero afectando la vida en Gran Bretaña y luego desplazándose hacia el resto del mundo, con distintos alcances y en diferentes épocas como se desprende de la revisión histórica de los Estados Unidos, de la Europa Occidental, de Latinoamérica, África y Asia; el cambio informacional en cambio, se extendió a todos los rincones del globo en tan solo 40 años[23].

---

[22] TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*, p. 8.

[23] Aunque, evidentemente, se pueda hablar en diferentes situaciones de apertura y estadio tecnológicos, el hecho es que ese tipo de tecnología se tornó de tan fácil acceso a cada individuo, que aun la opresión estatal o pobreza de un país no les permiten el aislamiento a esa "comunidad de información global", como demuestra el flujo constante de datos que podemos recibir de países tan distintos como Irán, Sudán, Brunei, Honduras o Albania (CASTELLS, Manuel. *La era de la información: economía, sociedad y cultura*. Vol. II. Barcelona: Alianza Editorial, 1997, p. 286). En especial, se destaca la consagración de la condición de Internet como servicio utilizado en general por la sociedad tan diseminada y natural como el suministro de agua y electricidad. Esa relevancia, como apunta el constitucionalista estadounidense JACK BALKIN, quedó muy bien expuesta durante el movimiento que derivó en la caída de Hosni Mubarak en 2011. Aunque las redes sociales fueran una de las principales maneras de circulación de la información dentro de las filas opositoras, el derrumbe de la conexión dentro del país fue una medida deslegitimadora del gobierno combatido, representando una

Vivimos hoy, por tanto, en una sociedad que, conforme la previsión orwelliana, la información ocupa un lugar esencial. Esa condición de imprescindible es fruto inicialmente de la radical urbanización de la sociedad, que empieza con la Revolución Industrial y se intensifica en el siglo XX, por razones de orden económico y político. La transmutación de la organización en torno a pequeños agrupamientos rurales hacia la vida en grandes ciudades, tornando extremadamente más compleja la división de bienes para la convivencia social adecuada, y la profundización de la democracia con la consagración del sufragio universal, exigieron del hombre el conocimiento del otro como condición de tornar factibles eses nuevos modos de vida[24]. De la misma forma que marchamos de una sociedad agraria hacia una sociedad industrial, hoy avanzamos de ella hacia una sociedad informacional[25].

La potencialidad de esa importancia de la información dependió del desarrollo acelerado de la "informática", entendida como ciencia del tratamiento automático de la información[26]. Las máquinas iniciales, de alto costo y dimensiones equivalentes a verdaderas viviendas, fueron gradualmente evolucionando hacia equipamientos que realizan millones de veces más rápido las mismas operaciones en pequeños circuitos electrónicos con precios accesibles a una buena parte de los individuos. Es posible incluso decir, que estamos siendo testigos de una 2ª revolución industrial, puesto que el avance científico en ese campo permitió transformaciones económicas, culturales,

---

demostración al mismo tiempo de debilidad y preanuncio de falta de respeto a los derechos humanos de la población, además de causar perjuicios económicos al comercio del país, notoriamente en el sector de turismo (BALKIN, Jack. "The First Amendment is an Information Policy." In *The 20th Annual Hugo L. Black Lecture on Freedom of Expression*. Wesleyan University, 2011).

24 PÉREZ ROYO, Javier. *Curso de derecho constitucional... cit.*, p. 324 e 325.

25 PITSCHAS, Rainer e SCHOLZ, Rupert. *Informationelle Selbstbestimmung und staatliche Informationsverantwortung*. Berlin: Duncker & Humblot, 1984, p. 18.

26 CONDE ORTIZ, Concepción. *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*. Madrid: Dykinson, 2005, p. 13.

sociales y políticas de magnitud semejante a las que se sucedieron cuando la fuerza animal fue reemplazada por la máquina a vapor[27]. Ello se suma al igualmente espectacular desarrollo de las telecomunicaciones que permiten prácticamente que exista una transmisión de datos en tiempo real y en cualquier lugar del mundo[28].

1.3. Técnicas actuales de recolección involuntaria de datos del individuo.

Es fácil constatar que en la economía actual la información se tornó la materia prima de mayor valor y el consumidor/elector un elemento central del patrimonio de las empresas/gobiernos. Con Internet, el marketing de masas puede ser reemplazado por la propaganda individualizada, lo que permite que aquel que pretende conquistar ofrezca la promesa de dar exactamente lo que aquel individuo quiere escuchar. La ventaja en la competencia por la facilidad de acceso a diversas ofertas que ofrece la navegación por los grandes motores de búsqueda, se ve neutralizada cuando el proveedor recoge tantos datos sobre las características, hábitos y preferencias de los particulares, de su potencial público o usuario que llega a conocer sus tendencias incluso, hasta mejor que él propio ciudadano. Y si los grandes procesadores resuelven el problema del procesamiento de ese total de informaciones, la recolección de estas es objeto de estrategias más sutiles.

---

[27] TÉLLEZ AGUILERA, Abel. *Nuevas tecnologías, intimidad y protección de datos: con estudio sistemático de la Ley Orgánica 15-1999*. Madrid: Edisofer, 2001, p. 22. Sintetiza BOBBIO la distancia histórica: "Hoy es imposible comparar el conocimiento que un monarca absoluto como Luis XIII o Luis XIV tenía de los propios súbditos con el conocimiento que el gobierno de un Estado bien organizado puede tener de los propios ciudadanos. Cuando leemos las historias de los jacqueries, reparamos cuan poco conseguía 'ver' el monarca con su aparato de empleados, y como las revueltas explotaban sin que el poder, a pesar de absoluto, estuviera en condiciones de prevenirlas, aunque no fuera sutil al reprimirlas" (BOBBIO, Norberto. *O futuro da democracia*. São Paulo: Paz e Terra, 2004, p. 120).

[28] MURILLO DE LA CUEVA, Pablo Lucas. *El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática*. Madrid: Tecnos, 1990, p. 106.

Existe en Internet un foco privilegiado para esa recolección involuntaria. Cuando estamos identificados (ya sea por medio de un login o de un IP ya conocido) durante el acceso a un sitio web de Internet, es posible que la empresa vea, ya sea a través del intercambio de páginas o incluso, al deslizar el cursor, todos aquellos elementos que atraen nuestro interés. Consecuentemente, puede establecer proyectos de atención personalizada en nuestra próxima visita y estimular voluntades que tal vez sean hasta inconscientes en nosotros mismos. En el ámbito colectivo, una empresa, por ejemplo, puede trazar perfiles de usuarios con los mismos perfiles socioeconómicos y de esta forma establecer mejor sus focos de actuación. La primera y más común es la *falsa gratuidad* de algunas ofertas. Esa no debe ser confundida con las posibilidades de cooperación de trabajo entre profesionales sin derecho a un interés económico, como se observa en la creación de *software* de código libre como el *Linux* y el *Open Office*. Se abordan aquí las propuestas encontradas abundantemente en la Gran Red de ciertos beneficios al internauta que dispensan toda contraprestación, especialmente la pecuniaria, salvo el registro de un "sencillo" formulario.

Tanto en esos casos, como en operaciones de comercio electrónico o cualquier atención no presencial (por teléfono, por ejemplo) se sucede frecuentemente esta práctica sutil de pasaje de los datos privados del usuario a una persona jurídica[29], que, debido a la ausencia de límites legales, los podrá utilizar o vender más adelante a otra empresa que desea conocerlo profundamente. Además de los campos a ser completados, los cuales los analistas prevén que se tornarán, paso a paso, más inquisitoriales, profundizándose en la intimidad del internauta[30], se negocia también todo que pueda ser

[29] TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*, p. 51.

[30] BELLEIL, Arnaud . *@-privacidade: o mercado de dados pessoais: protecção da vida privada na idade da internet*.Lisboa: Instituto Piaget, 2001, p. 21.

observado a distancia por el dueño de sitio sobre el individuo, como el origen de su IP y los *banners* que provocan mayor interés.

En las redes sociales (como *facebook, orkut,* etc.) la retirada de la información necesita una investigación por parte de la persona que quiere formar la base de datos (en regla no es el usuario que va hacia él), pero envuelve categorías más privadas, porque el individuo enumera características y opiniones cuyo conocimiento en principio estaría reservado a amigos y familiares[31]. Ello, claro, cuando no es el propio ente creador de la red social que pretende almacenar (y vender) las informaciones escritas sin preguntarle al usuario o, incluso, en contra de su voluntad[32].

También la falta de regulación en la formación de base de datos fortalece la proliferación de sitios que son utilizados por aquellos que pretenden aprovecharse de la información personal en beneficio propio y en desprecio del perjuicio que causan a los afectados para exponer detalles demeritorios, ciertos o no, sobre desafectos, el llamado *bullying virtual*.

Aun con el sencillo uso de ordenadores e Internet, desasociado de las situaciones antes mencionadas, ya permite registros. Las compañías telefónicas mantienen el constante control de quien utiliza un determinado IP en aquella hora y el sencillo *eliminar* de un archivo en el disco rígido no impide que un perito vea aquel registro posteriormente.

---

[31] Un fenómeno aun peor, ocurre cuando hay técnicas maliciosas de invasión de los ordenadores personales para retirar nuestras informaciones que no deseamos revelar. Para ello surgen, como defensa, los software de *firewall* , para controlar el flujo de datos entre nuestros ordenadores y la red de ordenadores, así como, de detección de *vírus* (TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*, p. 33).

[32] Para una contextualización de esa práctica dentro de la regulación de los datos personales, vea GRIMMELMANN, James. "Saving Facebook". *Iowa Law Review*, 2009, p. 1195 y siguientes.

No sólo a través de Internet y en la telefonía la recolección de datos forma parte de nuestras vidas. En las calles, es trivial ser fotografiados sin que lo percibamos o cámaras de seguridad grabando nuestras actitudes, y las técnicas de identificación facial automática se ven en franca expansión. Lo mismo sucede dentro del ambiente de trabajo. Aparatos con GPSs y vehículos más avanzados emiten nuestra latitud y longitud actual, frecuentemente por nuestra voluntad para protección y auxilio en el tránsito.

Por último, el abaratamiento en el uso de la identificación biométrica a través del ADN nos garantiza prácticamente verificar con absoluta certeza hechos pasados con determinados individuos y ya se habla incluso, de registros nacionales de datos genéticos de los ciudadanos[33]. Además, las organizaciones de medicina utilizan crecientemente técnicas de *telemetría*, recogida a distancia de datos sobre pacientes[34], como forma de centralizar (y disminuir) los costos de diagnósticos.

Llegamos a la realidad actual en que hay una serie de actividades rutinarias, públicas y privadas, en que el individuo se ve, muchas veces hasta subrepticiamente, monitoreado y catalogado por otro. El Gobierno impone todo el tiempo el relleno de formularios para cualquier autorización que concede. También los movimientos bancarios y las utilizaciones de tarjeta de crédito son constantemente monitoreados, en principio para evitar el lavado de dinero de la criminalidad y del terrorismo. Todos esos registros se tornan pasibles de amplios rastreos computadorizados[35].

---

33 FROOMKIN, A. Michael. "The Death of Privacy?." *Stan. L. Rev.*, 1999, p. 1495.

34 GARCÍA-BERRIO HERNÁNDEZ, Teresa. *Informática y libertades : la protección de datos personales y su regulación en Francia y España*. Murcia: Servicio de Publicaciones de la Universidad de Murcia, 2003, p. 78.

35 TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*, p. 60.

Los objetivos son idénticos independientemente de la titularidad de quien posee la información o de aquel que la desea: tornar posible que los individuos sean separados, clasificados y seleccionados para determinados objetivos.

1.4. La informática como un problema jurídico

Ese avance de la denominada "telemática", extendida exponencialmente por la consolidación de Internet, torna aun más apremiante nuestro análisis sobre el tema desde el punto de vista del Derecho, tal como técnica del ejercicio del poder que es en el Estado Moderno[36], pues la transformación de la tecnología garantiza la existencia también de un "Poder Informacional"[37].

Podemos decir que el sector jurídico tiene un interés interno y externo sobre ese nuevo método de investigación y documentación. Internamente las nuevas tecnologías permiten archivar y catalogar la enorme gama de informaciones vinculadas a la ciencia jurídica. El acceso a fuentes legislativas, jurisprudenciales y doctrinarias, que la tecnología actual permite a los investigadores y operadores del Derecho, es tan inmensa que al mismo tiempo aumenta la interconexión, facilita los análisis y los torna más completos. El interés externo, sin embargo, está vinculado a las soluciones y problemas jurídicos a la sociedad y a los ciudadanos provenientes de la difusión de sistemas de tratamiento electrónico.

---

[36] TROPER, Michel. *A filosofía do direito*. São Paulo: Martins Editora, 2008, p. 70.

[37] TINNEFELD, Marie-Therese, EHMANN, Eugen, , y GERLING, Rainer W.. *Einführung in das Datenschutzrecht... cit.*, p. 1.

De esa manera surge la necesidad de un estudio específico denominado "Derecho Informático", entendido como el conjunto de reglas jurídicas, nacionales e internacionales, que buscan regir la utilización de la tecnología vinculada a los sistemas informáticos sobre todos los matices de la existencia humana. A propósito, la doctrina más reciente ya alerta incluso sobre la insuficiencia de esa nomenclatura, observando la vinculación cada vez más cercana entre informática y comunicación y, por tanto, optando por la denominación "Derecho de las Nuevas Tecnologías", donde se estudiaría "el conjunto de normas y principios que regulan los actos y relaciones jurídicas constituidas por medio de las nuevas tecnologías de la información y de la comunicación y el uso y abuso de las mismas en cuanto afecte a los derechos y libertades de los ciudadanos o a los intereses generales"[38].

Surgen aquí varios temas con interés jurídico. Por ejemplo, existe un aspecto externo dentro del propio aspecto interno descripto, que es la cuestión de la *validad* de los actos jurídicos en general cuya comunicación o incluso existencia, solamente o primordialmente se brinde de forma digital. Es el crecimiento de una esfera que podemos llamar *e-government*[39] y de las contrataciones electrónicas entre particulares. También son nuevos objetos de estudio jurídico la aplicación del derecho de propiedad industrial e intelectual, pensada sobre términos físicos, con relación a la confección intelectual de códigos binarios sobre los cuales funcionan los *softwares* necesarios para nuestros ordenadores, y por último, el funcionamiento de las relaciones internacionales

[38] TÉLLEZ AGUILERA, Abel. *Nuevas tecnologías... cit.*, p. 44.

[39] Cuya consagración en el ordenamiento jurídico español se encuentra en el artículo 45 de la ley 30/1992, que regula el régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo, con especial interés a su apartado 5 ("Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras leyes.").

en cuanto al "flujo de datos transnacionales".

Los juristas de derecho público, desde las últimas décadas del siglo XX, reflexionan sobre esa importancia de la informática para la reforma de la Administración, para que ésta pueda cumplir adecuadamente los objetivos del Estado Social, pero también sobre los riesgos derivados[40]. Como afirma el Prof. PÉREZ LUÑO:

> "En una sociedad como la que nos toca vivir en la que la información es poder y en la que ese poder se hace decisivo cuando, en virtud de la informática, convierte informaciones parciales y dispersas en informaciones en masa y organizadas, la reglamentación jurídica de la informática reviste un interés prioritario. Es evidente, por tanto, que para la opinión pública y el pensamiento filosófico, jurídico y político de nuestro tiempo constituye un problema nodal el establecimiento de unas garantías que tutelen a los ciudadanos frente a la eventual erosión y asalto tecnológico de sus derechos y libertades."[41]

El fenómeno informático se conecta de esta forma directamente sobre la tensión poder – libertad– control típico del Estado Moderno[42].

Desde el punto de vista de los derechos fundamentales, y por tanto, conforme el tema de este trabajo, hay una preocupación de cómo se debe dar la relación entre el "poder informático" de quien es titular de una base de datos cuando entra en conflicto con la esfera de libertad del ciudadano cuyo perfil está almacenado[43].

---

[40] Destáquese en los primeros añosla reacción de la opinión pública francesa al proyecto SAFARI (*Systeme Automatisé pour les Fichiers Administratifs et le Répertoire des Individus*), en que el gobierno, a través del Instituto Nacional de Estadística, pretendía unificar los archivos públicos (y todos sus datos) de los ciudadanos sobre un número de identificación único (TÉLLEZ AGUILERA, Abel. *Nuevas tecnologías... cit.*, p. 27).

[41] PÉREZ LUÑO, Antonio Enrique. *La tercera generación de derechos humanos*. Cizur Menor: Thomson-Aranzadi, 2006, p. 32.

[42] CASTELLS ARTECHE, José Manuel. La limitación informática. In: *Estudios sobre la Constitución Española (Homenaje al Profesor Eduardo Garcia de Enterria): Tomo II ("De los derechos y deberes fundamentales").* Editora Civitas: Madrid, 1991, p. 939.

[43] FROSINI, Vittorio. "Problemas Jurídicos de la información y la documentación." In: PÉREZ LUÑO, Antonio-Enrique (director de la edición), *Problemas actuales de la documentación y la informática jurídica: actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986*. Madrid: Tecnos, 1987, p. 50.

1.5. Las perspectivas involucradas en el almacenamiento y uso de datos personales por parte de la Administración: información y protección de datos

La suma de los ámbitos en que somos obligados a suministrar los más diferentes tipos de datos al Estado, como por ejemplo, a la Seguridad Social, a la Administración Tributaria y a las Fuerzas Policiales, permite que, sin control, la interconexión de esos órganos torne posible el análisis de los aspectos más recónditos de nuestra personalidad. Al mismo tiempo, no puede haber engaño de que la amenaza a los datos personales también surge del poder empresarial. Las grandes corporaciones privadas poseen vastos intereses económicos sobre el control de datos del mayor número de personas, teniendo en cuenta que forman parte de posibles futuros clientes[44]. En ambos casos el medio de poder del titular de la base de datos es similar: intentan establecer *perfiles* de los seres humanos sobre los cuales poseen informaciones de forma que los manejen para sus propios propósitos[45].

Cuando la discusión acerca de los efectos sobre el hombre de la tecnología necesaria para el mantenimiento del nivel de vida proporcionado por el *Welfare State*[46] surgió, en la década del 60, la producción intelectual se inclinaba por abordar solamente

---

[44] Cítese, como ejemplo, empresas de crédito en los Estados Unidos que y poseían centenas de millones de personas registradas desde la década del 70 (PÉREZ LUÑO, Antonio Enrique. *Derechos humanos, estado de derecho y constitución*. Madrid: Tecnos, 2005, p. 352 y 387).

[45] Hay una interesante norma en el artículo 11 de la *Staatsvertrag* (entre el *Bund* y los *Länder*) de 1983 que impide toda investigación de competencia pública en las seis semanas anteriores a la elección, por su posibilidad de favorecer a los estrategas del partido en el gobierno (RODOTÀ, Stefano. *A Vida na Sociedade da Vigilância* . Rio de Janeiro: Editora Renovar, 2008, p. 63).

[46] Cabe recordar, a propósito, que hasta la Revolución Francesa la cantidad de información que el Estado guardaba sobre sus ciudadanos era ínfima (PÉREZ LUÑO, Antonio Enrique. *Derechos humanos, estado de derecho y constitución... cit.*, p. 339).

el efecto nocivo sobre el ser humano. Ello condujo a una serie de obras que alertaba sobre los peligros que tecnología acarrearía al desenvolvimiento de la libertad humana.[47].

Pues el manejo agregado de múltiples datos individuales, a principio insignificantes, permite fácilmente el análisis completo de su personalidad, tornándolo "transparente" a quien administra el archivo de las informaciones. La mutación de nuestras "sociedades de masa" en "sociedades de información", en vez de facilitar la fuga humana de la estandarización dentro del colectivo, conduciría a la híper clasificación que atrofia la libertad por el exceso de control[48]. La tecnología hoy existente torna posible el ideal *panóptico*, de conseguir la obediencia ininterrumpida por medio de la indicación a los vigilados de que son vistos incluso cuando no son visibles sus observadores[49].

La protección de los datos personales explica que aquel cuya información consta en una base de datos no es un mero proveedor de información, sino que es un ser humano cuyo dato registrado participa e *influye en* su experiencia como tal. Al garantizar al individuo los derechos sobre la circulación y uso de sus datos este derecho fundamental subraya la importancia de no considerar al hombre como medio u objeto de determinadas estrategias o políticas, sino, siempre como elemento primordial de valoración por la acción estatal[50].

---

47 Como representativo de esa visión, véase MARCUSE, Herbert. *El hombre unidimensional: ensayo sobre la ideología de la sociedad industrial avanzada*. Barcelona: Ariel, 1994.

48 RODOTÀ, Stefano. *A Vida na Sociedade da Vigilância... cit.,* p. 157.

49 FOUCAULT, Michel. *Vigiar e Punir : Historia Da Violência nas Prisões.* Petrópolis: Vozes, 2004, p. 165.

50 PÉREZ LUÑO, Antonio E.. "Informática y libertad. Comentario al artículo 18.4 de la Constitución." Revista de Estudios Políticos, Noviembre 1981, p. 38.

Sin embargo, la progresiva aceptación de la inevitabilidad y continuidad del avance de la técnica cambió esta perspectiva. Es innegable la importancia de algún conocimiento por parte del Estado de nuestras bases de datos personales. Es indispensable la recolección de datos de su población para la reorganización y mejora de la Administración Pública en una época de crisis financiera en que se requiere realizar una elección de los beneficiarios de las prestaciones del Estado Social[51]. El conocimiento de la población también es especialmente útil en los servicios públicos que tienen por objeto la protección en general, como se sucede en la seguridad pública o en la vigilancia sanitaria, y para ejercer de forma adecuada su política fiscal, estableciendo eficazmente su previsión de ingresos. La necesidad de la realización de la citada programación de los entes públicos se da como medio de reducir las injusticias y desigualdades; al mismo tiempo explica la imposibilidad de negar la existencia de un interés público en la intervención estatal en los datos personales[52].

La utilización y almacenamiento de datos personales por parte del Estado, aunque con distinta intensidad conforme el nivel de desarrollo tecnológico de una sociedad, alcanza indistintamente a todos los que pretenden sumar en su entereza los niveles de calidad de vida prometidos por la fórmula del "Estado Social"[53] con la legitimidad necesaria de un "Estado Democrático de Derecho". Así se expresa el profesor DIEGO LÓPEZ GARRIDO:

> "En efecto, el llamado Estado de 'bienestar', el Estado intervencionista moderno, expresa la gran contradicción, el gran *impase*, entre un desarrollo económico acelerado y unas estructuras políticas más propias de la sociedad decimonónica. Como se ha dicho por Ferrajoli, el Estado de bienestar contiene una bifurcación interna entre la estructura *legal* y *real* de la organización

[51] RODOTÀ, Stefano. *A Vida na Sociedade da Vigilância... cit.,* p. 57.
[52] BENDA, Ernst. "Dignidad Humana y Derechos de la Personalidad". In *Manual de derecho constitucional*. Madrid [etc.]: Marcial Pons, 2001, p. 131.
[53] MURILLO DE LA CUEVA, Pablo Lucas. "Perspectivas del derecho a la autodeterminación informativa." *IDP: Revista de Internet, Derecho y Política, Nº. 5*, 2007, p. 30.

> social. Se asiste a una actividad administrativa crecientemente tecnocrática; a una opacidad en la burocracia y en los aparatos del Estado; y frente a ello unos cada vez más impotentes principios clásicos del Estado de Derecho que sufren en su potencialidad. El principio de legalidad, el principio de publicidad, el principio de control, son a veces reliquias del siglo pasado que en absoluto pueden adaptarse a la complejidad ambiental de la nueva civilización.
> (...)
> Pues bien, la informática es aprovechada en esas circunstancias para potenciar los factores de crisis política, de descenso en la democraticidad de los aparatos estatales, que corresponde a un descenso también de la legitimidad del sistema. La informática es utilizada para una burocratización mayor, para un autoritarismo mayor (...)"[54]

Para la Administración Pública, el poseer el acceso a las informaciones sobre sus administrados le da la ventaja de realizar sus funciones de manera más exitosa, tomando las mejores[55] decisiones sobre las situaciones que le son presentadas. Sobre ese aspecto podemos decir que la exigencia de suministro de informaciones funciona como un tributo público más[56].

La Administración Pública se debe adaptar a las mejores formas de enviar y recibir información de los ciudadanos y aprender a utilizar la colaboración de entes privados y públicos dotados de bases de datos propios, pero, al mismo tiempo, tiene que establecer medios de protección de los datos individuales que maneje[57].

No obstante, las posibilidades resultantes del avance de esta tecnología durante el siglo XX hasta el presente siglo XXI, sobre todo para el tratamiento, almacenamiento y recuperación de datos, que hicieron que las relaciones humanas sean, cada vez más, llevadas a cabo virtualmente y que los datos personales hayan adquirido un gran valor

---

54 LÓPEZ GARRIDO, Diego. "La sociedad informatizada y la crisis del Estado de bienestar." *Revista de estudios políticos*, 1985, p. 40.

55 Lo que no equivale a aceptar el mito de la perfectibilidad de las decisiones computadorizadas, que así no serían sujetas a discusión o resistencia (BENDA, Ernst. "Dignidad Humana y Derechos de la Personalidad... *cit*, p. 141).

56 HOFFMANN-RIEM, Wolfgang, (ed.). *Verwaltungsrecht in der Informationsgesellschaft*. Baden-Baden: Nomos-Verl.-Ges., 2000, p. 13.

57 Además, esas elecciones deben ser frecuentemente revisadas, de modo que sean capaces de responder a los continuos desarrollos tecnológicos (BARNES, Javier. "Sobre el derecho administrativo de la información". *Revista catalana de derecho público*, 2007, p. 21).

económico, directo o indirecto[58], continúan acarreando el peligro de que la autonomía individual se vea rezagada por el hermetismo en el control total sobre los datos, que se encuentran depositados en algunos centros de poder. El costo de la anticipación administrativa y de la estructura burocrática planificadora es la posibilidad de disminución de los campos del control personal y de la instrumentalización de la persona humana[59].

Al contrario de retroceder, hay una agudización de esa tensión-llave "Protección de datos personales vs. Poder informático" en la política de los gobiernos actuales, muchos de ellos hoy obsesionados con la idea de una "ideología de seguridad" en detrimento de los valores democráticos[60]. Somos testigos de la proliferación de acciones policiales *preventivas*, que, al contrario de las denominadas *represivas*, que pretendían encontrar los ilícitos cometidos por un ciudadano en el pasado, se presta a descubrir a aquellos ciudadanos que cometerán delitos *futuros*, en una lógica en que surge un contenido de extensión casi interminable[61]. Señala NORBERTO BOBBIO:

> "Si manifesté alguna duda de que la computadoracracia pueda beneficiar a la democracia gobernada, no tengo ninguna duda sobre los servicios que puede prestar a la democracia gobernante. Lo ideal del poderoso siempre fue lo de ver cada gesto y escuchar cada palabra de los que están a él sometidos (si es posible sin ser visto ni escuchado) : hoy este ideal es alcanzable. Ningún déspota de la antigüedad, ningún monarca absoluto de la edad moderna, a pesar de cercado por mil espiones, jamás consiguió tener sobre sus súbditos todas las informaciones que el más democrático de los gobiernos actuales puede obtener con el uso de los cerebros electrónicos. La vieja pregunta que recorre toda la historia del pensamiento político - "¿Quién custodia a los custodios?" - hoy puede ser repetida con esta fórmula: "¿Quién controla a los controladores?"."[62]

Esa tensión es constante en la historia del surgimiento del derecho a la protección de datos personales. Tras la decisión del Tribunal Constitucional Alemán de

---

58 MURILLO DE LA CUEVA, Pablo Lucas. "Perspectivas del derecho a la autodeterminación informativa... *cit.*, p. 21.
59 BENDA, Ernst. "Dignidad Humana y Derechos de la Personalidad... *cit.*, p. 137.
60 LÓPEZ GARRIDO, Diego. "La sociedad informatizada y la crisis del Estado de bienestar... *cit.*, p. 36.
61 *Ibid.*, p. 39 e BENDA, Ernst. "Dignidad Humana y Derechos de la Personalidad... *cit*, p. 133.
62 BOBBIO, Norberto. *O futuro da democracia... cit.*, p. 43.

1983 que consagró el derecho fundamental en este país, ERHARD DENNINGER dividió en tres campos las reacciones que surgieron. Por una parte, estaban aquellos que disminuían al máximo las consecuencias de la decisión, e incluso, la reserva de ley exigida, entendiendo que las normativas que regulaban el "derecho de policía" en Alemania eran suficientes para el enfrentamiento de las cuestiones puestas por el Tribunal[63]. En el polo opuesto estaban los Comisarios de Datos, abogados a los que se presentaba un mandato para crear una reglamentación protectora del derecho fundamental, como expresaron en su Resolución 27/28 de marzo de 1984. La tercera respuesta sería una cierta combinación de las dos primeras: por un lado se esperaba una amplia regulación, aunque sin cortar el *status quo* vigente para las fuerzas de seguridad en Alemania[64].

La obsesión con seguridad, potencializada con los ataques terroristas de los últimos años sólo llevó al aumento de la vigilancia de nuestro "cuerpo electrónico" hacia el absoluto y exige reflexionar sobre los usos de tecnología democráticamente admisibles, frente a su indispensabilidad para el orden y el bienestar social, y aquellos que no son[65].

Existe por tanto, un conflicto constante entre el uso positivo y negativo de las

---

63 Representando bien esa posición está la doctrina RAINER PITSCHAS Y RUPERT SCHOLZ. Al comentar sobre la decisión de la "autodeterminación informativa", indicaron que esa no debería ser analizada sin observar la función estatal constitucional de la "previsión informativa" (*Informationsvorsorge*), corolario del principio del Estado Social y de Derecho (Art. 28 I / 20 I GG) y del "derecho fundamental a la seguridad". Además advirtieron los límites de la propia acción parlamentaria al normativizar la protección de datos, ya que no debería ser desconsiderado un espacio de conformación propio de las Administraciones Públicas, fruto de su responsabilidad informativa (*Informationsverantwortung*). La conclusión era inevitable: los intercambios de informaciones entre las policías y los demás órganos encargados de la seguridad pública no necesitan grandes cambios en fase del modo que ya eran hechas (PITSCHAS,Rainer y SCHOLZ, Rupert. *Informationelle Selbstbestimmung... cit.*, p. 201).

64 DENNINGER, Erhard. "El derecho a la autodeterminación informativa." In *Problemas actuales de la documentación y la informática jurídica : actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986*. Madrid: Tecnos, 1987, p. 269.

65 RODOTÀ, Stefano. "Democracia y protección de datos." *Cuadernos de derecho público*, 2003, p. 26.

técnicas de informática y comunicación por el Estado, la cual no es simplemente resoluble por una negación y rebelión contra las máquinas y contra ese proceso[66], incluso, porque dejaría lagunas de poder que fatalmente serían ocupadas por otros actores[67] y sería una medida simplemente inútil frente al estadio continuamente englobante de nuestras vidas por parte de las tecnologías de información y comunicación[68].

En verdad, la combinación del estadio actual de las tecnologías de almacenamiento de información y comunicación aumentó todavía de forma más acentuada el poder de control descentralizado de ciudadanos sobre otros, de lo que incrementó las capacidades de la vigilancia vertical de la burocracia. O sea, el Estado solo puede controlar mejor a sus ciudadanos con las nuevas tecnologías, pero aquellos también pueden con estas producir más daños a la omnipotencia del aparato de vigilancia. El derecho a la protección de datos es entonces un condicionamiento del derecho de información del ciudadano, pero también este complementa a aquel. Existe un evidente peso en sociedades democráticas en que la decisión popular tenga el mayor número de subsidios fácticos posibles y que se disponga de una Administración pública con transparencia y, por consecuencia, más próxima a la población[69].

La existencia de una regulación que organiza el funcionamiento de bases de datos personales se conduce, por tanto, dentro de un camino de su aceptación sin el

---

66 BENDA, Ernst. "Privatsphäre und 'Persönlichkeitsprofil'". In *Menschenwürde und freiheitliche Rechtsordnung : Festschrift fur Willi Geiger zum. 65. Geburtstag*, organizado por Gerhard Leibholz et al. Tübingen: Mohr, 1974, p. 25.

67 BENDA, Ernst. "Dignidad Humana y Derechos de la Personalidad". In *Manual de derecho constitucional*. Madrid [etc.]: Marcial Pons, 2001, p. 138.

68 PETERSEN, Stefanie. *Grenzen des Verrechtlichungsgebotes im Datenschutz*. Münster ; Hamburg [u.a.]: Lit, 2000, p. 124.

69 *Ibid.*, p. 194-195 e PÉREZ LUÑO, Antonio Enrique. *Derechos humanos, estado de derecho y constitución... cit.*, p. 347.

endiosamiento de sus potenciales ni el menosprecio de su afectación a la dignidad humana. Cómo garantizar la seguridad social sin perder de vista como la merma de control de datos personales afecta la comunicación y participación humana. Ese es el entorno de opciones que permeará las soluciones institucionales que ahora serán analizadas.

1.6. Conceptos centrales: Datos – Información - Conocimiento

Los tres conceptos esenciales para el propósito de este estudio son datos – información – conocimiento. La definición se torna sencilla cuando se observa desde el punto de vista de aquel que posee el archivo: un dato sólo se torna propiamente una información cuando agrega a su contenido la identificación de la persona a la que se refiere, y entonces permite interpretaciones[70]. Esa información, al principio atomizada, organizada dentro de un contexto y con objetivos mínimamente definidos se transforma en conocimiento[71].

Desde el punto de vista de las "teorías de las bases de datos", esa relación sería representada por la existencia de un identificador (clave primaria) y un dato a él relacionado. Este identificador puede ser considerado "real", cuando sólo puede estar relacionado a un único individuo (como, por ejemplo, en el número de identidad gubernamental) o "parcial", si ello no fuera posible (dígase una identificación por nombre y apellidos únicos, que incluya, así, todos los homónimos, sin que sean agregadas fecha de nacimiento, nombre de la madre, etc.)[72]. Además, el "identificador"

[70] TRUTE, Hans-Heinrich. "Der Schutz personenbezogener Informationen in der Informationsgesellschaft?." Juristenzeitung, 1998, p. 825.
[71] HOFFMANN-RIEM, Wolfgang (ed.). *Verwaltungsrecht in der Informationsgesellschaft... cit*., p. 12.
[72] BERCIC, Bostjan, y GEORGE, Carlisle. "Identifying Personal Data Using Relational Database

puede ser “explícito”, cuando envuelve datos calificativos (nombre, apellido, residencia, etc.), o “implícito”, solamente un número que vinculado (link) a otro archivo con esas informaciones permita que se vea quien es la persona referida.

Para la Ciencia de la Computación, el carácter “implícito” de cualquier registro no trae aparejada mucha diferencia en el tratamiento; en razón de la facilidad técnica de enlazar (link) diferentes campos de información a otras bases de datos. Por otro lado, para el Derecho, la protección, aunque nunca desguarnecida, dependerá de los medios que el operador de aquella base de datos tenga para observar de forma individualizada a aquel cuyos datos él está tratando, o sea, depende de su permiso de acceso a este otro archivo, que vincula número y nombre.

Diferentes también son los resultados para esos campos del conocimiento de identificadores “parciales”. Para la Computación ese dato simplemente es incapaz de producir una identificación unívoca. Sin embargo, en el Derecho, identificadores “explícitos”, incluso siendo “parciales”, pueden permitir a quien los maneja deducciones lógicas que garanticen, al menos, cierta probabilidad de conexión con una persona determinada, así amenazándola, permiten verificaciones adicionales.

Incluso archivos cuyos identificadores no sean acompañados por un campo de datos, la forma más básica de fichero computadorizado puede constituir un dato personal para efectos de protección jurídica, conforme al contexto en que se presenten. Se puede imaginar, por ejemplo, una lista sólo con números de identidad personal, sin ninguna otra información agregada, pero cuyo nombre del archivo sea “HIV”.

Design Principles.” *International Journal of Law and Information Technology*, 2009, p. 237.

Aceptando la seriedad de la información, evidentemente esa divulgación sin límites del listado causaría graves consecuencias sobre sus relacionados. Archivos solamente con identificadores vinculados, como, por ejemplo, nombre y número de contribuyente individual, revelan también informaciones indiscretas sobre el ciudadano[73].

Ese es el punto principal que le interesa a los derechos fundamentales. Datos sueltos, sin ningún reflejo en personas físicas[74], no tienen ninguna utilidad en el campo de los derechos fundamentales. Al contrario, cualquier elemento que caracterice al ser humano, por menor que sea, y respetadas las diferentes gravedades, debe ser protegido[75]. Pues el dato transformado en conocimiento se transforma en Poder para quien lo posee y puede resultar coercitivo y hasta sumisión para aquel que se torna un poco más expuesto.

En ese aspecto, por ejemplo, las legislaciones de protección de datos tratan todos los ramos de la cadena que conduce al proceso antes citado, desde la recolección de la información hasta su almacenamiento, pasando por el tratamiento de ésta y su comunicación, por medio de informes o de forma amplia, a otros, que podrán utilizarla o reorganizarla.

Es en eso posible una regulación con mínima pretensión de permanencia independientemente de la evolución de explosiva rapidez de la tecnología. Pues la información mantiene algunas características más allá del medio con que está archivada.

---

73 BERCIC, Bostjan , y GEORGE, Carlisle. "Identifying Personal Data Using Relational Database Design Principles... *cit.*, p. 247.

74 Piénsese en un archivo de una empresa que cree un número de serie para cada electrónico producido.

75 Nótese, a propósito, que la exposición, a veces excesiva, que vivimos en nuestra sociedad actual en las informaciones, por ejemplo, provistas en *redes sociales*, no permite la inferencia de que el dato personal no se somete más a nuestro derecho e interés humano de retirarlo a cualquier tiempo de las miradas ajenas (HOFFMANN-RIEM, Wolfgang. "Der Staat muss Risiken eines Missbrauchs durch Infiltrierung vorbeugen". Frankfurter Allgemeine Zeitung, 09.10.2011, [s.d.]).

Ella siempre produce *intelectualmente*, aun a través de una máquina, incluso con inteligencia artificial, ya que, al fin, todos son productos del ingenio humano. Además, el uso de esta información multiplicará sus fines conforme los designios de un ser humano y nunca (todavía) de una máquina. Existe sin duda un carácter *dinámico* en la producción de información, que conduce a la *expansión* y, paradójicamente, a su eterna insuficiencia. Por último, es un bien intangible naturalmente *compartible*, como cuando en la apertura de una "caja de Pandora", al ser revelada, sufre para ser recolocada dentro de un caparazón, con acceso limitado a los pocos designados[76].

Por eso, en cuanto,, lo manifestado, por la informática el término "dato", puro y simple, tiene una connotación bastante distinta de la idea de información, en el Derecho no hay necesidad de esa segmentación. "Dato", en nuestro estudio y en las legislaciones a ser destacadas, será eminentemente el dato *personal*, aquel ya transformado en *información* específica sobre un individuo y así, debiendo ser sometida al interés y a la regulación jurídica. Al contrario, cuando el dato no esté vinculado a una persona, se explicitará su *anonimización* o su existencia como mero *dato estadístico*.

1.7. Conclusiones

1. Hubo en los últimos sesenta años un enorme avance de las tecnologías referentes a almacenamiento y transmisión de datos. Ello fue resultado de la combinación de los avances en dos ramas de la ciencia. Dentro de la

[76] PÉREZ LUÑO, Antonio-Enrique. "Introducción a los sistemas informatizados de documentación jurídica." In Problemas actuales de la documentación y la informática jurídica : actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986. Madrid: Tecnos, 1987, p. 28.

computación está el continuo abaratamiento de los mecanismos para el almacenamiento y aumento de la capacidad de procesamiento, especialmente a través de la microelectrónica. Mientras que, en las telecomunicaciones se desarrollan materiales y estructuras que tornan factible la conexión inmediata entre distintos puntos del planeta, siendo Internet la más evidente consecuencia de este fenómeno.

2. Esas nuevas tecnologías provocan un cambio dentro del sistema de producción capitalista, pues, dentro de esta denominada *Sociedad de Información* se hace posible la cooperación y acumulación continua de conocimiento para fines de aumento de la eficacia de los medios de producción.
3. La relación del hombre con el medio en el que vive se ve directamente modificada, pues sus características y experiencias son ahora un elemento esencial para quienes poseen esas bases de datos. Se multiplican de esta forma, las maneras de observación del ser humano, ya sea en su navegación virtual en Internet, en su desplazamiento al aire libre (por medio de videocámaras) e incluso, por la verificación de los lugares donde deja depositado su ADN.
4. La juridicidad del estudio de estas nuevas tecnologías de información, evidentemente, va más allá de sus aspectos negativos, abarcando también la regulación de las esferas privadas y públicas donde el uso de estas puede ser útil al individuo. Sin embargo, también las relaciones de poder entre el Estado y el individuo son afectadas y, así, la temática de los derechos fundamentales se ve afectada.

5. El Estado actual, principalmente en las sociedades volcadas al modelo del Estado Social, necesitan la información para sobrellevar la complejidad de sus sociedades y de las tareas que le son otorgadas. No obstante, está la amenaza de la fijación con la temática de la acción preventiva en pro de la seguridad social, cuando su exacerbación permite la observación y análisis constante de cada ser humano.
6. Conceptos centrales en este estudio son la noción de dato, información y conocimiento. Pues datos sueltos, de naturaleza anónima, no tienen el don de por sí solos afectar la esfera individual, sino solamente cuando se los vincula a una identidad personal, y de esta forma, capaces de formar una información. El conjunto de esas informaciones compone el conocimiento captable por el dueño de cada base de datos.

2. La protección de datos personales como un derecho fundamental

2.1. El concepto de derecho fundamental como limitador del poder estatal

Desde la Antigüedad se observan, en la historia humana, textos de pensadores que abogan por conceptos de derechos y libertades. A partir de la Edad Media se encuentran documentos con fuerza vinculante que consagran ciertas posiciones jurídicas que deben ser respetadas por el mandatario. Sin embargo, en las relaciones jurídicas medievales, basadas en un sistema de fuertes dependencias personales, se conciben esas ventajas específicas como privilegios estamentales y libertades corporativas. La dignidad de un hombre es, en razón de un elemento externo, justificada como fruto de la posición jerárquica y de la voluntad divina.

Es a partir del pensamiento del siglo XV donde resurge la autonomía de la dignidad del individuo como un elemento inherente a su condición humana. Y con el auge del pensamiento ilustrado, en el siglo XVIII, el humanismo y el racionalismo consagran al hombre como centro del mundo[77]. Por lo tanto, encontramos que , solamente en la respuesta de un individualismo de cuño contractual a la centralización del poder efectivizada por el Estado Moderno puede concebirse el escenario preciso

[77] PECES-BARBA MARTÍNEZ, Gregorio. *La dignidad de la persona desde la filosofía del derecho*. Madrid: Dykinson, 2004, p. 26.

para la gestación de derechos y libertades con contenido normativo e intención de representar derechos de la humanidad, con pretensión de garantizar universalmente y de forma inalienable individuos, y no más, meros súbditos o vasallos[78].

En ese contractualismo que inspira el constitucionalismo moderno, esa sociedad civil de individuos existe antes del Estado, que surge, secundado por sus institutos e instituciones, para impedir los conflictos que amenacen las poses y derechos preexistentes[79].

La génesis de la constitucionalización de los derechos humanos, en la forma de la categoría aún hoy aceptada, surge con las revoluciones de fines del siglo XVIII[80]. Estos nacen como configuración de derechos de notoria naturaleza individualista y de "defensa" ante indebidas intromisiones de los Poderes Públicos sobre la esfera personal.

De acuerdo con la versión de la teoría liberal de los derechos que expusiera BÖCKENFORDE, vinculable a su caracterización en un Estado de Derecho típicamente burgués, los derechos fundamentales eran las posiciones individuales que deberían ser preservadas de la invasión estatal, siendo espacios de desarrollo de las plenitudes de la condición humana. Al Estado le cabrían solamente las medidas materiales y de regulación que fuesen necesarias para la preservación intacta de esa esfera individual verdaderamente pre-social, así como, su compatibilización dentro de la sociedad

---

78 SCHNEIDER, Hans Peter. *Democracia y constitución*. Madrid: Centro de Estudios Constitucionales, 1991, p. 121.

79 FIORAVANTI, Maurizio. *Los derechos fundamentales: Apuntes de historia de las constituciones*. Trotta, 2009, p. 41.

80 PÉREZ LUÑO, Antonio Enrique. *La tercera generación de derechos humanos*. Cizur Menor: Thomson-Aranzadi, 2006, p. 27.

existente[81].

La razón de la esfera de rechazo a intromisiones estatales, se debe a un método de protección de la dignidad de la persona humana, que encierra la posibilidad de elecciones tanto en la trayectoria de la vida como en la preservación de bienes centrales vinculados a dicha tarea, como la integridad corporal, libertad de expresión, libertad religiosa, etc.[82]. En una concepción más reciente del liberalismo, ,podríamos apuntar en relación con lo señalado, que los derechos fundamentales sirven para asegurar las facultades morales inherentes que la persona humana pueda ejercer a lo largo de su vida[83].

La positivación de derechos y libertades acontecidas con la Revolución Estadounidense y con la Revolución Francesa consagraron al menos cuatro importantes características: 1) son fundadas eminentemente a través de un jusnaturalismo racionalista; 2) conceden posiciones jurídicas favorables de forma universal a todos los individuos, situando en el pasado las declaraciones del soberano que favorecían solamente a determinados sectores, con carácter nítidamente privatista; 3) pretenden limitar el poder político, garantizando un Estado Liberal; y 4) tratan primordialmente de preservar el ámbito de autonomía del ser humano frente a intromisiones externas, o sea, constituyen puntos donde se rechaza la intervención estatal[84].

---

81 BÖCKENFÖRDE, Ernst-Wolfgang. "Teoría e interpretación de los derechos fundamentales." In *Escritos sobre derechos fundamentales*, traducido por Ignacio Villaverde Menéndez y Juan Luis Requejo Pagés. Baden-Baden: Nomos-Verlagsgesellschaft, 1993, p. 48.

82 BERNAL PULIDO, Carlos. *El principio de proporcionalidad y los derechos fundamentales: el principio de proporcionalidad como criterio para determinar el contenido de los derechos fundamentales vinculante para el legislador*. Madrid: Centro de Estudios Políticos y Constitucionales, 2003, p. 260.

83 RAWLS, John. *Liberalismo Politico*. São Paulo: Ática, 2000, p. 392..

84 ALVAREZ CONDE, Enrique, y TUR AUSINA, Rosario. "Los derechos en el constitucionalismo: tipología y tutela "multinivel"." *Teoría y realidad constitucional*, 2007, p. 234.

A partir de ese momento, en que la filosofía política y las sociedades consiguieron imponer al monarca soberano el individuo como integrante de una comunidad, y no más como un súbdito, dotándole de derechos naturales incontestables ante el Estado, las discusiones sobre la amplitud de ese catálogo de posiciones jurídicas se convirtió en uno de los principales centros de la lucha política dentro de la sociedad. Y ese problema que atañe a las fuerzas políticas se vuelve un problema jurídico conforme las constituciones fueron sometiendo las acciones de todos los poderes del Estado, Legislativo, Ejecutivo y Judicial, con relación al contenido de los derechos fundamentales[85], en una vinculación de manera directa e inmediata.

La primera vez en la historia de la humanidad que se conceden derechos de forma parecida con la que lo hacen nuestras actuales Constituciones, o sea, como un atributo inherente a la pertenencia al conjunto de un *pueblo*, fue en el artículo 1º de la Declaración de los Derechos de Virginia, del 12 de junio de 1776, en la cual se escribe:

> "Todos los hombres nacen igualmente libres e independientes, tienen derechos ciertos, esenciales y naturales de los cuales no pueden, por ningún contrato, privar ni despojar su posteridad: tales son el derecho de gozar la vida y la libertad con los medios de adquirir y poseer propiedades, de procurar obtener la felicidad y la seguridad."

Al positivarse de esa manera dejan de ser llamados "derechos humanos" o "derechos del hombre" y pasan a ser denominados, en conformidad con los diversos ordenamientos y enfoques, como "derechos constitucionales", "derechos civiles y políticos", "garantías constitucionales", o, en la expresión de origen alemana que se populariza en Europa Continental y en Latinoamérica en la 2ª mitad del siglo XX,

[85] ALEXY, Robert. *Teoría de los derechos fundamentales*. Madrid: Centro de Estudios Constitucionales, 1993, p. 21.

"derechos fundamentales"[86].

Hay un factor que torna especialmente adecuado el uso repetido del término derecho fundamental cuando nos referimos a derechos constitucionales con garantías reforzadas y representantes de un carácter "natural" humano en Constituciones como la de Brasil y España. Es que los citados países, así como Alemania, donde la expresión se originó , no poseían una tradición, hasta la segunda mitad del siglo XX, de respeto por parte de los gobiernos de las libertades fundamentales. Por tanto, el modelo alemán, tras ser reproducido por España y Brasil, fue fruto de un esfuerzo de domar jurídicamente eventuales tendencias totalitarias, notoriamente a través de la vinculación de los poderes y del control judicial de la constitucionalidad de las leyes[87].

2.2. Historicidad de los derechos fundamentales

La positivización exige, dentro de la abstracción y generalidad, que haya una especificación del campo de la realidad que será protegido, adquiriendo delimitación los amplísimos conceptos morales de protección de la *vida*, *seguridad* y *libertad*. Existe, fundamentalmente, un inevitable componente particular: los derechos son humanos, pero referidos al cuerpo social que se organiza constitucionalmente. Al constitucionalizarse, el derecho del individuo tiene un cierto destinatario, que es cada integrante del conjunto de los nacionales[88].

---

[86] RUBIO LLORENTE, Francisco. "Derechos Fundamentales, Derechos Humanos y Estado de Derecho." *Fundamentos: Cuadernos monográficos de teoría del estado, derecho público e historia constitucional*, vol. 4, p. 213.

[87] Vide sobre el caso alemán HESSE, Konrad. "Significado de los Derechos Fundamentales." In *Manual de derecho constitucional*. Madrid [etc.]: Marcial Pons, 2001, p. 86.

[88] RUBIO LLORENTE, Francisco. "Derechos Fundamentales, Derechos Humanos y Estado de

Evidentemente, al consagrar el carácter inalienable y sagrado de los derechos del hombre resalta su naturaleza de elemento preconstitucional, mero reconocimiento humano de factores a los cuales debe ser sometido el ejercicio del poder[89]. Sin embargo, los específicos derechos consagrados ya no son las anteriores pretensiones morales defendibles en razón de un previo *estado de naturaleza*, sino fórmulas con origen empírico y objetivos prácticos que, más que establecer los límites de las situaciones interindividuales, tienen el carácter de conformar sustancialmente la estructura política de las nuevas formas estatales[90].

Las declaraciones de derechos estadounidenses poseen el doble carácter de ser fruto de la inspiración del derecho natural, pero constituyen derecho positivo. Son *declaraciones* en el sentido jusnaturalista de afirmar derechos preexistentes a la vida en sociedad, pero también son normas, sujetas a perfeccionamientos en su proceso de revisión diferenciada.

Por ello, no sorprende que el conjunto de las diez primeras enmiendas a la Constitución Federal, del 15 de diciembre de 1791, se denomine *Bill of Rights*, resaltando su carácter normativo, o que el preámbulo de la Constitución del Estado de Pensilvania de 1976 indique expresamente, desde su comienzo, su mutabilidad, sin exceptuar la declaración de derechos, en pro del bien común[91].

La actualización del catálogo de derechos se observa con claridad en la Europa

---

Derecho... *cit.*, p. 213.

89 PÉREZ ROYO, Javier. *Curso de derecho constitucional*... *cit.*, p. 211.

90 CRUZ VILLALÓN, Pedro. "Formación y evolución de los derechos fundamentales." *Revista española de derecho constitucional*, 1989, p. 45.

91 *Ibid.*, p. 47.

del siglo XIX. A los *naturales* derechos de defensa de intromisiones indebidas del Estado (como la libertad de prensa, reunión y asociación) se extendió a derechos de participación en la vida política y también a obligaciones de prestaciones sociales[92].

Los derechos humanos, al tornarse *fundamentales* con su aceptación y garantía dentro del texto de las Constituciones, imponen un contenido que limita la amplitud de la soberanía popular. Sin embargo, las exactas medidas que conformarán ese contenido dependen de la construcción concreta de cláusulas que preserven todos los bienes jurídicos en conflicto con la realidad y protejan eficazmente a todos.

Cabe precisar que ello no significa que antes no fueran derechos humanos reconocibles. Por tanto, si hoy las categorías se superponen, no debe haber ninguna duda de que antes del reconocimiento interno en cada país ya podíamos clasificarlos como derechos del hombre, lo que atiende a sus orígenes de alguna protección jurídica en la positivización en el plano internacional y también su defensa en el plano filosófico[93]. Y ni siquiera evita que siendo su contenido nacionalmente contingente del rol de derechos del hombre reconocidos, no existan búsquedas de un consenso amplio y la armonización en su reconocimiento entre las naciones. En ese sentido, hay importantes avances en el plano del derecho internacional desde que, marcada por la barbarie nazi, la sociedad internacional, a través de la recién creada ONU pacta, el 10 de diciembre de 1948, una "Declaración Universal de Derechos del Hombre". El citado documento es complementado en el año 1966 con el "Pacto Internacional de Derechos Civiles y Políticos" y con el "Pacto Internacional de los Derechos Económicos, Sociales

[92] SCHNEIDER, Hans Peter. *Democracia y constitución... cit.*, p. 125.
[93] PÉREZ TREMPS, Pablo. "La interpretación de los derechos fundamentales." In *Estudios de Derecho Constitucional: homenaje al profesor D. Joaquín García Morillo*, Valencia: Tirant lo Blanch, 2001, p. 121.

y Culturales", proporcionando a los países una lista bastante completa de situaciones que merecerían la protección estatal[94]. Si durante la "Guerra Fría", la aceptación efectiva de los derechos humanos como un todo, de cuño liberal, político y social, en el plano interno, sirvió para establecer un corte jurídico claro entre las democracias capitalistas y los países adeptos al "socialismo real"[95], hoy esa defensa estatal todavía tiene más importancia. Con la caída del "Muro de Berlín", la aceptación del complejo moral de derechos humanos identifica verdaderas democracias[96] y las separa de sus simulacros o de dictaduras confesas.

Pero no hay manera de hablar de la categoría de *fundamentalidad* de determinados derechos, desde el punto de vista de las garantías de respeto y protección que ese término conlleva, en un espacio que supere las constituciones y comunidades nacionales[97]. Y en este sentido, el reconocimiento de cada una de sus emanaciones queda bajo la dependencia de muchos factores extrajurídicos, como las características similares, cultura y trayectoria histórica de un pueblo[98].

Como afirma HABERMAS, la interpretación del legislador constituyente funciona, por tanto, como un filtro que concretiza el mito del derecho natural positivado. La integridad transcendental de los derechos humanos, justificables por razones abstractas de Justicia, no debe cegar al jurista de que Constituciones son normas formadas en el seno de determinada comprensión histórica. No obstante, a los

---

94 SOMMERMANN, Karl-Peter. "Völkerrechtlich garantierte Menschenrechte als Maßstab der Verfassungskonkretisierung." AöR, 1989, p. 392.

95 RUBIO LLORENTE, Francisco. "Derechos Fundamentales, Derechos Humanos y Estado de Derecho... *cit.*, p. 207.

96 PECES-BARBA MARTÍNEZ, Gregorio. "Fundamental Rights: Between Morals and Politics." *Ratio Juris*, 2001, p. 73

97 Incluso quien denomina los derechos de los tratados como fundamentales, aduce aquí la adjetivación internacionales, para diferenciarlos de los f*undamentales nacionales* (BOROWSKI, Martin. *La estructura de los derechos fundamentales*. Bogotá: Univ. Externado de Colombia, 2003, p. 31).

98 HESSE, Konrad. "Significado de los Derechos Fundamentales... *cit.*, p. 85.

vencedores de las revoluciones políticas les fuera (y sea) conveniente consagrar su victoria como un momento transcendental de formación del Derecho, y que ello incluso, sea ventajoso desde el punto de vista de la estabilidad de un sistema constitucional de derechos, no se debe consagrar de manera absoluta la protección inicial otorgada a los derechos del hombre. Al contrario, debe buscarse siempre su actualización ante las nuevas amenazas que aparezcan[99].

El catálogo de los derechos reconocidos, aunque contingente al momento histórico y al entendimiento de la sociedad involucrada, deben por ello estar direccionados en pro de su ampliación conforme a las condiciones materiales, morales y sociales permitan que se presenten nuevos espacios dignos de la protección del individuo en pro de su creciente bienestar[100]. En ese sentido, la afirmación perentoria de HESSE: "los derechos fundamentales deben crear y mantener las condiciones elementales para asegurar una vida en libertad y la dignidad humana"[101].

No es difícil ubicar que la ya clásica "libertad de prensa" sólo surge en la Europa de los siglos XVIII y XIX con la consolidación de los periódicos y que el "secreto de la comunicación" viene a complementar la "inviolabilidad de la correspondencia" con la popularización del teléfono. Más recientemente, la protección fundamental del medio ambiente nace como consecuencia de la contaminación desenfrenada por el aumento de las capacidades industriales de afectar la naturaleza en la sociedad del siglo XX[102].

---

[99] HABERMAS, Jürgen. Direito e democrácia: entre facticidade e validade. 2 vols. Rio de Janeiro: Tempo Brasileiro, 1997, p. 166.

[100] RUBIO LLORENTE, Francisco. "Derechos Fundamentales, Derechos Humanos y Estado de Derecho... *cit.*, p. 206.

[101] HESSE, Konrad y BENDA, Ernst. Manual de derecho constitucional. Madrid [etc.]: Marcial Pons, 2001, p. 89.

[102] PECES-BARBA MARTÍNEZ, Gregorio. "La universalidad de los derechos humanos." In *La Corte y el sistema interamericano de derechos humanos*. San José, Costa Rica: Corte IIDH, 1994, p. 410.

Resulta evidente la *diversidad* de los derechos del hombre, aun en la corta historia de los últimos dos siglos. Esa ausencia de uniformidad no representa negar la característica de universalidad inicialmente pensada, ni rechazar la posibilidad de analizar objetivamente funciones, conformaciones y eficacia en un ordenamiento concreto[103]. Bien resume PECES-BARBA esa doble faceta:

> "Lo universal es la moralidad básica de los derechos, más que los derechos mismos, al menos en esta consideración «a priori». Que es la ética pública ilustrada, de la modernidad, tiene una vocación de universalidad que se fundamenta en los valores básicos que defiende y que arrancan de la idea de dignidad humana. Esta dignidad se expresa en que el hombre es un ser comunicativo, y social que vive en diálogo con los demás, a través del lenguaje racional, capaz de construir conceptos generales, y un ser moral y de fines que construye su propio ideal de vida, su propia moralidad privada, en convivencia con los demás. Son los valores morales que hacen posible una vida social conforme con esa dignidad humana, a través de organización social democrática y que desarrolla esa moralidad pública en forma de principios de organización social y de derechos humanos, lo que es universal. Hablar de universalidad de los derechos humanos en ese sentido racional es sostener la universalidad de esa moralidad básica que fundamenta los derechos. La universalidad temporal sería congruente con esa concepción, si se acepta su limitación en cuanto a la cristalización de la moralidad en la forma «derechos humanos», al mundo moderno y como concepto histórico. Es decir, que afirmar que los derechos humanos son un concepto histórico, no es incompatible con la universalidad de la moralidad básica de la dignidad humana."

La ausencia de una justificación metafísica absoluta no equivale a negar los fuertes argumentos en pro de la estructuración estatal en torno a derechos humanos[104]. Al contrario, esa amplia "ideología de derechos" en que vivimos se caracteriza por someter la legítima utilización del poder del Estado, especificado en las actuaciones del Legislativo, Ejecutivo y Judicial, la condición de que sea utilizado en pro de la realización de derechos de las personas y que realice y preserve su dignidad como seres humanos[105].

---

[103] HESSE, Conrado y BENDA, Ernst. Manual de derecho constitucional... *cit.*, p. 85.

[104] ZUCCA, Lorenzo. "The Limits of the Age of Rights." In *Analisi e diritto 2005 ricerche di giurisprudenza analitica*. Torino: G. Giappichelli Editore, 2006, p. 234.

[105] RUBIO LLORENTE, Francisco. "Derechos Fundamentales, Derechos Humanos y Estado de Derecho... *cit.*, p. 206.

2.3. Los intérpretes de la Constitución en la protección de datos

Los derechos humanos sólo pueden ser considerados como fundamentales cuando están presentes en la Constitución de un determinado pueblo en conjunto con los elementos de juridicidad, expresos o implícitos, que garanticen dicha fundamentalidad, los cuales consisten en su *eficacia directa* y *vinculación a todos los Poderes Públicos*, en su regulación solamente con *reserva de ley* y con respeto a un *contenido esencial*, garantizando el *control de la constitucionalidad* de dichas normas[106]. El profesor ROBERT ALEXY es claro en cuanto al significado de esa distinción:

> "Las preguntas acerca de qué derechos tiene el individuo como persona y como ciudadano de una comunidad, a qué principios está sujeta la legislación estatal y qué es aquello que exige la realización de la dignidad humana, la libertad y la igualdad, constituyen grandes temas de la filosofía práctica y puntos polémicos centrales de las luchas políticas pasadas y presentes. Se convierten en problemas jurídicos cuando una Constitución – como la Ley Fundamental de la República Federal de Alemania (LF) – establece que las normas de derecho fundamentales, en tanto derecho de vigencia inmediata, vinculan a la legislación, al Poder Ejecutivo y al Poder Judicial, y somete esa vinculación a un control amplio por parte de un Tribunal Constitucional.[107]

Hay dos intérpretes privilegiados de un texto Constitucional (y así también de los derechos fundamentales): legislador y el último tribunal que decide sobre la constitucionalidad en un país[108]. Ya la interpretación de los demás miembros de la

---

[106] PÉREZ ROYO, Javier. *Curso de derecho constitucional... cit.*, p. 228. Es de notar que mientras en la Constitución española todos esos elementos ya se encuentran por la lectura de su art. 53.1, en el derecho brasileño la hermenéutica es un poco más elaborada. Se puede afirmar que la eficacia directa y la vinculación de los Poderes Públicos advienen del párrafo 1º del artículo 5º y de la propia jerarquía superior de las normas relativas a derechos previstas en sede constitucional; que la reserva de ley, como principio general, está previsto en el art. 5º, inciso II; y por último, el control de constitucionalidad es amplio, coexistiendo el sistema difuso (art. 5º , inciso XXXV) y el concentrado (art. 102, I, "a"). El respeto a un contenido esencial, aunque, no se encuentra expresado, sería así, como máximo, un principio de inmanencia a fin de evitar el vaciamiento de los derechos fundamentales (cf. FERREIRA MENDES, Gilmar, MARTIRES COELHO, Inocêncio, y GONET BRANCO, Paulo Gustavo. *Curso de direito constitucional*. São Paulo, Brasília: Saraiva, 2008, p. 316). Por otro lado, hay quien entienda la necesidad de un "contenido esencial" como "de escasa relevancia práctica" (RODRÍGUEZ RUIZ, Blanca. "El caso "Valenzuela Contreras" y nuestro sistema de derechos fundamentales." In *Revista española de derecho constitucional*, 1999, p. 236).

[107] ALEXY, Robert. *Teoría de los derechos fundamentales... cit*, p. 1.

[108] PÉREZ ROYO, Javier. *Curso de derecho constitucional... cit.*, p. 119 y RODRÍGUEZ RUIZ, Blanca. *Privacy in telecommunications: a European and an American approach*. The Hague , Boston: Kluwer Law International, 1997, p. 90. Esa afirmación, sin embargo, necesita la debida contextualización. En

sociedad, incluyendo a los jueces, se da principalmente en relación al significado del contenido de leyes[109].

Tampoco hubo, en la protección de los datos personales, una competencia entre Judicial y Legislativo, sino una sucesiva cooperación, en que los jueces funcionaron más como quienes cubren zonas grises y balizadores de la legitimidad de normas emanadas. Hay que destacar igualmente la importancia del legislador, pues que, si la jurisdicción expandió el *área de protección* de ciertos derechos fundamentales para agregar la protección de datos[110], realizando así una auténtica *mutación* del texto, las específicas facultades del individuo necesarias para la protección del derecho, así como, los límites que tornan posible la acción del Estado, fueron todos frutos de la *concretización* realizada dentro de ese marco en las normas legales sobre el tema[111]. Estas elecciones legislativas se sujetan siempre al control de la jurisdicción constitucional en cuanto a su adecuación a la *Carta Magna.*

---

sistemas jurídicos como el español y el alemán es vedado al Judicial declarar, aunque sea incidentalmente en sus decisiones, la inconstitucionalidad de leyes dictadas por el Parlamento. Solamente el Tribunal Constitucional realiza este control y, a través de esa competencia, impone la última palabra en carácter general sobre el significado de determinada disposición. En Brasil eso no se da así, pues cualquier juez puede dejar de aplicar la ley en la solución del caso en concreto en virtud de su entendimiento de la inconstitucionalidad de la emanación legislativa. En ese caso su interpretación de la Constitución tiene un efectivo significado jurídico. Aunque esa posibilidad, fruto del sistema difuso de verificación de inconstitucionalidad resultante del modelo estadounidense, encuentra límites en el sistema de apelación constitucional brasileño, que constitucionalmente establece un Recurso Extraordinario para dudas sobre la interpretación de la Constitución y en un sistema de Súmulas Vinculantes, que impone al Ejecutivo, Legislativo y Judicial que siga la interpretación otorgada por la Suprema Corte Brasileña.

[109] Eso es también lo que ocurre cuando el juez utiliza la técnica de "interpretación de la ley conforme la Constitución", ya que no excluye campos de aplicación de la ley, pero elige entre las interpretaciones posibles la que se adecua a la fuerza normativa constitucional (SCHLAICH, Klaus y KORIOTH, Stefan. *Das Bundesverfassungsgericht*. München: Beck, 2004, p. 279 y SILVA, Virgílio Afonso da. "Interpretación conforme la constitución: entre la trivialidad y la centralización judicial." *Revista Direito GV 3*, 2006, p. 191).).

[110] Lo que de alguna forma simplemente realiza en la realidad el componente intencional que presidía la manifestación originaria del Poder Constituyente, y que es inamovible de su proceso de subsunción, en conjunto con la definición del contenido semántico del texto constitucional. (BOROWSKI, Martin. *La estructura de los derechos … cit.*, p. 55).

[111] En el ámbito del debate estadounidense, afirma con precisión SOLOVE que deben "(…) courts to apply Fourth Amendment principles and be open to allowing legislatures to fill in the details (...)" (SOLOVE, Daniel. "Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference". *Fordham Law Review*, Winter 2005, p. 777).

Esto se debe al hecho que los derechos fundamentales, además de ser elementos que definen el *status* del individuo, modelan el escenario de cumplimiento de sus tareas por parte de los Poderes Públicos, lo que impone para su efectiva aplicación que sean establecidos con *organización*, *limitaciones y garantías* en el orden jurídico estatal[112]. Dicho mando, al ser acatado por el legislador, facilita que se garantice una efectividad real a dichos derechos. Sea esta obligación expresa o no, es naturalmente deseable la labor legislativa para precisar con claridad los á*mbitos de la vida* que sufrirán influencia de determinada norma fundamental. Hay una *concretización* de los derechos inherente a la organización, aunque aquella no dependa de esta como regla general y varíe de intensidad conforme el derecho regulado[113]. Por tanto, el *contenido*[114] de un derecho fundamental está formado por el conjunto de facultades y posiciones jurídicas tuteladas (área de protección objetiva) otorgadas a personas específicas (*área de protección subjetiva*).

Sin embargo, aunque el derecho a la protección de datos sea un derecho de fuerte configuración normativa, en perjuicio de una cierta concepción naturalísimamente real, lo que amplifica bastante el *margen de acción* del legislador en la creación de sus contornos, esa ampliación del ámbito normativo del derecho fundamental, sin modificación del texto, a lo largo del tiempo, también posee un marco insuperable: la comprensión lingüística del texto constitucional.

---

[112] HESSE, Konrad, *Elementos de direito constitucional da República Federal da Alemanha*. Porto Alegre: S.A. Fabris, 1998, p. 232.

[113] Obsérvese, como ejemplo, la importancia de la definición de las reglas para el contenido del inciso XXVIII del artículo 5º de la CF en comparación con la eficacia del derecho de libertad de asociación aun sin norma infraconstitucional reglamentadora. Sobre el tema vide PIEROTH, Bodo, y SCHLINK, Bernhard . *Staatsrecht 2., Grundrechte*. Heidelberg: Müller, 2007, p. 51-52.

[114] MEDINA GUERRERO, Manuel. *La vinculación negativa del legislador a los derechos fundamentales*. McGraw-Hill Interamericana de España, 1996, p. 47.

Decir en ese sentido que el derecho fundamental, "aparece" en un texto constitucional, es lo mismo que decir que tras el proceso de *interpretación* de ciertas proposiciones en este texto jurídico, dichos contenidos de derecho surgen producidos[115]. Un fragmento o un conjunto de fragmentos de aquel lenguaje escrito tienen ese determinado sentido.

Este acto intelectivo de interpretación puede ser representado en la siguiente formulación: **"T"** (entre comillas porque es mera reproducción de la fuente elegida) significa **S**. Se denomina ese objeto **"T"** de la acción interpretativa de *disposición* y el resultado **S** de *norma*[116]. Esa operación es efectuada de forma idéntica, estemos ante un texto "claro"[117] u "oscuro"[118]. Por ello, conocer las normas de derecho fundamental implica conocer lo que significa la interpretación constitucional en sus propias peculiaridades.

En este tipo de interpretación de un derecho fundamental el objetivo es siempre establecer mínimamente con precisión el *área de protección* (*Schutzbereich*) del derecho fundamental[119]. Esa área de protección (también denominada en ocasiones *Normbereich*) representa las situaciones de la vida real con relación a las cuales cada

---

[115] GUASTINI, Riccardo. *Estudios sobre la interpretación jurídica*. México, D.F.: Universidad Nacional Autónoma de México, 1999, p. 8.

[116] Utilizando la misma terminología de GUASTINI, ROBERT ALEXY (*Teoría de los derechos fundamentales... cit*, p. 63). CARLOS SANTIAGO NIÑO usa también como sinónimo "proposición normativa" (SANTIAGO NIÑO, Carlos. *Fundamentos de derecho constitucional*. Buenos Aires: Astrea, 1992).

[117] Afirma PECES-BARBA: "En efecto, cuando no hay duda sobre el significado de una expresión es porque es fácilmente interpretable." (PECES-BARBA MARTÍNEZ, Gregorio. *Curso de derechos fundamentales: teoría general*. Madrid: Universidad Carlos III de Madrid [etc.], 1995).

[118] Textos legales "oscuros" pueden ser definidos aquí como aquellos en que surgen "problemas de interpretación" en razón de la vaguedad o ambigüedad en la manera empleada del lenguaje natural (vide sobre el tema GUASTINI, Riccardo. "Problemas de Interpretación." *Isonomía. REVISTA de Teoría y Filosofía del Derecho*, Octubre 1997).

[119] PIEROTH, Bodo, e SCHLINK, Bernhard. *Grundrechte*. Heidelberg: C. F. Müller, 2009, p. 57.

norma de derecho fundamental delimita como objeto de protección[120].

En el tema de la protección de datos personales podemos clasificar tipológicamente los textos constitucionales europeos y estadounidenses en tres grandes grupos[121].

Hay constituciones que no hacen ninguna referencia específica a la protección de datos personales, lo que impone que el mismo sea eventualmente identificado por medio de otras posiciones garantizadas, en particular intimidad o vida privada, dignidad de la persona humana o el libre desarrollo de la personalidad. Este es el caso de Alemania, Italia, Estados Unidos, Costa Rica, Chile y Uruguay, por citar algunos ejemplos.

En el segundo grupo encontramos constituciones que, sin mencionar expresamente un derecho específico de protección de datos personales, hacen referencias al asunto y, frecuentemente, a la importancia de tomar medidas por parte del legislador. En ese grupo encontramos los textos constitucionales de España[122], Holanda[123], Finlandia[124], Lituania[125], Guatemala[126] y Venezuela[127].

Por último, hay varios países que consagran facultades para la protección de datos personales expresa o implícitamente, sea a través de la concesión de un derecho

---

120 *Ibid.*, p. 54.

121 Categorización correctamente propuesta por ARENAS RAMIRO, Mónica. *El derecho fundamental a la protección de datos personales en Europa*. Valencia: Agencia Española de Protección de Datos, 2006, p. 379.

122 Art. 18.4 de la Constitución española

123 Art. 10.2 de la Constitución holandesa.

124 Art. 10 de la Constitución filandesa.

125 Art. 22, 3ª parte de la Constitución lituana.

126 Art. 25 de la Constitución guatemalteca.

127 Art. 60, 2 ª parte, de la Constitución venezolana, ya con sus reformas hasta 2009.

propiamente dicho o por medio de una garantía procesal, a veces denominada *habeas data*. En el continente europeo ese es el caso de Suiza[128], Suecia[129], Portugal[130], Eslovaquia[131], Eslovenia[132] y Polonia[133]. Por otro lado, en Latinoamérica encontramos la protección de datos expresamente como derecho en Colombia[134] y México[135], como pedido propio de acción constitucional en Paraguay[136], Argentina[137], Bolivia[138] y Brasil[139] y de ambas formas en Perú[140], Ecuador[141] y Panamá[142]. En general, las cartas magnas más recientes exhiben el reconocimiento de la protección de datos como derecho o garantía[143].

Como se observa, abordaremos una Constitución de cada uno de los grupos en conformidad con la clasificación propuesta. Aunque eso no es decisivo en la extensión mayor o menor de la protección de datos personales en cada país. Ello porque entre las normas que surgen de la interpretación de derechos fundamentales no existe solamente la clase de contenido más genérico, la de las "normas iusfundamentales directamente estatuidas", que resultan de la interpretación literal del contenido deóntico de cada disposición de derecho fundamental[144].

---

128 Art. 13.2 de la Constitución suiza.
129 Art. 3.2 del capítulo 2 de la Constitución sueca.
130 Art. 35 de la Constitución portuguesa.
131 Art. 19. 3 de la Constitución eslovaca.
132 Art. 38 de la Constitución eslovenia.
133 Art. 51 de la Constitución polaca.
134 2ª y 3ª parte del art. 15 de la Constitución colombiana.
135 Art. 16, 2ª parte de la Constitución mexicana.
136 Art. 135 de la Constitución paraguaya.
137 Art. 43, 3 ª parte de la Constitución argentina.
138 Art. 130 y 131 de la actual Constitución boliviana.
139 Inciso LXXII del art. 5º de la Constitución brasileña.
140 Incisos 5 y 6 del art. 2º e inciso 3 del art. 200 de la Constitución peruana.
141 Incisos 11 y 19 del art. 66 y art. 92 de la Constitución ecuatoriana.
142 Arts. 42 y 44 de la Constitución panameña.
143 ARENAS RAMIRO, Mónica. *El derecho fundamental a la protección de datos personales...cit.*, p. 379.
144 BERNAL PULIDO, Carlos. *El principio de proporcionalidad... cit.*, p. 114.

Para garantizar la eficacia normativa de la Constitución, los resultados que se alcanzan de la interpretación literal no son suficientes. La definición de la disposición de derecho fundamental sobre hipótesis reales de la vida social exige un paso más allá de la interpretación, lo que exige de los intérpretes de la Constitución la especificación de las denominadas "normas astrictas de derecho fundamental"[145]. Esa característica necesaria en la interpretación de un derecho constitucional que pretenda regular normativamente a la sociedad es descripta con precisión por KONRAD HESSE:

> "Así pues, y desde la perspectiva de las condiciones de realización del Derecho Constitucional, Constitución y ´realidad´ no pueden quedar aisladas una de otra. Lo mismo con respecto al proceso de realización. El contenido de una norma constitucional no puede regularmente realizarse sobre la única base de las pretensiones contenidas en la norma (sobre todo, expresadas en forma de un texto lingüístico), y ello tanto menos cuanto más general, incompleto e indeterminado se encuentre redactado el texto de la norma. Por tanto, con el fin de poder dirigir la conducta humana en cada una de las situaciones, la norma en mayor o menor medida fragmentaria necesita ´concretización´. La cual sólo será posible cuando se tomen en consideración en dicho proceso, junto al contexto normativo, las singularidades de las relaciones vitales concretas sobre las que la norma pretende incidir. La operación de realización de la norma constitucional no puede prescindir de estas singularidades, bajo pena de fracasar ante los problemas planteados por las situaciones que la Constitución está llamada a resolver."[146]

Ese es el punto clave donde se desarrolla el reconocimiento a la protección de datos personales. Por un lado, en virtud del reciente surgimiento de la amenaza, y así, del tema, por medio de una *mutación constitucional* interpretativa en que tribunales fueron reconociendo dentro de derechos constitucionales pretéritamente establecidos, como la intimidad y la dignidad de la persona, áreas de protección que abarcaban la recolección y uso de informaciones de individuos.

Se verificó así, en la formación del derecho del individuo a la protección de datos, la utilización por parte de la jurisprudencia de la característica de cierta

---

[145] BERNAL PULIDO, Carlos. *El principio de proporcionalidad... cit.,* p. 116.

[146] HESSE, Konrad. *Escritos de Derecho constitucional (Selección)*. Madrid: Centro de Estudios Constitucionales, 1983, p. 29. También admitiendo la central importancia de la concretización de los derechos fundamentales STERN, Klaus. *Das Staatsrecht der Bundesrepublik Deutschland*. Vol. 3.2 München: Beck, 1994, p. 1716 y sigs.

alterabilidad de las partes de la Constitución que tratan sobre las relaciones vitales, como medio para salvaguardar un contenido materialmente adecuado para la resolución de los conflictos surgidos por los cambios que sufre la sociedad a lo largo de la historia[147]. Es en el análisis argumentativo de la jurisprudencia constitucional en Alemania, España y Brasil donde se encuentra la justificación que cada país da para la protección de datos del individuo, y así, queden claros los *marcos* iniciales donde obligatoriamente transita el legislador. Aunque esa determinación no vede que se agreguen otras facultades suplementarias, esas decisiones de los Tribunales Constitucionales fijan las posiciones que son inherentes al legislador[148].

2.4. La protección de datos como derecho fundamental en Alemania

2.4.1 El reconocimiento del Tribunal Federal Alemán: la *Volkszählungsurteil* de 1983

La idea de la importancia de regular el flujo de datos personales por medio de una base de datos ya era objeto de regulación legislativa en dos estados alemanes, Hesse (en 1970) y Rheinland-Pflaz (en 1974), y la propia República Federal Alemana editó su norma el 27 de enero de 1977[149]. Ni un derecho a la protección de datos sería una novedad, ya que en 1978, la constitución de Nordrhein-Westfalen incluyó una

147 HESSE, Konrad. *Escritos de Derecho constitucional (Selección)... cit.*, p. 17.
148 MEDINA GUERRERO, Manuel. *La vinculación negativa... cit.*, p. 42 y 43.
149 Todas esas leyes fueron severamente afectadas por la decisión del Tribunal Constitucional en 1983, pues formuladas con una noción fuertemente de vincular la protección de datos a la defensa de la privacidad. Vide SIMITIS, Spiro. "Privacy–An Endless Debate?." *California Law Review*, 2010, p. 1997).

disposición en ese sentido[150]. Sin embargo, no había en 1983 ninguna otra constitución de estado federado con este derecho[151], así como modificación en la Ley Fundamental de Bonn sobre el mismo, al día de hoy no hay un reconocimiento expreso de un derecho a la protección de datos.

En la *Volkszählungsurteil* de 1983, el Tribunal Constitucional Federal Alemán (*Bundesverfassungsgericht* – BVerfG), juzgando un conjunto de reclamos constitucionales[152], declaró nulos algunos dispositivos de la ley que efectuaría el censo de la población alemana en aquel año, con énfasis al artículo 9, que posibilitaba que las Administraciones reciban los datos recogidos y los utilizará con fines no estadísticos, lo que ya había causado la preocupación pública del Comisario de Protección de Datos de la época, el Prof. HANS PETER BULL[153]. Antes de ser abordado el contenido de la decisión es necesaria una contextualización histórica para que este sea comprendido en su totalidad.

Nótese que el objeto de la acción no era inédito. Ni se trataba de la primera ley del censo de Alemania Occidental, ni era la primera vez que el Tribunal Constitucional Federal decidía sobre la constitucionalidad de la obligación de los ciudadanos en

[150] Art. 4.2: "Jeder hat Anspruch auf Schutz seiner personenbezogenen Daten. Eingriffe sind nur im überwiegenden Interesse der Allgemeinheit auf Grund eines Gesetzes zulässig." Además, en el ámbito de ese *Land*, la propia figura de un Comisario de protección de datos (*Landesbeauftragte für den Datenschutz*) tornó constitucional (art. 77a).

[151] El próximo Land a modificar su Constitución para incluir el derecho a la protección de datos fue Saarland, el 25 de enero de 1995. El texto del apartado 2 del artículo 2º repite de manera idéntica el texto de Nordrhein Westfalen. Vea más sobre ese tema en KLOEPFER, Michael, y SCHÄRDEL, Florian. "Grundrechte für die Informationsgesellschaft - Datenschutz und Informationszugangsfreiheit ins Grundgesetz?." *Juristenzeitung*, 2009, p. 454.

[152] Anótese que el primer reclamo, y que condujo a la concesión de la liminar del 5 de marzo de 1983 que impidió la entrada en vigencia de la ley del Censo de 1983, fue de autoría de dos abogadas de Hamburgo, Gisela Wild y Maja Stadler-Euler.

[153] HEREDERO HIGUERAS, Manuel. "La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del censo de población." *Documentación administrativa*, 1983, p. 142.

responder a los entrevistadores[154]. En ese caso *Mikrozensus*, juzgado el 16 de julio de 1969, *l*a reclamante se sublevó en cuanto a la obligación, sancionable con multa, de responder al Departamento de Estadística del estado de Baviera sobre sus viajes de vacaciones (*Urlaubsreisen*) y de reposo (*Erholungsreisen*). Mientras aquí ya se reconoce que determinadas preguntas, al invadir un ámbito privado de la vida humana, y por lo tanto, podrían afectar el derecho de autodeterminación, se contrapone que eso ya no se produce si la encuesta se refiriera a la conducta externa del individuo[155]. De esa forma aquí se desestimó el reclamo incluso de las preguntas que afectan el ámbito de la *vida privada*, pues no alcanzaban la *intimidad* o espacios no accesibles al mundo exterior, o sea, de carácter "confidencial"[156].

Esta fue entonces una decisión acorde con la denominada "Teoría de las Esferas" (*Sphärentheorie*), resultante del Derecho Civil, y otras veces aplicada por el BVerfG[157]. Según la citada teoría se podrían dividir las experiencias de un individuo en capas concéntricas. En el núcleo existiría un espacio intocable, la esfera íntima (*Intimsphäre*), caracterizada por la ausencia de comunicación con otro y, consecuentemente, por el secreto, y que poseería una protección absoluta del Derecho, sin admitir ningún tipo de ponderación a su eventual afectación[158]. Al lado de ésta, estarían las relaciones eminentemente privadas (*Privatsphäre*), como las familiares, donde se admitirían invasiones por miradas externas justificadas por intereses generales superiores[159]. Por último, los actos individuales no clasificables en los conceptos previos, efectuados en una esfera social (*Sozialsphäre*) no serían protegibles con base en un derecho general al

[154] Vide BVerfGE 27,1.
[155] BVerfGE 27,1 (7).
[156] BVerfGE 27,1 (8).
[157] De forma ejemplar, vide BVerfGE 34, 238 (245 a 248).
[158] PETERSEN, Stefanie. *Grenzen des Verrechtlichungsgebotes... cit.*, p. 9
[159] WÖLFL, Bernd. "Sphärentheorie und Vorbehalt des Gesetzes." NVwZ, 2002, p. 50.

desarrollo de la personalidad[160][161].

Tampoco había duda en la jurisprudencia del Tribunal[162], de que la divulgación de ciertos datos injustificadamente violaba la dignidad humana (Art. 1 I GG) y el libre desarrollo de la personalidad (Art. 2 I GG) de los afectados[163]. Y el uso de dichas cláusulas constitucionales como medio para complementar el rol clásico de los derechos de libertad ante los peligros de las nuevas tecnologías estuviera mencionado en el juicio del caso *Eppler*, tres años antes.[164]

El escenario, sin embargo, a principios de la década del 80 en Alemania Occidental era de gran inconformidad por parte de la población, no contra esa ley en particular, sino con los años de continuo crecimiento de la posesión, pública y privada, de sus datos. Era más una cuestión de indignación general, como en ciertos momentos surgen sobre otros asuntos, como el desempleo, la inflación o la corrupción, pero que creció sorprendentemente rápido en la opinión pública al inicio de 1983 pues existía la

---

160 HUBMANN, Heinrich. *Das Persönlichkeitsrecht*. Köln: Böhlau, 1967, p. 270.

161 Las críticas a esa teoría son apuntadas sin grandes distinciones por la doctrina más reciente: una definición poco segura de cuales situaciones cotidianas se encontrarían en cada una de las "esferas" de protección, proporcionando baja previsibilidad en cuanto a las decisiones en los casos concretos. (MARTINS, Leonardo, org. *Cinqüenta anos de jurisprudencia do Tribunal Constitucional Federal Alemão / coletânea original: Jürgen Schwabe*. Traducido por Beatriz Henning ... [et al.]. Montevideo: Konrad Adenauer Stiftung, 2005, p. 188, ALEXY, Robert. *Teoría de los derechos fundamentales...cit*, p. 350 e HUFEN, Friedhelm. "Schutz der Persönlichkeit und Recht auf informationelle Selbstbestimmung." In *Festschrift 50 Jahre Bundesverfassungsgericht*. Tübingen: Mohr Siebeck, 2001, p. 107.)

162 BVerfGE 15, 283 (286) y 27, 344.

163 BENDA, Ernst. "Dignidad Humana y Derechos de la Personalidad." In *Manual de derecho constitucional*. Madrid [etc.]: Marcial Pons, 2001, p. 129.

164 BVerfGE 54, 148 (158). *In verbis* : "2. a) Kommt hiernach eine Verletzung von Einzelgrundrechten nicht in Betracht, so bleibt als Prüfungsmaßstab nur das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verfassungsrechtlich gewährleistete allgemeine Persönlichkeitsrecht.aDieses ergänzt als "unbenanntes" Freiheitsrecht die speziellen ("benannten") Freiheitsrechte, die, wie etwa die Gewissensfreiheit oder die Meinungsfreiheit, ebenfalls konstituierende Elemente der Persönlichkeit schützen. Seine Aufgabe ist es, im Sinne des obersten Konstitutionsprinzips der "Würde des Menschen" (Art. 1 Abs. 1 GG) die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen zu gewährleisten, die sich durch die traditionellen konkreten Freiheitsgarantien nicht abschließend erfassen lassen; diese Notwendigkeit besteht namentlich auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen für den Schutz der menschlichen Persönlichkeit.".

perspectiva de que el próximo censo crearía un archivo concentrado, cuando antes las informaciones estaban diseminadas en diversas bases de datos. El Censo de 1983 no fue repudiado por el contenido especialmente invasivo de sus preguntas, sino a la posibilidad de que el Gobierno controlara una cantidad tan amplia de informaciones sobre su población[165].

En aquel año de 1983 irrumpieron protestas por todo el país contra la posibilidad de que el Estado recoja aquella amplitud de informaciones de su población. La revuelta social debe entenderse por el clímax de temor indistintamente presente del uso de métodos automatizados para conocer las características propias de cada individuo. La ley del censo permitió que amenazas puntuales del día a día se concentraran en una actividad que afectaba a todos[166].

Podemos desde aquí categorizar dos líneas diferentes de preocupaciones en cuanto al tratamiento de sus informaciones por medio de bases de datos. Por un lado está la preocupación con la súper categorización, con la creación de perfiles de cada individuo que les permita clasificarlos y separarlos sin ninguna intervención humana. Por otro lado, está el riesgo puro y simple de que, aun sin ese exceso, datos erróneos sobre nosotros sean archivados y reproducidos, sirviendo, aunque sea, para mínimas conclusiones falsas sobre nuestras características[167].

La decisión del Tribunal, por tanto, puede entenderse como una reverberación de

[165] SIMITIS, Spiro. "Privacy–An Endless Debate?.... *cit.*, p. 1997.
[166] SIMITIS, Spiros (org.). *Kommentar zum Bundesdatenschutzgesetz*. Baden-Baden: Nomos-Verlagsgesellschaft, 2003, p. 15.
[167] DI FABIO, Udo. "Rn 173. Das Recht auf nformationelle Selbstbestimmung als Ausprägung des Selbstdarstellungsschutzes, insbesondere gegenüber modernen Gefährdungsformen." In *Maunz/Dürig, Grundgesetz*. München: Beck, 2010.

los jueces a los temas que ya eran tratados en la discusión social[168], ya que, al final, la procedencia de esos temores en cuanto al archivamiento de datos es admitido por el Tribunal[169].

Todas las conclusiones del juicio derivan del establecimiento de que el tratamiento de informaciones de un individuo es una cuestión constitucional, una materia incluida en la temática de los derechos fundamentales. El tratamiento de datos no consentidos ya no es un tema de defensa simplemente por medio de la legislación infra constitucional[170]. En la dignidad humana (Art.1 I GG)[171] conjuntamente con el derecho de libre desarrollo de la personalidad (Art. 2 I GG)[172] se encontraba el fundamento de un derecho a la autodeterminación informativa (*Recht auf informationelle Selbstbestimmung*). Quién desconoce a quién, qué y cuánto conoce sobre sí y su existencia pierde la seguridad de actuar socialmente y de expresarse sin restricciones. De ahí que *autodeterminar* el flujo de los datos personales es un requisito, una exigencia, al libre desarrollo de la personalidad. Pero no solamente la esfera individual se favorece con el derecho a la autodeterminación informativa, ya que igualmente la libertad para ejercer la ciudadanía activa es preservada, y así, las propias

---

168 SCHLINK, Bernhard. "Das Recht der informationellen Selbstbestimmung." *Der Staat*, 1986, p. 234.

169 BVerfGE 65,1 (42)

170 Eso no equivale, sin embargo, a un menosprecio de la función legiferante, ya que su desarrollo necesita de concretización a través de la ley.

171 Aun así se resalta que el Tribunal Constitucional Alemán ya asume en sus juzgados la existencia de un "derecho fundamental a la protección de datos" (*Grundrecht auf Datenschutz* , BVerfGE 84, 239 , caso *Kapitalertragssteuer)*

172 "**Artículo 2** [Libertad de acción; libertad de la persona; derecho a la vida]
Toda persona tendrá derecho al libre desarrollo de su personalidad, en la medida en que no viole los derechos de otros y no infrinja el orden constitucional o la ley moral." En original: "Art 2 (1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.").
Dice HUFEN que en verdad la utilización por el Tribunal Constitucional del art. 2 nada más es que interpretarlo como una variación posible de la "regla de oro" kantiana, de que el ser humano es libre para hacer todo lo que quiera, limitado a no molestar la libertad del otro (HUFEN, Friedhelm. "Schutz der Persönlichkeit und Recht auf informationelle Selbstbestimmung... *cit.*, p. 108.)

precondiciones del régimen democrático[173]. Hay, por tanto, un fuerte sesgo en evitar un sentimiento general de coacción que podría causar en el individuo la ausencia de la autodeterminación informativa[174].

La amplitud del derecho implica que sea central el conocimiento de quién y para qué se utilizará la información. Esa defensa reforzada, tal como en otros derechos fundamentales, no impide que surja un "interés público reconocido" (*überwiegendes Allgemeininteresse*) que justifique su uso en perjuicio de la voluntad del afectado. Esa alegación de "interés público", nótese, no podría ser usada a la ligera, pues depende de una norma que fije con precisión su contenido, de modo que pueda ser sopesado con la "autodeterminación informativa" del afectado[175]. Además, la Corte exige que dichos límites sean expresados con claridad, de forma sencilla al ciudadano común y atiendan a la proporcionalidad[176]. De esta forma, la sentencia de 1983 del *Zensus* exige para la limitación de la autodeterminación informativa que sean, por medio de "reserva de ley", definidas situaciones concretas con fines específicos a fin de prescindir del consentimiento del afectado[177].

Por otro lado, observando las potencialidades del tratamiento de informaciones a través de las máquinas, se asegura que no hay más datos personales irrelevantes (*belangloses Datum*)[178], cualquier recolección y tratamiento involucra las mismas exigencias. La segmentación de la "teoría de las esferas" es considerada innecesaria

[173] BVerfGE 65,1 (43)
[174] El TFC expresamente asume esa protección contra el efecto intimidatorio (*Schutz vor einem Einschüchterungseffekt*) en BVerfGE 113, 029 (046) y BVerfGE 115, 166 (188).
[175] Como de modo claro afirma el Tribunal Administrativo Federal alemán el 20.02.1990 (BVerwGE 84, 375).
[176] BVerfGE 65,1 (44)
[177] DENNINGER, Erhard. "El derecho a la autodeterminación informativa... *cit.*, p. 273. También SIMITIS, Spiros (org.). *Kommentar zum Bundesdatenschutzgesetz... cit.*, p. 24.
[178] BVerfGE 65,1 (45)

para el establecimiento del ámbito normativo del nuevo derecho. Este es el cambio fundamental en esta decisión, ya que en casos anteriores, como *Mikrozensus, Ehescheidungsakten* (sobre datos relativos a la separación de un matrimonio)[179] o *Ärztliche Schweigepflicht* (en cuanto al secreto médico)[180] ya se indicaba una "autodeterminación informativa de la vida íntima". Sin embargo, vemos ahora una clara superación de la "Teoría de las Esferas"[181].

La cuestión de que la *finalidad* de uso de la información sea determinada ya previamente a la recolección y sea vinculante es resaltada por la Corte. Así, la práctica cooperativa entre las Administraciones Públicas implicó que se expresara la prohibición de *transmisión* y *utilización*[182]. La "separación administrativa informativa" ("*informationelle Gewaltenteilung*") exige, incluso, que se diferencie con claridad lo que es función pública estadística, de las demás[183]. Mientras no sea posible la eliminación de los datos identificativos, se urge que la transferencia de informaciones recogidas por la Estadística al resto de la Administración para los fines de planificación deba ser precedida por la anonimidad de los archivos cedidos[184].

La protección procesal adecuada al individuo debería envolver el establecimiento de deberes de *esclarecimiento, información y destrucción* de los datos

[179] BVerfGE 27, 344.
[180] BVerfGE 32, 373.
[181] DENNINGER, Erhard. "El derecho a la autodeterminación informativa... *cit.*, p. 271. En ese sentido también DI FABIO, Udo. "Rn 174. Verselbstständigung gegenüber dem Privatsphärenschutz." In *Maunz/Dürig, Grundgesetz*. München: Beck, 2010. Los fallos posteriores son especialmente cuidadosos en repetir como la autodeterminación informativa excede los límites de las situaciones ya protegidas por la privacidad (vide BVerfGE 118, 168 (185) y BVerfGE 120, 274 (312)). Incluso informaciones que sean accesibles al público se encuentran incluídas, vedándose su manipulación automatizada (BVerfGE 120, 378 (399)).
[182] Como bien aclara MARTINS, Leonardo, org. *Cincuenta años de jurisprudencia del Tribunal Constitucional Federal... cit.*, nota 242 en la p. 240.
[183] BVerfGE 65,1 (69)
[184] BVerfGE 65,1 (50)

al final del uso planificado. Sin embargo, esos derechos, para el BVerfG, no encubren la inherente debilidad del individuo para proteger todas las hipótesis de recolección de sus datos. La imposición de la mayor transparencia y de una acción preventiva en la implementación de la norma impone que exista la institucionalización de un control, durante todas las fases de una instancia independiente, un Comisario de Protección de Datos[185].

En ese aspecto, la decisión tiene la calidad de disociarse de intentos de conformar el derecho a la autodeterminación informativa como un derecho de propiedad sobre los datos. La sociabilidad de la existencia humana se manifiesta un desafío insalvable a la pretensión individual de imponer barreras a todos sobre el conocimiento acerca de sí[186]. La "autodeterminación informativa", de esta manera, comporta dos formas de protección. Una *pasiva*, *defensiva*, contra el descubrimiento de sus datos. Y otra *activa*, que exige que el ciudadano pueda saber siempre las condiciones actuales de sus datos anteriormente recogidos[187].

El reconocimiento del "derecho a la autodeterminación informativa" en el fallo de 1983 no debe ser nunca relativizado, pues, verdaderamente representó un marco, con efectos jurídicos y también políticos, pudiendo ser considerada como la verdadera *Carta Magna* de la protección de datos[188]. Sobre el particular, esa decisión representó la

---

185 BVerfGE 65,1 (46)

186 PAPIER, Hans-Jürgen. "Das Volkszählungsurteil des Bundesverfassungsgerichts." In *25 Jahre Volkszählungsurteil / Datenschutz - Durchstarten in die Zukunft*, organizado por Peter Schaar. Berlin: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2008, p. 17.

187 HUFEN, Friedhelm. "Schutz der Persönlichkeit und Recht auf informationelle Selbstbestimmung... *cit.*,p. 118.

188 Así tituló esa decisión HOFFMANN-RHIEM (HOFFMANN-RIEM, Wolfgang. "Informationelle Selbstbestimmung in der Informationsgesellschaft - Auf dem Wege zu einem neuen Konzept des Datenschutzes" *AöR*, 1998, p. 515), en lo que seguido por el entonces presidente del BVerfG HANS-JÜRGEN PAPIER en momento de la conmemoración de los 25 años de la decisión (PAPIER, Hans-Jürgen. "Das Volkszählungsurteil des Bundesverfassungsgerichts... *cit.*, p. 13).

generación de amplias expectativas sobre la acción del legislador, en razón de los extensos requisitos para la conformación legal del derecho expuesto[189].

Tampoco, se debe menospreciar la importancia de los juicios posteriores, anteriores o posteriores a las modificaciones a la ley de protección de datos. Inicialmente al aclarar algunos puntos no absolutamente claros para la doctrina jurídica en la época[190]. Así, se afirma que la voluntariedad u obligatoriedad tanto en la entrega de las informaciones al Estado, como en los datos que se pasan a la administración tributaria, no debilitan la protección otorgada por el derecho fundamental de impedir transmisiones o entregas de dichos datos a otras entidades administrativas[191]; y también, que tratamientos no automatizados (manuales) están alcanzados por esta nueva ley[192].

Hay también una serie de fallos que expresan hipótesis de aplicación en la vida práctica de la "autodeterminación informativa". Cítese la recolección, almacenamiento y el hecho de compartir muestras de ADN con fines de investigación criminal[193]; imposiciones de empleadores en conocer la biografía pretérita de sus subordinados (en el caso especialmente de actividades para el Ministerio de Seguridad en la antigua Alemania Oriental)[194]; en la exigencia por parte de la policía de que instituciones públicas o privadas entreguen los datos que posean sobre determinados grupos de personas[195]; determinaciones estatales para que instituciones financieras revelen datos

---

189 Vide en ese sentido SIMITIS, Spiro. "Zur Datenschutzgesetzgebung: Vorgaben und Perspektiven." *Computer und Recht*, 1987, p. 604.

190 Como bien señala GERHARD GROSS en "Das Recht auf informationelle Selbstbestimmung - mit Blick auf die Volkszählung 1987, das neue Bundesstatistikgesetz und die Amtshilfe." *AöR*, 1988, p. 164 e ssgs.

191 BVerfGE 67, 100 (143) – caso *Flick-Untersuchungsausschuß* . Con relación a la aplicación en el mismo sentido en instituciones privadas, ver BVerfGE 84, 239 (279).

192 BVerfGE 78, 77 (84).

193 BVerfGE 103, 21 (32).

194 BVerfGE 96, 171 (181).

195 BVerfGE 115, 320 (341).

de cuentas bancarias[196]; y en la incautación de la información relativa a los registros almacenados de contactos telefónicos de presuntos delicuentes[197].

Contemporáneamente en la jurisprudencia del Tribunal Constitucional Alemán la "confiabilidad e integridad de los sistemas de tecnología de información" (*Vertraulichkeit und Integrität informationstechnischer Systeme*) comienza a destacarse como nuevo derecho fundamental, igualmente interpretó el contenido del derecho general de la personalidad (Art. 1 I GG combinado con Art. 2 I GG), pero sin confundirla con la "autodeterminación informativa"[198].

2.5. La protección de datos como derecho fundamental en España

2.5.1. La colocación del apartado 4 del artículo 18 en la Constitución Española de 1978

La definición del bien jurídico defendido por medio del apartado 4 del artículo 18 de la Constitución Española como una ejemplificación de la protección de la intimidad del apartado 1 del mismo artículo o como un nuevo derecho fundamental fue

196 BVerfGE 118, 168 (183).
197 BVerfGE 115, 166 (189).
198 BVerfGE 120, 274 (302). El Tribunal Constitucional alemán comprendió en esta decisión de 2008 que la "autodeterminación informativa" no otorgaba la protección necesaria al uso por las fuerzas del Estado de *malwares* (denominados también "caballos de Troya") para infiltrar ordenadores y observar el uso de sus sistemas y contenido del disco rígido. Se asentó así, por la 2ª. vez en su historia, el nacimiento de un derecho fundamental (también llamado *Computer-Grundrecht*), que exige para esas medidas, a principio sujetas la *reserva de jurisdicción*, que estén evaluados concretos indicios de peligros, presentes o futuros, para bienes jurídicos relevantes, como el bien común, la existencia del Estado y de la persona humana o la salud, libertad y vida de personas. Otro sí debe el Estado salvaguardar que sus *malwares* no sean utilizados para otros fines que no los autorizados, o sea, debe garantizar la seguridad técnica en su invasión de otro ordenador. Sobre el tema, vea la esclarecedora entrevista del ex- juez del Tribunal Constitucional WOLFGANG HOFFMANN-RIEM ("Der Staat muss Risiken eines Missbrauchs durch Infiltrierung vorbeugen". Frankfurter Allgemeine Zeitung, 09.10.2011, [s.d.].), el cual participó de la decisión.

objeto de calurosos debates en la doctrina española, que se inicia debido a la propia ambigüedad que se sucede durante el debate constitucional.

El texto del Anteproyecto[199], reflejo de las inquietudes que ocurrían desde fines de la década del sesenta entre investigadores españoles y la legislación ya presente en el derecho comparado, señala que el constituyente había decidido describir una esfera jurídica propia de protección al ciudadano frente a todos los abusos informáticos. Aunque, en el debate llevado a cabo el 19 de mayo de 1978 en la Comisión de Asuntos Constitucionales y Libertades Públicas del Congreso de Diputados, el diputado Sancho Rof, del Grupo Parlamentario de la UCD, defendió la exclusión simple del último párrafo del actual artículo 18, debido a que según su parecer,, el derecho fundamental a la intimidad en nada se incrementaría por la adición a la cláusula general de una fórmula referente al peligro informático y que, por el contrario, dicha mención podría dejar al ciudadano indefenso frente a otros peligros que surjan por el avance de la ciencia[200]. Por otro lado, en el debate del Senado hubo un voto particular de Zarazaga Burillo que alteraba el texto de forma que protegía todos los derechos y libertades fundamentales de los españoles con relación a cualquier amenaza por medio de aparatos técnicos.

Sus propuestas, sin embargo, no lograron el apoyo de la mayoría que terminó admitiendo otra redacción, similar a otra enmienda del Grupo Mixto, surgida del diputado Roca Junjent, en nombre de la minoría catalana, y que terminó siendo la fórmula promulgada ("La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus

[199] "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos" (BOC de 5 de enero de 1978).

[200] MURILLO DE LA CUEVA, Pablo Lucas. *El derecho a la autodeterminación informativa...cit.*, p. 151.

derechos"). Demuestra el núcleo de esa amplia concordancia la intervención del representante del grupo socialista, Martín Toval, al decir que su grupo votaría "favorablemente a todo aquello que signifique incluir limitaciones de la informática en la Constitución"[201].

No obstante, cabe mencionar igualmente la insuficiencia del texto de la Constitución Española[202]. Su intención de proteger todavía podía ser leída, como lo destacó el diputado Rof, solo para garantizar la intimidad individual, con un alcance innegable y eminentemente defensivo, especialmente cuando se compara, por ejemplo, con el texto del antecesor artículo 35 de la Constitución portuguesa de 1976[203], que fue el primer país (y único anterior a España) en constitucionalizar la defensa frente a la informática. Esa incertidumbre constitucional, en que las garantías del derecho fundamental deben ser formuladas a través de la orden de limitar el fenómeno informático[204], se completa con la no concretización del artículo 18.4, que no define como objeto específico la protección de los datos personales y remite su regulación a la *ley*[205], lo que garantiza al legislador, al principio, una enorme libertad en la configuración de la protección constitucional[206]. Aquella vertiente que deseaba una gran

---

[201] PÉREZ LUÑO, Antonio Enrique. *Derechos humanos, estado de derecho y constitución... cit.*,p. 382.

[202] SERRANO PÉREZ, María Mercedes. "El derecho fundamental a la Protección de Datos. Su contenido esencial." *Nuevas Politicas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, Nº. 1 (Exemplar dedicado a: Los derechos fundamentales y las nuevas tecnologías), 2005, p. 246.

[203] "Artículo 35.Utilización de la informática

1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización.

2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos.

3. Se prohíbe atribuir un número nacional único a los ciudadanos."

[204] TRONCOSO REIGADA, Antonio. "La protección de datos personales: una reflexión crítica de la jurisprudencia constitucional." *Cuadernos de derecho público*, Nº 19-20, 2003, p. 246.

[205] Art. 18.4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

[206] Sin perjuicio de que acarree, al mismo tiempo, el refuerzo de la importancia de la definición de cual es

limitación en la lectura de ese artículo no era ni siquiera molestada por el artículo 105, b) de la CE, que, aunque loable, parece solamente intentar asegurar *transparencia* en los documentos *administrativos*, y no, verdaderamente, garantizar el "derecho de acceso" inherente al contenido esencial del derecho a la autodeterminación informativa[207].

2.5.2. El reconocimiento de la jurisprudencia del Tribunal Constitucional Español

El legislador español, inicialmente, mantuvo la protección del apartado del artículo 18 de la CE dentro de la protección general a la intimidad proporcionada por la Ley Orgánica 1/1982[208], retrasando, hasta de forma excesiva, en emitir la norma propia exigida por la C*arta Magna*. Por eso, es correcto decir que la defensa doctrinaria de la autonomía del derecho fundamental a la autodeterminación informativa sólo alcanzó algún fundamento en el derecho positivo infra-constitucional español con la ley orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), publicada en el BOE el día 31 de octubre, en la que se manifiesta en la exposición de motivos tratar la creación de un nuevo derecho fundamental, aunque bajo el anglicismo de denominarlo "privacidad", que expresa, desde luego, el carácter positivo de protección de datos íntimos o no.

---

el contenido esencial inquebrantable (TRONCOSO REIGADA, Antonio. "La protección de datos personales... *cit*., p. 270).

[207] CASTELLS ARTECHE, José Manuel. La limitación informática... *cit.*, p. 913.

[208] Ley Orgánica 1/1982, de 5 mayo
DISPOSICIONES TRANSITORIAS.
Primera. [Intromisión ilegítima derivada del uso de la informática]
En tanto no se promulgue la normativa prevista en el art. 18, apartado 4 , de la Constitución (RCL 1978, 2836) la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley."

Podemos señalar como el primer momento en que el Tribunal Constitucional español tuvo que enfrentarse con relación a bases de datos, intimidad humana y tecnologías de información en la STC 110/84. Se trata de causa de cuño tributario, ya que el contribuyente le reclamaba a la Corte protección contra la intromisión, la cual consideraba indebida, del Fisco español sobre sus movimientos bancarios y de crédito, activos y pasivos.

En este fallo de 1984, el Tribunal abordó escasamente los derechos constitucionales del ciudadano en cuanto a sus datos archivados, prefiriendo atenerse a la consideración de que hay bienes jurídicos constitucionales que autorizan amplios poderes a la fiscalización tributaria. Sin embargo, el FJ 3 de la citada decisión ya apuntaba que, aunque el derecho a la intimidad fuera de constitucionalización reciente, debería ser expandido para más allá de las fronteras del domicilio, frente a la amplitud de alcance de las nuevas tecnologías.

El tema retorna a la Corte pocos meses después del LORTAD. El Tribunal Constitucional Español, en la sentencia 254/1993, del 20 de julio, refrendó esa expresión legislativa, admitiendo la existencia de una "libertad informática" en la Constitución Española basada en su artículo 18.4 y en el contenido que se puede deducir de él por la utilización, por medio de la remisión al Derecho Internacional del artículo 10.2 de la Constitución de 1978, de los principios existentes en el Convenio Nº 108 del Consejo de Europa. Es relevante el reconocimiento por parte del Tribunal de la eficacia normativa directa del Convenio (aunque este deba, en principio, ser internalizado), ya que esta decisión es dada en un recurso de amparo relativo a hechos anteriores a la

creación en 1992 de una legislación específica de protección de datos en España[209]. Afirma el Tribunal en su Fundamento Jurídico 6º:

> "(...) los textos internacionales ratificados por España pueden desplegar ciertos efectos en relación con los derechos fundamentales, en cuanto pueden servir para configurar el sentido y alcance de los derechos recogidos en la Constitución, como hemos mantenido, en virtud del art. 10.2 CE , desde nuestra STC 38/1981 (RTC 1981/38), fundamentos jurídicos 3.º y 4.º Es desde esta segunda perspectiva desde la que hay que examinar la presente demanda de amparo.
> Dispone el art. 18.4 CE que 'la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos'. De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'".

Además, se observa, en la decisión del Tribunal Constitucional la verificación de que las nuevas tecnologías también representan nuevos riesgos a la esfera personal de los individuos. Aun así se mantenía la defensa de la inexistenciade un nuevo derecho. Solamente era reconocida la existencia de una "intimidad informática" con relación a la "intimidad física", entendida esta de la forma tradicional de un espacio reservado de invasiones externas (como en las SSTC 73/1982 y 231/1988), en razón del surgimiento de nuevas formas de lesión al ámbito privado y la consecuente necesidad de la protección de datos. Esto está demostrado en la STC 254/93 en su fundamento jurídico 7º que hesita en afirmar la desvinculación del nuevo derecho de la "intimidad", al expresar que:

> "(...) la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas

[209] PUENTE ESCOBAR, Agustín. "Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal." In: CANALES GIL, Alvaro, BLANCO ANTÓN, María José, PIÑAR MAÑAS, José Luis (coords.). *Protección de datos de carácter personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 de junio de 2003*. Valencia : Libreria Tirant lo Blanch, 2005.

data).”[210].

Podemos decir entonces que aún el Tribunal no se desvinculaba de decisiones en que la protección de datos era relacionada de forma general al derecho a la intimidad, como, por ejemplo, ocurre en la STC 110/1984[211]. En verdad, la solución jurisprudencial aquí parece relacionarse más bien con la situación enfrentada, que con una convicción jurídica en cuanto a un nuevo derecho autónomo. El hecho es que este recurso de amparo se refería a un ciudadano que no tuvo respuesta a su pedido al Gobierno Civil de Guipúzcoa en cuanto a la existencia de datos personales suyos en las bases de datos de la Administración, del porqué de su recolección y la identidad de los responsables. No existe directamente en la demanda la imputación de ilegalidad a la Administración por la posesión de los datos (situación sabida por todos y expresamente aceptada por el Tribunal en el STC 110/1984), y ninguna vinculación clara que la que encontraba en el ámbito íntimo del reclamante. La decisión fue tomada, de manera que permite el pronunciamiento favorable al amparo, sin provocar una cisión clara del concepto de intimidad hasta entonces adoptado.

Esa impresión se confirma con la STC 143/1994, del 9 de mayo, también de la Sala Primera del Tribunal Constitucional, en que teniendo como relator al magistrado Rodríguez-Piñero(que en la STC 254/1993 había redactado voto particular para rechazar

[210] Critíquese aun el TC en este pasaje al mezclar el concepto de “derecho de acceso”, constitutivo de una de las facultades relativas al contenido esencial del derecho fundamental, con el medio procesal de hacer efectivas esas facultades, el *habeas data*. Como establece Perez Luño: “el *habeas data* constituye, en suma, un cauce o acción procesal para salvaguardar la libertad informática, que cumple una función paralela, en el seno de los derechos humanos de la tercera generación, a la que en los de la primera generación correspondió al *habeas corpus* respecto a la libertad física o de movimientos de la persona. No es difícil, en efecto, establecer un marcado paralelismo entre la 'facultad de acceso' en que se traduce el *habeas data* y la acción exhibitoria del *habeas corpus*” (PÉREZ LUÑO, Antonio Enrique. *Derechos humanos, estado de derecho y constitución... cit.*, p. 407).

[211] PIÑAR MAÑAS, José Luis. “El derecho fundamental a la protección de datos personales.”In: CANALES GIL, Alvaro, BLANCO ANTÓN, María José, PIÑAR MAÑAS, José Luis (coords.). *Protección de datos de carácter personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 de junio de 2003*. Valencia: Librería Tirant lo Blanch, 2005, p. 30.

la aplicación directa del Convenio), se afirma, en el FJ 7 de, la existencia de ese contenido positivo en el derecho a la intimidad ("es un hecho también admitido en la jurisprudencia de este Tribunal que el incremento de medios técnicos de tratamiento de la información puede ocasionar este efecto y, correlativamente, se hace precisa la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestas en práctica a través de cualquier instrumento, aun indirecto, que produzca este efecto, y a incrementar las facultades de conocimiento y control que se otorgue al ciudadano, para salvaguardar el núcleo esencial de su derecho [STC 254/1993]").

Sin embargo, la sentencia 143/1994 aunque no difiera en cuanto a las conclusiones de la decisión de 1984, admitiendo que el Fisco puede, dentro de sus funciones la de evitar la evasión fiscal, promover un análisis sobre operaciones particulares del individuo, por otro lado, ya apunta que junto a la verificación judicial, precisa de la limitación del derecho en beneficio de finalidades constitucionales que no podrían de otra forma ser alcanzadas, deben en general ser preservadas las posibilidades del ciudadano de proteger sus datos y no soportar su conocimiento por otros[212].

A pesar que la STC 11/1998, en su fundamento jurídico 5, haya señalado el comienzo de un cambio en la opinión del Tribunal al afirmar la instrumentalidad del art. 18.4 con relación a otros derechos distintos de la intimidad, puesto que "el artículo 18.4 en su último inciso establece las limitaciones del uso de la informática para garantizar el pleno ejercicio de los derechos. Esto significa que, en supuestos como el presente, el artículo citado es, por así decirlo, un derecho instrumental ordenado para la protección

[212] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos : análisis y comentario de su jurisprudencia*. Organizado por Carlos Lesmes Serrano. Valladolid: Lex Nova, 2008, p. 51.

de otros derechos fundamentales, entre los que se encuentra desde luego, la libertad sindical", otras sentencias posteriores repetían la jurisprudencia que otorgaba facultades de acceso y control de la información dentro del derecho a la intimidad, incluso cuando los datos no pudieran ser objetivamente considerados como íntimos, como se ve en el párrafo 7º del FJ 8 de la STC 44/1999.

La STC 44/99 tiene, no obstante, el valor de destacar la "privacidad" (conforme la exposición de motivos de la LORTAD) en el campo de la informática, datos no obligatoriamente insertos en el ámbito reservado del hogar y de la familia, pero que pueden causar consecuencias discriminatorias a los individuos. Con la prohibición de la utilización por parte de una empresa de los datos sindicales de sus empleados para definir a quien descontar los días no trabajados por motivo de una huelga, el TC preserva la libertad sindical, pero, al mismo tiempo, fija la idea de que hay determinados "datos sensibles" que no deben ser invadidos. La sentencia 202/1999 tiene el mismo sentido, al negar la posibilidad al empleador (en este caso un banco) de que controle los gastos médicos de sus empleados de otro tiempo por medio de su posibilidad de acceder a las fichas médicas de todos.

Por tanto, eventuales dudas sobre el surgimiento en la jurisprudencia del Tribunal Constitucional de un nuevo derecho fundamental sólo fueron verdaderamente enterradas con la STC 292/2000, del 30 de noviembre, que concede un recurso de inconstitucionalidad del Defensor del Pueblo contra artículos de la LOPD.

Hay una clara declaración del Tribunal Constitucional de que el derecho a un tratamiento legítimo de sus informaciones en poder de otros, deriva de los propios

peligros que ello trae a la dignidad y a la libertad de cada ser humano, no siendo sencillamente un aspecto de otro derecho fundamental a ser defendido[213]. En el fundamento jurídico 4, el TC establece ese posicionamiento en cuanto al sentido del apartado 4 del artículo 18 de la Constitución Española, al defender el destaque del bien jurídico presente en este con relación al valor de la "intimidad" presente en el apartado 1 del mismo artículo:

> "Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dato que una persona puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE) no aporte por sí solo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico.
> Ahora bien, con la inclusión del vigente art. 18.4 CE el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía «como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona», pero que es también, «en sí mismo, un derecho o libertad fundamental» (STC 254/1993, de 20 de julio, F. 6). Preocupación y finalidad del constituyente que se evidencia, de un lado, si se tiene en cuenta que desde el anteproyecto del Texto Constitucional ya se incluía un apartado similar al vigente art. 18.4 CE y que éste fue luego ampliado al aceptarse una enmienda para que se incluyera su inciso final. Y más claramente, de otro lado, porque si en el debate en el Senado se suscitaron algunas dudas sobre la necesidad de este apartado del precepto dato el reconocimiento de los derechos a la intimidad y al honor en el apartado inicial, sin embargo fueron disipadas al ponerse de relieve que estos derechos, en atención a su contenido, no ofrecían garantías suficientes frente a las amenazas que el uso de la informática podía entrañar para la protección de la vida privada. De manera que el constituyente quiso garantizar mediante el actual art. 18.4 CE no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto".

Por tanto, podemos caracterizar que en el Derecho Español el Tribunal Constitucional define que hay un "derecho a la protección de datos", como norma adscripta de derecho fundamental, entendiendo de esta forma que dicho contenido no se encuentra directamente previsto en el texto constitucional, pero puede ser inferido de otras normas iusfundamentales definidas expresamente[214].

Además, en el fundamento jurídico 6º, el Tribunal se presta a contrastar derecho a la intimidad y derecho a la protección de datos en cuanto a sus funciones y

[213] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 57.
[214] ALEXY, Robert. *Teoría de los derechos fundamentales... cit,*, p. 52.

contenido[215]. Por tanto, afirma que mientras el primero posee el sentido de alejamiento de intromisiones externas, involucrando deberes de abstención *erga omnes*, el último evita manipulaciones indeseadas de las informaciones personales consistentes en facultades positivas e imposiciones de obligaciones de hacer sobre terceros como medio de garantizar el control sobre el flujo de sus datos:

> "La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio [RTC 1999, 144] , F. 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio [RTC 1999, 134] , F. 5; 144/1999, F. 8; 98/2000, de 10 de abril [RTC 2000, 98] , F. 5; 115/2000, de 10 de mayo [RTC 2000, 115] , F. 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.
> (...)
> Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (SSTC 73/1982, de 2 de diciembre [RTC 1982, 73] , F. 5; 110/1984, de 26 de noviembre [RTC 1984, 110] , F. 3; 89/1987, de 3 de junio [RTC 1987, 89] , F. 3; 231/1988, de 2 de diciembre [RTC 1988, 231] , F. 3; 197/1991, de 17 de octubre [RTC 1991, 197] , F. 3, y en general las SSTC 134/1999, de 15 de julio, 144/1999, de 22 de julio, y 115/2000, de 10 de mayo), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, F. 7). "

El Tribunal también distingue, en este mismo fundamento jurídico 6, entre la especie de datos protegidos, es decir, en cuanto al *objeto* del derecho, ya que afirma que en la protección de datos se incluyen informaciones que ya están bajo conocimiento público. Por consiguiente, la inexistencia de carácter privado no retira el sentido de

[215] SEOANE RODRÍGUEZ, José Antonio. "Ética, Derecho y datos personales." *Cuadernos de derecho público*, Nº 19-20 (Ejemplar dedicado a: Protección de datos), 2003, p. 102.

amenaza al individuo de la manipulación descontrolada de datos personales:

> **"De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal** (STC 170/1987, de 30 de octubre [RTC 1987, 170] , F. 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.
>
> De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, **también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos.** También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino **que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo."**

Nuevamente en esta ocasión es palpable en la solución del TC la influencia del derecho europeo, ya que el fallo es pronunciado pocos días antes del reconocimiento comunitario del derecho, en el artículo 8º de la Carta de Derechos Fundamentales de la Unión Europea[216] y además distinguir este aspecto dentro de un concepto superior el de *vida privada* que permitió al Tribunal Europeo de Derechos Humanos a admitir en el año 2000 la protección de este derecho en los casos *Amann contra Suiza* y *Rotaru*

[216] "Artículo 8. Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la Ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3 .El respeto de estas normas quedará sujeto al control de una autoridad independiente."

Nótese incluso que el artículo 7 de la misma Carta representa la protección clásica de la intimidad:

"Artículo 7. Respeto de la vida privada y familiar

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones."

contra Rumania[217].

El derecho a la protección de datos se presenta como un derecho de configuración legal, es decir, sometidos a los contenidos y límites conformados por el legislador, desde que no sea transpuesto su contenido esencial constitucional y sea respetada la ponderación adecuada de los bienes constitucionales. Ello significa igualmente que dichos parámetros deben ser fruto de la decisión del Poder Legislativo, por lo tanto, están sometidos a la *reserva de ley*.[218]

En el ordenamiento jurídico español, la autonomía jurídica del derecho de protección a los datos personales parte de la suposición de que una reformulación del derecho a la intimidad no es suficiente para abarcar todas las cuestiones que el avance de la tecnología de datos, afecten al ser humano. La "limitación a la informática" a la que se refiere el artículo 18.4 de la Constitución no debe ser comprendida como una intención de impedir la evolución de la tecnología en el territorio español, sino de conformarla a lo que debe ser su objetivo último, la mejora de la calidad de vida de los ciudadanos sin perjuicio de sus libertades y de su dignidad[219]. En consecuencia, hay un bien jurídico en ese apartado que pretende precisamente impedir la agresión al ciudadano en el almacenamiento y cesión de informaciones suyas sin respetar su derecho y sin su control[220]. Es lo que afirma el TC en la sentencia 290/2000, relativa también a la Ley Orgánica 5/92, donde al final el Tribunal Constitucional rechaza que la fiscalización de archivos públicos y privados por medio de la Agencia de Protección de

[217] MURILLO DE LA CUEVA, Pablo Lucas. *El derecho a la autodeterminación informativa... cit.*,p. 34.
[218] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 58.
[219] SERRANO PÉREZ, María Mercedes. "El derecho fundamental a la Protección de Datos... *cit.,* ,p. 247.
[220] ÁLVAREZ-CIENFUEGOS SUÁREZ, José María. *La defensa de la intimidad de los ciudadanos y la tecnología informática* . Pamplona: Aranzadi, 1999, p. 25.

Datos española afecte competencias autonómicas, con miras a la necesidad de igualdad de gozo y protección de los ciudadanos en cuanto a los derechos fundamentales, que expresa en el FJ 7 que:

> "(...) tanto el examen del precepto que se acaba de transcribir como el objeto y finalidad de la Ley en la que se encuadra aconsejan que el examen de la presente disputa competencial se lleve a cabo partiendo de dos presupuestos, a saber: el contenido del derecho fundamental a la protección de datos personales y, en segundo término, los rasgos generales que caracterizan a la Agencia de Protección de Datos dato que la función general de este órgano es la de «velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación», como se expresa en el primer inciso del apartado a) del art. 36 LORTAD.
> En lo que respecta al primer presupuesto, si el art. 1 LORTAD establece que su objeto es el «desarrollo de lo previsto en el apartado 4 del art. 18 CE» ,es procedente recordar que este precepto, como ya ha declarado este Tribunal, contiene un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que es, además, en sí mismo, «un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama "la informática"»(STC 254/1993, de 20 de julio [RTC 1993, 254] , F. 6, doctrina que se reitera en las SSTC 143/1994, de 9 de mayo [RTC 1994, 143] , F. 7; 11/1998, de 13 de enero [RTC 1998, 11] , F. 4; 94/1998, de 4 de mayo [RTC 1998, 94] , F. 6 y 202/1999, de 8 de noviembre [RTC 1999, 202] , F. 2)."

Y en las sentencias del Tribunal Constitucional en que fue más cercana la definición del "contenido esencial" de ese derecho, o sea "aquella parte del contenido del derecho que es absolutamente necesaria para que los intereses jurídicamente protegibles, que dan vida al derecho resulten real, concreta y efectivamente protegidos" (STC 11/1981, 8 de abril), son resaltadas sus facultades de naturaleza positiva, cuáles sean las posibilidades de actuación y control que permite al individuo decidir sobre la información concerniente sobre sí mismo[221]. Por tanto, podemos comprender el núcleo del derecho fundamental a la autodeterminación informativa, conforme la jurisprudencia del TC, basado en el trinomio: *conocimiento, legitimidad y control.* De un lado, los principios que vinculan a aquel que maneja la información exigen que este dé cuenta de los fines y sea autorizado por el afectado para el tratamiento correcto que realizará y para eventuales traspasos a terceros. Al mismo tiempo, ello no impide que el individuo

[221] HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales en la sociedad de la información*. Bilbao : Universidad de Deusto, 2003, p. 21.

posea una gama de derechos que le permitan verificar y garantizar en cualquier momento que la utilización se da respetando la dignidad y la verdad relativa a su condición humana. En el FJ 7 de la STC 292/2000 se confirman esas ideas:

> "De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.
> En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele."

Estos fragmentos de las decisiones, que, como ya se ha dicho, tienen influencia indeleble del derecho europeo, se sistematizan las facultades básicas que componen el "derecho a la autodeterminación informativa" en los derechos de: información, acceso, rectificación, cancelación y oposición. Este contenido esencial del derecho fundamental, por evidente, tenía que ser respetado por el legislador para regular el tema, en la actual Ley Orgánica Nº 15/99. A esto, se suman los principios de la calidad del tratamiento, del consentimiento, de la información y de la seguridad, dirigidos a quien maneja la información, como forma de evitar la existencia de lesiones al bien jurídico protegido.

2.6. La protección de datos como derecho fundamental en Brasil

2.6.1 La protección de datos en el texto de la Constitución Brasileña

Aunque un "derecho a la protección de datos" no sea directamente previsto por la Constitución Federal de la República Federativa de Brasil (CF), ni el Supremo Tribunal Federal (STF) lo haya reconocido como adscripto al texto constitucional en ninguno de sus fallos, eso no significa que no haya protección constitucional en Brasil sobre los datos personales que se encuentren archivados en base de datos públicos o privados.

Hay tres incisos del artículo de la Constitución brasileña que se refieren a los "derechos y deberes individuales y colectivos" de forma tangencial al tema. El inciso X del artículo 5º define como inviolable la vida privada y la intimidad; el inciso XII[222] garantiza el "sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas"y el inciso LXXII se refiere a la acción de *habeas data*, para permitir el derecho de acceso y rectificación de datos personales.

2.6.1.1 La protección de datos por medio de los incisos X y XII de la Constitución brasileña

La interpretación del "sigilo de dados" del inciso XII se dejo abierta por el Supremo Tribunal Federal desde la sesión del juicio por crimen común cometido

[222] "XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;"

durante la presidencia del ex presidente Fernando Collor de Mello[223]. En aquel caso, fue considerada como prueba ilícita la aprehensión de un ordenador en una empresa sin autorización judicial porque sería transgredida la inviolabilidad domiciliaria constitucional (art. 5 º inciso XI CF). Pero el relator, Ministro. Ilmar Galvão fue más allá y afirmó que aunque las hipótesis fácticas o la determinación judicial exigida en el inciso XI del artículo 5 º de la Constitución estuviesen presentes, no sería dado a la Policía Federal el análisis del contenido de informaciones presentes en la ordenador porque habría un sigilo de contenido de datos en el inciso XII del mismo artículo que no se confundiría con el sigilo de las correspondencias o comunicaciones genéricamente consideradas. El Min. Galvão hace expresa mención a los "dados estritamente particulares", bajo los cuales no habría duda de una protección constitucional *absoluta*[224]. También el revisor, Min. Moreira Alves, destaca la protección constitucional otorgada a "dados em geral" por el inciso XII, agregando que ello, por consecuencia, garantiza informaciones que los dueños de ordenadores en ellos almacenan[225].

Además, de ser esta interpretación justificada por la literalidad del texto, había también una doctrina que entendía ese inciso XII como una actualización de la 4ª Enmienda de la Constitución estadounidense ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the

[223] AP nº 307-3, juzgada el 13 de diciembre de 1994.
[224] AP nº 307-3, volumen n. 1804 - 11 del Ementario, p. 2188.
[225] AP nº 307-3, volumen n. 1804 - 11 del Enmentario, p. 2441. El Min. Moreira Alves no afirma, sin embargo, la protección absoluta entendida por el Min. Galvão. O sea, mientras que el último defiende que la ausencia de restricción expresada en la Constitución al "sigilo de datos" impediría la actuación del legislador ordinario en definir cualquier bien constitucional como limitaciones al derecho fundamental, aquel deja la cuestión en abierto, resaltando, no obstante, la ausencia de cualquier ley vigente con ese contenido.

persons or things to be seized.“), en un sentido de que la intangibilidad de los “papeles” personales avanza en un mundo computarizado para la preservación de sus datos almacenados en chips[226].

Sin embargo, a lo largo de los debates en el juicio de RE 418.416/SC, el 10 de mayo de 2006, el Supremo Tribunal Federal afirmó por unanimidad que la protección del inciso XII tiene como ámbito normativo solamente diferentes formas de comunicación de datos y no favorece la información personal propiamente dicha[227]. Esta interpretación comprende que la protección aquí tiene la libertad de enviar a otros, los conocimientos que posee, favoreciéndose la intersubjetividad, lo que puede darse por medio de cartas, telegráficamente, por teléfono y también por ordenador. En esa confidencialidad solamente se impide la interceptación del dato informático en tránsito, objeto de intercambio de mensajes entre dos personas.

En ese juicio de 2006, ambos ministros, Moreira Alves e Ilmar Galvão, ya se encontraban jubilados, el Tribunal se vinculó expresamente[228] a la lección del Prof. TÉRCIO SAMPAIO FERRAZ JÚNIOR, que defendía que el uso del término “datos” en ese inciso es fruto de una cierta impropiedad del constituyente. Este, al buscar actualizar el §9º del artículo 150 de la Constitución de 1967[229], desearía preservar no el objeto que podría ser transmitido a otro, sino la *modalidad de comunicación* que se realizaba por medio de ordenadores. Hay una garantía al *momento* en que se da la charla, pero no al *contenido* que posee[230].

---

[226] WALD, Arnoldo . “A legislação sobre "lavagem" de dinheiro.” *Revista CEJ*, Dezembro 1998, p. 73.
[227] RE 418. 416/SC volumen n. 2261-6 del Enmentario, p. 1264, voto vencedor del relator Min. Sepúlveda Pertence.
[228] RE 418. 416/SC volumen n. 2261-6 del Enmentario, p. 1254.
[229] “São invioláveis a correspondência e o sigilo das comunicações telegráficas e telefônicas”
[230] FERRAZ JUNIOR, Tercio Sampaio. “Sigilo de dados: o direito à privacidade e os limites à función

Se reconoce que esta visión tiene relación con las discusiones al momento de la asamblea constituyente. La inserción del término "datos" en su texto, en la época de los trabajos constituyentes, vino de la enmienda agregada n. ES 32893-0, del entonces diputado Artur da Távola, y fue justificada por el avance en las *comunicaciones* de datos[231]. También el profesor CELSO RIBEIRO BASTOS indica que la protección sería sobre los intercambios de mensajes entre individuos[232], siendo la remisión a datos tan solo una búsqueda de actualización de la antigua defensa de la correspondencia epistolar.

Exactamente porque la decisión termina por entender lícita una orden de búsqueda y aprehensión de un ordenador y el uso de los datos allí guardados para una denuncia criminal, o sea, admitiendo la licitud de la prueba, hay cierto esfuerzo en indicar cuando la información registrada encuentra posición *ius-fundamental* en Brasil. El Min. Cezar Peluso afirma su comprensión en general de que informaciones registradas no gozarían de confidencialidad y que no hay ninguna razón para diferenciar aquellas colocadas en papel o en ordenadores[233].

El Min. Carlos Ayres Britto, a su vez, superpone la protección de datos personales con la inviolabilidad del domicilio del inciso XI y con la vida privada e intimidad del inciso X. Habría, por lo tanto, no una confidencialidad de cualquier

---

fiscalizadora do Estado." In *Sigilo Fiscal e Bancário [Reinaldo Pizolio, Jayr Viégas Gavaldão Jr., coordenadores]*. São Paulo: Quartier Latin, 2005, p. 23. En sentido crítico ANTONIO SCARANCE FERNANDES ("O polêmico inciso XII do artículo 5º da Constitucional Federal." *Justitia*, Diciembre 2007, p. 19).

231 TERRIGNO BARBEITAS, André. O sigilo bancário: e a necessidade da ponderação dos intereses. São Paulo: Malheiros, 2003, p. 25.

232 RIBEIRO BASTOS, Celso. *Curso de direito constitucional*. São Paulo: Saraiva, 1999, p. 200.

233 RE 418. 416/SC volume. 2261-6 del Ementario, p. 1310. Eventual distinción en virtud del tratamiento automatizado o no de las informaciones no es considerado en ese juicio por ninguno de los ministros votantes.

información, sino de aquellas en conexión con el alcance de estos otros derechos constitucionales. Mencionando la idea de la teoría de "tres círculos" de convivencia, afirma la protección de las informaciones que confinamos en nosotros mismos (parte de la "intimidad", como lo que se escribe en un diario) y aquellas que pasamos solamente a parientes y amigos (integrantes de la "privacidad")[234]. Por lo tanto, el dato individualmente considerado solo estaría constitucionalmente garantizado *prima facie* en cuanto a su revelación si es de contenido *íntimo* o *privado*. Eso significa que no se admite en Brasil la inclusión de cualquier dato de registro en la garantía de inviolabilidad de la intimidad y de la vida privada dispuestos en el inciso X del artículo 5º de la Constitución Federal[235], siendo mayoritariamente aceptada la posición de TÉRCIO SAMPAIO FERRAZ JÚNIOR que :

> "Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos – como nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial, etc., condicionam o intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido."[236]

En la definición de *íntimo* y *privado* no se empeña, en general, el Supremo Tribunal Federal en estandarizar una conceptualización que rompa con la doctrina dominante, tan solo establecer casuísticamente las situaciones de datos que se refieran a

---

234 RE 418. 416/SC volume. 2261-6 del Ementario, p. 1304.

235 Podría haber cambiado esa jurisprudencia el juzgamiento de la Acción Cautelar 1928. En medida preliminar en esta AC, el Min. Gilmar Mendes dio efecto suspensivo a un recurso contra decisión interlocutoria del Tribunal Regional Federal de la 4ª Región que concedía acceso directo al Ministerio Público Federal y a la Policía Federal a meros datos de registro de clientes de telefonía móvil y fija. La decisión justifica en la "proteção ao sigilo de dados, tido como projeção do direito à privacidade" y que cualquier limitación depende de ley y razonabilidad. Sin embargo, hay dos factores que no recomiendan el uso de esa decisión. Primero, porque el principal precedente invocado para la cautela (MS 22.801) trata de sigilo bancario, donde es firme la posición de la corte de que son datos que se incluyen en el inciso X. Y, principalmente, porque el Tribunal en su todo no llegó a pronunciarse, en razón de la extinción de la acción cautelar por la pérdida de su objeto, ya que sobrevino sentencia de mérito en el tribunal recorrido, superando la decisión interlocutoria, antes del proceso ir al pleno del STF.

236 FERRAZ JUNIOR Tercio Sampaio. "Sigilo de dados: o direito à privacidade e os limites à función fiscalizadora do Estado... *cit.*, p. 28..

la intimidad y a la privacidad. Y aquí son especialmente numerosos los reiterados fallos que afirman la preservación de confidencialidad fiscal y bancaria en el ámbito del inciso X del artículo 5º[237].

La sentencia en la medida cautelar del MS nº 23.452-RJ, porque se refiere al uso de estos datos por las Comisiones Parlamentarias de Investigación (CPIs), o sea, por el Poder Legislativo, por medio de la autorización constitucional del §3 º del artículo 58 de CF, es el intento más exhaustivo que la Suprema Corte brasileña hace para abordar de forma general la protección constitucional de los datos. Aquí el voto del relator, Min. Celso de Mello, adoptado de forma unánime, se refiere sucesivamente a tres especies de información; bancarias, fiscales y de registros/datos telefónicos, usualmente utilizados en investigaciones por CPIs, para afirmar su carácter de objeto de una "libertad pública" en virtud de su vinculación con la *intimidad* del inciso X y así su inherente confidencialidad, solo quebrantable motivadamente. Es importante en ese juicio, una vez más, diferenciar la confidencialidad de los datos y las comunicaciones, ya que esta, está protegida en el inciso XII, y por lo tanto, estaría más allá de los poderes de las CPIs, habiendo una reserva de jurisdicción que haría imprescindible una orden judicial[238].

Además, hay otros dos registros profesionales de datos de terceros que merecieron la atención esporádica del STF. Habría un *status* especial en las informaciones que abogados resguardasen de clientes, también por fuerza de la propia

[237] Bajo la égida de la Constitución de 1988, posición firmada en el Pet 577-5, relator Mtro Carlos Velloso, juzgamiento el 25 de marzo de 1992.

[238] MS 23.452-RJ, juzgamiento el 16 de septiembre de 1999, volumen n. 1990-1 del Enmentario, págs. 117 a 132.

intangibilidad profesional del abogado, prevista en el artículo 133 de la CF[239], y en los datos médicos[240]. Eso no equivale, sin embargo, así como en los casos anteriores, que se revistan de un carácter absoluto y que no puedan ser alejados en pro de otros bienes constitucionales.

En verdad, también la propia utilización de la palabra "sigilo" (*secreto)* demuestra el predominio de la protección estática y limitada de los datos en el derecho brasileño. A fin de cuentas, la idea de sigilo se conecta a una obligación de quien tiene acceso a determinadas informaciones de mantenerlas con un contenido secreto, no revelable a terceros[241]. La protección dinámica, el mantenimiento de un control del particular después de esa revelación, a ser realizada por medio del habeas data, queda relegada predominantemente a segundo plano.

2.6.1.2 La protección de datos en el derecho brasileño por medio del *habeas data*

Al contrario del STF, en la doctrina brasileña, JOSÉ AFONSO SILVA, importante asesor de los principales relatores de la Constitución de 1988 y principal comentador de la misma en sus primeros años distinguía intimidad y privacidad. Él defendía, por la redacción del inciso X del artículo 5º de la CF, la distinción en el derecho brasileño entre ambos términos, aunque reconociendo que es común el empleo

[239] HC 71.231-RJ, juzgamiento el 5 de mayo de 1994, relator Min. Carlos Velloso, volumen n. 1848 - 01 del Enmentario , p. 62.

[240] RE 60176 / GB, juzgamiento 17 de junio de 1966, y RE 91218 / SP, juzgamiento el 10 de noviembre de 1981.

[241] BARROS, Marcos Antonio de. "Sigilo profissional. Reflexos da violação no âmbito das provas ilícitas." Justitia, Septiembre 1996, p. 18.

de los vocablos para tratar el mismo derecho.

El inciso X albergaría cuatro valores protegidos como derechos fundamentales del individuo: su *honra*, o sea el conjunto de cualidades que conforman su reputación; su *imagen*, que sería la autonomía sobre la reproducción de su aspecto físico; la *intimidad* y la *vida privada*. En estas dos últimas, aquella sería caracterizada por la idea de esfera *secreta* del individuo, en tesis distanciante de la vista de *todos* los demás. Se incluye así, en el derecho fundamental a la intimidad, la inviolabilidad del domicilio (CF, art. 5º, inciso XI), en todas sus facetas, inclusive la de la libertad sexual, la confidencialidad de las correspondencias y el deber de secreto de las informaciones conocidas por medio de ciertas actividades profesionales[242]. La vida privada tendría un alcance más amplio, abordando todos los actos y documentos que, aún pudiendo involucrar familiares y amigos, no tiene como destinatarios al público en general, y también esta *vida interna* además de la intimidad debería ser preservada de observación, investigación y divulgación[243].

> "Já a proteção ao indivíduo definida neste inciso X, quando respondendo à específica ameaça do *fenômeno informático*, possui um instrumento processual constitucionalmente próprio, , que é o *habeas data*, que se presta a ser adequado para enfrentar as peculiaridades deste possível lesionador. Assim, a questão informática e do "esquadrinhamento" sobre o individuo através da ligação entre os gigantes bancos de dados que ela possibilita, não teria passado em branco das preocupações do constituinte originário, estando dentro desse conceito de privacidade e, *principalmente*, na garantia especifica do habeas data"[244].

Y aquí él reconoce la significativa diferencia entre el abordaje de los institutos en la Constitución Brasileña y en las Cartas Españolas y Portuguesa: mientras en aquella se crea una garantía sin el correspondiente derecho expreso, en estas se establece que habrá derecho, sin ninguna mención a los instrumentos procesales.

---

[242] SILVA, José Afonso da. *Curso de direito constitucional positivo*. São Paulo: Malheiros, 2006, p. 207
[243] *Ibid.*, p. 208.
[244] *Ibid.*, p. 210.

La diferencia no es insignificante ni sucedió por accidente, como testigo, la historia de la evolución del actual inciso LXXII del artículo 5º de la Constitución brasileña desde la elaboración del anteproyecto de norma fundamental, descrita por el propio JOSÉ AFONSO DA SILVA:

> "(...) propusemos perante a Comissão Provisoria de Estudos Constitucionais (Comissão Afonso Arinos) um Anteprojeto de Constituição cujo art. 17 reconhecia o direito nos termos seguintes : ´1. Toda pessoa tem direito de acesso aos informes a seu respeito registrados por entidades publicas ou particulares, podendo exigir a retificação de dados, e a sua atualização 2. É vedado o acesso de terceiros a esse registro 3. Os informes não poderão ser utilizados para tratamento de dados referentes a convicções filosóficas ou políticas, filiações partidárias ou sindical, fé religiosa ou vida privada, salvo quando se tratar do processamento de dados estatísticos não individualmente identificáveis. 4. Lei federal definirá quem pode manter registros informáticos, os respectivos fins e conteúdo´. No art. 31 instituíamos o remédio constitucional específico: ´Conceder-se-á habeas data para proteger o direito à intimidade contra abusos de registros informáticos públicos e privados.´, curto e seco, como se vê. O Anteprojeto da Comissão acolheu a declaração do direito em seu art. 17 com aperfeiçoamentos e o remédio no art. 48: ´Dar-se-á habeas data ao legítimo interessado para assegurar os direitos tutelados no art. 17´. Daí saiu para o debate constituinte, andando o direito e sua garantia específica em dispositivos separados até que no Projeto da Comissão de Sistematização fosse aprovado num único dispositivo, ou seja: reconhecia-se o direito mediante sua garantia específica (art. 6 º , § 52). Daí sofreu modificações para pior até o texto do atual art. 5 º, LXXII (...)"[245]

Ese encuadramiento durante el proceso constituyente refleja poca propensión de la doctrina y jurisprudencia en Brasil de avanzar más allá de la temática de la intimidad y de la revelación de los archivos políticos de la dictadura de 1964 a 1985 que existió en Brasil.

Esta inconsistencia de la materialidad constitucional en la protección de datos está muy bien representada en el *curso* de Derecho Constitucional escrito por el actual miembro del Supremo Tribunal Federal brasileño, GILMAR FERREIRA MENDES, donde en el análisis del "derecho a la intimidad y vida privada" se insiste en la idea de que esto comprende tan solo la posibilidad de ver sus informaciones separadas del

[245] *Ibid.*, p. 454.

conocimiento ajeno[246], que como vimos no abarca el contenido protegido por la legislación europea, donde más importante que el conocimiento de otro es el control constante sobre el flujo de las informaciones. Esta postura se mantiene de forma similar en el análisis específico del secreto bancario y fiscal, que, sin embargo, sirve para ayudar a demostrar la influencia de dichas notas en Brasil al justificar un tratamiento propio por separado.

Por otro lado, a diferencia de JOSÉ AFONSO DA SILVA, GILMAR MENDES no apuesta por el habeas data como medio para garantizar la autodeterminación informativa en el derecho brasileño, lo toma como un instrumento limitado, tanto por la contingencia que inspiró su creación, como la preocupación por el surgimiento de nuevos archivos secretos amplios, como los que utilizaba la dictadura brasileña, en cuanto a su contenido, que siendo limitado al "conocimiento o rectificación de datos" demuestra un objeto de protección "por demais restrito"[247].

En el mismo sentido afirma LUÍS ROBERTO BARROSO que se debe tomar en cuenta que la motivación del constituyente brasileño no fue primordialmente el control del potencial nocivo de las tecnologías de información, y sí impedir el restablecimiento de las prácticas de tortura y eliminación de los adversarios del régimen dictatorial vigente de 1964/1985 que dependían eminentemente del conocimiento de la identidad de los ciudadanos vinculados a movimientos revolucionarios de la "izquierda armada" y que el "habeas data" tiene un carácter "simbólico"[248].

---

[246] FERREIRA MENDES, Gilmar, MARTIRES COELHO, Inocêncio, e GONET BRANCO, Paulo Gustavo. *Curso de direito constitucional*. São Paulo, Brasília: Saraiva, 2008, p. 379.
[247] *Ibid.*, p. 544.
[248] BARROSO, Luís Roberto. "A Viagem Redonda: habeas data, direitos constitucionais e as provas ilícitas." In *Habeas Data*. São Paulo: RT, 1998, p. 212.

Hay también un sector de la doctrina que no ve ninguna novedad en la creación del *habeas data* con relación a lo que ya permitía la garantía constitucional del "mandado de segurança", presente en Brasil desde la Constitución de 1934[249].

En verdad, se puede decir que es hasta preferible el uso del "mandado de segurança", en defensa del ciudadano, pues el *habeas data* encuentra un fuerte elemento que impide su viabilidad procesal: la necesidad de definir un principio de prueba jurisprudencialmente negativa a proporcionar informaciones al afectado, bajo pena de fulminar el *interés de actuar* en la acción constitucional[250]. Esta prueba es de difícil entrega, ya que es común que la negativa se dé por vía oral o por la mera inacción.

La práctica judicial de la utilización del *habeas data* confirma su tendencia a la irrelevancia y una existencia de hecho contingente a un momento histórico ya pasado. Mientras en los dos primeros meses de vigencia de la Constitución de 1988 fueron solicitados en el STF diez *habeas data*[251] que involucraban la búsqueda del conocimiento del contenido de los archivos personales de los impetrantes que estaban en el "Servicio Nacional de Informaciones" (SNI), órgano de espionaje de la dictadura brasileña, más de 20 años después, el número de este tipo de proceso en el STF aún no llegó a 100[252].

---

249 CRETELLA JÚNIOR, José. *Os "Writs" na Constituição de 1988 : Mandado de segurança, mandado de seguridad coletivo, mandado de injunção, habeas data, habeas corpus, ação popular*. Rio de Janeiro: Forense Universitária, 1996, p. 120.

250 En ese sentido STJ, HD 102/DF, relator Min. Luiz Fux, juzgado el 18/10/2004, reproduciendo la Súmula 02 de la jurisprudencia del Superior Tribunal de Justicia (STJ). Nótese que ese enorme limitador del uso procesal del Habeas Data fue ya la 2ª. Súmula editada por ese tribunal, tras su creación con la CF/88, ya el 8 de mayo de 1990, fruto de decisiones repetidas de su 1ª. Sección en ese sentido en el 2º semestre de 1989, en los HDs 2, 4, 5, 8 y 9.

251 HDs 1, 2, 3, 4, 5, 6, 7, 9, 10 e 14.

252 O HD 93 fue impetrado el 26 de noviembre de 2010. En el STJ el Habeas Data n. 210 fue juzgado el 9 de febrero de 2011.

Un hecho revelador de cómo ve el STF brasileño la acción del *habeas data* se da en el juicio del Agravo Regimental en el Habeas Data 90 – DF, el 18 de febrero de 2010. Al negarse que la empresa tenga acceso al proceso del Tribunal de Cuentas donde era citada, el pleno del STF, por unanimidad, afirmó el carácter *estricto* de su uso para conocimiento y rectificación de informaciones personales que ya estén ordenadas e individualizadas en un registro de una base de datos. Además justificó esa medida procesal con la defensa de la *privacidad* que podría sufrir perjuicios morales y materiales por una divulgación de informaciones inexactas[253].

De todas maneras es justo decir que el texto constitucional brasileño, en lo referente a las facultades positivas al individuo en su protección de datos, alcanzó solo algunos aspectos de los reconocidos en el ordenamiento jurídico europeo, específicamente el *conocimiento* del contenido de lo que está sobre uno archivado y la *rectificación* de aquello que no corresponde a la realidad, sin involucrar etapas importantes en la utilización y tratamiento de datos[254]. Por otra parte, no se prevé ningún medio que le proporcione al ciudadano el conocimiento de donde se encuentran guardados sus datos, solo posibilitando, por lo tanto, el uso en etapa de quien obtuvo sus datos directamente, de forma aparente.

No se observa, que el *habeas data* sea un instrumento inadecuado para la protección de datos. En otra interpretación él podría tener el carácter emancipador con relación a los datos personales que el *Habeas Corpus Act*, de 1679, provocó sobre la

[253] AgReg HD 90-DF, relatora Mtra. Ellen Gracie, volumen n. 2394 - 1 del Enmentario , p. 5.
[254] LEITE SAMPAIO, Jose Adercio. *Direito à intimidade e a vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informa pessoais, da vida e da morte*. Belo Horizonte: Del Rey, 1998, p. 548-549.

realización de la libertad de locomoción del cuerpo físico[255]. A propósito, cuando se coloca una acción procesal en el capítulo referente a los derechos y deberes individuales y colectivos, como *garantía constitucional*, con fuerza y celeridad destacadas, solo tiene sentido si corresponde a un derecho sustantivo con idéntica protección en la Carta Magna[256]. Sin embargo, la jurisprudencia mayoritaria en Brasil no permite ningún alcance que sobrepase los límites ya reconocidos de la intimidad y establece obstáculos procesales que desalientan el uso judicial del instrumento.

2.7. Características de la protección de datos

2.7.1. Propiedades materiales de un derecho fundamental

La idea de los derechos innatos del hombre surge, antes de su positivización en las Constituciones de finales del siglo XVIII, como una cuestión de naturaleza ética y filosófica. Pero que solo con la positivización en las Constituciones Nacionales se vuelven derechos fundamentales. Hay así una intrínseca doble cara en esos derechos, de fruto natural de la naturaleza humana y resultado de un proceso de creación técnica[257].

Por eso es posible hablar de propiedades materiales y formales de los derechos fundamentales[258]. Siendo las propiedades materiales derivadas de las concepciones ideales sobre la relación entre hombre y Estado, ellas a su vez, corresponden a una

[255] FROSINI, Vittorio. "Bancos de datos y tutela de la persona". *Revista de Estúdios Políticos*, noviembre 1982, p. 24.
[256] RIBEIRO BASTOS, Celso. *Curso de direito constitucional. cit.*, p. 183.
[257] PÉREZ ROYO, Javier. *Curso de derecho constitucional... cit.*, p. 220.
[258] O de concepción material y formal de lós derechos fundamentales como utiliza MARTIN BOROWSKI (*La estructura de los derechos ... cit.*, p. 34-35).

visión del mundo que imagina determinadas funciones que los derechos fundamentales alcanzarían para maniobrar el poder estatal y así ponerlo al servicio de los intereses de los individuos[259].

Las propiedades materiales son necesarias en la relación de dichas expresiones normativas, con un *concepto de persona*, individualmente considerada y en su interacción con la sociedad, que deba tener reconocimiento universal y que merezca ser *fortalecido* por el Estado, ya sea por medio de acciones u omisiones. Existe, consecuentemente, un carácter de justificación en las propiedades materiales. Concretamente eso significó la existencia de libertades privadas ausentes de intervenciones estatales, participación en la formación democrática de la voluntad estatal, determinación de igualdad jurídica entre las personas y, con el advenimiento del Estado Social, prestaciones materiales que garanticen las condiciones básicas de existencia y de igualdad fáctica[260].

Históricamente esta búsqueda de fundamentación para los derechos del hombre en teorías sirvió para favorecer la coherencia de la argumentación y así se vuelve más responsable el debate político referente a las estructuras que se desea modificar[261]. Solo con determinadas concepciones de las necesidades de los individuos y la relación entre el Estado y la persona, es que se confluyen las fuerzas sociales que difundieron el concepto de derechos humanos para servir simultáneamente a funciones tan diversas como impedirle al Estado intervenir en la libertad privada, garantizar la participación de los ciudadanos en la formación de la voluntad política y promover medios que

[259] BERNAL PULIDO, Carlos. *El principio de proporcionalidad... cit.*, p. 257.
[260] BERNAL PULIDO, Carlos. "La metafísica de los derechos humanos." *Revista Derecho del Estado*, diciembre de 2010, p. 128.
[261] WALDRON, Jeremy. "Rights and Needs." In *Legal Rights: Historical and Philosophical Perspectives*. Ann Arbor: University of Michigan Press, 1995, p. 109.

estimulen la igualdad fática en el seno social[262]. Este es un campo en que claramente los aportes de la filosofía política influyó en la formación del sistema jurídico. La identificación de las tesis subyacentes, por lo tanto, es fundamental para entender la posterior institucionalización de derechos y también para mantener las condiciones de la crítica democrática[263][264].

Y, desde el punto de vista, práctico, especialmente cuando hay dudas de la constitucionalización como derecho fundamental de determinada posición jurídica, es útil preguntarnos por las razones que justificarían este reconocimiento[265].

Sin embargo, corresponde a la teoría buscar lo que supera la pertinencia geográfica y/o histórica. Y en este aspecto podemos apuntar que hay elementos materiales y formales que identifican a los derechos fundamentales. Materialmente hablando, podemos trabajar con la definición de HESSE para la función primordial de los derechos fundamentales: ellos "deben crear y mantener las condiciones elementales

---

[262] BERNAL PULIDO, Carlos. "La metafísica de los derechos humanos... *cit.*, p. 128.

[263] MICHELMAN, Frank I.. "Human Rights and the Limits of Constitutional Theory." *Ratio Juris*, 2000, p. 75.

[264] Nótese, sin embargo, que esa identificación de una teoría condecente con la defensa de un derecho fundamental a la protección de datos poco dice definitivamente sobre el complejo de posiciones jurídicas que serán concedidas al particular a través de ese mismo derecho fundamental, lo que es llamado de "derecho fundamental como un todo" (*das Grundrecht als Ganzes*) por ROBERT ALEXY (*Teoría de los derechos fundamentales...cit.,*, p. 240 y ss..). Lo que ya se va tornando posible identificar con más clareza es lo que ROTH denomina, analizando los niveles de protección, de derechos *primarios*, o sea, los comportamientos sobre los bienes jurídicos que el Estado y sus órganos se tornan obligados a no afectar. Por otro lado, los *derechos secundarios*, las pretensiones de auxilio surgen para el individuo exactamente para asegurar la ausencia, o restricción de la lesión al bien ius-fundamental. Necesitan un análisis específico de cada derecho fundamental en cada ordenamiento (ROTH, Wolfgang. *Faktische Eingriffe in Freiheit und Eigentum: Struktur und Dogmatik des Grundrechtstatbestandes und der Eingriffsrechtfertigung*. Berlin: Duncker & Humblot, Cop., 1994, p. 71). En sentido similar KLAUS STERN divide el derecho fundamental en un derecho principal y derechos auxiliares. Estas (*Hilfsrechten*) serian las pretensiones (directamente) "no escritas" que se destinan a proteger y tornar real el bien iusfundamental expresamente protegido en el texto constitucional (STERN, Klaus. *Das Staatsrecht der Bundesrepublik Deutschland.* Vol. 3.1. München: Beck, 1988, págs. 588 e sigs.).

[265] BOROWSKI, Martin. *La estructura de los derechos … cit.,* p. 35.

para asegurar una vida en libertad y la dignidad humana"[266]. Pero el sentido de qué son esas "condiciones elementales" no está manifestado por la citación. Al contrario, un análisis de esa reciente historia de la positivización de derechos humanos demuestra lo vastas que son las posibilidades de definición que son necesarios para garantizar la libertad y la dignidad humana[267].

En el campo de la protección de datos podemos notar de una forma muy notoria dos diferentes concepciones en cuanto a su alcance. De un lado, podemos hablar de una idea de *libertad negativa*, en que bastaría garantizar que el ser humano tenga la facultad de negación o prohibición para que las informaciones salgan de su esfera íntima para terminar archivadas en base de datos automatizadas o no. Pero la protección de datos puede tener una concepción más ambiciosa. En esa, sin que sea descuidada la idea del poder de vedar el trámite ya inicial de la información, las facultades se multiplican para asegurar un control de estos aún cuando ya están incluidas en los archivos de otros[268]. El área de protección en los datos personales, por lo tanto, no escapa de la constante autonomía individual, ya que son objeto de consentimiento o sufren las limitaciones constitucionalmente aceptables.

2.7.2 La protección de datos como libertad negativa

La protección de datos como exclusión del conocimiento de los demás tiene una clara conexión con el derecho a la intimidad. En verdad, bajo este prisma la protección de datos sería una adaptación de la intimidad clásica a los desafíos de la tecnología de

[266] HESSE, Konrad. "Significado de los derechos fundamentales... *cit.*, p. 89.
[267] BRUGGER, Winfried. "Menschenrechte im modernen Staat." AöR, 1989, p. 541.
[268] FROSINI, Vittorio. "Bancos de datos y tutela de la persona... *cit.*, p. 24.

los últimos 50 años.

Aunque exista una noción de *privado* como círculo de *intimidad* desde los últimos momentos de la historia de Roma antigua, esta se desvincula completamente de la definición moderna, pues ésta es definida en función de un diferente contrapunto. Lo *privativo* en los antiguos romanos era la característica de aquel que era *privado* de la más importante de las capacidades, la de, por falta de interés o capacidad, ser capaz de participar de la vida política de su colectividad, como ocurría con los bárbaros y esclavos. La casa representaba el lugar de la *necesidad*, donde el hombre era obligado diuturnamente a luchar contra los elementos externos para traer los medios de subsistencia para el hogar. Era la atmósfera eminentemente pre política, terreno de la fuerza y de la violencia, de la sumisión y de la desigualdad. La esfera pública, sin embargo, era el lugar de desarrollo libre, del ser humano, de aquel que se *liberaba* de esa existencia para convivir con sus *iguales*[269].

En la Edad Media, a su vez, la grandiosidad del espacio ocupado por el fenómeno religioso hace que las actividades seculares se concentren en todas las relaciones humanas, en cualquier evento común de la vida diaria. Explica HANNAH ARENDT:

> "El concepto medieval de 'bien común', lejos de indicar la existencia de una esfera política, reconocía solo que los individuos privados tienen intereses materiales y espirituales en común (…) Lo que distingue de la realidad moderna esa actitud esencialmente cristiana en relación a la política no es tanto el reconocimiento de un 'bien común' como la exclusividad de la esfera privada y la ausencia de aquella esfera curiosamente híbrida que llamamos 'sociedad', en la cual los intereses privados asumen importancia pública.
> No es sorprendente, por lo tanto, que el pensamiento medieval, preocupado exclusivamente con el secular, haya permanecido ignorante del abismo entre la vida resguardada en el hogar y la impiedosa vulnerabilidad de la vida en la polis."[270]

[269] ARENDT, Hannah. *A condição humana*. Rio de Janeiro: Forense Universitária, 2007, p. 40 -42 y 48.
[270] *Ibid*., p. 44.

Por eso la importancia de observar el cambio que ocurrió en el paso de fines de la Edad Media a la Edad Moderna y Contemporánea. Si al final del siglo XV el ser humano se encontraba envuelto en una intrincada y constante red de relaciones, cuando llega el siglo XIX ya se encuentra una expectativa de espacios de elección recónditos[271].

El estudio de la iconografía de los periodos demuestra el cambio. En cuanto a las pinturas no sagradas en la Edad Media, observamos la importancia que en aquel momento era dada a la calle medieval, escenario de relaciones familiares, de sociabilidad con los amigos y de ejercicio por cada hombre de su oficio[272]. Al contrario, a partir del siglo XVI comienzan a volverse más frecuentes las representaciones de habitaciones personales, muchas veces con la imagen del parto (que evoca a la Virgen María) o del momento de la muerte, cocinas y pequeñas salas. Sintetiza ARIÈS:

> "La representación más frecuente del dormitorio y de la sala corresponde a una nueva tendencia del sentimiento, que se vuelve entonces a la intimidad de la vida privada. Las escenas de exterior no desaparecen, es verdad, son el origen de los paisajes, pero las escenas de interior se vuelven más numerosas y más originales. Caracterizarían la pintura del género durante todo el tiempo de su existencia. La vida privada, rechazada en la Edad Media, invade la iconografía, particularmente la pintura y el grabado occidentales en el siglo XVI y sobre todo en el XVII: la pintura holandesa y flamenca y el grabado francés comprueban la extraordinaria fuerza de ese sentimiento, antes inconsistente o menospreciado. Sentimiento ya tan moderno, que para nosotros es difícil comprender cuan nuevo era."[273]

ARIÈS sitúa así el prenuncio de la reclusión humana iniciándose a fines del siglo XVII e inicio del siglo XVIII, cuando las casas comienzan a ser construidas garantizando un mínimo de privacidad internamente. Existía un establecimiento de pasillos, que reemplazaban que las habitaciones se comunicasen unas con otras, exigiendo el paso por dentro para el movimiento en la habitación, y la definición de

[271] SEOANE RODRÍGUEZ, José Antonio. "Ética, Derecho y datos personales." In *Cadernos de direito público*. 19, 2003, p. 93.
[272] ARIÈS, Philippe. *História social da criança e da família*. Traducido por Dora Flaksman. Rio de Janeiro: Zahar, 1981, p. 188.
[273] *Ibid.*, p. 194.

funciones para cada uno de los compartimientos de la casa, en que se separa, por ejemplo, espacio para una específica sala de cenar, dormitorios determinados para que cada persona duerma y así sucesivamente[274], haciendo posible el *aislamiento*.

El elemento externo también empieza a ser evitado, por la disminución constante de la extensa cantidad de sirvientes que convivían bajo el mismo techo que sus patrones. Es importante destacar que la noción de "casa grande" de los siglos anteriores está siempre directamenteligada al sentido de casa densamente poblada. Evidentemente no hay homogeneidad en este fenómeno entre las diferentes clases sociales. Solo los hombres verdaderamente ricos, fuesen nobles, burgueses, artesanos o campesinos, podían darse esos lujos. Las familias pobres también pasaban más tiempo en las aldeas, campos y en los palacios de sus "amos" que en sus propias casas, minúsculas y simplemente usadas para reposo y, tal vez, para comer algo, eso cuando tenían condiciones de poseer una[275]. Y aunque las clases intermedias del Antiguo Régimen vivían por demás *dependientes* de las pequeñas y grandes relaciones y fuentes de poder para prescindir de una "cantidad inimaginable de visitas, conversaciones, encuentros e intercambios"[276] en una sociedad en que la *reputación* aún tenía un peso más grande que la *fortuna* acumulada. La aceptación de su entorno era fundada en un medio en que la *amabilidad* superaba la importancia de la capacidad técnica o intelectual.

En general, sin embargo, hasta fines del siglo XVII, vivíamos en un mundo en

[274] En la lengua ese fenómeno se observa lingüísticamente. Si antes todos eran *rooms*, ahora habrá un prefijo definiendo una *dining room*, un *bed-room*, etc.

[275] ARIÈS, Philippe. *História social da criança e da família...cit.*, p. 16. Cuenta incluso el historiador francés: "Existe un estudio sobre la población de Aix-en-Provence en final del siglo XVII, realizado con base en el registro de capitación de 1695. Bajo la luz de ese análisis, se percibe un contraste bastante nítido entre los barrios pobres y densos y los barrios ricos y menos poblados: los primeros poseían casas pequeñas y poco habitadas, y los segundos, casas grandes llenas de gente. Algunas casas abrigaban 3 o menos de 3 habitantes, mientras otras albergaban a 31 personas (2 patrones, 6 niños y 17 empleados) o 17 personas (2 patrones, 8 niños, 7 empleados)." (*ibidem*, p. 248)

[276] ARIÈS, Philippe. *História social da criança e da família...cit.*, p. 229.

que “nadie estaba solo”[277]. No había como referirse a *intimidad* en un mundo en que las personas convivían continuamente y los hogares estaban siempre abiertos para la visita de los allegados. El fortalecimiento de la privacidad en la vida real se consigue a expensas de debilitar la participación en la convivencia social, en el espacio dado a las fiestas colectivas y a las idas a la Iglesia, y de la importancia de la vida total del hombre de sus relaciones con sus vecinos, profesionales y sus amistades.

A partir de ahí, se produce un brutal cambio de *costumbres*. La antigua etiqueta de eterna vida en público y representación, que exigía la casa esté siempre abierta y preparada para invitados, es substituida en la moral vigente por la noción de *cortesía*, en que el contacto excesivo era visto como una señal de provincianismo. La presión social de la eterna sociabilidad comienza a resistirse.

La densificación de la noción del *secreto* de la esfera privada se vuelve ese péndulo favorable a las fuerzas centrípetas del núcleo íntimo familiar ya en el siglo XVIII. Para la burguesía dominante del siglo XVIII la yuxtaposición diaria de riqueza y pobreza, considerada natural desde la Edad Media, y hasta buscada por la nobleza, fue un factor considerado como una promiscuidad indeseada. La visión y contacto con los miserables les provoca un sentimiento de repugnancia y el ideal de vida pasa a ser la existencia de contacto solamente con su misma clase social. La búsqueda de la uniformidad supera la atmósfera anterior de diversidad[278].

Esse transpasse é possibilitado também pela noção burguesa de contrato entre patrão e empregado, que enfraquece a noção de *destino comum* e *proximidade* (diga-se

[277] ARIÈS, Philippe. *História social da criança e da família...cit.*, p. 256.
[278] *Ibid.*, p. 274.

porém que nem por isso mais inserida de dignidade) do senhor/servo.

Este traspaso es posible también por la noción burguesa de contrato entre patrón y empleado, que debilita la noción de *destino común* y *proximidad* del señor/funcionario. Este relacionamiento anterior más profundo es definido con precisión y poesía en los versos de MIGUEL DE CERVANTES para un Don Quijote que mira a su criado Sancho Panza adormecido:

> "Oh tú, bienaventurado más que todos los que viven en la faz de la Tierra, pues, sin tener envidia, ni ser envidiado, duermes con tranquilo espíritu, sin perseguirte hechiceros, ni sobresaltar nigromandas. Duerme repito, y repetiré cien veces, sin inspirarte continuada vigilia celos de tu dama, ni te desvelen pensamientos de pagar deudas, ni de lo que has de hacer para comer el día siguiente, tú y tu pequeña y angustiada familia, ni la ambición te inquiete, ni la vana pompa del mundo te fatigue, pues los límites de tus deseos no se extienden más allá de tu jumento que el de tu persona carga en mis hombros, contrapeso y carga que pusieron la naturaleza y la costumbre a los amos. Duerme criado, está el amo de vela, pensando como lo has de sustentar y mejorar, y hacerle favores. La angustia de ver que el cielo se hace de bronce, sin acudir a la tierra con el conveniente rocío, no aflige al criado, aflige al amo, que ha de sustentar en la esterilidad y en el hambre al que le sirvió en la fertilidad y en la abundancia."[279]

El proceso de construcción de un espacio privado, distante de la mirada de los demás, desde el punto de vista legal - constitucional, se da, en un primer momento, por el ímpeto de las revoluciones de fines de siglo XVIII, impedir que el Estado ejerza búsquedas arbitrarias en la casa de cada ciudadano.

Pero son con los aparatos tecnológicos que surgieron a partir del siglo XIX cuando más se colocan en la tradición de *ius- fundamentación* en que ahora se presenta el uso de la informática. En el ámbito de la intimidad el éxito se fundamenta en la necesidad de evitar ciertos aspectos de la experiencia humana de ser vistos y oídos por los otros, de forma que no sean ejercidos de manera superficial en razón de la

[279] CERVANTES SAAVEDRA Miguel de. *O engenhoso cavaleiro D. Quixote da Mancha : segundo libro*. Traducido por de Viscondes de Castilho e de Azevedo. Vol. 2. Rio de Janeiro: R.B.A. Editores, 1994, p. 106.

indiscreción, pero alcancen la calidad derivada de la vivencia con profundidad[280].

Esta cuestión es evidente en el debate norteamericano en cuanto al contenido de *privacy,* de gran influencia en el debate europeo de la intimidad[281]. Este concepto no es expresamente reconocido en la Constitución estadounidense, siendo fruto de un artículo de los abogados de Boston, SAMUEL D. WARREN y LOUIS D. BRANDEIS, para "Harvard Law Review", vol. IV, n. 5, de diciembre de 1890. La idea central, gira sobre el "derecho de ser dejado solo" (*the right to be let alone*), la misma habría sido influenciada con el objetivo de impedir la cobertura de la prensa sobre el estilo de vida de Warren, casado con la hija de un Senador[282].

La lectura de periódicos ya no estaba restringida a unos pocos, en aquella etapa de la sociedad norteamericana. Entre 1850 y 1890, los periódicos pasaron de alrededor de 100 periódicos con 800000 lectores a más de 900 con 8 millones de lectores. En ese crecimiento, la popularidad, fue un gran factor, después de la Guerra Civil, la popularidad de un estilo sensacionalista de prensa, denominada "yellow journalism", que era extremadamente exitoso. Se seguían los pasos del *The Sun*, periódico creado en Londres en 1833, que creó la fórmula de periódicos baratos (vendido a un *penny*) y cuya temática invariablemente circulaba en torno a la peleas familiares, consumo de alcohol

---

280 ARENDT, Hannah. *A condição humana...cit.*., p. 81.

281 RODRÍGUEZ RUIZ, Blanca. *El secreto de las comunicaciones: tecnología e intimidad*. Madrid: McGraw-Hill Interamericana de España, 1998, p. 6. Se usará el término directamente en inglés, ya que entiende la doctrina que, aunque se haya convenido traducirlo por "intimidad", se trata de vocablo sin correspondiente directo en las lenguas latinas (PÉREZ ROYO, Javier. *Curso de derecho constitucional... cit.*, p. 330)

282 Esa versión de las razones que llevaron a la redacción del artículo es extremadamente reproducida y fue adoptada con gran influencia por WILLIAM L. PROSSER. "Privacy." *Cal. L. Rev.*, 1960. No hay duda de los hechos: Samuel Warren era un rico abogado en Boston en la época y tenía (había abandonado un año antes para asumir las empresas de la familia) como socio del bufete a Louis Brandeis (que posteriormente sería juez de la Suprema Corte Estadounidense). Warren se había casado con Mabel Bayard, hija de un senador de Delaware, y las fiestas que promovía en su casa en *Back Bay* atraían la atención de los periódicos que cubrían con detalles las actividades de la elite, en especial el *The Saturday Evening Gazette*.

en la vía pública y casos policiales[283].

El concepto de un derecho a la *privacy* permitiría que fuesen prohibidas las publicaciones de hechos concernientes a la vida privada, hábitos, actos y relaciones ("private life, habits, acts and relations") que no tuviesen relación con la posibilidad del afectado para ocupar cargos y ocupaciones públicas o que no fuesen practicados en lugares públicos[284].

La *privacy* de WARREN y BRANDEIS es, por lo tanto resultado de la creación de máquinas que puedan vigilar al hombre en sus momentos de reclusión o que simplemente permitan el análisis de aspectos recónditos de su vida. Las cámaras fotográficas y filmadoras registran hoy nuestros momentos, cuando queremos y cuando no, en situaciones normales del día a día, como cuando atravesamos la calle, sacamos dinero en los cajeros electrónicos o hasta cuando estamos dentro de casa[285]. No hay como, no dejar de señalar que eran sobre esas mismas cuestiones que giraban las preocupaciones de WARREN y BRANDEIS: "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ´what is whispered in the closet shall be proclaimed from the house-tops.´"[286]

Bajo este aspecto se podría entender, inicialmente, la comprensión de la guarida ius-fundamental a los datos personales solo como una prolongación de la más antigua

[283] SOLOVE, Daniel J., y ROTENBERG, Marc. *Information privacy law*. New York: Aspen Publishers, 2003, p. 3.
[284] WARREN, Samuel D. y BRANDEIS, Louis D.. "The Right to Privacy." *Harvard Law Review*, 1890, p. 216.
[285] Como demuestra la polémica del *Google Street View* al final de esa primera década del siglo XXI.
[286] WARREN, Samuel D. y BRANDEIS, Louis D. "The Right to Privacy." *Harvard Law Review*, 1890.

protección de la *intimidad*. Cuando ALAN WESTIN, a fines de la década del 60 e inicios de la década del70, estudia los efectos de los bancos de datos en la sociedad estadounidense, desde luego informa que entiende que se enfrenta a otro campo de aplicación del *right to privacy*[287]. La necesidad de evolución del concepto llevó a WESTIN, en la década de los60, a definir: "privacy as the claim of an individual to determine what information about himself or herself should be known to others (...). This, also, involves when such information will be obtained and what uses will be made of it by others."[288].

La tecnificación y modernización del Estado impulsan el interés de los ciudadanos en resguardar aspectos de su esfera reservada que no desean que sea expuesto a una posible curiosidad externa, impulsado por la capacidad aumentada de aprehensión de aspectos de la personalidad de cada uno. Hay un desarrollo realmente similar, pues también la intimidad es una creación que surge finalmente con la necesidad humana de protegerse más fuertemente de las miradas ajenas[289].

La *privacy* sería compuesta por 4 etapas: *solitude* (soledad), *intimacy* (relaciones íntimas), *anonymity* (anonimato) y *reserve* (reserva). Estos diferentes contenidos serían una actualización de la comprensión de las necesidades humanas de abstracción de sí, de su relación con los demás, para decidir si prefiere la soledad; o para realizar su intimidad sexual; para exponer sus pensamientos a los demás sin el riesgo de limitaciones o juicios; y, por último, para crear una barrera que impida la divulgación. Este último sentido explica la *informational privacy*, la cual consiste en la imposibilidad

[287] WESTIN,Alan F. y BAKER, Michael A.. *Databanks in a free society... cit.*, p. 20.
[288] WESTIN, Alan F. "Social and Political Dimensions of Privacy... *cit.*, p. 431.
[289] BENDA, Ernst. "Dignidad Humana y Derechos de la Personalidad". In *Manual de derecho constitucional*. Madrid [etc.]: Marcial Pons, 2001, p. 130.

de grabación de informaciones no anónimas sin consentimiento; lo que serviría también para garantizar la esfera de aislamiento que aseguraría que nuestras elecciones no se sujeten a la constante observación de los demás. Eso hace posible la construcción de una personalidad individualizada[290].

También en la jurisprudencia de la Suprema Corte estadounidense relativa al sentido de *informational privacy*, encontramos dicho enfoque. En *Whalen v. Roe,* de 1977, al analizar una ley del estado de Nueva York que imponía un registro de los datos compulsivo sobre individuos que tenían recetas médicas para comprar determinados medicamentos que podían resultar en un vicio, el juez Stevens, en nombre de la Corte, afirmó que hay dos distintos intereses involucrados en el "*right to privacy*", el de preservar la autonomía individual en la toma de ciertas decisiones, como ya fue afirmado desde 1965 en *Griswold v. Connecticut*[291], y el de impedir la revelación (*disclosure*) de asuntos personales[292].

Nótese que no es que el *privacy* exija el aislamiento, ya que en verdad aunque en la enunciación como "right to be alone" lo que existe es la autorización para que cada persona establezca los límites con relación a los cuales desea que sean expuestos sus pensamientos, sentimientos y emociones a los demás[293]. La idea de control sobre las fronteras secreto/revelación es igualmente inherente a la noción del derecho continental de "intimidad"[294].

---

[290] COHEN, Julie E.. "Examined Lives: Informational Privacy and the Subject as Object." Stan. L. Rev., 1999, p. 1425.
[291] 381 U.S. 479.
[292] 429 U.S. 589, p. 599-600. La ley fue al final no invalidada, pues la intervención estatal no fue considerada irrazonable, ya que no sería más grave que las que cotidianamente ocurren en atenciones médicas (p. 602).
[293] WARREN, Samuel D. y BRANDEIS, Louis D.. "The Right to Privacy... *cit.*, p. 198.
[294] RODRÍGUEZ RUIZ, Blanca. *El secreto de las comunicaciones... cit.*, p. 17.

Podemos justificar la decisión del legislador político por la existencia de una esfera de datos personales protegida del conocimiento de otros, de igual forma que por la defensa de las condiciones adecuadas al desarrollo de un régimen democrático. La protección de datos permite al individuo elegir libremente los debates públicos en los que desea participar y, en aquellos que haya esa opción, le permite que no sea coaccionado en sus manifestaciones por relaciones de dominación derivadas de la posesión por parte de otros de informaciones sobre sí, o que soporte en situaciones fácticas de inferioridad (por ejemplo, relaciones de empleo) un acoso aún mayor, inclusive cuando todos poseen el mismo nivel de conocimiento unos sobre los otros[295].

La *fundamentalidad* del derecho a la autodeterminación informativa está por lo tanto justificada también por la "teoría del discurso" de JÜRGEN HABERMAS. Como se sabe, el autor alemán defiende que la razón posible en un mundo de intereses tan multifacéticos depende de arreglos comunicativos adecuados y, así, que la legitimidad de la ley depende, en último grado, que los asociados sociales, que serán destinatarios de la norma, tengan la posibilidad de encarar la ley válida formada como fruto de su aceptación y autoría después del debate público.

Deriva de esto, la necesidad de que el sistema de derechos sea establecido para que la autonomía privada garantice una efectiva autonomía pública, lo que reconciliaría las ideas de soberanía popular y derechos humanos.[296] Así, habría un haz de derechos fundamentales que serían urgentes para garantizar una "libertad comunicativa" (o sea la

[295] RODRÍGUEZ RUIZ, Blanca."The Right to Privacy: A Discourse-Theoretical Approach." *Ratio Juris*, 2002, p. 166. "HABERMAS confirma la importancia del impedimento de las consecuencias aquí presentadas: "cuando los involucrados son excluidos de la participación, o temas son retirados, contribuciones relevantes son reprimidas, intereses específicos no son honestamente articulados o convincentemente formulados, cuando los otros no son respetados en su alteridad, podemos esperar que tomas de posición racionalmente motivadas no se hagan valer o ni siquiera sean exteriorizadas." (HABERMAS, Jürgen . *Verdade e justificação : ensaios filosóficos*. São Paulo: Loyola, 2004, p. 292).

[296] HABERMAS, Jürgen. *Direito e democracia: entre facticidade e validade... cit*., p. 138.

posibilidad de participar activamente o no en procesos de reconocimiento intersubjetivo) en el procedimiento de formación del derecho y, con ello, la propia realización del ideal democrático y de la legitimidad legal. Dice HABERMAS:

> "La idea de autolegislación de ciudadanos no puede ser deducida de la autolegislación moral de personas singulares. La autonomía tiene que ser entendida de modo más general y neutro. Por eso introduje un principio del discurso, que es indiferente con relación a la moral y al derecho. Este principio debe asumir, por la vía de la institucionalización jurídica, la figura del principio de la democracia, el cual pasa a ver fuerza legitimadora al proceso de normatización. La idea básica es la siguiente: el principio de la democracia resulta de la interconexión que existe entre el principio del discurso y la forma jurídica. Yo veo ese entrelazamiento como una génesis lógica de derechos, la cual puede ser reconstruida paso a paso. Ella comienza con la aplicación del principio del discurso al derecho a libertades subjetivas de acción en general, constitutivo para la forma jurídica como tal y termina cuando se realiza la institucionalización jurídica de condiciones para un ejercicio discursivo de la autonomía política, la cual puede equipar retroactivamente la autonomía privada, inicialmente abstracta, con la forma jurídica. Por eso, el principio de la democracia solo puede aparecer como núcleo de un sistema de derechos. La génesis lógica de esos derechos forma un proceso circular en el cual el código del derecho y el mecanismo para la producción del derecho legítimo, por lo tanto el principio de la democracia, se constituyen de modo cooriginario."[297]

Nótese que, al contrario de la doctrina liberal, HABERMAS niega que exista una configuración jurídica de esos derechos previa a la acción del legislador en el momento histórico, solo aseverando que el principio democrático (que es la aplicación del principio del discurso por medio del *medium* del derecho) demanda *condiciones de socialización comunicativa*[298].

2.7.3. La protección de datos como control después de revelar la información

En la jurisprudencia de la Suprema Corte estadunidense, en el momento que un tercero tiene acceso franqueado a las informaciones, se supera la expectativa de

[297] *Ibid.*, p. 158.
[298] *Ibid.*, p. 165.

protección con base en el texto constitucional de la 4ª enmienda[299]. Por lo tanto los registros bancarios de un ciudadano no son considerados como parte de sus "papeles privados"[300] y bajo números discados, suministrados por la compañía telefónica, no hay expectativa de privacidad[301].

Sin embargo, hay etapas posibles de protección de los datos personales que no son cubiertas por la mera posibilidad de exclusión de la mirada externa de nuestros datos clasificables como íntimos. Cuanto más crece el potencial global de adquisición de información por medio de la tecnología, más se encogen nuestras esferas distanciadas de los demás[302]. En un mundo tan dependiente de los ordenadores, no es suficiente que la protección del derecho se desvanezca con la inclusión en bases de datos[303].

La información y su correlato la comunicación son la *sangre* de la *sociedad de la información* y no su *veneno*.[304]

---

[299] El texto del derecho constante en la 4ª Enmienda es el siguiente: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" (en traducción libre, "el derecho del pueblo a la inviolabilidad de sus personas, casas, papeles y haberes contra la búsqueda y aprehensión arbitrarias no podrá ser infringido; y ningún mandato será expedido a no ser mediante indicios de culpabilidad confirmados por juramento o declaración, y particularmente con la descripción del lugar de la búsqueda y la indicación de las personas o cosas a ser aprehendidas").

[300] United States v. Miller, 425 U.S. 435 (1976).

[301] SMITH V. MARYLAND, 442 U. S. 735 (1979). Son, por tanto, solamente algunas relaciones de comunicación cliente profesional que reciben el privilegio de la confidencialidad, en pro de garantizar la debilidad de parte a parte, como en el caso de médicos y abogados (SOLOVE, Daniel J. y ROTENBERG, Marc. *Information privacy law*. New York: Aspen Publishers, 2003, p. 218). Además, el hecho de no ser contenido de la *privacy*, no impidió al Congreso estadounidense la edición de una serie de normas sectoriales que limitan el uso de bases de datos por controladores y/o aumentan los derechos de los afectados (vide en ese sentido, SOLOVE, Daniel J.. "Privacy and Power: Computer Databases and Metaphors for Information Privacy". *Stan. L. Rev.*, 2000.)

[302] SCHERZBERG, Arno. "Die öffentliche Verwaltung als informationelle Organisation ." In Verwaltungsrecht in der Informationsgesellschaft. Nomos, 2000, p. 195.

[303] SOLOVE, Daniel J.. "Privacy and Power... *cit.*, p. 1438.

[304] BARNES VÁZQUEZ, Javier. "Una reflexión introductoria sobre el Derecho Administrativo y la Administración Pública de la Sociedad de la Información y del Conocimiento." *Administración de Andalucía: revista andaluza de administración pública*, 2000, p. 49.

El avance de la tecnología tornó de poca utilidad una fórmula que hable solo de la mera exclusión del conocimiento de los demás. En un momento de la historia humana en que los ojos (cámaras de vigilancia) y oídos (escuchas telefónicas) pueden surgir en cualquier lugar y en que es difícil perseguir una vida normal sin estar constantemente suministrando informaciones personales; hasta por la necesidad de confianza de quien está tratando con las mismas, y por la gran capacidad que tienen los ordenadores de almacenar informaciones, imágenes y conversaciones y procesarlas digitalmente y toda información referente a cualquier aspecto de nuestras vidas, la verdadera protección está en impedir toda forma de control social o de estigmatización[305].

Hay una multiplicación de las amenazas a la individualidad, ya que hay una concomitante diseminación de posibles miradas y archivos invasores de la privacidad ajena. Una explosión de *micropoderes*, en el sentido foucaultiano del término, con capacidad de opresión[306], especialmente fuerte por el incentivo de alcanzar el poder político o el beneficio económico.

Por ello, aunque haya razones comunes para proteger la intimidad física del destinatario de los derechos fundamentales y las informaciones sobre él que se encuentran archivadas, hay importantes distinciones también. La evolución de la tecnología informática produce dos aspectos muy distintos del sujeto a proteger en este campo: su cuerpo *físico* y su cuerpo *electrónico*[307]. Esa dicotomía en el abordaje permite distinguir la protección defensiva, negativa, *estática*, con que es descripta la *intimidad* con relación a las protecciones obligatorias que exigen el movimiento en la utilización

[305] RODOTÀ, Stefano. *A Vida na Sociedade da Vigilância... cit.,* p. 144.
[306] CASTELLS, Manuel. *La era de la información... cit.,* p. 331.
[307] RODOTÀ, Stefano. *A Vida na Sociedade da Vigilância... cit.,* p. 17.

de nuestros datos personales.

Aunque sea seductor afirmar que "el hombre honesto nada tiene que temer", de hecho la metáfora del "hombre de vidrio", el cual es íntegramente transparente, cumple la práctica para sellar estructuras con tendencias totalitarias en que pocos saben demasiado sobre muchos[308].

La protección de datos debe, por lo tanto, ser regulada para mantener el desarrollo de las individualidades sin que eso impida al Estado utilizar de dichas informaciones como medio para desarrollar el todo social. Eso explica que las legislaciones más protectoras sobre el tema mantengan niveles distintos de protección, más reforzadas en los "datos sensibles", aquellos que se refieran a minorías, hasta llegar a la inexistencia en los datos obtenidos sin identificación[309]. Esas clasificaciones permiten de esa manera que se *discriminen* seres humanos, ya sea con el objetivo de elegir, los más adecuados para una campaña publicitaria o para una averiguación policial[310].

La distinción inicial entre el derecho a la protección de datos y el derecho a la intimidad radica en que no es necesario dividir entre características que el sujeto se dispone a revelar y otras que deben quedar al margen de los demás. Como dice Rodotá "publicidad y control no son términos contradictorios como publicidad y

[308] RODOTÀ, Stefano. *A Vida na Sociedade da Vigilância... cit.,* p. 150.
[309] RODOTÀ hace algunas observaciones en cuanto a esas reglas genéricas, entendiendo que datos socioeconómicos, especialmente los de propiedad y tributarios, tienen el don de facilitar el debate público sobre los rumbos de un país y que datos, inclusive anónimos, levantados sobre específicas minorías pueden ser utilizados para oprimirlas (*A Vida na Sociedade da Vigilância... cit.*,p. 32).
[310] FROOMKIN, A. Michael. "The Death of Privacy?... *cit.*., p. 1471.

confidencialidad"[311].

La solución para el *conundrum* del "hombre de vidrio" no pasaría por blindarlo solamente, sino hacer también de vidrio, la "casa"[312]. Nuevas categorías jurídicas buscan adaptar el Derecho y dar a él nuevas estructuras que respondan a los intensos efectos causados por la evolución tecnológica, que transformó la información en un elemento central de nuestra realidad.

No hay ningún dato individual que deba estar fuera del objeto del derecho fundamental a la autodeterminación informativa, donde quiera que esté guardado, pues la combinación de mínimas especificidades sobre los individuos tiene el potencial de servir para que él pueda ser manipulado por el dueño de la base de datos. La única forma de impedir que el titular del archivo donde hay almacenamiento, use lo que conoce, es someterlo al máximo de transparencia y observancia, ya sea por el individuo afectado o por órganos estatales para este fin. Este nuevo tipo de dominación del ser humano por la tecnología es potencialmente más grave, pues se da de forma subrepticia, no negando derechos, sino simplemente emasculando nuestra capacidad de reacción[313].

O sea, podemos contraponer una tutela de exclusión de interferencias sobre la intimidad privada y familiar, de carácter negativo y estático, y la nueva tutela de la protección de datos personales, cuya intervención es dinámica, persiguiendo la información durante su circulación. Es creado así un "poder permanente de control sobre sus propios datos"[314]. Además esos propios datos son distintos del típico objeto de

[311] RODOTÀ, Stefano.*A Vida na Sociedade da Vigilância... cit.*, p. 36
[312] *Ibid..*, p. 48.
[313] *Ibid.*, p. 58.
[314] RODOTÀ, Stefano. "Democracia y protección de datos... *cit.*, p. 18.

defensa de la esfera íntima, ya que incluyen, un nivel agravado de protección; declaraciones claramente de naturaleza pública, como filiación sindical y opiniones políticas, además de otras que no son íntimas, pero en que el ciudadano quiere tener la medición de para quien y con qué objeto son divulgadas, como en el secreto bancario y profesional[315]. Una recopilación de esas múltiples actividades diarias a las cuales nos exponemos, aunque aisladamente no pueden afectarnos en nada, en conjunto pueden formar un *mosaico* de nuestra personalidad a ser manipulado por terceros[316].

Así, cuanto más control se tenga de dónde, con quién y con qué contenido sobre informaciones propias con interlocutores se cuente, habrá mayor seguridad para la manifestación. Además, los principios vinculados a la protección de datos, como el de la *calidad de la información*, consecuencia de un sistema que valora la integridad de la veracidad del registro almacenado en la base de datos y da medios a los ciudadanos para ver la corrección de este contenido, enriquecen la discusión en el espacio público y dan subsidios más confiables para la toma de decisión.

2.7.4 La nomenclatura y autonomía en la protección de datos

La nomenclatura de esa protección involucrando restricción al uso, pero también control, merece un análisis aparte, ya que hay notable multiplicidad de términos que tratan del mismo contenido, destacándose "derecho a la protección de datos", "libertad informática" y "autodeterminación informativa".

[315] ÁLVAREZ-CIENFUEGOS SUÁREZ, José María. *La defensa de la intimidad de los ciudadanos...cit.*,p.. 21.
[316] MURILLO DE LA CUEVA, Pablo Lucas. "La Constitución y el derecho a la autodeterminación informativa". *Cuadernos de derecho público*, 2003, p. 36.

Hay quien comprende que la terminología "autodeterminación" resbala en un carácter de absoluto control por parte del ciudadano que desprecia las facultades que también son concedidas a aquellos que tratan la información, prefiriendo la idea de "libertad", que también podría ser interpretada como "libertad de control" y como límite a los titulares de las bases de datos[317].

Al contrario, aquellos que optan por el término consagrado en la jurisprudencia del Tribunal Federal Alemán lo hacen resaltando, que esta expresión tiene mayor rigor técnico, al concentrar en un único nombre las ideas de control personal sobre tránsito de datos relativos a uno, sea cual fuera la tecnología utilizada, criticando la terminología "libertad informática" por ser más vaga y al mismo tiempo restringida científicamente, sin observar que la violación al bien jurídico central a este derecho fundamental no depende del medio elegido[318]. La terminología "autodeterminación" también facilitaría la conexión con la idea tan fundamental de manifestación de voluntad en el "consentimiento" necesario para el uso de la información[319]. Por último, critican también que el nombre de "derecho a la protección de datos" falla en el momento de colocar el sentido de la defensa sobre el objeto, cuando lo que se pretende es advertir la integridad del sujeto a quien ellos se refieren[320].

Pero, en realidad, el uso de "libertad informática" peca por estar inevitablemente vinculado a la idea de defensa de las "libertades negativas"[321] y no recoger los avances

[317] ORTI VALLEJO, Antonio *Derecho a la intimidad e informática* . Granada: Comares, 1994, p. 68.
[318] MURILLO DE LA CUEVA, Pablo Lucas. "La Constitución y el derecho a la autodeterminación informativa... *cit.*, p. 39.
[319] TRONCOSO REIGADA, Antonio. . "La protección de datos personales... *cit.*, p. 295.
[320] CONDE ORTIZ, Concepción. *La protección de datos personales... cit.*, p. 29.
[321] Aunque podamos hablar también en "libertades positivas" (también llamadas "libertades de los antiguos"), la idea de "libertad como no interferencia" es usualmente la aplicada en textos jurídicos, fruto especialmente de las obras de Hobbes y Bentham. Compruébese sobre el tema PETTIT, Philip. *Republicanism: a theory of freedom and government*. Oxford: Oxford University Press, 1997, capítulo

tecnológicos, así como la violación del uso no automatizado, de la expresión "protección de datos" pues la misma tiene la cualidad de garantizar la claridad que la unificación terminológica presenta. Así, se argumenta que, además de haber sido el nombre utilizado por el TC en la sentencia 292/2000, se trata también de la expresión utilizada en la Carta Europea de Derechos Fundamentales, lo que garantiza la consolidación como vocablo común para los Estados miembros de la Unión Europea[322].

Así, parece mejor la utilización de los nombres "derecho a la protección de datos" y "derecho a la autodeterminación informativa" como sinónimos. La multiplicidad de expresiones puede ser adecuadamente justificada por la juventud del tema y por el interés provocado en notables juristas concomitantes. Por eso, en este momento de la dogmática, hay que reconocer la validez de los argumentos en favor de ambas nomenclaturas.

Aunque es innegable el mayor apuro técnico de la expresión creada inicialmente por la doctrina alemana (y por eso se la utiliza para titular el presente trabajo), es también un hecho que el derecho positivo no debe ser despreciado, y el legislador viene inclinándose por la idea de "protección de datos". Hay que resaltar que el término "protección de datos", aún pudiendo pasar por una idea equivocada de concentración, solamente sobre la integridad de los archivos, también puede ser interpretado como una expansión del objeto protegido con relación a la intimidad, a fin de resaltar los cuidados necesarios que se deben continuar observando por los dueños de bases de datos aún después de la salida legítima de las informaciones del control de su titular[323].

1.

[322] SERRANO PÉREZ, María Mercedes. "El derecho fundamental a la Protección de Datos... *cit.*, ,p. 252.

[323] DI FABIO, Udo. "Rn 173. Das Recht auf nformationelle Selbstbestimmung als Ausprägung des

Asiente que las características deben involucrar una libertad negativa y una libertad positiva de controlar y que esto involucra cualquier dato, y no solo algunos "íntimos", la cuestión de la autonomía de un "derecho a la protección de datos" (o "a la autodeterminación informativa") con relación a la intimidad o de ser meramente instrumental a esta se hace una cuestión de poca relevancia de orden práctica.

La afirmación de una lista "numerus a pertus" de derechos fundamentales, que serviría para complementar la labor del constituyente originario, sujetos a las limitaciones de conocimiento de los futuros peligros para la sociedad, dando mayor permanencia en el tiempo al texto constitucional o a la decisión de órganos jurisdiccionales, como el TEDH, en fundamentar la protección de datos en la vida privada, en función de la imposibilidad natural de encontrar en el texto de 1950 previsiones en cuanto a peligros que solo se mostraron posteriormente, debe ser entendido como una opción de cada Tribunal Constitucional frente a las especiales características de la concepción de su derecho constitucional y de los medios de integración del rol de derechos fundamentales.

Lo que se debe comprender es que el carácter instrumental del derecho a la autodeterminación informativa a la protección de otros derechos no debe servir de óbice a aceptarse su autonomía, puesto que, además de todos los derechos fundamentales ser, en última instancia, instrumentales a la dignidad de la persona humana, es cierto que hay otros derechos indiscutiblemente autónomos en las Constituciones actuales que son

---

Selbstdarstellungsschutzes, insbesondere gegenüber modernen Gefährdungsformen." In *Maunz/Dürig, Grundgesetz*. München: Beck, 2010. Agréguese que el propio BVerfG no es inflexible en el uso del término "autodeterminación información", aplicando en algunos fallos también la expresión "protección de datos" (*Datenschutz*), como en BVerfGE 84, 239 (279).

igualmente instrumentales de forma indiscutible. Podemos decir, por ejemplo, que la inviolabilidad del domicilio es un medio al servicio de la intimidad y de las libertades personales[324]. Igualmente la autodeterminación informativa funciona instrumentalmente a otros derechos fundamentales, a citar la libertad religiosa, la libertad de expresión y la libertad política y sindical[325].

2.8 Conclusiones

1. El concepto de derechos y libertades consagrados con la Revolución Estadounidense y la Francesa, referentes a una concepción universalista de titularidad a todos los individuos, independiente de otros factores externos, tiene como destinatario primordial el poder del Estado. El formato alemán de este modelo en la postguerra, cuando se solidifica la alcurnia de "derechos fundamentales", es impulsada especialmente por esa característica de impedimento de tendencias totalitarias por parte del Poder Público. Esta razón también impulsa las vigentes experiencias constitucionales española y brasileña.
2. Aunque esos "derechos fundamentales" tengan el componente apriorístico de atributo inherente a la naturaleza humana, sus específicas emanaciones positivadas son fruto de construcciones históricas propias de los desafíos reales enfrentados por las sociedades nacionales. Al mismo tiempo, el origen en el tratamiento digno para cada ser humano estimula listados en tratados supranacionales y una convergencia entre los países de la comunidad

[324] MURILLO DE LA CUEVA, Pablo Lucas. *El derecho a la autodeterminación informativa... cit.*, p. 158.
[325] RODOTÀ, Stefano. "Democracia y protección de datos... *cit.*, p. 21.

internacional.

3. La interpretación del contenido exacto y los límites de los derechos fundamentales son fruto de un movimiento en que cooperan la Jurisdicción Constitucional y el Poder Legislativo. Eso involucra definición del *área de protección* de cada derecho fundamental, establecimiento de las facultades a él inherentes y definición de sus límites en la confrontación con otros bienes constitucionales. La conjugación de esfuerzos, sin embargo, no significa que el Poder Judicial no deba, en primer lugar, proceder a la fijación de las posiciones iusfundamentales del individuo.
4. En el derecho a la protección de datos personales, el reconocimiento de la *norma* constitucional parte de distintas formas de *texto* constitucional. Podemos categorizarlos en tres grandes grupos: las constituciones donde no hay referencia específica a la protección de datos personales, como la alemana, donde la protección debe venir por medio del contenido de otros derechos más amplios; constituciones donde, sin tratarse claramente de un *derecho* a la protección de datos, se hace referencia al tema, estimulándose al legislador a providencias (este es el caso de la constitución española); y constituciones que indican expresamente que son otorgadas facultades referentes a un derecho individual a la protección de sus datos personales. En esta última forma, puede ocurrir que este derecho venga informado por medio de una garantía procesal, en la acción de *habeas data*. Esta es precisamente la situación en la constitución brasileña.
5. Las búsquedas por regular el uso de base de datos en el territorio alemán surgen en la primera mitad de la década del 70 en dos estados miembros, Hesse y Rheinland-Pflaz, y, a continuación, en 1977 en la legislación federal.

También es a nivel de los estados federados donde primeramente es consagrado como derecho constitucional (en Nordrhein-Westfalen). Sin embargo, el reconocimiento de su existencia en la Ley Fundamental de Bonn solo se da en 1983, por medio de la sentencia del Tribunal Constitucional Alemán conocida como *Volkszählungsurteil*.

6. Este fallo representa, más que una creación sin precedente, una evolución innovadora de la jurisprudencia del Tribunal, muy en reverberación de preocupaciones expuestas por manifestaciones sociales en cuanto a los peligros del volumen de informaciones que se encontraría en poder del Estado después del futuro censo a ser realizado. La *autodeterminación informativa*, o sea, el poder de controlar la obtención y manipulación de la información sobre uno, intrínseca a la dignidad humana (art. 1 I GG) y al derecho de libre desarrollo de la personalidad (art. 2 I GG), abarca cualquier dato personal, constituyendo un avance con relación uso de la "Teoría de las Esferas" (*Sphärentheorie*) en la protección del individuo en este campo.
7. La realización del derecho, para el Tribunal Constitucional alemán, exigiría de la Administración la aclaración previa y el uso vinculado a la *finalidad* que preside la necesidad de la obtención. Límites a estos mandamientos o a la voluntariedad de la entrega estarían bajo "reserva de ley", o sea, exigirían norma legal que explicitase las situaciones concretas proporcionales que justificasen la priorización sobre otros intereses constitucionales.
8. La jurisprudencia posterior a este juicio del Tribunal Constitucional Alemán sirvió para reforzar el significado fundador de la *Volkszählungsurteil*, al aclarar puntos que son ambiguos en este juicio, como la imposibilidad de compartir datos entre órganos de la Administración sin la presencia de norma

limitadora al derecho y a su aplicabilidad también a los tratamientos manuales de los datos. Además demostró, a lo largo de esas tres décadas, su conformidad con la realidad del mundo moderno, al ser invocado en cuestiones tan distintas como el uso de muestras de ADN o el contenido de cuentas telefónicas en investigaciones criminales o verificaciones sobre el pasado del trabajador para admisiones, entre otros.

9. Más recientemente el Tribunal Constitucional alemán viene destacando como nuevo derecho del hombre, aliado de la autodeterminación informativa, la necesidad de "confiabilidad e integridad de los sistemas de tecnología de información" (*Vertraulichkeit und Integrität informationstechnischer Systeme*).
10. En España, las dudas en cuanto al significado del apartado 4 del artículo 18 de la constitución española son un reflejo del propio debate constitucional. Al fin, el texto de 1978 presenta un carácter dudoso, al resaltar la defensa de atributos de la intimidad del individuo a ser realizados por el Parlamento al legislar regulando las consecuencias del uso de la informática.
11. El Tribunal Constitucional, en consecuencia, demora a desvincular las hipótesis de protección de datos personales del tradicional derecho a la intimidad. Aún después de la edición de una ley de "regulación del tratamiento automatizado de datos de carácter personal" (LO 5/1992), en la STC 254/1993, se habla de una "intimidad informática" que no sostiene autonomía conceptual.
12. Es con la STC 292/2000, prenunciada de forma tímida en la STC 44/99, que queda admitida la existencia de un propio "derecho a la protección de datos" como derecho fundamental español, distinto de la intimidad al suministrar al

titular también facultades positivas de actuar sobre su dato ya almacenado en la base de datos existente y no un mero derecho oponible *erga omnes* de abstención y por su *objeto* involucrar también informaciones que ya tengan el conocimiento externo y no puedan ser calificadas como *íntimas*. Igual al derecho alemán, se admiten limitaciones al nuevo derecho sometidas a la *reserva de ley*.

13. Hay ausencia de una norma expresa previendo el derecho a la protección de datos en la constitución brasileña. Sin embargo, también las múltiples posibilidades de reconocerse un derecho a la protección de datos como *norma adscripta* de derecho fundamental se vieron hasta el momento frustradas en la jurisprudencia del Supremo Tribunal Federal (STF) brasileño. Así, la protección del inciso XII del artículo 5o.de la Constitución Federal de 1988 tiene como bien jurídico el medio de *comunicación* interpersonal y no el contenido de las informaciones intercambiadas. Los datos personales solo tienen salvaguarda constitucional cuando son conectados a la esfera *íntima* o *privada* humana (términos empleados por la Corte de manera indistinta), por fuerza del inciso X de este mismo artículo 5º. La idea clave en la protección constitucional brasileña se revela por el empleo reiterado por la jurisprudencia de la palabra "sigilo" (*secreto*), notablemente en informaciones bancarias y fiscales, y siempre teniendo como relevancia el impedimento del conocimiento (o de su uso legítimo) por otro.
14. La jurisprudencia y la doctrina brasileñas en lo que respecta al *habeas data* (CF, artículo 5º, inciso LXXII) son altamente restrictivas y de forma alguna tendientes al reconocimiento de un nuevo derecho a la protección de datos

por medio de él. En vez de la pretensión original del anteproyecto constitucional de una amplia configuración del derecho individual relacionado a las bases de datos informatizados, la comprensión mayoritaria en Brasil ve esa acción constitucional sin ningún avance con relación a la protección de la intimidad. Al contrario, hay toda una serie de dificultades en su manejo, por la limitación de los pedidos al acceso y rectificación de datos, por la inexistencia de medios para conocer donde hay base de datos que sin el consentimiento del usuario obteneron sus datos y, principalmente, por las restricciones procesales, en la cual se destaca la exigencia de la prueba de la negativa al acceso. En la práctica, hubo en estos más de 20 años un número bastante limitado de *habeas data* presentados en Brasil, casi confirmando el análisis de que se trata de un instrumento propicio específicamente para el conocimiento de los archivos dictatoriales en el inicio de la redemocratización brasileña.

15. Del análisis de los fallos de los tres tribunales podemos deducir los fundamentos de la protección a los datos del individuo. De un lado, es consensual que la protección de datos personales debe involucrar un prisma de *libertad negativa*, o sea, la de poseer un espacio reservado que este a salvo, a criterio del afectado, de las miradas no deseadas de terceros. Ese contenido favorece la formación por cada miembro del cuerpo social de elecciones y personalidad individualizadas, sin presiones excesivas externas. Igualmente fortalece el propio debate público, al fortalecer la posibilidad de participación de deliberación autónoma, sin limitaciones de los demás participantes.
16. Pero existe también la indicación de que esta defensa, modelo clásico de

protección de una esfera íntima, es insuficiente en una sociedad en que el avance tecnológico hace tan fácil la observación, almacenamiento y conjugación de las informaciones sobre cada ser humano. Se suma al resguardo de un espacio particular la importancia de que aún las informaciones ya divulgadas solo lo sean en la medida de la autorización de cada individuo y que cada base de datos sea transparente a la verificación de su regularidad por cada uno que tenga características almacenadas. Finalmente, hay beneficios adicionales al ser multiplicado el control social sobre las bases de datos, ya que la información en estos tiende a hacerse más próxima a la realidad y así se vuelve más confiable la decisión con base en esta.

17. La opción de nomenclatura del derecho de cada individuo con relación a sus datos personales es influenciado por estas consideraciones. En este sentido, existe el rechazo del término "libertad informática" por indicar una errónea vinculación solamente a libertades negativas. A su vez, el uso de "autodeterminación informativa" presenta con precisión la importancia de que cada persona pueda definir con autonomía de qué modo se dará la circulación de sus datos. Aunque "protección de datos" pueda pasar la idea de que lo central sea la defensa de los sistemas de información y no el ser humano, tiene a su favor el amplio uso en las legislaciones del tema y el empleo genérico del vocablo "dato", que resalta su amplitud y desvinculación de cualquier limitación calificativa, espacial o temporal, cuando se conecta a un titular de derecho fundamental.
18. Definidas las características ínsitas a una efectiva "protección de datos personales" su autonomía o colocación dentro de otro derecho constitucional

se hace un tema de menor relevancia y atinente esencialmente a las peculiaridades de cada sistema constitucional en agregar nuevos derechos fundamentales a su lista de forma simple o no. Cierto es, sin embargo, que no debe el refuerzo que la protección de datos hace a otros derechos, como la libertad sindical, servir de óbice a su autonomía, ya que en esto también ocurre con varios otros derechos de aceptación pacífica.

3.- La protección de datos en el plan supranacional y la búsqueda de la uniformidad de tratamiento

El gran impulso en la propagación supranacional de reglas para la protección de datos personales se debe a las estructuras europeas[326]. A lo largo de las décadas del '70 al '90 las iniciativas supranacionales alimentaron e impulsaron las medidas internas en los países para, finalmente, ser determinantes en las codificaciones. Aunque una motivación importante en la búsqueda de criterios comunes haya sido el interés de asegurar la constancia del flujo de informaciones entre países[327], el proceso fue también estimulado por la voluntad de asegurar bases comunes de protección a los derechos humanos y a la seguridad social.

A lo largo de décadas de influencias mutuas, la jurisprudencia del Tribunal Europeo de Derechos Humanos y la Dirección de la Unión Europea de 1995 terminaron por convertirse en repositorio y síntesis de los marcos a ser seguidos por los Poderes Judicial y Legislativo de cada país, estableciendo al mismo tiempo parámetros para otros países que deseen intercambiar informaciones con países del continente europeo. Extendiéndose desde este escenario, podemos determinar como otras disposiciones que influyeron de manera relevante para la creciente codificación interna sobre la protección

[326] SIMITIS, Spiros, org. *Kommentar zum Bundesdatenschutzgesetz*. Baden-Baden: Nomos-Verlagsgesellschaft, 2003, p. 63.

[327] En especial al comercio internacional (ARENAS RAMIRO, Mónica.*El derecho fundamental a la protección de datos personales...cit.*, p. 151).

de datos como la recomendación de OCDE de 1980 y el Convenio n. 108 del Consejo de Europa de 1981[328].

Numéricamente podemos medir esta influencia. A mediados de 2011 podíamos contar en el mundo 76 países que contaban con una legislación interna de protección de datos personales que reflejaban esos patrones mínimos de garantía al individuo impulsados por la legislación internacional. De esos, en conjuntos que naturalmente se intercalan, hay 27 países de la Unión Europea y 41 países miembros del Consejo de Europa que ratificaron el Convenio Nº 108[329]. También podemos encontrar leyes con esas características en países africanos (Angola - 2011, Benin – 2009, Burkina Faso – 2004, Cabo Verde – 2001, Marruecos – 2009, Mauricio – 2004, Senegal – 2007 y Túnez – 2004), de Oriente Medio/Asia (Australia – 2001, Hong Kong – 1995, India – 2011, Israel – 1981, Japón – 2003, Kirguistán – 2008, Macao – 2005, Malasia – 2010, Nueva Zelandia – 1993, Corea del Sur – 2011 y Taiwán – 2010) y americanos/caribeños (Argentina – 2000, Bahamas – 2003, Canadá – 2002, Chile – 1999, Colombia – 2008, México – 2010 y Uruguay – 2008).

De los países africanos, cuatro (Benin, Burkina Faso, Cabo Verde y Senegal) son miembros de la Comunidad Económica de Estados de África Occidental (en inglés, ECOWAS), la cual adoptó un tratado fuertemente inspirado por la dirección de la Unión

[328] GREENLEAF, Graham. "Global data privacy laws: Forty years of acceleration". *Privacy Laws and Business Special Report*, September 2011, p. 6.

[329] Armenia, Georgia y Turquía son los únicos miembros del Consejo de Europa que no poseen una ley de protección de datos. Rusia posee desde 2011 una ley de protección de datos, aunque haya solamente firmado y no ratificado la Convención Nº 108 de 1981. Aun hay leyes en otros Estados europeos que no ratificaron la Convención ni forman parte de la Unión Europea, como las Islas Faroé (legislación esta que es considerada "adecuada" a la directiva 95/46), Gibraltar, Montenegro y San Marino (GREENLEAF, Graham. "Global data privacy laws: Forty years of acceleration... *cit.*, p. 3 a 6).

Europea[330]. De los otros 18 países no europeos, 8 (Australia, Canadá, Chile, Israel, Japón, México, Nueva Zelandia y Corea del Sur) forman parte de la OCDE, Argentina tiene legislación considerada "adecuada" a la directiva 95/46 y Uruguay está en vías de conquistar el mismo estatus.

Así, considerando que desde inicios del siglo XXI se adhirieron 40 países (siendo 8 a partir de 2010) de la comunidad internacional a la reglamentación internacional de protección de datos[331], se ve que más del 50% se encuentra fuera de los confines de Europa, notándose que en este período aumentó más de 6 veces la presencia de normas relativas a la protección de datos en países no europeos. El movimiento internacional de protección de datos, por lo tanto, se intensifica y se diversifica por las regiones del planeta, bajo el reflejo de una legislación internacional que, como veremos, posee un núcleo claramente común.

3.1. La Jurisprudencia del Tribunal Europeo de Derechos Humanos relativa a la protección de datos

3.1.1. Introducción

El Consejo de Europa fue creado en 1949, aún bajo la influencia determinante de los eventos trágicos de la Segunda Guerra Mundial, con el objetivo de , garantizar la unidad de los países europeos en torno a su común identidad cultural y a los valores a defender. Así, se destacó por ser una de las primeras instituciones internacionales en

[330] GREENLEAF, Graham. "Global data privacy laws: Forty years of acceleration... *cit.*, p. 7.
[331] *Ibid.*., p. 2.

colocar la dignidad humana en el frente de su actuación[332], dentro de la idea de que el patrimonio común incluía la preservación de las mejores prácticas constitucionales. En ese aspecto su principal fuente normativa es el Convenio Europeo de Derechos Humanos.

El denominado Convenio Europeo de Derechos Humanos, documento sustantivo de derecho internacional es el nombre dado al Convenio de Roma para la Protección de los Derechos Humanos y de las Libertades Fundamentales, celebrado el 4 de noviembre de 1950 y gracias al cual el Tribunal Europeo de Derechos Humanos, situado en Estrasburgo, ejerce su jurisdicción. Este documento jurídico entró en vigencia el 3 de septiembre de 1953 y hoy cuenta con la adhesión de 45 países, o sea, va más allá de los participantes de la Unión Europea.

Hay un punto que desde siempre destaca del Convenio con relación a documentos similares protectores de derechos humanos en la esfera internacional, que es, su capacidad de imponer medidas vinculantes a los países participantes mediante los fallos del Tribunal Europeo de Derechos Humanos, al responsabilizarlos por sus incumplimientos del acuerdo. Ese es el factor fundamental de la transformación del Tribunal de Estrasburgo a lo largo de su historia cincuentenaria en una influencia relevante de su enfoque sobre las legislaciones nacionales en derecho material y procesal[333]. La conjugación de sus decisiones con las emanadas por los tribunales constitucionales de cada país forma la estructura de derechos en que son relevadas las bases del ordenamiento comunitario[334].

---

[332] MACHADO, Jónatas E. M.. *Direito Internacional... cit.*, p. 332.
[333] SIEMEN, Birte. *Datenschutz als europäisches Grundrecht*. Berlin: Duncker & Humblot, 2006, p. 26.
[334]Hay una no despreciable influencia de la formación de un espacio comunitario, ya que "era, a todas luces, constitucionalmente lógico, por imposible, que existiera un derecho comunitario ajeno a la fuerza o

Se resalta que, en menor intensidad, esa postura fue secundada por el Tribunal de la Comunidad Europea, que, desde 1969[335], afirmó la importancia de los derechos del hombre. Estos serían reconocidos en las listas de derechos fundamentales de las Constituciones de los países miembros[336] y en las convenciones internacionales sobre el tema, integrando el conjunto del Derecho Comunitario como *derecho primario*, y, así, pudiendo también ser invocados en sus juzgados. Esto fue consagrado, a comienzos de la década de los 90 en el artículo F del Tratado de Maastricht, hoy artículo 6º del Tratado para la Unión Europea[337].

Por último, la firma de la Carta de Derechos Fundamentales de Nice, en 2000, aún con todos los contratiempos para su entrada en vigencia, lo que llevó en la práctica a la necesidad de reafirmarla en el cuerpo del Tratado de Lisboa, representó el éxito de ese contrato, pues confirmó la jurisprudencia del TEDH, inclusive en lo que respecta a la autodeterminación informativa como integrante del patrimonio común constitucional europeo. La historia del Tribunal cumple de esta forma un ciclo completo, con la transmutación en ley de sus decisiones que buscaron exactamente concretar los derechos fundamentales previstos en la convención de 1950[338].

Tanto para España, como para Alemania, el Convenio y las decisiones del TEDH sobre los derechos fundamentales tienen una importancia palpable.

---

virtualidad de los derechos fundamentales" (ÁLVAREZ-OSSORIO MICHEO, Fernando. "Los Derechos Fundamentales". In *Hacia la europeización de la Constitución española: la adaptación de la Constitución española al marco constitucional de la Unión Europea*. Bilbao: Fundación BBVA, 2006, p. 78).

335 Caso *Stauder*.

336 Vide caso *Nold*, de 1974.

337 SIEMEN, Birte. *Datenschutz als europäisches Grundrecht... cit.*, p. 28.

338 *Ibid.* , p. 35.

El Tribunal Constitucional Español afirmó que el carácter de norma de derecho interno del Convenio (de conformidad con el artículo 96.1 de CE) y, por medio del artículo 10.2 de la Constitución Española, la obligación de tener en cuenta, a la hora de interpretar los derechos y libertades[339]. Ratificó igualmente al TEDH como organismo c*alificado* para decidir sobre el sentido de las normas del Convenio y el carácter vinculante y obligatorio de sus decisiones para el Estado español, mientras es demandado[340].

La influencia en la jurisprudencia alemana no es tan extensa, pero aún así es significativa. Según decidió el Tribunal Constitucional Federal el 14 de octubre de 2004[341], el texto de la Convención no tiene *status* constitucional[342], pero sí de ley federal, ya que es un tratado aprobado regularmente por el Parlamento. Como tal, tiene efecto vinculante sobre la Administración y los Tribunales (art. 20.3 GG) y las decisiones del TEDH forman parte de una interpretación metodológicamente justificable de la ley. Esta interpretación "amigable" al derecho internacional solo puede ser desestimada si resulta en una protección menor que la otorgada por el ordenamiento jurídico alemán (realmente la Convención en su artículo 53 afirma tratarse de mínima protección) o en caso de que la Constitución alemana resulte no respetada[343].

339 CRUZ VILLALÓN apunta este artículo 10.2 como un *mandato interpretativo*, que además de vincular ciudadanos y todos los poderes públicos, tienen la peculiaridad de también vincular mismo el "intérprete supremo de la Constitución", el Tribunal Constitucional (CRUZ VILLALÓN, Pedro. "El Ordenamiento Constitucional: una indagación empírica". In *La curiosidad del jurista persa, y otros estudios sobre la Constitución*. Madrid: Centro de Estudios Políticos y Constitucionales, 2006, p 114-115).

340 FJ 3 de la Decisión 245/1991 del Tribunal Constitucional español.

341 2 BvR 1481/04.

342 De la misma forma que en España, como afirmó el FJ 5 de la STC 36/1991.

343 De forma crítica, aun más, reconociendo que esa decisión *fortaleció l*a posición del CEDH y del TEDH en Alemania vide MEYER-LADEWIG, Jens. "Artikel 46". In *Europäische Menschenrechtskonvention : Handkommentar*. Baden-Baden: Nomos, 2010, Rn 28-37.

3.1.2 Historial de fallos sobre protección de datos

3.1.2.1 Reconocimiento de la protección de datos personales dentro del Derecho a la Vida Privada

Evidentemente en un documento de los años cincuenta, como es la Convención Europea de Derechos Humanos, no se podría esperar una protección expresa contra la utilización de bases de datos informatizados, técnica aún en su joven edad en esa época. Pero existe en su artículo 8º una norma que protege de forma general la "vida privada" y es en dicha cláusula que se basa el Tribunal para sus decisiones concernientes a la protección de los datos individuales. La Corte, por lo tanto, en lo que respecta al desarrollo del derecho a la protección de datos siempre se mantuvo ante una encrucijada: resguardar el respeto por sus interpretaciones por parte de los tribunales de los países miembros, lo que significaba encontrar un posible patrón mínimo de conformidad con el derecho constitucional de la comunidad, y al mismo tiempo conservar la actualidad de la Convención frente a la realidad de su tiempo[344].

La Convención Europea de Derechos del Hombre prevé la defensa de la vida privada en su artículo 8º, en una protección que se asemeja a la que existe en el artículo 12 de la Declaración Universal de Derechos del Hombre, de solo dos años antes. Dice el documento europeo:

> "1. Cualquier persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
> 2. No puede haber injerencia de la autoridad pública en el ejercicio de este derecho sino cuando esta injerencia estuviese prevista en la ley y constituir una providencia que, en una sociedad democrática, sea necesaria para la seguridad nacional, para la seguridad pública, para el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la

[344] Como expresó en Tyrer v. Reino Unido, el 25 de abril de 1978. Aqui se expresa que la convención debe ser vista como un "living instrument which must be interpreted in the light of present-day conditions.".

> protección de la salud o de la moral, o la protección de los derechos y de las libertades de terceros."

La técnica legislativa se repite después en los artículos 9 al 11 de la Convención: mientras el apartado 1 describe la extensión de la protección, el apartado 2 indica posibles limitaciones al derecho. Pero el artículo 8 se destaca con relación a los otros pues presenta un objeto muy amplio, que comporta distintas defensas de ámbitos humanos, debido a que la idea sobre el contenido de "vida privada" permite múltiples interpretaciones[345].

Una primera opción interpretativa de la Comisión, que más adelante facilitaría la inclusión de la protección de los datos personales, fue realizada en el caso *X v. Iceland*[346], juzgado el 18 de mayo de 1976. Se trataba del caso donde el dueño del perro en Reykjavik se revelaba contra la prohibición de que mantuviese su animal. Aunque su demanda haya sido denegada, en virtud de la necesaria afectación a los demás, causada por la presencia del animal, la Comisión ha señalado el rechazo de una concepción de "vida privada" (*private life*) en lo que respecta a un sinónimo de la *privacy* del derecho anglosajón o hasta del derecho francés, o sea, constituida solamente de aquellos momentos en que el individuo se aísla de los demás. Al contrario, afirmó que formarían parte también todas las interacciones y relacionamientos con otros seres humanos, inclusive, como más tarde afirmará la Cámara en el caso *Niemitz v. Alemania*[347], en aquellos de naturaleza profesional (ítem 29). Además la protección de la vida privada no fue considerada solamente un fin en sí misma, sino también un medio indispensable para garantizar el derecho humano a la formación y conocimiento de identidad y

[345] SIEMEN, Birte. *Datenschutz als europäisches Grundrecht... cit.*, p. 52.
[346] Ap. 6825/74.
[347] Ap. 13710/88, juzgamiento el 16 de diciembre de 1992.

desarrollo de la propia personalidad[348]. Fue un notable desarrollo en la jurisprudencia del Tribunal, ya que solo 3 años antes, en el caso *X. v. United Kingdom* (ap. 5877/72, 12 de Octubre de 1973) la Comisión entendiera que el uso por parte de las autoridades de fotos de manifestantes no podría ser considerada una violación del artículo 8, exactamente porque sacadas en espacio público, no existe invasión del recinto domiciliar de la reclamante.

Hay, por tanto, para el TEDH, dos aspectos a ser observados en la frase "vida privada", uno de efectos negativos, que impide la invasión de otras sub esferas individualmente preservadas, que de igual forma busca facilitar y estimular las relaciones sociales. Ese concepto de "vida privada" del TEDH, que suma al retiro aislado las demás interacciones públicas que sean importantes para nuestra formación humana[349], permite que, en cuanto a datos personales, la protección pueda ocurrir independientemente de si el origen de la información deriva de fuente pública o privada, si fue obtenida de forma clara o de forma subrepticia. En todos los casos, podría afirmarse el derecho del ciudadano a ser protegido de obtenciones y almacenamientos abusivos[350].

Mas eso implicaba en otro paso: decir que las informaciones sobre cada ser humano formaban parte de su vida privada, pues son esenciales para su desarrollo. En realidad, en dos ocasiones la Comisión tuvo la oportunidad de abordar el tema y rechazó el reclamo sin mayores consideraciones de fondo sobre el tema. El 6 de febrero de 1967,

---

[348] Ese entendimiento amplio en cuanto al contenido de la protección a la vida privada fue reafirmado por la Comisión también en un juzgamiento poco después, *Bruggemann and Scheuten v. The Federal Republic of Germany* (ap. 6959/75, 19 de mayo de 1976).Vide también en ese sentido *Peck v. Reino Unido* (2003) y *Odièvre v. Francia* (2003).

[349] SIEMEN, Birte. *Datenschutz als europäisches Grundrecht... cit.*, p. 74.

[350] OVEY,Clare e WHITE, Robin. *The European Convention on Human Rights*. Oxford: Oxford Univ. Press, 2010, p. 374.

en el caso *X. v. Netherlands*[351], un campesino holandés se quejó de la obligación que tenía de prestar declaraciones anuales sobre toda su actividad rural, bajo pena de multa o hasta de prisión, a la "Corporación de Agricultura", (ente privado dotado por el gobierno holandés de autoridad pública), violaba, entre otros artículos de la Convención, el artículo 8º, lo que fue rechazado sucintamente en pro de la ordenación económica nacional.

El caso *Klass and others v Federal Republic of Germany* (juzgado el 6 de septiembre de 1978) aunque a primera vista no involucre datos personales, y nuevamente este tema no haya sido tratado directamente en el fallo, representa un cierto avance del TEDH en pro de adoptar una defensa clara en la protección de la información del individuo. Pues en verdad, la colocación de las conversaciones telefónicas dentro de la protección que establece el artículo 8º, sea por el concepto de "vida privada" o por la análoga protección de las correspondencias, y la reivindicación de existencias de "remedios" en la legislación que permitan el control de eventuales abusos en la vigilancia de estas, funciona con una misma razón: impedir el uso indiscriminado por parte del Estado, de datos que solo nos deberían importar a nosotros mismos y a nuestros interlocutores[352].

La Comisión toma, el 6 de octubre de 1982, su propia decisión sobre los reflejos de un Censo Nacional sobre los derechos fundamentales, en el caso *X. v. United Kingdom* (Ap. 9702/82). En esta decisión se asume que el nivel de detalle de los campos del formulario obligatorio, involucrando lugar de nacimiento, estado civil, etc., afecta *prima facie* el bien jurídico del apartado 1 del artículo 8º de la Convención. Sin

[351] Ap. 2290/64.
[352] SIEMEN, Birte. *Datenschutz als europäisches Grundrecht... cit.*, p. 83.

embargo, tampoco aquí se llega a afirmar un derecho a la protección de datos, pues más allá de la medida ser socialmente necesaria para la planificación nacional, el grado de *anonimato* y *confidencialidad* existente en la ley inglesa permitirían la medida.

Esa timidez de la Corte fue expuesta de forma precisa en el voto del juez Pettiti en el caso *Malone v. The United Kingdom* (ap. 8691/79, decisión del 2 de agosto de 1984). Aunque concordando con la mayoría que condenó al Estado, ese magistrado lamentó en su voto el hecho de que el Tribunal hubiera perdido una vez más la oportunidad de expresarse con claridad sobre cuáles son las medidas justificativas y protectoras necesarias para que un país pueda catalogar los datos de sus ciudadanos (en la hipótesis de que hubiera un sistema que permita un control directo de números discados y duración de las comunicaciones del reclamante), aunque en la práctica la mayoría de los países europeos ya operase con el uso computarizado de cientos de bases de datos de sus ciudadanos y que el Tribunal Constitucional Alemán ya hubiese asumido la existencia de una "autodeterminación informativa".

La primera vez que se hace claramente tal ilación entre la vida privada y la protección de datos personales en los juzgados del TEDH es en el denominado tema *Leander*[353]. Este caso involucró a un empleado del Museo Naval en Karlskrona (al sur de Suecia), es decir, un empleado de la Marina de Guerra, dependiente de la base Naval en la misma localidad. Este señor fue forzado a dejar su empleo por razones de "seguridad nacional" en virtud de una investigación administrativa que descubrió su militancia en periodo pretérito en el Partido Comunista, su participación en una editorial que publicaba un periódico de contestación política y su afiliación a un sindicato de

[353] *Leander v. Sweden*, ap. 9248/81, decisión el 26 de marzo de 1987.

soldados.

Esa sentencia es la pionera en admitir que los derechos individuales pueden ser lesionados por la existencia de base de datos en que son almacenadas y utilizadas informaciones sobre nuestra existencia, en especial cuando se inhibe la facultad del individuo a rectificar o cancelar las informaciones allí dispuestas. Sin embargo, en el caso concreto el Tribunal entendió como legítimas las garantías (*safeguards*) previstas en la legislación sueca, pues la formación y manipulación de los registros era fiscalizada por varios organismos, destacándose la oposición parlamentaria y un *ombudsman* independiente[354].

En *Hilton v. The United Kingdom* (ap. 12015/86, el 6 de julio de 1988), la Comisión reafirmó que la obtención y almacenamiento de datos sobre temas privados del ciudadano, y su uso posterior perjudicial sobre su persona, efectivamente viola la protección del art. 8º. Aunque en el citado caso la periodista Isabel Hilton no haya conseguido probar este hecho, la comprensión de datos personales como incluido en el concepto de "vida privada", iniciado en *Leander*, se solidificaba[355].

Incluso después de *Leander* y *Hilton*, el TEDH indicaba que no todos los datos personales merecerían la protección del artículo 8º. En *Reytjens v. Belgium* (ap. 16810/90, el 9 de Septiembre de 1992) la Comisión entendió que la presentación de identidad personal a policías y el archivo de los datos consignados, que podrían incluir

[354] Ítems 65 a 67. La decisión en Leander fue reforzada en el caso *Turek v. Eslovaquia* (2006), ya que en una situación similar, en la cual se motivó para despedir empleado sus anteriores vínculos con el comunismo, pero no se las reveló con exactitud en función de su "carácter secreto", el TEDH entendió violado el artículo 8º por la inexistencia de posibilidad del afectado en conocer su dato archivado que le perjudica.

[355] SIEMEN, Birte. *Datenschutz als europäisches Grundrecht... cit.*, p. 96.

nombre, sexo, lugar de nacimiento, dirección principal y nombre del cónyuge, ni siquiera afectaba el contenido del artículo 8º de la Convención, pues no formarían parte de la "vida privada del reclamante". Hay aquí un cierto retroceso, ya que en 1985, asumida la protección de datos personales después de la decisión de la Comisión en el caso *Leander,* el Tribunal prefirió dejar abierta su postura sobre si el posible uso del número de identificación personal por parte de la Administración Tributaria para el descubrimiento de rendimientos e imposición de tributos violaba el artículo 8 o no[356].

Esa categorización propia en el Tribunal de Estrasburgo fue paulatina, resultado de una colección de decisiones que listaban, uno a uno, especies de datos que merecerían una protección especial.

Por ejemplo, la afirmación de que los *datos médicos* merecerían la protección del art. 8º fue inicialmente relevada en el caso *L. v. Germany*[357]. Pero fue apartada en ese caso pues no había declaración de doctores particulares del reclamante, pero sí de *experts* en un Tribunal.

En el caso de *Z v. Finland*[358] la hipótesis involucró la revelación por parte de los médicos de la paciente infectada con el virus del HIV de su historial clínico en un proceso judicial destinado a establecer la responsabilidad penal de su marido en un crimen de violación agravado por su condición de seropositivo, como forma de compensar la negativa de la demandante en testificar hechos que podrían incriminar a su cónyuge. Además de eso la confidencialidad del historial médico, que ya sería solamente por 10 años, hasta 2002, no se mantiene y estos hechos son difundidos por

[356] *Lundvall v. Sweden*, ap. 10473/83, 11 de diciembre de 1985, ítem 4.
[357] Ap. 12793/87 , 13 de outubro de 1988.
[358] Ap. 22009/93, 25 de Janeiro de 1997.

los medios de comunicación.

Concluye la Corte que hubo una doble violación de la protección a los datos personales de Z: primero al ver sus datos médicos expuestos en el proceso judicial contra su voluntad y, después, en el historial médico que se volvería público en 10 años, incluso antes. Mientras en el primer caso existiría una justificación legítima de la investigación criminal[359], las demás situaciones deberían ser cohibidas, ocasionando responsabilidad estatal.

Cabe resaltar, sin embargo, que la gran evolución presente en el juicio del caso *Z v. Finland* es, va más allá que la decisión; pues en el ítem 95 de la fundamentación, es admitido por primera vez la conexión entre la garantía de confidencialidad de las informaciones médicas y el bienestar de los pacientes, así como la íntima relación entre una parte del concepto de vida privada del artículo 8º del CEDH y la Convención 108 de 1981 del Consejo de Europa[360]:

> "In this connection, the Court will take into account that the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention (art. 8). Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general.
> Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community (see Recommendation no. R (89) 14 on "The ethical issues of HIV infection in the health care and social settings", adopted by the Committee of Ministers of the Council of Europe on 24 October 1989, in particular the general observations on confidentiality of medical data in paragraph 165 of the explanatory memorandum).
> The domestic law must therefore afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention (art. 8) (see, mutatis mutandis, Articles 3 para. 2 (c), 5, 6 and 9 of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, European Treaty Series no. 108, Strasbourg, 1981).""

[359] Justificación que, por ejemplo, no se encuentra para esposa que divulga datos médicos de su marido en un proceso de divorcio (*LL v. France*, 2006).

[360] Especialmente en lo que respecta a este y otros datos allá considerados como "sensibles".

Pocos meses después, en *M.S. v. Sweden* (ap. 20837/92, juzgada por cámara de la Corte el 27 de agosto de 1997), el Tribunal reafirmó la importancia de la confidencialidad en los datos médicos, indicando también, en el ítem 35, el carácter *sensible* que ellos pueden representar.

Además, también en ese ítem, la cuestión de la *finalidad* específica de la obtención y de la consecuente *prohibición de la transmisión a terceros* es reconocida, al definirse que la cesión de datos médicos afecta el derecho individual incluso cuando involucra a servidores como cedentes y cesionarios[361]. Fue tratada incidentalmente en aquel mismo día en la decisión de *Andersson v. Sweden* (ap. 20022, decisión de la Corte el 27 de Agosto de 1997),en ocasión del voto parcialmente discordante del juez De Meyer. En ambos casos se afirma que la obligación impuesta por la legislación sueca de que los médicos informen en determinadas situaciones sobre los datos de sus pacientes constituye una intromisión en su "vida privada", no obstante, dicha limitación pueda ser justificable según el sistema de protección de derechos de la Convención.

Datos obtenidos en espacios públicos comienza a merecer atención del TEDH en el caso *Friedl v. Austria*[362]. Aquí, al criterio de no incluirse fotos tomadas en lugares públicos como integrantes de la "vida privada", establecido en *X. vs. The United Kingdom* de 1973, expresó que el uso de esa imagen para establecer la identidad del fotografiado, y el archivo de esos incidentes en carpeta propia, sí afectaría las cuestiones privadas del reclamante, no obstante pudiese ser justificada por otras razones de derecho (ítem 52). En *Tsavachidis v. Greece*, el informe de la Comisión[363] avanza aún más esa

[361] Nótese que eso depende que, al final, la injerencia por la Administración sueca es justificada por el "test de proporcionalidad" frente a los intereses públicos a ser defendidos.
[362] Ap. 15225/89, informe de la Comisión adoptado el 19 de mayo de 1994.
[363] Ap. 28802/95, informe adoptado el 28 de octubre de 1997.

noción, al afirmar que personas no famosas tienen en su "vida privada" también acciones al aire libre, sin la pretensión de secreto (ítem 47). Por eso el archivo de esas informaciones, fruto de la vigilancia del Gobierno, constituye también una violación del artículo 8º de CEDH.

Al contrario, el mero uso de fotografía de patente de vehículo en vía pública por radar para aplicación de multa, sin uso para otro fin o divulgación pública, no posee ninguna afectación sobre la vida privada del conductor[364]. También en *Herbecq v. Belgium* (ap. 32200/96, del 14 de enero de 1998) se afirma que la mera grabación pública de imágenes, con fines de mejorar la seguridad pública y *sin posteriores tratamientos*, no afecta el contenido del derecho del art. 8º de la Convención. Sin embargo, existe también aquí alguna protección, pues las imágenes nunca pueden ser divulgadas al gran público sin que se garantice el anonimato del individuo involucrado[365].

El caso *Amann*[366] tiene la importancia de representar el reconocimiento expreso de la ampliación del concepto de "vida privada" por la "Gran Cámara" del TEDH, frente a los límites del texto de la norma, para incluir los ámbitos protegidos por el Convenio 108, confirmando también en la protección de los datos personales la posición expuesta en *X v. Iceland* de 1976. Por eso, entiende el Tribunal en el ítem 65 de la decisión que:

> "the term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore,

364 Caso *Campion contre la France*, ap. 25547/94, pronunciamiento de la 2 ª Sala de la Comisión el 6 de Septiembre de 1995.
365 *Peck v. The United Kingdom* (ap. 27798/95, 28 de enero de 2003), ítems 61 y 62.
366 *Amann v. Switzerland* (ap. 44647/98, 16 de febrero de 2000).

> there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life" (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and the Halford judgment cited above, pp. 1015-16, § 42). That broad interpretation corresponds with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2)"

Esos fallos modelan una postura más actual del TEDH en no establecer zonas claras y fijas que dividan la intimidad de lo público para fines de protección de datos dentro del concepto de "vida privada". Al mismo tiempo se presenta la dificultad del TEDH en destacar la autonomía de una "autodeterminación informativa" en los modelos divulgados por la jurisprudencia del Tribunal Federal Alemán. Por eso, la maleabilidad del concepto de vida privada corresponde a la ausencia de una interpretación actualizada de la Convención sobre la existencia de un propio "derecho a la protección de datos"[367]. Se admite el contenido y las facultades inherentes, pero no, la novedad en el rol y aplicación a cualquier dato personal.

El uso de la casuística en la definición de los datos a ser protegidos fue expresamente admitido en los ítems 56 a 58 de la decisión de la 3ª Sección de la Corte en *P.G. and J.H. v. The United Kingdom* (ap. 44787/98, del 25 de Septiembre de 2001), en que los reclamantes protestaron que las grabaciones realizadas a sus respuestas cuando estaban presos fuesen utilizadas para análisis posteriores por la inteligencia policial. De forma semejante, se puede hablar sobre la utilización de filmaciones de presos para fines de reconocimiento judicial por parte de testigos[368]. En esos casos la

[367] SIEMEN, Birte. *Datenschutz als europäisches Grundrecht... cit.*,p. 132.

[368] Caso *Perry v. The United Kingdom* (ap. 67737/00, 17 de julio de 2003). Además el tema de la *finalidad* del levantamiento o recogimiento es reforzado como elemento esencial a la legalidad del mantenimiento. Así se refuerza el concepto de que registros tomados en locales públicos se tornan lesivos al servir a otros propósitos que no la prevista de aquel momento y mismo los archivos de bases de datos públicos, independientemente del contenido sensible o no de las informaciones, deben existir

relevancia está en el reconocimiento de cuáles situaciones que involucran, en un principio, el secreto en las comunicaciones y la protección de la imagen desembocan en la protección de datos al servir como identificación de los ciudadanos.

El Tribunal reconoció igualmente que hay intervención en la "vida privada" en los almacenamientos de ADN e impresiones digitales[369], aunque esas medidas pueden ser consideradas necesarias en la prevención de crímenes en una sociedad democrática.

3.1.2.2 Obligaciones positivas de los Estados en el derecho a la protección de datos

En el campo de la protección de datos el tema *Gaskin v. United Kingdom*[370], que llega a juicio en el Tribunal dos años después de *Leander*, brinda un buen ejemplo de aplicación de los efectos de la convención para forzar prestaciones positivas estatales. Se trata de un ciudadano británico que, habiendo pasado su infancia y adolescencia en instituciones de cuidado para menores, desea tener acceso a los informes sobre sus internaciones, porque alega haber sido víctima de maltratos. Después de varios requisitos el reclamante consigue finalmente el acceso a todos los documentos relativos a sí mismo, salvo los que involucran informaciones de terceros que no hayan consentido en su divulgación.

El TEDH aquí reconoce haber violado el derecho presente en el artículo 8º no en

solamente mientras continúen manteniendo conexión con las razones de recogimiento.

369 Caso *S. and Marper v. the United Kingdom* (ap. 30562/04 y ap. 30566/04).

370 Ap. 10454/83, juzgamiento el 7 de julio de 1989.

razón de cualquier uso impropio realizado por el Gobierno, sino por la inexistencia de una autoridad independiente que verificase si tal negativa al acceso por parte de otro particular involucraría justificación razonable o no (ítems 41 y 49 de la decisión):

> "41. The Court agrees with the Government that the circumstances of this case differ from those of the Leander case in which the respondent State was found to have interfered with Article 8 (art. 8) rights by compiling, storing, using and disclosing private information about the applicant in that case. Nevertheless, as in the Leander case, a file exists in this case concerning details of Mr Gaskin's personal history which he had no opportunity of examining in its entirety.
> However, it is common ground that Mr Gaskin neither challenges the fact that information was compiled and stored about him nor alleges that any use was made of it to his detriment. In fact, the information compiled about Mr Gaskin served wholly different purposes from those which were relevant in the Leander case. He challenges rather the failure to grant him unimpeded access to that information. Indeed, by refusing him complete access to his case records, the United Kingdom cannot be said to have "interfered" with Mr Gaskin's private or family life. As regards such refusal, "the substance of [the applicant's] complaint is not that the State has acted but that it has failed to act" (see the Airey judgment of 9 October 1979, Series A no. 32, p. 17, para. 32).
> The Court will therefore examine whether the United Kingdom, in handling the applicant's requests for access to his case records, was in breach of a positive obligation flowing from Article 8 (art. 8) of the Convention.
> (…)
> 49. In the Court's opinion, persons in the situation of the applicant have a vital interest, protected by the Convention, in receiving the information necessary to know and to understand their childhood and early development. On the other hand, it must be borne in mind that confidentiality of public records is of importance for receiving objective and reliable information, and that such confidentiality can also be necessary for the protection of third persons. Under the latter aspect, a system like the British one, which makes access to records dependent on the consent of the contributor, can in principle be considered to be compatible with the obligations under Article 8 (art. 8), taking into account the State's margin of appreciation. The Court considers, however, that under such a system the interests of the individual seeking access to records relating to his private and family life must be secured when a contributor to the records either is not available or improperly refuses consent. Such a system is only in conformity with the principle of proportionality if it provides that an independent authority finally decides whether access has to be granted in cases where a contributor fails to answer or withholds consent. No such procedure was available to the applicant in the present case.
> Accordingly, the procedures followed failed to secure respect for Mr Gaskin's private and family life as required by Article 8 (art. 8) of the Convention. There has therefore been a breach of that provision."

Queda claro que no todas las especies de datos y situaciones exigen esa obligación positiva estatal de asegurar el *derecho de acceso*. En el denominado *derecho de conocer el origen*, o sea, de conocer la identidad del padre y la madre, el Tribunal tomó dos decisiones distintas. En *Mikulić v. Croatia* (ap. 53176/99, del 7 de febrero de 2002) admitió, como en *Gaskin*, que el concepto de *vida privada* involucra el derecho a crecer y formarse como ser humano conociendo informaciones importantes para la

identidad, como en la hipótesis la calificación del verdadero padre. Por eso la ley croata, al no definir medios (que pueden ser desde la creación legal de una presunción de paternidad hasta el permiso de imposición de sanciones por la negativa a la pericia) para que una autoridad independiente decida rápidamente sobre las dudas en cuanto a la paternidad, cuando el supuesto padre se niega a realizar el examen de ADN, violaba los derechos del art. 8º de la reclamante, una niña de 5 años de edad en el momento de la decisión.

En *Odièvre v. France* (ap. no. 42326/98, del 13 de febrero de 2003), en una decisión en que 7 jueces de los otros 10 que formaron la mayoría no estuvieron de acuerdo, el Tribunal entendió que no existía el derecho de una mujer adoptada, entonces con 38 años, de conocer la identidad de su verdadera madre, que exigió mantenerse en el anonimato cuando entregó la guarda de los niños sin responsables al gobierno. Para la minoría, liderada por el juez Wildhaber, la idea de *autonomía* personal involucra obligatoriamente su *derecho a la identidad*, que se ve violado cuando no se concibe en la legislación francesa cualquier medio de discusión del veto a ser conocido, opuesto en cuanto al nacimiento por la madre natural. Para la mayoría, la legislación francesa, al buscar garantizar el anonimato como forma de evitar abortos ilegales y abandonos hechos a la intemperie, además, salvaguardar los nuevos vínculos familiares formados con los padres adoptivos, no sobrevaloró la privacidad de la madre natural que no deseaba a su bebé. Al contrario, preservó dentro del derecho a la protección de datos su fundamental característica de depender de su voluntad el servicio de informaciones sobre sí, pero observando el punto de vista de la progenitora desconocida[371].

[371] SIEMEN, Birte. *Datenschutz als europäisches Grundrecht... cit.*, p. 200.

En cuanto a la *rectificación* de datos personales, y en ese caso con íntima conexión con la autodeterminación individual[372], se encuentra un cambio de orientación del Tribunal en pro de reconocer una prestación positiva estatal que se da en el caso de *Christine Goodwin v. the United Kingdom* (ap. 28957/95, juicio el 11 de julio de 2002).

Anteriormente, varios precedentes hubiesen aceptado dentro del margen de apreciación estatal la negativa del cambio de nombre y género en los registros de nacimiento de transexuales operados[373]. En este juicio, sin embargo, observó el Tribunal que la evolución legal interna e internacional en la aceptación de las consecuencias del cambio de sexo justificaba que fuesen eliminadas las barreras restantes en el ordenamiento que dificultasen la autonomía y la dignidad de los transexuales en la pos operación de vivir según la opción sexual elegida[374].

Además de la sanción del cumplimiento de los actos de las autoridades gubernamentales en sí, la teoría de las obligaciones positivas facilita a la Corte producir el llamado "efecto horizontal" de los derechos de la Convención también en las relaciones entre particulares, ya que el sistema europeo de derechos humanos ocasiona la responsabilidad siempre que eso provenga de tolerancia o falla protectora estatal[375].

En el caso *Craxi (n. 2) v. Italy* (ap. 25337/94, juicio el 17 de Julio de 2003) se

---

372 *Ibid.*, p. 194.

373 Como en *Rees v. the United Kingdom* (decisión de 17 de octubre de 1986), *Cossey v. the United Kingdom* (27 de septiembre de 1990); *X., Y. and Z. v. the United Kingdom* (22 de abril de 1997) y *Sheffield and Horsham v. the United Kingdom* (30 de julio de 1998). Sin embargo, aun en esos casos ya se observan algunas medidas favorables a la identidad de los transexuales por parte del gobierno del Reino Unido, como la emisión de pasaportes y registros de conducir ya con el nuevo nombre y género.

374 Ítems 89 a 91 de la decisión.

375 AKANDJI-KOMBE, Jean-François. *Positive obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention on Human Rights*. Human rights handbooks No. 7. Strasbourg: Council of Europe, 2007, p. 15.

observó una de esas utilizaciones del concepto de "prestaciones positivas" como medio de exigir del Estado que garantice también los derechos humanos en las relaciones entre particulares, con el carácter adicional de entrar en conflicto dos derechos humanos: la protección de datos personales y la libertad de prensa. En el proceso penal contra el ex primer ministro italiano (de 1983 a 1987) Bettino Craxi, en que se sospechaba de que estuviera involucrado en un esquema de corrupción en el Consejo de Dirección de la *Metropolitana Milanese*, fue autorizada una interceptación telefónica, sobre la cual fueron divulgadas por diversos periódicos italianos fragmentos de conversaciones que no se referían a la acusación en sí, a pesar de los intentos de Craxi, con la ayuda de otros políticos italianos, de desacreditar a sus acusadores y enemigos.

El TEDH reafirmó en este juicio el derecho del público a ser informado sobre el contenido de acusaciones penales contemporáneas al proceso, así como las figuras públicas tienen el derecho de reserva de sus declaraciones particulares:

> "63. As concerns more specifically reporting by the press of news concerning pending criminal proceedings, it is to be pointed out that there is general recognition of the fact that the courts cannot operate in a vacuum. Whilst the courts are the forum for the determination of a person's guilt or innocence on a criminal charge, this does not mean that there can be no prior or contemporaneous discussion of the subject matter of criminal trials elsewhere, be it in specialised journals, in the general press or amongst the public at large (see, *mutatis mutandis*, *Sunday Times v. the United Kingdom (no. 1)*, judgment of 6 November 1980, Series A no 38, p. 40, § 65).
> 64. Reporting, including comment, on court proceedings contributes to their publicity and is thus perfectly consonant with the requirement under Article 6 § 1 of the Convention that hearings be public. Not only do the media have the task of imparting such information and ideas: the public also has a right to receive them (see *Worm v. Austria*, judgment of 29 August 1997, *Reports* 1997-V, pp. 1551-1552, § 50). This is all the more so where a public figure is involved, such as, in the present case, a political man and former Prime Minister. Such persons inevitably and knowingly lay themselves open to close scrutiny by both journalists and the public at large (see, among other authorities, *Lingens v. Austria*, judgment of 8 July 1986, Series A no. 103, p. 26, § 42).
> 65. However, public figures are entitled to the enjoyment of the guarantees set out in Article 8 of the Convention on the same basis as every other person. In particular, the public interest in receiving information only covers facts which are connected with the criminal charges brought against the accused. This must be borne in mind by journalists when reporting on pending criminal proceedings, and the press should abstain from publishing information which are likely to prejudice, whether intentionally or not, the right to respect for the private life and correspondence of the accused persons (see, *mutatis mutandis*, *Worm v. Austria*, judgment

quoted above, *ibidem*).
66. The Court observes that in the present case some of the conversations published in the press were of a strictly private nature. They concerned the relationships of the applicant and his wife with a lawyer, a former colleague, a political supporter and the wife of Mr Berlusconi. Their content had little or no connection at all with the criminal charges brought against the applicant. This is not disputed by the Government."

Admitiendo eso y que no había ningún interés en la divulgación de las conversaciones, la Corte, notando que el informe fuera practicado por periódicos *privados*, imputa al Estado italiano la responsabilidad de no haber garantizado las protecciones necesarias para el mantenimiento de confidencialidad de las grabaciones de llamadas telefónicas que había legalmente realizado[376].

En el caso *K.U. v. Finland*[377] , juzgado el 2 de diciembre de 2008, el TEDH da otro paso importante en la protección de los datos personales, al condenar a un Estado porque no había, en 1999, legislación que obligase a un proveedor de Internet a divulgar el nombre de quien había contratado una publicación de anuncio, en este caso, simulando tratarse de un menor real de 12 años, que buscaría relaciones sexuales con hombres adultos. Se encuentra en el ítem 48 de este fallo:

"The Court accepts that in view of the difficulties involved in policing modern societies, a positive obligation must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities or, as in this case, the legislator. Another relevant consideration is the need to ensure that powers to control, prevent and investigate crimen are exercised in a manner which fully respects the due process and other guarantees which legitimately place restraints on crimen investigation and bringing offenders to justice, including the guarantees contained in Articles 8 and 10 of the Convention, guarantees which offenders themselves can rely on. The Court is sensitive to the Government's argument that any legislative shortcoming should be seen in its social context at the time. The Court notes at the same time that the relevant incident took place in 1999, that is, at a time when it was well-known that the

[376] Ítem 75 de esa decisión. La Corte agrega que el Estado italiano no investigó adecuadamente el origen de la violación de sigilo. En ese aspecto, sin embargo, hay una severidad excesiva, ya que parece ser más realista el voto minoritario del juez Zagrebelsky, que indagó cual medida investigativa más efectiva podría haber sido aplicada sin, con ello, violar otros derechos en la Convención de Roma: "The Court should take into account the fact that normally the only effective method is to compel journalists to reveal their sources or to make use of very intrusive procedures against them, such as intercepting their communications or searching their homes or offices. However, this kind of investigation was found to be in violation of the Convention (Article 10) in *Roemen and Schmit v. Luxembourg* (judgment of 25 February 2003, no. 51772/99) and the protection of journalistic sources is one of the basic conditions for press freedom.(...)"

[377] Ap. 2872/2002.

> Internet, precisely because of its anonymous character, could be used for criminal purposes (see paragraphs 22 and 24 above). Also the widespread problem of child sexual abuse had become well-known over the preceding decade. Therefore, it cannot be said that the respondent Government did not have the opportunity to put in place a system to protect child victims from being exposed as targets for paedophiliac approaches via the Internet."

Por lo tanto, la Corte exige que en el campo de los derechos fundamentales los Estados parte se abstengan de lesionar el derecho (prestaciones negativas) y además que no haya un atropello sistemático a los derechos humanos en dichas sociedades, lo que incluye la represión a los que actúan delictivamente en la sociedad (prestaciones positivas). Pero no solo eso. El concepto de "prestaciones positivas"[378] involucra, en las decisiones de la Corte, todo tipo de determinación para que el Estado realice algo, sea mejorando el marco legal, garantizando procedimientos de control al lesionado, en cuanto medidas concretas, como producir investigaciones con efectividad, para salvaguardar los derechos previstos en la Convención, dando realidad práctica a lo teóricamente previsto en la norma internacional[379].

En cuanto a la violación estatal en las obligaciones negativas se da por una acción, o sea por una interferencia en el campo humano del desarrollo del derecho, mientras que en las obligaciones positivas eso ocurre en su omisión. En estas, al contrario, exige el TEDH que el Estado se esfuerce para garantizar el cumplimiento de la convención. Este modelo doble de prestaciones negativas y positivas utilizado por el Tribunal Europeo de Derechos Humanos corresponde a obligaciones de los Estados miembros que también podrían ser divididas como "obligaciones de respetar", "obligaciones de proteger" y "obligaciones de implementar"[380].

---

[378] Cuja primeira utilização deu-se no chamado *Belgian linguistic case*, julgado em 23 de julho de 1968.

[379] Como celebremente afirmado en el ítem 24 de la decisión de *Airey v. Ireland* (ap. 6289/73), del 9 de octubre de 1979.

[380] AKANDJI-KOMBE, Jean-François. *Positive obligations... cit.*, p. 5.

3.1.2.3 Limitaciones posibles en la protección de datos personales según el TEDH

En el artículo 8.2 de la Convención ganan un especial destaque las limitaciones aceptadas de los derechos que, en el caso de la "vida privada" y consecuentemente de la "protección de datos", están en el apartado 2 del artículo 8 de la Convención, ya que estas pueden pecar por falta, como visto en *K.U. v. Finland* , o por exceso.

Este apartado 2, similar, aunque no idéntico, al de los artículos 9 al 11, expresan cláusulas genéricas de interés social que equilibran los derechos individuales que los preceden[381]. Por otro lado, la Corte de Estrasburgo ya se manifestó más de una vez rechazando la noción de limitaciones implícitas o no escritas a los derechos en general que busca garantizar[382] y su interpretación de la limitación tiene siempre una valoración restrictiva (*narrow*) de las hipótesis presentes en la ley nacional[383], o sea, las encara como un rol exhaustivo, sin apertura para analogías.

El método de la Corte, en general, involucra tres pasos.

Inicialmente hay una verificación si existe un límite previsto en el ordenamiento del país al derecho del individuo. Esta norma, cuyo sentido por el TEDH sigue, en regla, fielmente al de la interpretación del Poder Judicial y de las demás autoridades del país demandado en la Corte[384], no necesita ser obligatoriamente de derecho interno ni

[381] OVEY,Clare y WHITE, Robin. *The European Convention on Human Rights... cit.,* p. 309.
[382] Vide las decisiones en los casos *Golder v. United Kingdom* (1975) y *Hirst v. United Kingdom* (2005).
[383] Como expresado en el caso *Sidiropoulos and others v. Greece* (1998).
[384] Ello no impide, excepcionalmente, que el Tribunal Europeo de Derechos Humanos entienda que la aplicación de la norma fue realizada de forma equivocada por las autoridades internas. Esta situación ocurrió de forma resaltada en el caso *Craxi (n. 2) v. Italy* (ap. 25337/94, juzgamiento el 17 de Julio de

escrita[385]. Pero, independiente del origen, la norma debe ser accesible al individuo como aquella aplicable al caso concreto y ser formulado por medio de un vocabulario que haga posible evaluar sus consecuencias (*foreseeability*). Esto busca impedir que la norma sea redactada de forma tan oscura que admita cualquier nivel de arbitrariedad estatal[386]. Por lo tanto, esta primera etapa en que es otorgada de *conformidad con la ley nacional*, exige de esta *existencia*, evidentemente, pero también cierta c*alidad*.

Ese carácter de *previsibilidad* de las situaciones donde la ley es aplicable en el requisito de c*alidad* alcanza relevancia en diversos de esos casos que tratan de la protección de los datos individuales, en especial en aquellos donde la verificación de las informaciones es realizada por órganos estatales de naturaleza por decir de alguna manera secreta. Por ejemplo, en *Leander* el Tribunal entiende que la combinación de suficiente claridad de los términos con que la "Personnel Control Ordinance" listaba las posibilidades de chequeo del pasado de los empleados contratados con instrucciones administrativas infralegales detalladas a los controladores aleja cualquier posibilidad de despotismo administrativo (ítem 51 de la decisión). Por el contrario, en *Amann*, aunque existiendo en la legislación suiza previsión de la catalogación de informaciones adquiridas con interceptaciones telefónicas, ellas no abordaban con precisión la situación del reclamante, oyendo de forma "fortuita", sin ser investigado o acusado, en una conversación con ex miembro de la embajada soviética en Berna (ítem 61 de esa

---

2003), pues se concluye que el Juicio de Milán que, durante el juzgamiento del ex primer ministro italiano por crimen de corrupción, entendió inaplicable el artículo 268 del Código de Proceso Penal, el cual autoriza la eliminación de las partes de las conversaciones grabadas que no se relacionaban con el objeto de la acusación en momento previo al juzgamiento, no explicó suficientemente porque tampoco utilizó el art. 295, §3 º del mismo Código, que permite que eso sea hecho durante aquel estadio procesal, "si posible".

385 Esas excepciones a la ley escrita del parlamento (ley ordinaria) envuelven el uso de regulaciones profesionales (la del consejo de Veterinarios en el caso *Barthold v. Germany*), de regulación de sector económico emitida por la Comunidad Europea (*´Bosphorus Airways´ v. Ireland*), de tratado internacional bilateral (*Slivenko v. Latvia*) y del derecho consuetudinario de desacato (*common law of contempt)* en el caso *Sunday Times v. United Kingdom*.

386 OVEY,Clare y WHITE, Robin. *The European Convention on Human Rights... cit.*, p. 314.

decisión)[387].

El segundo paso que la Corte realiza es verificar si el objetivo de la limitación del ordenamiento de cada país se legisla según los valores sociales genéricos expresados en la Convención, que en el caso del artículo 8 son la "seguridad nacional", o sea buscando impedir enemigos de invadir el país o derrumbar ilegalmente al gobierno[388]; "seguridad pública", fundamento que raramente es aceptado en la jurisprudencia del TEDH aisladamente y es tratado frecuentemente como sinónimo de mantenimiento del "orden público"[389]; "bienestar económico del país", lo que ya justificó la autorización de ingreso en domicilios por agentes aduaneros[390]; así como permisos de vuelos nocturnos[391]; "prevención de infracciones penales", la cual es, sin duda, la razón de limitación más utilizada y también más aceptada por la Corte, sin que se pierda de vista que el medio debe tener la función de impedir nuevos crímenes y no descubrir los culpables de los ya ocurridos[392]; "protección de la moral o de la salud" y "protección de derechos y de las libertades de terceros". Este penúltimo fundamento en verdad se divide en dos: justifica medidas que preserven el sentido moral social, mismo a costa de

[387] La lógica del Tribunal Europeo de Derechos Humanos para juzgar la *previsibilidad* cuando de medidas de seguridad que exigen al menos una cierta ignorancia del afectado de su realización fue definida de forma precisa en el ítem 67 del juzgamiento de *Malone v. The United Kingdom* (ap. 8691/79, el 2 de agosto de 1984) : "(...) Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident (see the above-mentioned Klass and Others judgment, Series A no. 28, pp. 21 and 23, paras. 42 and 49). Undoubtedly, as the Government rightly suggested, the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence."

[388] En el caso *Klass v. Germany* (1978), por ejemplo, las medidas de vigilancia del gobierno alemán fueron justificadas con miras a impedir espionaje y el terrorismo interno.

[389] OVEY,Clare y WHITE, Robin. *The European Convention on Human Rights... cit.,* p. 319.

[390] *Miaihe v. France* (1993).

[391] *Hatto v. United Kingdom* (2003).

[392] OVEY, Clare y WHITE, Robin. *The European Convention on Human Rights... cit.,* p. 320.

restringir la libertad de expresión como en el caso de obtención de pinturas con imágenes sexualmente explícitas[393], y en segundo lugar preserven la integridad física y mental de grupos de individuos, como admitió el TEDH al admitir la criminalización por parte de la legislación del Reino Unido de actos de naturaleza sadomasoquista[394]. Y el último fundamento legítimo para establecer limitaciones de la "vida privada" es el más amplio de todos, pues permite la ponderación con los demás derechos de los ciudadanos. ,[395].

El último paso que la Corte da es la de verificar si la medida es "necesaria en una sociedad democrática". Como se asentó en *Silver v. United Kingdom* (1983), "necesario" se ubica entre con menos flexibilidad que lo meramente "razonable", pero también con menos severidad que lo "indispensable".

Hay una clara diferencia en relación al "principio de la proporcionalidad" en la forma del derecho alemán, pues el requisito de "necesidad" es prescindible, bastando al legislador nacional que busque un fin legítimo por medio de una medida no excesiva[396], que compatibilice mínimamente intereses sociales e individuales.

De hecho la evaluación se centra en gran medida en el "margen de apreciación" que es dado al país demandado. La llamada "doctrina del margen de apreciación" desarrollada por el TEDH es marcada por una "deferencia judicial" (*judicial deference*) que este tribunal de carácter internacional concede a las autoridades nacionales en el

393 *Muller and others v. Switzerland* (1988).
394 *Laskey, Jaggard and Brown v. United Kingdom* (1997).
395 Comúnmente se dispensa esa formulación más general por el uso de los otros intereses con redacción más específica. De toda manera en el caso *Chappel v. United Kingdom* (1989), justificó las medidas cautelares de búsqueda y aprehensión en protección a derechos de propiedad intelectual.
396 SIEMEN, Birte. *Datenschutz als europäisches Grundrecht... cit.,* p. 154.

ámbito de su margen de discrecionalidad para la *aplicación* de las normas de la convención y por una "flexibilidad normativa" (*normative flexibility*) en su interpretación del significado de cada artículo, que más que comandos unidos, suministran zonas de legalidad que permiten distintas y hasta así legítimas codificación país a país[397]. Su importancia es permitir que el Tribunal considere que hubo derogación de la convención o limitación desproporcionada solamente en casos verdaderamente más graves.

Tal "autocontención judicial" (*judicial self restraint*) se presentó en la jurisprudencia de la Corte inicialmente para permitir la legalidad de determinadas "legislaciones de emergencia", con fundamento en el permiso del artículo 15 de la CEDH, aún sin que el Tribunal analice si el contexto realmente indicaba esta excepcionalidad, pero solamente con la aceptación de la evaluación realizada por el Gobierno del Estado demandado[398].

Pero su expresa y más frecuente utilización involucra la limitación de los derechos de los artículos 8º (privacidad), 10º (libertad de expresión), 9º (libertad religiosa) y 11º (libertad de reunión y asociación), en ese orden. Más recientemente, el concepto de "margen de apreciación" también fue utilizado para confirmar "obligaciones positivas" de los Estados sobre estos derechos, o sea, protección verdadera y para, en estos, analizar distinciones que configuren las discriminaciones vedadas por el artículo 14 de la Convención[399].

---

[397] SHANY Yuval. "Toward a General Margin of Appreciation Doctrine in International Law?." *European Journal of International Law*, 2005, p. 910.

[398] BREMS, Eva. "The Margin of Appreciation Doctrine in the Case-Law of the European Court of Human Rights." *Heidelberg Journal of International Law (HJIL)*, 1996, p. 243.

[399] *Ibid.*, p. 247.

El uso del "margen de apreciación", a lo largo de décadas de jurisprudencia del TEDH, tiende a ser más restricto cuando la situación pueda impedir el libre desarrollo de la existencia e identidad del individuo[400], salvo cuando esto también involucre valores morales aún no consolidados en los países signatarios del acuerdo[401]. Al contrario, la discrecionalidad de los países es por lo general valorada al tratarse de seguridad nacional, protección de menores, planificación urbana y protección del medio ambiente[402].

Se puede decir así que, aunque no haya reglas claras elaboradas por el Tribunal para el uso de esa teoría, que varía según las circunstancias y el escenario de fondo del caso y según los derechos involucrados en el objeto de la demanda, hay un método que valora la confrontación de las diversas legislaciones nacionales[403] y una práctica que limita el espacio de conformación del legislador nacional y exige más justificación según sea más íntima o intensa la invasión de la situación del individuo[404].

En el estudio de los casos que involucran la protección de datos individuales se observa fácilmente esa graduación de control. Por ejemplo, archivo de informaciones cuya obtención tuvo el conocimiento del reclamante, en simples registros específicos de la policía, sin posibilidades directas de cruces y procesamiento con relación a otras fuentes (una intervención leve sobre el derecho individual), realizadas con el objetivo de

---

400 Vide , por ejemplo, la importancia que es dada a la relación médico paciente en *Z. v. Finland*.

401 Sea al mantener el impedimiento de una mujer al embarazar con embriones congelados sin la autorización de su compañero (*Evans v. United Kingdom*), o de transexuales cambiar el sexo en sus registros civiles (*Rees v. United Kingdom*).

402 OVEY,Clare y WHITE, Robin. *The European Convention on Human Rights... cit.*, p. 331.

403 En el ítem 40 del juzgamiento de Rasmussem v. Denmark (ap. 8777/79, el 28 de noviembre de 1984), eso fue afirmado en su entereza: "The scope of the margin of appreciation will vary according to the circumstances, the subject-matter and its background; in this respect, one of the relevant factors may be the existence or non-existence of common ground between the laws of the Contracting States"

404 Como fue hecho, por ejemplo, por el plenario de la Corte en el juzgamiento de *Dudgeon v. The United Kingdom* (ap. 7525/76, el 22 de octubre de 1981).

combatir la criminalidad en la sociedad (un valor estatal relevante), aunque no resulten en procedimientos criminales contra aquel individuo o combatan crímenes especialmente graves, como el terrorismo[405], son juzgadas por el TEDH como válidas[406]

Los registros secretos, como en *Klass* y *Leander*, merecen mayores cuidados. La primera decisión fija la definición de que en estos casos las medidas deben adherirse a lo estrictamente necesario (*strictly necessary*), sin que eso signifique que el Tribunal menoscabe también la mayor sofisticación de las amenazas de criminalidad que los Estados vienen teniendo que enfrentar. La solución encontrada aquí es mantener la discreción del Estado en definir los medios, duración e hipótesis de la vigilancia, siempre que promueva las adecuadas garantías contra abusos que terminen por solapar la democracia bajo el pretexto de defenderla[407].

La importancia de las consecuencias de la acción secreta sobre el desarrollo del individuo es de la misma forma, un factor que influye en la aceptación de medidas secretas tomadas por el país reclamado. Mientras en Klass se refiere a las medidas de descubrimiento del contenido de las comunicaciones del individuo, en *Leander*, el daño que la Corte vio provocado sobre el reclamante fue solamente el de su prohibición de acceso a un cargo público. De esta forma, respetada la existencia de garantías adecuadas contra el abuso en el uso de la posibilidad legal de análisis de las informaciones sobre

[405] En el caso de crímenes más graves, como el terrorismo, el Tribunal indica inclusive que hay un espacio mayor para la acción estatal, como se deduce de estos pasajes de *McVeigh and others v. The United Kingdom* (aps. 8022/77 ; 8025/77 ; 8027/77, Plenario de la Comisión, el 18 de marzo de 1981), en la cual se trata sobre la retención por la Policía de las fotografías e impresiones digitales de sospechosos tras su detención: "The Commission is aware of the critical importance which intelligence material and forensic evidence may have in the detention of those responsible for terrorist offenses (…) taking into account the nature of the records at issue, it must balance what, in its view, is at most a relatively slight interference with the applicants´ right to respect for their private life against the pressing necessity to combat terrorist activity."

[406] Vide, en ese sentido, el ítem 66 del informe de la Comisión, de 19 de mayo de 1994, en *Ludwig Friedl v. Austria*.

[407] Ítems 42 a 50 y 68 de la decisión del Plenario en *Klass* el 6 de septiembre de 1978.

su pasado, se optó por entender que la medida no era desproporcionada a los fines perseguidos[408].

La importancia del caso *Leander* para la jurisprudencia de la protección del TEDH no significa que aún aquí no haya habido también una completa evaluación de los maleficios de la ausencia de cualquier posibilidad de revisión del contenido de sus datos archivados en los archivos electrónicos públicos por parte del individuo puede causar a su vida, lo que fue resaltado en el voto parcialmente disidente de los jueces Pettiti y Russo:

> "Consideration also needs to be given to the dangers of electronic links between the police registers and other States' registers or Interpol's register. The individual must have a right of appeal against an entry resulting from a fundamental mistake, even if the source of the information is kept secret and is known only to the independent authority that has jurisdiction to determine the applicant's appeal.
> A supervisory system such as is provided by the Supreme Administrative Courts (in Belgium, France and Italy) ought to afford an effective remedy, which is lacking at present in our view.
> The State cannot be sole judge in its own cause in this sensitive area of human-rights protection."

Los archivos políticos no tardarían en retornar a la jurisprudencia del TEDH. Con el fin de la Guerra Fría, Europa Occidental tuvo que enfrentar la cuestión de qué hacer con los archivos de las policías secretas de los países del antiguo bloque comunista.

Uno de los primeros casos no involucró víctimas, sino verdugos. En *Knauth v. Germany* (ap. 41111/98, decisión el 22 de noviembre de 2001), la 3ª Sección de la Corte enfrentó el caso de Ursula Knauth, una profesora de guardería infantil en Alemania Oriental que fue agregada al cuerpo funcional del *Land* de Berlín después de la reunificación alemana, y que había sido dimitida al ser descubierto que había mentido al

[408] Ítem 67 del juzgamiento de la Sección de la Corte el 26 de marzo de 1987.

declarar que no había trabajado para la Policía Secreta de la República Democrática Alemana, cuando había, ocasionalmente de forma remunerada, participado de 14 operaciones de espionaje durante la década del 70.

Aunque el TEDH, en este caso, haya garantizado que también hay interferencia en la vida de un servidor público cuando son utilizados datos de su vida anterior contra su voluntad[409], admitió, de forma unánime, ser justificada la pérdida de empleo como una medida "necesaria para la sociedad democrática" del país reclamado, en razón del derecho del Estado a exigir de sus empleados un historial de defensa de la Constitución y de la democracia, de la ruptura de la relación de confianza patrón-empleado por la mentira en cuanto a las acciones en el pasado y para la prevención de desórdenes que podrían ocurrir en el mantenimiento en sus cuadros de empleados de las fuerzas de represión de la antigua Alemania comunista. Todos estos factores, involucrados en esa peculiar situación, para el TEDH justificaban la despedida de la reclamante, medida cancelada por las Cortes alemanas.

La deficiencia de especial consideración sobre el significado para el ser humano de los datos sobre actividades profesionales y sindicales y preferencias políticas en el caso *Leander y*, principalmente, *Knauth* es absolutamente diversa a la importancia intrínseca que garanticen la protección de los registros médicos en *Z. v. Finland* y *M.S. v. Sweden*[410]. En estos se establece como presupuesto que la posibilidad que el

[409] Expresamente se afirmó: "The Court reiterates that as a general rule the guarantees in the Convention extend to civil servants (see, in particular, *mutatis mutandis*, *Vogt v. Germany*, judgment of 26 September 1995, Series A no. 323, pp. 22-23, § 43). It follows that the applicant's status as a civil servant did not deprive her of the protection of Article 8.(...) The use of information about the political and/or private past of an individual may be regarded as an interference with private life (see, *mutatis mutandis*, *Leander v. Sweden*, judgment of 26 March 1987, Series A no. 116, p. 22, § 48; *Amann v. Switzerland* [GC], no. 27798/95, § 65, ECHR 2000-II; and *Rotaru v. Romania* [GC], no. 28341/95, § 46, ECHR 2000-V)."

[410] Vide expresamente los ítems 96 de la decisión en *Z* y 41 de la decisión de *M.S.*

contenido de una historia clínica sea revelada puede perjudicar el desarrollo de una vida. Son dados como una protección diferenciada, considerados más "sensibles" en la jurisprudencia del Tribunal.

Aún así no hay ni siquiera limitaciones al derecho a la protección de datos automáticamente vedadas en esos casos. El Estado finlandés es condenado *Z.* no por la revelación del historial de los médicos para la investigación de su marido (con apoyo en ese punto expresamente en el artículo 9 de la Convención Europea de Protección de Datos de 1981), pero sí porque la identidad de la reclamante y su enfermedad se hicieron públicas por el Tribunal[411]. Exactamente no hay condena de Suecia en violación de la vida privada en *M.S.* porque no se quiebra la confidencialidad, siendo el registro utilizado solamente para la verificación del merecimiento de una indemnización por incapacidad física.

Desde el punto de vista de las intervenciones estatales, por la lectura de los antiguos archivos de las policías secretas, pero bajo el prisma de la temporalidad de la existencia del archivo, se destaca también el caso *Rotaru*[412]. Aquí, el reclamante Aurel Rotaru tuvo que enfrentar la revelación de archivos de más de cinco décadas de la policía secreta rumana que expuso varios datos sobre su pasado, en su mayoría equivocados, en cuanto a su afiliación a asociaciones, declaraciones por medio de panfletos políticos y formación universitaria. Desde el punto de vista del derecho a la protección de datos, hay dos cuestiones principales que se trabajan en este juicio. Desde el punto de vista procedimental se afirma que no se colocan, tal como en el caso *Leander*, medios a la disposición del interesado para el análisis e impugnación del

[411] Vide ítems 97, 113 y 114.
[412] *Rotaru v. Romania* (ap. 28341/95, 4 de mayo de 2000).

origen y de la veracidad de los registros, tampoco hay forma de supervisión, especialmente judicial, de la actuación de órganos que obtienen la información[413]. Pero también está la cuestión del tiempo aceptable en las actividades que, en este caso realizadas en el espacio público, de naturaleza empresarial o profesional, , pueden continuar en poder del Estado. En el caso del pasado político público del demandante no poseía más relevancia social, debiendo retornar al espacio estrictamente privado de su vida[414]. Por lo tanto la intervención estatal en la protección de datos añade a los "tres pasos" del análisis de las limitaciones legales la exigencia de que su *duración* sea también analizada. La cuestión fue preocupadamente resaltada en el voto por separado del Presidente de la Corte de entonces, juez Wildhaber, que fue acompañado por otros 6 (Makarczyk, Türmen, Costa, Tulkens, Casadevall y Weber) de los 18 jueces que participaron del juicio:

> "In the Rotaru case, data collected under a previous regime in an unlawful and arbitrary way, concerning the activities of a boy and a student, going back more than fifty years and in one case sixty-three years, some of the information being demonstrably false, continued to be kept on file without adequate and effective safeguards against abuse. It is not for this Court to say whether this information should be destroyed or whether comprehensive rights of access and rectification should be guaranteed, or whether any other system would be in conformity with the Convention. But it is hard to see what legitimate concern of national security could justify the continued storing of such information in these circumstances. I therefore consider that the Court would have been entitled to find that the impugned measure in the present case did not pursue a legitimate aim within the meaning of Article 8 § 2.
> This finding would have rendered it unnecessary to determine whether the measure in question was necessary in a democratic society, because that test depends on the existence of a legitimate aim. If, however, the Court had preferred to accept the existence of a legitimate national security aim, it would have recalled that States do not enjoy unlimited discretion to subject individuals to secret surveillance or a system of secret files. The interest of a State in protecting its national security must be balanced against the seriousness of the interference with an applicant's right to respect for his or her private life. Our Court has repeatedly stressed "the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it" (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 25, § 60; see also the Klass and Others v. Germany judgment of 6 September 1978, Series A no. 28, pp. 21 and 23, §§ 42 and 49, and, mutatis mutandis, the Chahal v. the United Kingdom judgment of 15 November 1996, Reports 1996-V, pp. 1866-67, § 131, and the Tinnelly & Sons Ltd and Others and McElduff and Others v. the United Kingdom judgment of 10 July 1998, Reports 1998-IV, pp. 1662-63, § 77). This is why the Court must be satisfied that the secret surveillance of citizens is strictly necessary for safeguarding democratic

[413] Ítems 59, 71 y 72 de la decisión.
[414] MARTÍNEZ MARTÍNEZ, Ricard. *Una aproximación crítica a la autodeterminación informativa*. Madrid: Civitas, 2004, p. 204.

institutions and that there exist adequate and effective safeguards against its abuse."

Este tema del plazo de mantenimiento de registros de otros por las fuerzas de seguridad de un país es también el elemento central de *S. and Marper v. United Kingdom*[415]. Los reclamantes S., un menor, y Marper, obtuvieron muestras de sus ADN e impresiones digitales en un caso que no resultó en condena criminal, en cuanto al primero en razón de absolución y del último sin ser juzgado el mérito. Pero, sin abalarse por sus diversos pedidos, la policía inglesa, apoyada en la legislación nacional, se negó a destruir las pruebas obtenidas. La decisión fue en el sentido de que la ausencia de límite de tiempo tanto en Inglaterra, como Irlanda del Norte y País de Gales, situación única entre los signatarios del Tratado, sobrepasa lo razonable, promoviendo una posible *estigmatización* social de algunos en razón de errores en la juventud. En *Williams v. The United Kingdom* (ap. 19404/1992, decisión del 1º de julio de 1992), la Comisión comprenderá que el mantenimiento de muestras de ADN durante 11 meses para una investigación de un determinado crimen de homicidio, sin ningún otro uso, no se muestra irrazonable y por tanto, no viola los derechos presentes en la Convención.

Con excepción de la temporalidad de las limitaciones a las facultades de acceso del individuo a sus datos por un individuo en dos casos, en que se asume el carácter definitivo. Primero, como ya visto en *Odièvre* y *Gaskin*, en caso de que afecten los derechos de terceros y no haya consentimiento para la revelación. Y también, excepcionalmente, por el interés público cuando, si la información perjudica el referido, deberá ser compensado el secreto con medidas favorables a su persona durante el procedimiento que le afecta[416].

---

[415] Aps. 30562/04 y 30566/04, juzgada por la Gran Cámara el 4 de diciembre de 2008.

[416] Como expresamente admitido en el § 68 de la decisión del 25 de septiembre de 2001 en *P.G. and J.H. v. the United Kingdom.*

3.1.2.4. Conclusión sobre la jurisprudencia de protección de datos TEDH

La sistematización de los fallos del TEDH sobre protección de datos no busca negar las dificultades del Tribunal en tratar el tema. Esas barreras son fruto de la ausencia de una clara base normativa y de una autocontención en tomar para sí la defensa de un tema aún no solidificado y que, mal evaluado, podría provocar fuerte restricciones en su campo de acción, principalmente para garantizar la seguridad de la sociedad.

Por otro lado, en los últimos años se nota un aumento de frecuencia de las decisiones que abordan la protección de los datos de los individuos, como también una mayor intensidad de decisiones de mérito favorables a los reclamantes. Esto es provocado por la madurez, en las sociedades europeas, de la noción que esa es otra faceta individual que merece protección, pero también, por la densificación del cuerpo de jurisprudencia de la Corte, que hace más cómodo a los jueces decidir sobre un entendimiento ya adoptado anteriormente.

La enunciación del derecho y de sus facultades aún no se ha dado explícitamente en su totalidad, pero hay una clara influencia de las demás normas internacionales que han surgido en las últimas décadas y una preocupación por compensar con la exigencia de recursos procesales internos las dificultades de las jurisprudencias caso a caso y en la superación del concepto de “margen de apreciación” de cada país integrante de la CEDH.

De cualquier forma, exactamente por ese cuidado en observar diferentes puntos

de vista y avanzar cautelosamente en la protección de datos personales, la jurisprudencia del TEDH aparece como un importante modelo externo para subsidiar el análisis crítico de la "protección adecuada" de la conformidad con la Directiva 95/46/CE.

3.2. Las legislaciones internacionales de protección de datos

3.2.1 Características históricas de las leyes de protecciones de datos: Las tres generaciones de la legislación de protección de datos

La definición de los delineamientos del derecho individual a la protección de datos personales fue una conquista, fruto de un proceso histórico de poco más de 40 años de producción legislativa, con distintos grados vinculantes, tanto de origen estatal, como, y sobre todo, internacional[417].

Uno de los estudios precursores en la defensa y conceptualización de una "intimidad informática" fue, en Gran Bretaña, el *Informe Younger*, de 1972, en que la idea de un derecho de control sobre el flujo de la información personal, fue concebida como una etapa del derecho más amplia que el derecho a la intimidad[418].

El avance en el terreno del derecho positivo puede ser clasificado en tres etapas, según las características más patentes en las legislaciones más relevantes.

[417] PUENTE ESCOBAR, Agustín. "Breve descripción de la evolución histórica... *cit.*, p. 38.
[418] MURILLO DE LA CUEVA, Pablo Lucas. *El derecho a la autodeterminación informativa... cit.*, p. 121.

La denominada primera generación de leyes, por ejemplo, surge en un momento en que el incipiente desarrollo de la informática permitía la búsqueda de medidas de rigor en la utilización de la misma, destacándose la idea de autorización previa de las bases de datos y el establecimiento de órganos de vigilancia.

En Alemania, esta primera fase legislativa es claramente marcada por tres leyes. La pionera, es la ley del *Land* de Hesse que surge el 30 de septiembre de 1970. Cuatro años después, Rheinland-Pflaz edita su propia norma. Finalmente, el 1º de febrero de 1977 aparece la primera Ley Federal, cuyo disputado proceso legislativo comenzaría poco antes, el 12 de noviembre de 1976. Igualmente en la década del '70 son editadas las siguientes normas nacionales: el *Privacy Act* norteamericano de 1974, el *Privacy Comitee Act* de la provincia australiana de New South Wales, en 1975, el *Human Rights Act* canadiense, una serie de legislaciones nacionales europeas que son editadas en 1978 (Francia, Dinamarca, Noruega y Austria) y, finalmente, la legislación de Luxemburgo destaca por ser la última de este período, en 1979, antes de la Convención Europea de 1981[419].

Hay algunas características básicas de ese primer momento. Inicialmente, existe una fijación sobre el tratamiento automatizado de datos: las iniciales leyes de protección de datos son una respuesta frontal al uso de ordenadores para manipular las informaciones de los ciudadanos.

La legislación de la primera generación mantiene el esquema civilista clásico de defensa de la privacidad, el permiso para la utilización y el no acceso posterior al modo

[419] Ello no significa, sin embargo, que legislaciones de la década del 80 todavía no fuesen influenciadas por ese primer grupo de normalizaciones, como demuestra la lectura de la ley israelí de 1981 o británica de 1984 (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 56).

de uso del destinatario. Si la suposición que llevó al legislador a modificar estas normas es la misma, la necesidad de dar una respuesta a sus electores de los numerosos casos de uso indebido de los datos personales que venían ocurriendo desde finales de la década anterior, la respuesta también puede ser considerada un todo común[420].El Legislativo se enfrentaba a una cuestión sin precedentes, y, comprensiblemente, por la ausencia de modelos previos a seguir, la reguló con gran inseguridad. En ese primer momento, ese modelo funcionó porque garantizó la satisfacción tanto a los Poderes administrativos y económicos como a la población. Esta se sentía segura nuevamente por la respuesta legislativa y aquellos no tuvieron que crear casi ningún aparato adicional a las máquinas que archivarían las informaciones[421].

Las soluciones para ese *déficit* de conocimiento, sin embargo, son diversas. La legislación federal alemana y la norma austríaca, por ejemplo, al ser ambiciosas en la búsqueda de una total regulación de la materia, utilizaron la técnica de repetición de "cláusulas generales", poco concretas, pero muy flexibles, una forma de no dejar la cuestión abierta, así como no debilitar la acción ejecutiva. La opción sueca, al contrario, fue absolutamente a la inversa: en vez de prever un medio de regular algo que no conocía, sometió todos los tratamientos de datos a una instancia previa de control, cuyo proceso de permiso permitiría aumentar la experiencia para normalizar la materia[422].

El peligro directo que entonces se combatía no era sólo teórico en cuanto a la violación del "hombre de vidrio", sino, motivado por las situaciones reales de la divulgación amplia de informaciones equivocadas sobre los individuos que

[420] SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 53.
[421] RODOTÀ, Stefano. *A Vida na Sociedade da Vigilância... cit.*, p. 50.
[422] SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 54.

proporcionaba una tecnología en sus primeras prácticas y sin ningún control. No obstante, innegablemente el escenario de una burocracia indomada, utilizando la técnica, en teoría para hacer más eficiente al Estado, como medio de dominación de la población también estaba en la mente de los legisladores. La "protección de datos", inicialmente, es una respuesta legislativa a la cuestión político - constitucional de las posibilidades que la Administración adquiría con las nuevas tecnologías más que una respuesta a estas como un problema en sí mismas[423]. Añadir al destino del sector público una regulación que basaba el combate a la amenaza del control sobre la información en medidas preventivas, que bloqueen el tratamiento nocivo antes de su realización[424].

La ley del estado alemán de Hesse, el primer texto con fuerza de ley sobre protección de datos informatizados, por ejemplo, disciplinó el uso de los archivos automatizados de su Administración Pública (art. 1), siendo una norma típica de la primera etapa; contenía límites estrictos para la creación de base de datos, para la obtención y procesamiento de los mismos y la de instituir un Comisario Parlamentario (art. 7 y ssgs.) como una especie de *Ombudsman* con la función de vigilar el manejo de informaciones en las bases de datos[425].

En el artículo 6, la ley presenta una solución que pareció lógica en aquella época: en cuanto a los datos almacenados en la Administración que se garantizaba la libertad de información del Parlamento, mayoría y minoría. La razón era impedir que la oposición fuese coaccionada en sus acciones por los datos guardados por la

[423] En ese aspecto la BDSG de 1977 rompe ese estándar eminentemente publicista, pues permite la interpretación de que su aplicación también abarcaba a los entes privados.
[424] SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 9.
[425] ORTI VALLEJO, Antonio. *Derecho a la intimidad e informática... cit.*, p. 14.

Administración, o que quede eliminada de la verificación de lo que estaba siendo realizado. Pero ese concepto que iguala libertad de información y protección de datos, comienza a ser revisado a partir del fin de la década del 70, debido a que menosprecia el carácter del derecho individual a la "autodeterminación informativa", o sea, el derecho del individuo de buscar que nadie sepa de sí, salvo con su permiso o si fuera absolutamente necesario, su elemento de la personalidad que fue tan explorado por el Tribunal Constitucional Alemán en su decisión de 1983.

A continuación se edita la ley de protección de datos (*Datalag)* sueca, del 11 de mayo de 1973, similar, también con normas relativas a las limitaciones para el surgimiento de bases de datos sobre ciertos temas y una autoridad de control sobre el cumplimiento de la ley, la "Comisión de Inspección de Datos", vinculada al Ministerio de Justicia, pero con composición plural (un magistrado, cuatro parlamentarios, tres sindicalistas, un empleado, un médico y un técnico en informática).

Una segunda fase de la legislación involucra el reconocimiento de la categoría de datos con especial protección, más adelante llamados sensibles, en una tutela aún estática basada en la "calidad de la información" a ser almacenada, con un inicio tímido de mayor liberalización para las bases de datos combinadas con algunos derechos, como los de acceso y rectificación, para los afectados[426]. Esos parámetros de las leyes de segunda generación fueron sugeridos legislativamente por la Convención Europea de 1981 y por la normativa de la OCDE. Sin embargo, su influencia comenzó a volverse más significativa en la legislación interna de los países hacia fines de la década del '80, cuando entra en vigor la ley nacional irlandesa (*Data Protection Act*, 1988), definiendo

[426] ORTI VALLEJO, Antonio. *Derecho a la intimidad e informática... cit.*, p. 14 e 15.

una protección especial en la categoría de datos especiales (§ 2, (6)) y una relación de derechos con los individuos (§ 6). La legislación suiza de 1992 *(Bundesgesetz über den Datenschutz – DSG)* también nace con la manifiesta intención que el país, que no forma parte de la Unión Europea, adaptase tanto su sector público como privado para la normativa del Consejo de Europa.

Por fin, en la tercera fase se da la aceptación de que solamente la consagración del control dinámico de medios procesales y administrativos de protección sería capaz de responder a los desafíos de la esfera personal[427], en razón de la multiplicación de medios y fuentes de obtención y almacenamiento de datos, desplazándose el enfoque de un control preventivo hacia un múltiple control represivo. Con este paso concluye, por el momento, el proceso evolutivo de las llamadas tres generaciones o etapas de las leyes de protección de datos[428].

3.2.2 Normas internacionales no vinculantes

En 1967, la Asamblea Parlamentaria del Consejo de Europa dictó la *Recomendación* 509, para el Comité de Ministros que destacaba, la insuficiente protección que las diferentes legislaciones nacionales concedían a la privacidad individual en lo que respecta a la manipulación de sus datos personales.

Cinco años después se decide por la emisión de recomendaciones en el seno del Consejo de Europa. Con la Recomendación 22 de 1973 y 29 de 1974 respectivamente el Comité de Ministros aconsejó a los gobiernos de sus Estados-Miembros que, las bases

[427] REBOLLO DELGADO, Lucrecio. *Derechos fundamentales y protección de datos*. Madrid: Dykinson, D.L., 2004, p. 61.
[428] ORTI VALLEJO, Antonio.*Derecho a la intimidad e informática... cit.*, p. 12.

de datos privados y públicos observasen, al menos, los siguientes puntos: que la información almacenada fuese exacta y obtenida por medios legales; que el ciudadano tuviese el derecho de conocer la información almacenada sobre el mismo; que la seguridad en el archivo fuese capaz de mantener el secreto y evitar el desvío de las informaciones: y que los datos con fines estadísticos fuesen desvinculados de las personas que los suministraban[429].

El consejo, también reconoció, rápidamente, que medidas no vinculantes no serían suficientes, que la estandarización debería ser forzosamente común en el espacio europeo para el establecimiento de verdaderos límites en el uso de datos personales. Así, instituyen una comisión de estudios en 1976, la cual presenta un proyecto de convención en 1979[430].

También en 1974 se mostró a favor de una regulación del flujo de informaciones la OCDE (Organización para el Desarrollo y Cooperación Económica)[431], órgano creado en 1960 (y que involucra hoy a 31 países, que representan más del 80% del PBI mundial, sin contar los 11 países, que participan solamente en el comité de inversiones, como Brasil, Argentina y Egipto), para armonizar las políticas económicas y ayudar al crecimiento económico de sus integrantes.

El 23 de septiembre de 1980, después de tres años de trabajos de una comisión de *experts* creada para este fin, la OCDE edita una *recomendación*, que reconoce, desde

[429] TÉLLEZ AGUILERA, Abel. *Nuevas tecnologías... cit.*, p. 93.
[430] SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 64.
[431] La OCDE, a su vez, es el órgano de la OECE (Organización Europea para Cooperación Económica), la cual fue creada en 1948 como medio de auxiliar en la administración de los recursos resultantes del Plan Marshall a Portugal, Reino Unido, Francia, Alemania, Italia, Países Bajos, Bélgica, Luxemburgo, Austria, Dinamarca, Noruega, Grecia, Suecia, Suiza, Turquía, Irlanda e Islandia. España entra en 1958 y la transmutación en OCDE representa la ambición de tener un carácter además del continente europeo, con la entrada, inicialmente, de Canadá y Estados Unidos.

su *prefacio*, los esfuerzos internos de casi la mitad de sus miembros de haber emitido, o estar por crear, "leyes de protecciones de datos", pero asume que esos esfuerzos en la protección de derechos fundamentales son inútiles sin la armonización del *flujo internacional de datos*.

La recomendación es bastante avanzada en su redacción, adoptando la necesidad de consentimiento para la obtención de los datos (ítem 7); la finalidad precisa para el uso del dato (ítem 9) y de la precisión y actualidad (c*alidad* – ítem 8), así como el delineamiento de los derechos para el afectado y para un órgano de control que permitan que la verificación adecuada de las prácticas de los dueños, privados y públicos, de bases de datos (ítems 13 y 14). Además, no establecía restricciones para ser usada en sectores públicos o privados (art. 2) y no prohibía su aplicación a, inclusive, tratamientos no automatizados (art. 3, letra c).

Pero posee una debilidad que impidió la propagación directa de sus efectos: no tiene carácter vinculante para el Derecho Internacional[432]. Existe un intento de superar esta deficiencia al no ser dirigida solamente a los cuerpos legislativos, también estimulando la observación de sus principios por medio de "códigos de conducta" que constituyesen autorregulación de determinados sectores (art. 19 letra b).

Esta misma dificultad de obligar a los países a seguir sus normas encuentran los "Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales" que la Asamblea General de las Naciones Unidas decide el 14 de diciembre

[432] TINNEFELD, Marie-Therese, EHMANN, Eugen, , y GERLING, Rainer W.. *Einführung in das Datenschutzrecht... cit.*, p. 98.

de 1990, que solo sirve como *consejo* para los países miembros[433].

De todos modos, la iniciativa de la OCDE brindó al menos un importante apoyo y contribución en pro de los esfuerzos del Consejo de Europa[434]para su regulación, que finalmente daría lugar al Convenio n. 108, debiendo ser encarada la similitud intrínseca de estas iniciativas como esfuerzos *cooperativos*[435] en pro del marco internacional.

3.2.3 Normas internacionales Vinculantes

3.2.3.1 El Convenio Nº 108 del Consejo de Europa

Este fue el primer intento de regular internacionalmente el flujo de datos, estableciendo un elenco uniforme de derechos a los individuos y de medidas de seguridad, reconociendo que las regulaciones nacionales eran insuficientes para una protección adecuada.

La ambición del consejo de Europa de ir más allá de las fronteras del continente se mide a partir de la elección de este tipo de instrumento en detrimento de la realización de un Protocolo del Convenio Europeo de Derechos Humanos (CEDH) para ampliar la protección a la vida privada otorgada en su artículo 8º. Esto queda explícito en el artículo 23 del convenio 108 que fue elaborado, que abre su adhesión a países no

[433] *Ibid.*, p. 99.
[434] Es de notar que la OCDE nunca dejó de estimular la contínua actualización de la protección de datos, como se ve por ella su Recomendación a los países miembros sobre la política de criptografía, del 27 de marzo de 1997 y su Guía de orientación para la política de privacidad en datos personales, de 2000.
[435] GARCÍA-BERRIO HERNÁNDEZ, Teresa. *Informática y libertades ... cit.*, p. 51.

europeos[436]. De la misma forma, premeditadamente, se excluye del título del Convenio el adjetivo "europeo"[437].

El 1º de octubre de 1985, cuando finalmente había 5 países que ratifican el convenio (Francia, Noruega, Suecia, España y Alemania), según el apartado 2 de su artículo 22, entró en vigor.

Así el Convenio Nº 108 del Consejo de Europa, *para la protección de las personas con respecto al tratamiento automatizado*[438] *de datos de carácter personal*, del 28 de enero de 1981[439]constituye un gran marco legislativo, pues los Estados que lo ratificaban se comprometían a crear normas en su derecho interno para hacer valer los principios de protección de datos (art. 4)[440]. Las mismas deberían tener eficacia interna y externa, al impedir la transferencia de datos de estos a otros países sin protección semejante (art. 12.3) y concentró en un documento, dirigido tanto al sector público como al sector privado (art. 3.1), las principales características de las experiencias previas, unificando los valores involucrados en términos actuales hasta el día de hoy.

El art. 1 torna al Convenio aplicable solo a tratamientos automatizados. El Convenio también aclara que la protección alcanza solamente a personas físicas ("individuos", según el art. 2.a), no así a las personas jurídicas. En ambos casos apostó

[436] SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 64.

[437] ARENAS RAMIRO, Mónica . *El derecho fundamental a la protección de datos personales...cit.*, p. 154.

[438] El énfasis en el tratamiento automatizado de datos, clarificado en el art.1 del Convenio, no debe ser visto como un menosprecio del potencial nocivo del tratamiento manual, sino como una priorización del combate al mal que veían como más urgente. Por ello, a los países que se adhirieran al Convenio quedaba abierta la posibilidad de extenderlo también a las utilizaciones de datos no automáticas (art. 3.2.c). Vide, en ese sentido, SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 65.

[439] Firmado por España el 28 de enero de 1982, ratificado por instrumento de 27 de enro de 1984 y que fue publicado en el *Boletín Oficial del Estado* de 15 de noviembre de 1985.

[440] Aunque fuera un *non-self-executing treaty*, o sea, el particular no podría invocar sus normas directamente en tribunales nacionales (ítem 38 del "Informe Justificativo" del convenio).

el convenio a estándares mínimos. Las legislaciones nacionales de protección de datos de Austria (§ 3 n. 2) y de Noruega (§ 1 párrafo 2) admitían la protección para cualquier ente personalizado y por eso se incluye también en el Convenio la cláusula de cumplimiento prudencial por cada país que se adhiriera[441], así como su aplicación también a tratamientos no automatizados (art. 3.2.c).

Sus rasgos principales involucran en primer lugar el reconocimiento de la importancia de la ca*lidad* de los datos (art. 5) sometidos al tratamiento automatizado, lo que significa que haya *lealtad* en la obtención de las informaciones; establecimiento de una clara *finalidad* en la creación de la base de datos, que haga posible evaluar la *pertinencia*, la *utilización no abusiva* y la *temporalidad* del mantenimiento de los datos solo durante el plazo estrictamente necesario (el llamado "*derecho al olvido*") y *exactitud* en su inscripción y en su almacenamiento a lo largo del tiempo. También el Convenio, en su artículo 6, resaltó la protección reforzada de los datos referentes al origen racial, opiniones políticas, convicciones religiosas o de otro tipo, vida sexual o salud y eventuales condenas penales, surgiendo esa categoría de informaciones "sensibles"[442].

Además se reconoce la importancia de la *publicidad* del registro de los archivos, y define los derechos del afectado: *acceso* (así como la identidad y dirección del responsable) *y*, eventual, *rectificación y cancelación* de sus datos individuales, con obligatoriedad de que exista recurso procesal a la posible denegación de la petición en cuanto a estos (art. 8) y de la necesidad de medidas de *seguridad* física y lógica en la

[441] SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz...*cit.*, p. 66.

[442] Teniendo en vista la gran disparidad de categorías objeto de protección reforzada en las legislaciones nacionales europeas, el Consejo de Europa, en la consideración Nº. 48 que precede el convenio, admitió que esta lista fuera complementada por cada país (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 68).

conservación de las informaciones (art. 7).

Existe en esas listas una interesante demostración de la utilización de principios con objetivos diversos, listados tales como una lista de *mandamientos* sobre la materia. Así encontramos órdenes que se dirigen a quien manipula los datos (por ejemplo *finalidad* de la creación del archivo y *utilización no abusiva*,), algunas que obligatoriamente exigen la fiscalización directa estatal (*seguridad*, *pertinencia*, etc.) combinadas con derechos individuales de naturaleza *material* (*calidad* de los datos guardados y *temporalidad*, que, como ya fue dicho, concede un derecho al *olvido* de ellos) y otros de carácter instrumental (*acceso*, *rectificación* y *cancelación*). De toda forma este conjunto, que aún hoy es la base de la protección de datos en la Unión Europea, representa una clara combinación de elementos *estáticos* de protección, que involucra intentos de limitación de la invasión en la esfera individual, con factores *dinámicos*, relacionados a la posibilidad de intervenir en la utilización donde quiera que el dato se encuentre.

El artículo 10 es el origen de la creación de potestades sancionadoras como forma de dar lugar a la efectiva aplicación de la ley de protección de datos. La intención aquí se vuelve evidente en el art. 1 del Protocolo adicional al Convenio donde se habla de la creación de instancias de control completamente independientes. Este es el origen de la creación de las agencias nacionales de protección de datos europeas.

Por otro lado, el art. 9.2 permite que se restrinja la aplicación de los artículos 5, 6 y 8 en caso de "necesidad para una sociedad democrática", sea en pro de la seguridad del Estado, de la seguridad pública, de intereses monetarios, para la represión de

infracciones penales o para la protección del afectado o de los derechos y libertades de otros- El ejercicio de los derechos individuales relativos a los datos personales pueden también ser limitados cuando las investigaciones estadísticas o científicas no poseen el potencial de afectar la vida privada del ciudadano (art. 9.3).

Sin embargo, se nota en el Convenio una fuerte vinculación al principio de la "libertad de información" y un cierto sentido de inevitabilidad de que las personas puedan huir del manejo por parte de la informática de sus datos, puesto que en ningún momento se exige el consentimiento del afectado en la obtención de los datos.

No obstante sea una norma vinculante, en cuanto a la estandarización de las normas internacionales sobre protección de datos su objetivo no es alcanzado, ya que el excesivo apoyo en principios y no en reglas y la amplitud con que otorga excepciones permitieron regímenes absolutamente distintos en los países que suscribieron la Convención[443].

3.2.3.2 El tratamiento comunitario de la protección de datos

La regulación del uso de los datos personales en el escenario del desarrollo de tecnologías de almacenamiento (información) y comunicación, en el ámbito de la Unión Europea, surge bajo la justificativa de regulación de sus aspectos económicos, por pertenecer esta al campo de competencias de los órganos comunitarios[444], lo que no impidió que las directivas europeas provocasen los efectos más amplios sobre los derechos de los individuos en esa área.

[443] ARENAS RAMIRO, Mónica. *El derecho fundamental a la protección de datos personales...cit.*, p. 156.
[444] SIEMEN, Birte. *Datenschutz als europäisches Grundrecht... cit.*, p. 212.

La primera y principal norma comunitaria dirigida a los Estados miembros[445] en dicho campo es la Directiva 95/46/CE, cuyo tema es la "protección de las personas singulares en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos". Junto a estas fueron enseguida creadas otras para regular campos específicos. Son en ese sentido la Directiva 97/66/CE, que hablaba solamente del tratamiento de datos y protección de la privacidad en el campo de las telecomunicaciones y que fue revocada por la Directiva 2002/58/CE, que abarca la misma materia bajo el enfoque más actual y amplio de la *comunicación electrónica pública*[446] y la Directiva 1999/93/CE, que crea el marco legal comunitario para firmas electrónicas y trata sobre la protección de datos de los servicios de certificación en el artículo 8º. En todos los casos no se niega la aplicación de la Directiva 95/46/CE. Al contrario, expresamente se manifiesta su adecuación integral también a esos casos.

En ese sentido, la Directiva 2000/31/CE, que regula los "servicios de la Sociedad de Información"[447], en especial sobre el *comercio electrónico*, es ilustrativa en su *Considerando 14*, donde está escrito que:

> "La protección de los individuos en lo que se refiere al tratamiento de los datos personales es regida exclusivamente por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995, relativa a la protección de las personas singulares en lo que respeta al tratamiento de datos personales y a la libre circulación de esos datos y por la Directiva 97/66/CE

[445] Pues hay también actos normativos que regulan la protección de datos dentro de la plataforma institucional de la propia UE, como el Reglamento (CE) nº 45/2001, de carácter general a las instituciones y órganos comunitarios, y la Convención de Europa, que entró en vigencia el 1º de enero de 2010 y fue establecida por la decisión del Consejo del 6 de abril de 2009.

[446] Conforme art. 3.1 de esta directiva. Así, por tanto, regulan básicamente la comunicación por Internet, excluidas las intranets, que continúan bajo regulación de la Directiva 95/46 (TINNEFELD, Marie-Therese, EHMANN, Eugen, , y GERLING, Rainer W.. *Einführung in das Datenschutzrecht... cit.*, p. 127).

[447] Concepto cuya definición se encuentra en otra norma europea, en el artículo 2 de la consolidación de las directivas 98/34/CE y 98/48/CE, como "cualquier servicio prestado normalmente mediante remuneración, a la distancia, por vía electrónica y mediante pedido individual de un destinatario de servicios.".

del Parlamento Europeo y del Consejo, del 15 de Diciembre de 1997, relativa al tratamiento de datos personales y a la protección de la privacidad en el sector de las telecomunicaciones, que se aplican plenamente a los servicios de la sociedad de la información. Estas directivas crean un marco legal comunitario en el dominio de los datos personales, por lo que no es necesario tratar esa cuestión en la presente directiva para garantizar el buen funcionamiento del mercado interno, en especial la libre circulación de los datos personales entre Estados-Miembros. La ejecución y aplicación de la presente directiva deberán efectuarse en absoluta conformidad con los principios respectivos a la protección de los datos personales, especialmente en lo que se refiere a las comunicaciones comerciales no solicitadas y a la responsabilidad de los intermediarios. La presente directiva no puede impedir la utilización anónima de redes abiertas, como, por ejemplo, internet."

En general, no obstante la Directiva 2002/58 tenga algunas pocas especificidades[448], en general su régimen está en absoluta conformidad según las reglas existentes en la directiva de protección de datos de 1995, como deja patente su considerando Nº 10.

Por lo tanto, es prioritario observar cómo se da la configuración de la protección de datos en los términos de la Directiva 95/46/CE, aprobada el 24 de octubre de 1995, norma marco[449] de la Unión Europea que sirve de inspiración e impulso unificador para las legislaciones internas ya que determina en su artículo 32 la obligatoriedad de que las normas nacionales se adapten en 3 años a su contenido.Además, el Tribunal de Justicia de la Unión Europea admitió, en la Sentencia del 20 de mayo de 2003, *Rundfunk y otros*, Asuntos C-465/00, C-138/01 y C-139/01, que la Directiva, respecto a sus normas suficientemente precisas e incondicionadas, como, por ejemplo, el apartado 1º de su

[448] De las cuales los grandes destaques son su aplicación también a las personas jurídicas (2ª parte del apartado 2 del artículo 1º de la Directiva 2002/58), y no solamente a las físicas, como consta en el apartado 1 del artículo 1 de la Directiva 95. Sin embargo, mismo aquí, la distancia es menor de lo que parece, ya que legislaciones nacionales (como hizo Austria) no están prohibidas de expandir la protección también a las personas no naturales (TINNEFELD, Marie-Therese, EHMANN, Eugen, , y GERLING, Rainer W.. *Einführung in das Datenschutzrecht... cit.*, p. 128) y una obligación extendida en el tiempo (seis meses a dos años) de conservación de una serie de informaciones de los usuarios de Internet, como forma de combatir la *cybercriminalidade* (considerando 7 y artículos 5º y 6º de la directiva 2006/24, que la deroga parcialmente).

[449] Agréguese la existencia en el ámbito comunitario de dos Directivas más que regulan el tratamiento de datos personales en campos específicos, la Directiva 97/66/CE, sobre el sector de las telecomunicaciones, y la Directiva 2002/58/CE, sobre comunicaciones electrónicas. La aplicación de esta, a su vez, es complementada por otras dos no directamente relativas al tema de nuestro estudio, a saber, la Directiva 2000/31/CE, sobre comercio electrónico, y la 1999/93/CE, sobre firma electrónica.

artículo 6 y artículo 7, posee efecto directo, en detrimento de normas nacionales contrarias a sus disposiciones[450].

Hay una cuestión competencial que atraviesa el análisis de ese derecho comunitario *derivado*. Al final de cuentas las directivas tienen como destinatarios los Estados miembros y demandan ser autorizadas por los Tratados Comunitarios, derecho comunitario originario (o primario), bajo pena de invasión de atribuciones también reservadas internamente a los países.

No caben dudas que esa cuestión era una preocupación en cuanto a la edición de la directiva 95/46/CE, tanto que ya buscó ser reconocida en algunos de los *considerandos* de su preámbulo. Veamos entonces, si el artículo 1º de la directiva no esconde que se resguardan en ella libertades y derechos fundamentales de individuos en el campo de la protección de datos, el ítem 3 del preámbulo conecta esa defensa a una necesidad, en razón del establecimiento y funcionamiento de un mercado interno europeo, ya que como los datos personales estarían dentro del concepto de "libre circulación de mercaderías, personas, servicios y capitales", no podría ocurrir esto descuidándose los derechos de los ciudadanos involucrados. El *considerando* 12 completa esta justificación vinculada a actividades regidas por el derecho comunitario, excluyendo la aplicación de la directiva de la manipulación exclusivamente personal o meramente doméstica de las informaciones.

Aunque no directamente con relación a las directivas específicamente de protección de datos, el Tribunal de Justicia de la Unión Europea tuvo la oportunidad de

[450] Apartados 99 a 101 de la decisión.

analizar esa argumentación en el juicio sobre el pedido de anulación del Reglamento (CE) Nº 515/97 del Consejo, del 13 de Marzo de 1997, "relativo a la asistencia mutua entre las autoridades administrativas de los Estados miembros y a la colaboración entre estas y la Comisión, teniendo en cuenta la de asegurar la correcta aplicación de las reglamentaciones aduanera y agrícola"[451]**.** En el artículo 34.1 del citado Reglamento se imponía al país que tenga la intención de introducir datos personales en el "Sistema de Información Aduanera" (SIA) que estaba siendo creado que, al menos concomitantemente a este tipo de uso, posea en vigor una legislación interna de protección de datos personales. El *considerando Nº 15* de este Reglamento era aún más explícito, determinando al menos el respeto a los principios existentes en la directiva 95/46/CE.

El Tribunal de Justicia de la UE niega la sustanciación del recurso, entendiendo que no hay ningún problema en que normas comunitarias de aplicabilidad directa, como los reglamentos, tengan como efecto accesorio la aproximación de las legislaciones internas nacionales[452], aún cuando eso provoque reflejos en la normalización de derechos individuales. O sea la "protección de datos" es claramente asumida aquí como un elemento obligatoriamente en común en el mercado interior europeo.

Esta comprensión fue reafirmada en la búsqueda de anulación por parte de Irlanda de la Directiva 2006/24/CE. El TJCE entendió que las disposiciones que afectan el uso de datos personales, como en ese caso, su período de conservación, deben ser consideradas independientes de su posible finalidad, aunque eso involucre seguridad pública. La prioridad de la afectación recae siempre sobre el mercado interior y su

[451] Fallo del Tribunal (Sexta Sección) del 18 de Noviembre de 1999 - Proceso C-209/97.
[452] Ítems 36 y 37 de esa decisión.

necesidad de uniformidad[453].

Esta protección cruzada de los datos personales, genera incertidumbres bajo la posición real de un derecho a la protección de datos en el escenario comunitario, mejora sustancialmente con la entrada en vigencia del "Tratado de Lisboa".

Este Tratado, que buscó resolver el impase ocurrido después del rechazo por Francia y Holanda del proyecto de Constitución Europea de 2004, realizó básicamente una reforma en el "Tratado de la Unión Europea" y en el "Tratado de Funcionamiento de la Unión Europea". Desde el punto de vista de los Derechos Fundamentales hay una "integración acumulativa" de dos importantes documentos, ya que con la nueva redacción de los artículo 6.1 y 6.2 del Tratado de la Unión Europea son reconocidos oficialmente por la UE los derechos, libertades y principios constantes de la "Carta de Derechos Fundamentales de la Unión Europea", que pasa a tener *status* de Tratado internacional también, y, a continuación, se adhiere la propia Unión Europea a la Convención Europea para los Derechos del Hombre[454]. Esto significa un doble refuerzo al carácter jurídico vinculante de los derechos humanos dentro de la Unión Europea, aún más cuando el artículo 6.3 los asume con naturaleza jurídica de *principios* dentro del derecho de la Unión, terminando con la duda en cuanto a su importancia para el estudio jurídico[455].

En otras palabras, la protección de datos en la Unión Europea tiene la salvaguarda sobre el concepto de "vida privada", según la jurisprudencia del TEDH,

[453] Ítems 81 a 85 de la sentencia de la gran sala del TJCE, el 10 de febrero de 2009 (asunto C-301/06).
[454] HÄBERLE, Peter. "El Tratado de Reforma de Lisboa de 2007." *Revista de Derecho Constitucional Europeo 9*, Junio 2008, p. 12.
[455] *Ibíd.*, p. 16.

pero también como derecho autónomo, debido aque la redacción de 2007 de la "Carta de Derechos Fundamentales de la Unión Europea"[456] mantuvo en su artículo 8º el derecho a la protección de datos de carácter personal, con tres apartados con el siguiente texto:

> "1. Todas las personas tienen derecho a la protección de los datos de carácter personal respecto a ellos.
> 2. Esos datos deben ser objeto de un tratamiento leal, para fines específicos y con el consentimiento de la persona interesada o con otro fundamento legítimo previsto por ley. Todas las personas tienen el derecho de acceder a los datos recogidos respecto a ellos y de obtener la respectiva rectificación.
> 3. El cumplimiento de estas reglas queda sujeto a la fiscalización por parte de una autoridad independiente."

Como si eso no fuera suficiente el propio artículo 16 del actual "Tratado de Funcionamiento de la UE" repite la idea de un *derecho a la protección de datos para las personas singulares*, que está conforme a las normas emanadas en el proceso legislativo ordinario por el Parlamento Europeo y por el Consejo de Europa, cuyo cumplimiento será fiscalizado por autoridades independientes[457], y su aplicación alcanza a los órganos comunitarios y a los *Estados miembros* (apartado 2 de este artículo 16 del TFUE). Afirma BLASI CASAGRAN que "la supresión de los llamados 'pilares' permitirá una homogeneización de criterios entre el primer y el tercer pilar, obteniendo de este modo un refuerzo de los controles democráticos en esta esfera."[458].

---

[456] Solamente no vinculante para Polonia y Reino Unido.

[457] Ese artículo 16 fue objeto de *excepciones* por parte de Reino Unido, Irlanda y Dinamarca y mereció dos *declaraciones adicionales*: la primera (de nº 20) apuntando la necesidad de limitación del derecho por medio de su ponderación con las exigencias de seguridad nacional, valor, no obstante, ya reconocido en la Directiva 95/46/CE; además (declaración nº 21) resaltó la posible necesidad de normas específicas en los dominios de la cooperación judicial en materia penal y cooperación policial. Por otro lado, ese artículo 16, al constituirse como repetición del antiguo art. 286 del TCE, permite que se mantengan en vigor para las instituciones comunitarias las determinaciones del Reglamento (CE) n.° 45/2001 del Parlamento Europeo y del Consejo, del 18 de Diciembre de 2000, "relativo a la protección de las personas singulares en lo que respecta al tratamiento de datos personales por las instituciones y por los órganos comunitarios y a la libre circulación de esos datos".

[458] BLASI CASAGRAN, Cristina. "La protección de los derechos Fundamentales en el Tratado de Lisboa". *Quaderns de treball*, outubro 2010, p. 27.

Ni decir que el antiguo Tercer Pilar de la Unión Europea, la Cooperación Policial y Judicial en materia penal, está excluida del influjo de las normativas sobre protección de datos, en razón de la declaración 20[459] y 21[460] relativas a las disposiciones de los Tratados, ya que se trata solamente de la enunciación de una *posible* (y quizá necesaria) limitación al derecho, sobre las cuales no son desconocidas ni de la directiva europea, ni de las legislaciones nacionales[461]. Esta perspectiva está confirmada por la Decisión Marco 2008/977/JAI del Consejo de la Unión Europea, que explica la importancia de reglas comunes de respeto a la vida privada y al "elevado nivel" de protección de datos personales en el ámbito de la cooperación policial y judicial en materia penal entre los estados miembros, como también de contribución al combate contra la criminalidad (considerandos 2, 3, 6, 8, 10 y 16 de dicha decisión marco).

3.2.3.2.1 La Directiva 95/46/CE de la Unión Europea

3.2.3.2.1.1 Introducción

La principal regulación comunitaria del derecho a la protección de datos es definida también por la necesidad de perfeccionar los múltiples intereses en confrontación por la inevitable realidad de la existencia de base de datos, lo que llevó a

[459] "La Conferencia declara que, cuando haya que adoptar, con fundamento en el artículo 16.o, reglas sobre protección de datos personales que puedan tener implicaciones directas para la seguridad nacional, las especificidades de esta cuestión deberán ser debidamente ponderadas. La Conferencia recuerda que la legislación actualmente aplicable (ver, en especial, la Directiva 95/46/CE) prevé derogaciones específicas en esta materia."

[460] "La Conferencia reconoce que, atendiendo a la especificidad de los dominios en causa, podrán ser necesarias disposiciones específicas sobre protección de datos personales y sobre la libre circulación de esos datos, en los dominios de la cooperación judicial en materia penal y de la cooperación policial, con base en el artículo 16 º del Tratado sobre el Funcionamiento de la Unión Europea."

[461] BLASI CASAGRAN, Cristina. "La protección de los derechos … *cit.*, p. 37. Nótese aun que si la Directiva 95/46 no impuso su aplicación sobre la jurisdicción penal y la policía, salvo en funciones típicamente administrativas, la LOPD española no excluyó la cobertura de la jurisdicción penal.

una legislación que combinará preocupaciones por las "prohibiciones de exceso" con los límites a la protección de las informaciones archivadas relativas a cada individuo, con definición de excepciones en que también no se permitiese que el derecho perjudicase la seguridad de la sociedad. Este equilibrio entre derecho subjetivo y obligaciones estatales se encuentra con claridad en la Directiva 95/46/CE.

Esa necesidad de establecer parámetros involucrando intereses tan distintos en un campo que se podría decir tan inédito llevó al legislador comunitario a establecer las fronteras del desarrollo del nuevo derecho fundamental por medio de una serie de *principios* que se refieren a objetivos de comportamiento de los involucrados en relación con la protección de datos, o sea, persona a quien la información se refiere y titular de la base de datos y un campo de excepciones a las reglas generales, para permitir el mantenimiento de la eficacia de la acción del Estado[462].

La influencia de la Directiva 95/46 es innegable. Es verdad que con la edición del Convenio Nº 108 de 1981 ya hay una secuencia de nuevas leyes estatales europeas que se adaptan a ese marco[463], asimismo, porque aún antes de la Directiva ya había convenios comunitarios, notablemente en materia de seguridad y cooperación policial, que exigen que los Estados signatarios se adapten al Convenio 108, como, por ejemplo, el de Schengen, del 19 de enero de 1990 y el Europol, del 26 de julio de 1995.

Pero, con la *obligatoriedad* de la introducción en el orden interno, reafirmada por el artículo 32 de la Directiva 95/46/CE se provoca un frenesí legislativo en los

[462] HOFFMANN-RIEM, Wolfgang. (ed..). *Verwaltungsrecht in der Informationsgesellschaft... cit.*, p. 43.

[463] Surgen en función del convenio n. 108 nuevas leyes en Suiza (1981, después reemplazada por la Ley nº 231, del 19 de enero de 1992), en Gran Bretaña (1984), en Finlandia (1987), en Holanda (1988), en Islandia (1989), una nueva ley en Alemania reunificada (1990), en Portugal (1991), y también en Hungría, en Checoslovaquia y en España en 1992.

países de la UE y con parámetros mucho más estrictos. Cronológicamente esa adopción de la normalización unificadora de la protección de datos se inicia exactamente con los países que no habían insertado aún las disposiciones del Convenio 108, por ejemplo, Italia y Grecia. Esa laguna se suprimió con la Ley italiana Nº 675 del 31 de diciembre de 1996 y con la ley griega Nº 2472, del 30 de abril de 1997.

En los países en que ya existía alguna norma infraconstitucional para regular la cuestión hubo una demora un poco mayor, debido a la duda entre la utilización de instrumentos de reforma de las leyes ya existentes o en la confección de nuevas reglamentaciones. Esa opción, en la mayoría de los casos, prevaleció, y , de esta forma, surge en el Reino Unido un nuevo *Data Protection Act* el 16 de julio de 1998, en Finlandia la Ley Nº 523 de 1999, en Holanda la Ley del 6 de julio de 2000, en Islandia la Ley Nº 77 de 2000, en Alemania la *Bundesdatenschutzgesetz* del 23 de mayo de 2001, en Portugal la Ley Nº 67 del 26 de octubre de 1998 y, separada de Eslovaquia, en República Checa la Ley del 4 de abril de 2000. En España la Ley Orgánica de Protección de Datos (LOPD), que será más adelante analizada, es la 15/1999 del 13 de diciembre y substituyó a la LO Nº 5/1992, denominada Ley Orgánica Reguladora del Tratamiento Automatizado de Datos (LORTAD)[464]. Por lo tanto, poco más de 6 años, surgió toda una nueva estructura legislativa de protección de datos.

3.2.3.2.1.2 Disposiciones especificas de la Directiva

Por otro lado, en el artículo 1º se establece al ámbito subjetivo de aplicación del

[464] Para el análisis de la normativa específica de cada país de Europa es indispensable la lectura del estudio de TÉLLEZ AGUILERA, Abel. *La protección de datos en la Unión Europea: divergencias normativas y anhelos unificadores*. Madrid: Edisofer, 2002.

derecho fundamental, solamente personas físicas y no jurídicas[465] (apartado 1) y el principio de libertad de flujo de datos en el ámbito comunitario (apartado 2). Aunque ese mismo artículo 1º también trate de una defensa "en particular" del derecho a la intimidad él debe ser interpretado en conjunto con el considerando 14 de la Directiva, que amplía la defensa a la protección de datos de las personas físicas en general[466].

El artículo 3º (combinado con el Considerando 27) responde a la eficacia objetiva de la norma, al establecer que tanto las bases de datos automatizadas como también aquellos manuales automatizados o no, serán sometidos al reglamento. El apartado 2 de ese mismo artículo excluye la aplicación de la Directiva a los archivos domésticos y aquellos que tengan por objeto la seguridad o defensa del Estado y materia penal, además de los temas en las disposiciones establecidas en los títulos V y VI del Tratado de la Unión Europea. La sentencia del 6 de noviembre de 2003, *Lindqvist*, Asunto C-101/01 del Tribunal de Justicia de la Unión Europea (TJCE) es importante para la interpretación de esa regla de excepción, ya que el órgano jurisdiccional deja en claro que tales "archivos domésticos" deben tener una conexión intrínseca con la vida privada de esos particulares que lo crearon, no prestándose para hacer soportar la lista de acceso general, como se da, en el caso, de las páginas de Internet[467].

---

[465] Esa opción excluyente de las personas jurídicas recibía en la doctrina española anterior a la Directiva, pues aunque no se pueda admitir que "esa persona moral puede gozar de los derechos inherentes a la individualidad de cada ser humano", también es verdad que "erigir un ente moral como titular del derecho a la autodeterminación informativa supone elevar un primer mecanismo de protección de sus socios, más fácil de activar, pues lo pueden ejercer los órganos sociales y de eficacia más amplia, ya que el ejercicio del derecho por la persona jurídica beneficia a todos sus componentes a la vez" (MURILLO DE LA CUEVA, Pablo Lucas. *El derecho a la autodeterminación informativa... cit.*, p.. 181 y 182). Nótese incluso que la legislación italiana (ley número 675, artículos 1, 2.c y 2.f) aumenta la protección de datos también a las personas jurídicas.

[466] "(14) Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;".

[467] Apartado 46 a 48.

El principio fundamental al tratamiento de datos personales, es el de la "calidad" que encontramos en el artículo 6º, en que son descritos a lo largo de los párrafos todos sus sub-principios, o sea, *lealtad* y *licitud* en el tratamiento, obtención con finalidad *determinada, explícita y legítima* y mantenimiento solamente de los datos *adecuados, pertinentes* y *no excesivos* a los fines, archivando con *exactitud* y *actualización*, cuando es necesario y conservación con *identificación de los interesados* solamente durante el plazo necesario a los fines. A su vez algunos de esos conceptos jurídicos indeterminados ya están definidos en su significado por medio de llamados "principios de aplicación" o "interpretación" que se encuentran en el citado articulado[468]. Por tanto, el "tratamiento lícito" es aquel que "se efectúa con el fin de proteger un interés esencial para la vida del interesado" (Considerando 31) y el "tratamiento leal" se refiere a aquel en que "los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención" (Considerando 38).

El artículo 7º, a su vez, define como regla general para la legitimidad del tratamiento el *consentimiento inequívoco* (párrafo "a"), aunque sus demás párrafos, así como el artículo 9º, permitan diversas excepciones, entre las cuales están la disposición contractual del interesado (párrafo "b"), la protección de un interés vital suyo ("d"), la satisfacción de interés legítimo ("f") o el cumplimiento de misión de interés público ("e") por el responsable del el tratamiento y la preservación del derecho a la libertad de expresión y de comunicación (art. 9º).

[468] REBOLLO DELGADO, Lucrecio. *Derechos fundamentales y protección de datos... cit.*, p. 135.

El principio del consentimiento inequívoco también es la excepción, ahora en dirección a una mayor protección, en el caso del tratamiento de los llamados "datos sensibles" (art. 8º). En los, relativos a aspectos raciales, de salud, de orden sindical y de convicciones políticas, religiosas y filosóficas hay un caso común, el impedimento en el uso de bases de datos (apartado 1). Sin embargo, también aquí ocurren importantes posibilidades de reserva, a destacarse el consentimiento explícito del interesado (apartado 2, párrafo "a") a situaciones en que impera relevante interés público, como la prevención y el diagnóstico de enfermedades que afecten el cuerpo social como un todo (art. 8.3 combinado con la lectura del Considerando 34) o la utilización por instituciones constitucional o internacionalmente reconocidas, como las asociaciones religiosas y los partidos políticos (art. 8.4 combinado con la lectura del Considerando 35). El artículo 8.5, a su vez, aumenta los requisitos de manipulación de registros de condenas penales, al definir que tendrán control por parte de las autoridades públicas, favoreciendo de esta forma la reinserción social.

Sobre el presupuesto en la utilización de las facultades otorgadas a los ciudadanos en la "protección de datos" es su *derecho*, independientemente que hayan o no hayan sido obtenidos los datos de sí mismo, la *de ser informado*, al menos, de la identidad de quien trata sus datos, de la finalidad de su uso, para garantizar la lealtad del tratamiento, del destinatario y categoría de los datos, del deber o no de responder y de las consecuencias de la negativa y de la existencia de un derecho de acceso y de rectificación (arts. 10 y 11). La obligación de encontrar al interesado para comunicarle no se aplica cuando es imposible o desproporcional, sin perjuicio de las garantías razonables (art. 11.2).

Existe previsión de un *derecho de acceso a los datos, de rectificación, supresión y bloqueo* de utilizaciones que no respeten los principios de la directiva (art. 12) y *de oposición* al tratamiento condicionada a las hipótesis del artículo 14. Se añade también el *derecho a no verse sometido a decisiones automatizadas* (art. 15). Pero, en el art. 13, encontramos la posibilidad de que tales derechos sean limitados en pro de situaciones en que debe prevalecer el interés público[469].

3.2.3.2.1.3 La transferencia internacional de datos de la Unión Europea a terceros países

En el artículo 25 de la directiva queda patente esa característica de la legislación de protección de datos en comparación con otras similares referentes a otros derechos fundamentales, al tratarse de regulación de una materia que involucre inherentemente un escenario difuso y poco atento a las fronteras políticas de las naciones. El derecho interno aquí, y las estructuras administrativas que pueden ser por él creadas, solo pueden *ayudar*, por medio de la fiscalización del cumplimiento y sanciones, al establecimiento de la fuerza del nuevo derecho transnacionalmente pactado, pero sólo, es prácticamente impotente[470], ya que, sin la adopción de reglas uniformes, los dueños de bases de datos simplemente migran hacia países con una protección menos intensa. La eficacia en la protección de datos depende siempre de una solución de esta naturaleza, pues, de otra manera, se vuelven naturales las fugas hacia países con menos amarras en la legislación de datos personales como forma de substraerse de sus obligaciones y del cumplimiento de derechos y garantías de los afectados.

[469] HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales … cit.*, p. 33.
[470] HOFFMANN-RIEM, Wolfgang (ed.). *Verwaltungsrecht in der Informationsgesellschaft... cit*., p. 45.

Por eso una regulación eficaz pasa por dos soluciones: o se llega a un acuerdo amplio entre los participantes del campo de actividades en disciplinar sus conductas, es decir, se establece un "código de comportamiento" social (como se ve, por ejemplo, en algunos sectores de Internet) o una producción legislativa impulsada finalmente por una organización internacional. La Directiva apuesta a esta última opción.

El artículo 25 de la Directiva europea sobre protección de datos exige que para la transferencia de datos a terceros países[471] exista un nivel de protección *adecuado*. Este adjetivo es menos restrictivo para la verificación que el requisito de protección *equivalente* presente en el artículo 12.3 de la Convención 108.

Este artículo 25, en lo que se refiere al Estado, es una fuerte representación de como la realidad de la creación de las redes transnacionales de intercambio de información (que se proliferan por las Administraciones Públicas en temas diversos como política monetaria, medio ambiente, seguridad, propiedad intelectual, etc.), cada vez más van prescindiendo de los tradicionales canales de la diplomacia y de restringirse al contacto con altas autoridades, puede establecer valores como transparencia, acceso a información, participación y responsabilidad administrativa en su realización dentro del Estado nacional, aumentando el diálogo entre sociedad y el Poder Administrativo[472]. En ese sentido, es de destacarse que la directiva europea no veda que la decisión sobre la "protección adecuada" se dé individualmente por cada

[471] No es necesario que el artículo 25 trate de los demás países de la Unión Europea porque el artículo 30 de la Directiva ya prevé otro modo de control. A través del Grupo de protección de datos personales, creado a través del art. 29, se verificaran las disposiciones y la práctica interna de los estados miembro para garantizar una protección *equivalente* dentro de la Comunidad (artículo 30 de la Directiva 95/46).

[472] BARNES VÁZQUEZ, Javier. "Sobre el procedimiento administrativo: evolución y perspectivas... *cit.*, p. 325-329 y 340.

país, por medio de sus autoridades nacionales de protección de datos, sin perjuicio de que la propia Comisión, ayudada por un Comité[473], pueda emitir también esa certificación (apartados 2 y 6 del artículo 25 de la directiva). La coherencia exige que cuando el análisis se incline por la ausencia de protección adecuada, ocurra también entre Estado miembro y Comisión este aviso (apartado 3 del mismo artículo).

La Comisión Europea, realizado su certificado, relaciona a los países en ese nivel adecuado de protección, en una llamada "Lista Blanca". Los hoy reconocidos como parte de esta lista, sin restricciones, son: Andorra[474], Isla Faroe[475], Suiza[476], Hungría[477], Canadá[478], Argentina[479], Jersey[480], Guernesey[481] y la Isla de Man[482]. Además poseen manifestación favorable del grupo de trabajo en cuanto a la adecuación, aunque tampoco haya decisión final, Nueva Zelanda y Uruguay.

El parecer WP 12 DG XV D/5025/98 del 24 de julio de 1998, adoptado por el grupo de trabajo sobre "protección de las personas singulares en lo que respecta al tratamiento de datos personales", describe minuciosamente como se deben dar esas apreciaciones realizadas por la Unión Europea. Metodológicamente, el análisis se divide, inicialmente, en dos grandes campos, en los cuales se describen por un lado el contenido material de las normas aplicables y, por el otro, cuales son los medios utilizables para garantizar su aplicación.

473 Formado conforme el artículo 31 de la directiva.
474 Decisión 2010/625/UE.
475 Decisión 2010/146/UE.
476 Decisión 2000/518/CE.
477 Decisión 2000/519/CE.
478 Decisión 2002/2/CE.
479 Decisión 2003/490/CE.
480 Decisión 2008/393/CE.
481 Decisión 2003/821/CE.
482 Decisión 2004/411/CE.

Como una ilustración de lo mínimo exigido, el contenido material del ordenamiento del país *importador* de los datos debe respetar al menos los principios de limitación sobre la finalidad en el uso de los datos, de precisión de la información archivada, de relevancia y no exceso en la obtención, de la transparencia al afectado y de seguridad en el almacenamiento. Deben ser garantizados a los individuos derechos de acceso, rectificación y oposición, con protección adicional cuando se trate de sus "datos sensibles". Las decisiones automatizadas deben tener su lógica exposición, para permitir que el individuo la discuta y, en el marketing directo, él debe ser capaz de darse de baja (el denominado *opt-out*). Además, evidentemente, el tercer país receptor debe comprometerse a ser igualmente exigente en sus transmisiones a otros países[483].

En los medios, aunque se reconozca la imposibilidad de imponer el consenso europeo de un sistema de "supervisión externa" por medio de una autoridad independiente, el modelo adoptado debe servir para, al menos, tres objetivos: dar lugar a un buen nivel de cumplimiento de las reglas de contenido, ayudar al afectado de forma rápida, efectiva y con pocos costos financieros a que pueda ejercer sus derechos y garantizar una estructura independiente que obligue reparaciones e imponga sanciones sobre aquellos que no respeten las normas de protección de datos[484].

Concretamente, se observa que para alcanzar esas decisiones la protección de datos en el tercer país tiene sus efectos jurídicos ser vinculantes sobre todo el territorio nacional de manera uniforme y si los principios inherentes a la protección de datos se aplican al sector público y al sector privado, o, si no, sobre cuales áreas y sectores hay límites; si los límites al derecho se dan en pro de intereses públicos relevantes, como los

[483] WP 12 DG XV D/5025/98, p. 6-7.
[484] WP 12 DG XV D/5025/98, p. 8.

previstos en el apartado 2 del artículo 11 y en el artículo 13 de la directiva; y si hay garantías judiciales y administrativas suficientes para proteger al ciudadano. Es interesante notar también que la legislación del país analizado es verificada según explicaciones de este, relativas a la interpretación existente en su derecho vigente y, también, que las decisiones afirmativas que la adecuación pueden tener en su ámbito restringido a un sector específico.

Aunque no se hable directamente, de la regulación existente en los países miembros de la Unión Europea y por el texto del art. 1.1 de la directiva y de sus considerandos 1, 2, 7, 8, 9, 10 y 11, es en la práctica exigida del tercer país una protección *jusfundamental*, ya que no sería posible de otra manera cumplir los estándares de protección de los datos personales de manera adecuada[485].

Aunque existan posibles garantías que pueden ser exigidas de los países que no tengan nivel de protección adecuado (art. 26.1 de la Directiva 95/46/CE), es innegable que el flujo de datos entre la Unión Europea y el tercer país gana un enorme impulso verificándose la compatibilidad[486], inclusive porque garantiza la aplicación de la "reciprocidad", inherente al Derecho Internacional. Además, en razón de la multiplicidad de transmisiones necesarias diariamente, una certificación del tercer país en carácter general garantiza seguridad a todas las partes involucradas. Por último, desde el punto de vista de la sociedad internacional, es relevante tal estímulo para que cada vez más países adopten medidas legales eficaces para preservar el derecho a la

[485] SIMITIS, Spiros. "Der Transfer von Daten in Drittländer -ein Streit ohne Ende?" *Computer und Recht*, 2000, p. 524.

[486] Numéricamente en la comparación de los países de Latinoamérica significó, en el período entre 2003 y 2009 que Argentina, único país de la región con la afirmación de protección adecuada por la Comisión Europea, recibió la transferencia de 214 bases de datos, mientras que Brasil, en el período de 2007 a 2009, recibió tres bases de datos, en la forma de ese artículo 26 (MATUS, Jessica. "Transferencias Internacionales a Países con Niveles Adecuados y no Adecuados de Protección. Aspectos Prácticos." Montevideo, Uruguay, 2010, p. 11).

protección de datos de sus ciudadanos.

Las dificultades de no adecuarse son perfectamente traducidas en la situación de transferencia de datos entre Estados Unidos y Europa. Aunque sea evidente la importancia de la transferencia de datos entre esos dos polos, notablemente por razones comerciales y de seguridad, la legislación norteamericana posee una protección muy inferior a la europea, siendo formada por leyes esparcidas, normalmente aplicables solo al sector público y, cuanto mucho, a sectores económicos privados e, invariablemente, por medio de reglas poco extensas[487], y, así, en muchos puntos con lagunas en la vida práctica. Esto motivó un acuerdo específico, en el ámbito eminentemente privado, y siendo aplicable por la adhesión una a una de empresas interesadas, de los llamados principios de "*safe harbor*" (notificación, opción, transferencia posterior, seguridad, integridad de los datos, acceso y aplicación)[488].

De hecho, esta es la afectación al derecho constitucional de la transformación de una sociedad internacional basada en la simple coexistencia a otra que está tan interconectado, depende de la cooperación. No es ninguna coincidencia que el acuerdo normativo (progresivo) se produce a través de una agenda de derechos humanos, ya que tienen un sentido de "validación universal" explicable por el hecho de que puede justificarse sólo por razones morales, a diferencia de otros reglas suelen depender de

[487] BLANKE, Jordan M. "'Safe Harbor' and the European Union's Directive on Data Protection". *Albany Law Journal of Science & Technology*, 2000, p. 58.

[488] Anexo I de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000. Sin embargo, ni este acuerdo es ausente de resistencias por la Euro cámara, ni resuelve los problemas gubernamentales, como se ve ppr las tensiones en las cuestiones de los datos de pasajeros de compañías aéreas (vide sobre el tema Ioannis Ntouvas. "Air Passenger Data Transfer to the USA: the Decision of the ECJ and latest developments". *International Journal of Law and Information Technology*, 2008.) y en el acceso a los datos bancarios a través de la compañía belga SWIFT (Society for Worldwide Interbank Financial Telecommunication), cuyo acuerdo internacional fue rechazado por la Eurocámara, ya con base en los nuevos poderes concedidos por el Tratado de Lisboa, el 11 de febrero de 2010, con 378 votos contrarios y solamente 116 a favor, fuertemente con base en preocupaciones concernientes al respecto de la privacidad.

otras justificaciones de ética, política y pragmática

De hecho,, esta es la afectación al derecho constitucional de la transformación de una sociedad internacional basada en la simple coexistencia a otra que está tan interconectada, depende de la cooperación[489]. No es por casualidad que el (progresivo) acuerdo normativo se produzca por medio de una pauta de derechos humanos, ya que estos poseen un sentido de "validez universal" explicable por el hecho de puede justificarse sólo por medio de razones morales, a diferencia de otras normas que, usualmente, dependen de otras justificaciones de carácter ético político y pragmático[490].

Otros factores que favorecen la aceptación amplia de los derechos humanos es el establecimiento de Estados Constitucionales que los buscan hacer efectivo por medio de una carta similar de derechos fundamentales, como forma de representar su identidad a una comunidad de países que los tratan responsablemente[491]. Pues aún admitiendo la existencia de distintos momentos históricos de realización de los derechos humanos en los diversos países conviviendo concomitante, son nítidos los regímenes que solo los defienden "de fachada"[492]. Esta tendencia, de parcialidad comparatista, también está fortalecida en las sociedades que adoptan verdaderamente la fórmula del Estado Democrático de Derecho como un medio de aprender de los errores pasados de sus modelos inspiradores[493].

---

489 HÄBERLE, Peter. *Estado constitucional cooperativo.* Rio de Janeiro: Renovar, 2007, p. 71.

490 HABERMAS, Jürgen. *A inclusão do outro: estudos de teoria política.* São Paulo: Loyola, 2002, p. 215.

491 HÄBERLE, Peter. *El Estado Constitucional*. México, D. F.: Universidad Nacional Autónoma de México, 2003, p. 75. En la misma dirección argumenta JOHN RAWLS: "respect to the human rights is one of the conditions imposed on any political regime to be admissible as a member in good standing into a just political society of people" (RAWLS, John. "The Law of Peoples." *Critical Inquiry*, Autumm 1993, p. 65)

492 HABERMAS ,Jürgen. *Verdade e justificação: ensaios filosóficos... cit.*, p. 60.

493 SCHMIDT-ASSMANN, Eberhard. "Cuestiones fundamentales sobre la reforma de la Teoría General del Derecho Administrativo. Necesidad de innovación y presupuestos metodológicos." In *Innovación*

En el caso de la protección de datos, la existencia de una regulación en común es efectivamente una necesidad para la verdadera protección del individuo, pues se trata de un bien jurídico cuya lesión por medios de un tratamiento o uso indeseado fácilmente traspasa las fronteras del Estado nacional[494]. La coordinación entre los países por medio de la existencia de pautas jurídicas comunes se muestra como indispensable a la hora de la preservación de su defensa[495].

Esto no significa la negación de la estatalidad en pro de una gobernanza internacional, hasta porque son los Gobiernos democráticos que celebran los tratados internacionales, sus parlamentos electos que los aprueban y los tribunales constitucionales que los interpretan realzando su fuerza vinculante en los dispositivos que consagran los derechos humanos[496], sino la verificación de crecientes pautas comunes internacionales. Resume bien la cuestión SCHMIDT-ASSMANN:

> "Los desafíos que actualmente se plantean no deben ser afrontados, sin embargo, con concepciones cerradas de estatalidad que partan de la mayor unidad posible frente al exterior y conciban la internacionalización, ante de todo, como una amenaza. Resulta necesario, en cambio, tomarse en serio la *concepción de estatalidad abierta*, como ha hecho ya el Constituyente alemán en los artículos 23 a 25 y 59 GG, al erigirla en modelo normativo. El Tribunal Constitucional Federal alemán, en este sentido, destaca acertadamente hoy en día que el Derecho Internacional público 'pretende ser el fundamento de la legitimidad de todo ordenamiento estatal'.
> Tras semejante sentencia constitucional no puede considerarse la internacionalización de las relaciones jurídicas como un molesto efecto colateral, sometido al mayor número posible de 'reservas' sino como *normalidad constitucional estatal (verfassungsstaaliche Normalität)*; se trata de un fenómeno que, ciertamente, al igual que la actuación soberana intraestatal, no está

---

y reforma en el derecho administrativo / coord. por Javier Barnes Vázquez. Sevilla: Derecho Global, 2006, p. 78. Tbm. AHUMADA RUIZ, Marían. *La jurisdicción constitucional en Europa: bases teóricas y políticas*. Cizur Menor (Navarra): Thomson-Aranzadi, 2005, p. 227.

494 PETERSEN, Stefanie. *Grenzen des Verrechtlichungsgebotes... cit.*, p. 126.

495 HOFFMANN-RIEM Wolfgang. "Der Staat muss Risiken eines Missbrauchs durch Infiltrierung vorbeugen". Frankfurter Allgemeine Zeitung, 09.10.2011, [s.d.].

496 Hay juzgados que expresan, fuera del ámbito de la Unión Europea, fuertemente esa realidad, como vemos en *Lawrence vs. Texas*, sobre la criminalización de las relaciones sexuales de adultos homosexuales, de la Suprema Corte estadounidense y en el Recurso Extraordinario n. 466.343-1/SP, que trató sobre la prisión civil de deudor en alienación fiduciaria, del Supremo Tribunal Federal brasileño.

> exento de problemas y peligros, pero que no debe ser visto como una evolución radical que acabará con el Estado."[497]

Las disposiciones de la Directiva Europea sobre transferencia internacional de datos tienen una particular importancia para países en desarrollo, como Brasil. En primer lugar, existe presión de volverse destinos deseados para inversiones externas que les permitan mejorar la situación económica de su población, lo que involucra superar las posibles barreras de tráfico comercial[498].

Sin embargo, no se debe menoscabar que, para un país en vías de desarrollo, adoptar en sus líneas generales un modelo exitoso de una nación desarrollada significa buscar replicar una experiencia institucional que es deseada para su sociedad. Más allá del menor costo de no crear una nueva estructura a partir de la nada, reflejarse en proficuas legislaciones ajenas permite creer en lo que se implementó independientemente de eventuales incomodidades iniciales, y garantiza interlocutores externos que puedan dialogar sobre posibles ajustes necesarios a cada realidad[499].

Además, la búsqueda de una "protección adecuada" demuestra que el constitucionalismo global no necesita estar basado solamente en la formación de amplios consensos y estructuras supranacionales, sino también puede tener frutos importantes por medio de búsquedas de mutuo reconocimiento por medio de esfuerzos

---

[497] SCHMIDT-ASSMANN, Eberhard. "La ciencia del Derecho Administrativo ante el reto de la internacionalización de las relaciones administrativas." *Revista de administración pública*, 2006, p. 23. En sentido similar, HABERMAS habla que a "transition from the law of nations to cosmopolitan law can indeed be understood as a constitunalization of international relations but not as a logical continuation of the evolution of the constitucional state leading from the national to a global state" (HABERMAS, Jürgen. *The divided West*. Cambridge; Malden: Polity, 2006, p. 132).

[498] MILLER, Jonathan M. "A Typology of Legal Transplants: Using Sociology, Legal History and Argentine Examples to Explain the Transplant Process." *The American Journal of Comparative Law*, Fall 2003, p. 847.

[499] *Ibid.*, p. 872-873.

de los poderes nacionales en ese sentido[500]. Se hace posible en esa unificación constitucional del significado de un derecho a la protección, fenómenos de comunicación y recepción[501], los cuales facilitarían la adaptación de las normas jurídicas a las peculiaridades de cada sociedad. Existe entonces, en el trasplante de estructuras bastante exitosas el espacio para re-contextualizarlas en base a cada sociedad, fenómeno propicio para un estudio comparado[502].

3.3 Conclusiones

1. La jurisprudencia del Tribunal Europeo de Derechos Humanos, la Directiva 95/46 de la Unión Europea, el Convenio Nº 108 del Consejo de Europa y la Recomendación de 1980 de la OCDE son los instrumentos internacionales centrales en la conformación de la legislación interna actual de los países en la protección de los datos personales al pautar la experiencia europea que, en la secuencia, sirvió de marco a los países no europeos.
2. El Tribunal Europeo de Derechos Humanos sirve como última instancia de aplicación del Convenio Europeo de Derechos Humanos, fuente normativa principal consignada del Consejo de Europa para preservar los derechos del hombre en la post Segunda Guerra Mundial, con especial significado en el derecho internacional por la capacidad de imponer medidas vinculantes y responsabilidades a los Estados parte. A lo largo de sus 60 años de historia,

[500] SHAFFER, Gregory. "Transnational Mutual Recognition Regimes: Governance without Global Government". *Law and Contemporary Problems*, Summer/Autumn 2005, p. 314.
[501] PÉREZ LUÑO, Antonio- Enrique. "La tutela de la libertad informática en la sociedad globalizada". *Isegoría*, 2000, p. 67.
[502] FRANKENBERG, Günter. "Constitutional transfer: The IKEA theory revisited". *Int J Constitutional Law*, 2011, p. 579.

el TEDH, en conjugación con los tribunales constitucionales de los países, se afirmó como reproductor de decisiones judiciales que respetan las mejores tradiciones de protección a los derechos del hombre. En los poderes judiciales español y alemán se reconoce esa importancia y la necesidad de respetar las decisiones del TEDH, como órgano preparado para la interpretación del Convenio, con la reserva, en el último país, de que el ordenamiento jurídico Tedesco no promueva mayor protección o que no haya falta de respeto a la Constitución.

3. Siendo el Convenio Europeo de Derechos Humanos un tratado firmado en 1950 no se podría esperar en él una previsión expresa de protección de datos personales. Por eso el TEDH basa sus juicios sobre el tema en la protección de la vida privada otorgada por el artículo 8º del CEDH.
4. En 1976, en el caso *X v. Iceland*, el TEDH rechazó una concepción de vida privada constituida solo por los momentos de aislamiento, afirmando que las relaciones sociales también necesitan protección y son esenciales para el desarrollo de la personalidad. Sin embargo, hay aún pocas referencias sobre la afectación de los derechos del hombre por las amplias catalogaciones de datos sobre los miembros de la población que ya hacían los países signatarios de la convención, como alerta el juez Pettiti en su voto divergente en el caso *Malone v. United Kingdom*, en 1984.
5. El pionero en la afirmación de la obtención, almacenamiento y utilización de registros personales en bases de datos externas como integrante del derecho a la vida privada le cabe al caso *Leander v. Sweden*, del 26 de marzo de 1987, aunque el Tribunal haya entendido que las garantías previstas en la legislación sueca impidieron la violación al derecho. Además, se afirma en

M.S. v. Sweden (27 de agosto de 1997) que es inherente a la protección, el no desvirtuar de la finalidad en relación a qué datos son obtenidos.

6. Sin embargo, no son todos los datos personales que admite el TEDH como parte de protección en la Convención, como, por ejemplo, los datos básicos identificativos (*Reytjens v. Belgium*), aunque en *Amman v. Switzerland* (ap. 44647/98) se asevere la insuficiencia de restringirse la protección de datos personales a informaciones no vinculadas a relaciones de carácter externo (como las de naturaleza profesional). En esa catalogación la casuística preside la actuación del tribunal. Ejemplificativamente, los *datos médicos* son afirmados claramente como protegibles por el "derecho a la vida privada" en *Z v. Finland* (ap. 22009/93) e informaciones obtenidas al aire libre, por medio de imágenes, para identificación de transeúntes, en *Friedl v. Austria* (informe de la Comisión el 19 de mayo de 1994), confirmándose en *P.G. and J.H. v. The United Kingdom* que grabaciones (y no solamente escritos) que componen registros afectan la vida privada. En *S. and Marper v. the United Kingdom* (ap. 30562/04 y ap. 30566/04) muestras de ADN e impresiones digitales también son considerados datos susceptibles de archivo relacionados con la vida privada.

7. El TEDH no condena solamente a los Estados en razón de sus *acciones* en cuanto a registro y uso de informaciones individuales lesionantes de los derechos de los afectados, sino también cuando sus *omisiones* no permiten que los ciudadanos hayan preservado sus derechos de *acceso* (a partir del caso *Gaskin v. The United Kingdom*), *rectificación* (como ocurre a favor del cambio de género y nombre de transexuales operados, a partir de *Christine Goodwin v. The United Kingdom* – ap. 28957/95) y de no ver divulgadas en

la prensa transcripciones bajo sigilo judicial (*Craxi (n.2) v. Italy* – ap. 22337/94). Al mismo tiempo impone al Estado que regulando el almacenamiento de datos personales no permita que ese derecho individual sirva de escudo para que se cometan crímenes (*KU v. Finland* – ap. 2872/2002).

8. Las limitaciones a derechos fundamentales deben ser, en la forma de jurisprudencia del TEDH, emitidas en norma aplicable internamente que sea *accesible* y con consecuencias *previsibles* al ciudadano. Esas hipótesis, a continuación, deben ser compatibles con los valores de las cláusulas de interés público presentes en el artículo específico del derecho respectivo de la CEDH y, finalmente, constituirse en una medida "necesaria en una sociedad democrática". Todo eso evaluado dentro de un "margen de apreciación" que concede una cierta amplitud de posibles regulaciones al legislador nacional, con rigor que frecuentemente es proporcional a cuál y cuánto está vulnerado el derecho individual.
9. Esto justifica, por ejemplo, mayores cuidados cuando el análisis involucre registros secretos, con relación a los cuales el particular no tiene conocimiento de la existencia, como se da en los casos *Klass* y *Leander*. Pero, al mismo tiempo, hipótesis en que el individuo solo tiene como consecuencia del acto estatal el impedimento de acceso a empleo tienden a ser menos valorados, como se ve en *Knauth v. Germany* (ap. 41111/98). Al contrario, se reconoce la relevancia de registros médicos por su carácter de "datos sensibles", como en *Z. v. Finland* y *M.S. v. Sweden*.
10. Existe en la protección de datos una especial evaluación de la *duración* del mantenimiento del registro en poder del Estado, aunque inicialmente

justificable, en razón de la preocupación de que la existencia sin límites de fichas sobre los ciudadanos pueda macular la existencia saludable de una sociedad democrática, como se ve en las decisiones en *Rotaru v. Romania* y en *S. and Marper v. United Kingdom*. Las limitaciones al individuo solo pueden ocurrir de manera definitiva en cuanto al acceso a sus datos en caso de que afecten irremediablemente el derecho del tercero que no consiente la revelación o si fueran medidas proporcionadas favorables en el procedimiento que transcurre contra sí y en que el dato es relevante.

11. En general, no hay como negar la parsimonia con que el TEDH aborda la cuestión de la protección de datos como derecho del individuo. Al mismo tiempo, esa postura es útil en el análisis de un tercer país, ya que esa cautela es fruto de la búsqueda de avanzar solamente en cuanto a puntos ya solidificados en el constitucionalismo comparado y que atenta a las peculiaridades y necesidades de las sociedades de cada país.
12. Desde la década del 70´del siglo XX hay legislaciones específicas, de fuente nacional e internacional, para regular la manipulación por parte de la informática de datos personales. Las primeras legislaciones se caracterizan por ser dirigidas a los poderes públicos y estar fundadas en medidas de carácter eminentemente preventivo, intentando impedir el registro y uso de los datos. También en la segunda fase legislativa existe una protección eminentemente *estática*, de impedimento al acceso de los datos. Pero se agrega la jerarquización de la relevancia de los datos personales, con la fijación del carácter *sensible* de algunos y el inicio del fortalecimiento de derechos a los afectados, como la posibilidad de *acceso* y *rectificación*. La tercera (y actual) generación legislativa está marcada por la profundización

de esas posibilidades de control procesal y administrativo, que fortalece las medidas represivas por la insuficiencia de la concentración en medidas preventivas.

13. En lo que respecta a la legislación internacional en el ámbito del Consejo de Europa las primeras iniciativas datan de 1973/74, con *recomendaciones* a los gobiernos de Estados miembro en pro de un mayor cuidado con la veracidad y seguridad de las bases de datos en estos basados. También a partir de 1974 la OCDE inicia gestiones en pro de la regulación internacional del flujo de informaciones entre países, culminando con una *recomendación* suya en 1980, en que atenta a la insuficiencia, no obstante la importancia, de las legislaciones simplemente nacionales ya existentes. Sin embargo, aunque avanzada, igualmente esa norma padecía de su carácter no vinculante.
14. La primera iniciativa más ambiciosa en el plano internacional le cabe al Convenio Nº 108 de 1981 del Consejo de Europa, al imponer la internalización a los países que lo ratifiquen y al abrir adhesión a países no europeos. Además, el Convenio apostó por tratar de estándares mínimos, sin perjuicio de que los países adherentes extendiesen la protección. Así debe ser entendido su ámbito, al principio involucrando solamente los tratamientos automatizados y teniendo como protegidos a las personas físicas.
15. El concepto de *calidad* de datos es definido, para imponer que la información personal archivada debe ser recogida de forma leal y en cantidad y duración en concordancia con el fin perseguido. Igualmente se habla de *seguridad* de los datos y en la relevancia de una categoría de datos *sensibles*.
16. El particular es protegido por la *publicidad* de los registros y por sus

derechos de *acceso* y posible *rectificación* y *cancelación*. Hay una indicación de la importancia de instancias administrativas nacionales de apoyo al ciudadano (las futuras Agencias Nacionales de Protección de Datos) e de valores que justificarían limitaciones al derecho.

17. Pero, exactamente la flexibilidad en el uso de principios y cláusulas generales que buscaba facilitar la adhesión de países interesados, perjudicó la uniformidad en las transposiciones legislativas al orden interno, perjudicando el establecimiento del intencionado régimen común.
18. Este orden más uniforme de la protección de datos personales se consigue con la edición de la Directiva 95/46/CE dentro de la Unión Europea, exactamente respaldada por la importancia de regular el tráfico de datos dentro del mercado común. Esta norma, que debía ser obligatoriamente introducida en el ordenamiento de cada país, buscó el balance entre la concesión de facultades a los individuos afectados con el mantenimiento de importantes posibilidades de límites para facilitar la acción estatal.
19. La Directiva se dirige a proteger a las personas físicas y, en cuanto a estas, tiene amplia aplicación, ya sea el tratamiento de sus datos automatizados o no automatizados. La exclusión de los archivos domésticos tiene refuerzo de una importante decisión del TJCE en el caso *Lindqvist*, al conceptuarlos como aquellos absolutamente relacionados con situaciones claras de la vida privada, sin acceso a extraños.
20. La idea principal de obtención y uso de los datos con *calidad* se repite, y se agregan dispositivos sobre la forma del *consentimiento* a ser dado por el afectado en cada hipótesis y el nivel de información previa que él debe presuponer.

21. Los derechos del individuo son expandidos para *acceso, rectificación, supresión, bloqueo y oposición*, más allá de *no verse sometido a decisiones automatizadas*.
22. En el artículo 25 de la Directiva 95/46/CE existe el establecimiento de requisitos para transferencias internacionales de datos a países no sometidos a la directiva, lo que requiere que proporcionen una "protección adecuada" a los datos de los individuos. Hay aquí, en cuanto al sector público, una apuesta a la relevancia de las redes transnacionales y en su capacidad de ser reproductoras e impulsadoras de buenas prácticas en la defensa de los derechos humanos.
23. En el análisis de la *protección adecuada* de cada país son observados el respeto a los principios de la protección de datos y a los derechos relativos a los individuos, y si existen medios compatibles para garantizar el contenido material de la protección. Esto, sin embargo, no exige una protección *equivalente* a la europea, y se abre espacio a las peculiaridades de cada sociedad.
24. En esa posible certificación se estimula un derecho constitucional de cooperación, fundado en los derechos humanos y en los desafíos comunes, y de gran significado económico y ético para los países que asuman la recepción del derecho comunitario en la protección de datos personales.

4- Las legislaciones nacionales de Alemania, España y Brasil en la protección de datos personales

Un estudio que se destina a comparar la plataforma jurídica sobre protección de datos en la Unión Europea, específicamente en dos países europeos, como son los casos de España y Alemania, con la defensa del ámbito individual que existe en Brasil, debe terminar enfrentando la cuestión central, es decir, cómo se verifica la existencia de protección a los derechos, sí determinadas posiciones jurídicas están garantizadas (y cuánto están) en el orden jurídico de cada nación.

El término "derecho a la protección de datos", por tanto, se refiere aquí inicialmente a la habitual definición de "derecho jurídico subjetivo". El texto se centrará en analizar, en los ordenamientos estudiados, quienes son los sujetos titulares de facultades con relación a sus datos almacenados en bases de datos de otros. Abstractamente, ello involucra analizar sí hay una *pretensión* jurídica reconocida por el derecho objetivo, cuáles son los contenidos de esa posición jurídica[503], sus límites y sus garantías.

[503] Utilizando la taxonomía de HOHFELD, podemos decir que, tal cual otros derechos, cuando se habla de forma que abarque un "derecho a la protección de datos" en verdad tratamos de 4 diferentes categorías. Así, encontraremos en las normas, utilizando su terminología, *derechos*, caso haya una correspondiente obligación de alguien de proporcionar un bien al titular; *privilegios*, cuando haya la libertad del titular de hacer algo o se abstenga, o sea, ausencia de obligación; *poderes* de formar relaciones jurídicas e *inmunidades* con relación a los poderes de otros. Por tanto, inmunidades se contraponen a poderes como privilegios se contrapone a derechos (HOHFELD, Wesley Newcombe. *Fundamental legal conceptions as applied in judicial reasoning : and other legal essays*. New Haven: Yale University Press, 1920, p. 36-50.).

4.1 La función del legislador en los derechos fundamentales

4.1.1 La configuración de derechos

La interpretación de los derechos fundamentales realizada por el legislador, son de carácter político, así como todas las demás interpretaciones suyas de la Constitución, y las mismas se suceden a través de una ley por él creada[504]. El parlamento complementa el poder constituyente, garantizando las condiciones de realización del texto constitucional, a través de una regulación del derecho que sea *posible* dentro de su marco constitucional. En esa regulación puede estipular garantías procesales e institucionales al derecho, limitarlo ante otros bienes constitucionales e inclusive *configurarlo*[505].

Estas acciones del legislador deben ser vistas como fruto de una vinculación suya a los derechos fundamentales que no se limita a la visión liberal de que las intervenciones son impedidas[506]. Todos los órganos del Estado deben funcionar como defensores y protectores de cada derecho fundamental, no como sus enemigos[507].

---

504 PÉREZ ROYO, Javier. *Curso de derecho constitucional*... *cit.*, p. 119.

505 CRUZ VILLALÓN, Pedro. "Derechos Fundamentales y Legislación." In *La curiosidad del jurista persa, y otros estudios sobre la Constitución*. Madrid: Centro de Estudios Políticos y Constitucionales, 2006, p. 247. Configurar y limitar corresponden, respectivamente, a dos sentidos posibles que el término "concretizar" puede tener para el legislador. En la primera acepción de "concretizar" el legislador ayuda a definir el ámbito de protección del derecho fundamental, mientras en la segunda decide preferencias entre bienes constitucionales. En ese sentido BLANCA R. RUIZ. (*Privacy in telecommunications : a European and an American approach*. The Hague , Boston: Kluwer Law International, 1997, p. 90.)

506 BETHGE, Herbert, WEBER-DÜRLER, Béatrice, SCHOCH, Friedrich K., e TRUTE, Hans-Heinrich. *Der Grundrechtseingriff*. Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 57. Berlin ; New York: de Gruyter, 1998, p. 14-15.

507 HESSE, Konrad. "Significado de los derechos fundamentales... *cit.*, p. 95.

La propia noción de protección de derechos fundamentales a través de un "ámbito normativo" incita tal idea, ya que las "realidades" se tornan defendidas a través del código jurídico, o sea, a través de la concesión al individuo de una serie de libertades, prestaciones, instituciones y procedimientos. Es por medio de esos efectos jurídicos que concebimos que una norma *ius-fundamental* garantice cierto campo de la realidad humana[508].

En el campo de la legislación, se destacan las regulaciones de organización y procedimiento en pro de conceder eficacia práctica a derechos fundamentales. Ese "design" (*Ausgestaltung*) de derechos fundamentales puede coincidir parcialmente con una "concretización" (*Konkretisierung*)[509]. Pues también en el ámbito material de derechos fundamentales hay algún espacio de precisión y diferenciación para el legislador. Derechos fundamentales pueden ser "acuñados" por la norma en mayor o menor medida conforme la relación que su objeto tenga con conceptos pre-jurídicamente sedimentados. Derechos fundamentales como la libertad artística, de conciencia y científica tratan acerca de elementos materiales con profunda significación en las realidades sociales, políticas y culturales de la sociedad, como son las nociones de arte, conciencia y ciencia, y así conceden poco espacio para una densificación por el intérprete. Al contrario, el concepto de "debido proceso legal" o de las garantías institucionales como "ciudadanía", "propiedad" y "matrimonio" poseen un espacio mucho más amplio para la actuación del legislador.

---

[508] GOMES CANOTILHO, José Joaquim. *Direito Constitucional e Teoria Da Constituição*. Coimbra: Almedina, 1993, p. 633.

[509] HESSE, Konrad. *Elementos de direito constitucional da República Federal da Alemanha... cit.*, § 303 e ss. En el Tribunal Federal Alemán el precursor en que dicho tema se presentará con clareza fue el voto particular de los jueces Helmut Simon y Herman Heußner en BVerfGE 53, 30 (71) .

Detalladamente en cuanto a las *formas* de conformación (o configuración) por el legislador, LERCHE dice que en la determinación del contenido y carácter de un derecho fundamental (*Grundrechtsprägung*) podemos encontrar, en el mayor grado de indeterminación de la realidad, normas que verdaderamente *constituyen* el derecho fundamental, a través de la determinación de contenido y regulación, lo que sucedería, por ejemplo, en conceptos constitucionales típicamente jurídicos, como el de "propiedad", o en mandatos constitucionales amplios al legislador, como los referentes a la libertad de profesión de la Ley Federal de Bonn (Art. 12 I GG). Ya, otras normas *concretizarían* los derechos fundamentales, cuando aclaran (*verdeutlichen*) ciertas definiciones constitucionales (como el significado exacto de "reunión), especialmente cuando esa opacidad provenga de evoluciones sociales y tecnológicas; cuando extendieran los efectos de protección de los derechos fundamentales a la amenaza de terceros; cuando tornen posible el ejercicio real por el individuo del derecho fundamental, a través de presuposiciones de organización e instrumentos procesales; o cuando, de manera más fluida, definieran los contornos de la libertad de acción del individuo[510].

En la tipología de KLAUS STERN hay cinco grandes grupos de derechos fundamentales que piden la acción legislativa: derechos que dependan intrínsecamente de una determinada organización o procedimiento, como en el caso de la "objeción de conciencia" y del "derecho de petición"; derechos fundamentales cuya materia afecta al derecho procesal; derechos cuyas reglas de organización y proceso son instrumentales para provocar sus efectos de manera inmediata, como en la libertad de radiodifusión y en la libertad de investigación y docencia universitaria; derechos contradictorios, como

[510] LERCHE, Peter. "Schutzbereich, Grundrechtsprägung, Grundrechtseingriff." In *Handbuch des Staatsrecht der Bundesrepublik - Bd.V : Allgemeine Grundrechtslehren*, organizado por Josef Isensee y Paul Kirchhof. Heidelberg: Müller Juristischer Verlag, 1992, p. 762 y sigs.

libertad sindical y propiedad, como medio de delimitarlos; y derechos de participación, para conformar las posiciones relativas al derecho de ser escuchado y a lo contradictorio[511].

DENNINGER ve las relaciones entre derechos fundamentales y sus reglas de organización y procedimiento divisibles en cuatro grupos, conforme el propio proceso sea el objeto de la norma ius-fundamental; si el ejercicio del derecho fundamental en un caso concreto depende de un procedimiento, como forma de controlar su utilización; o para cotejarla con derechos de terceros o intereses generales; y, por último, si el derecho involucra la coordinación de diversos titulares al mismo tiempo, como medio de organizar las voluntades y participación[512].

En todos los casos hay una "colaboración inter-normativa" entre Constitución y legislador en el campo de los derechos fundamentales, compuesta por una "prefiguración" por los poderes constituyentes que es complementada por una "configuración" legal[513]. Y es en esa vigilancia de los límites legislativos que actúan Tribunales Constitucionales[514], asegurando que el ámbito de protección que la Constitución normativamente prevé no sea suplantado y, al contrario, que justifique esa actuación legislativa. Ese control es absolutamente más intenso conforme sea menor el margen de conformación del legislador[515].

---

511 STERN, Klaus. "Idee und Elemente eines Systems der Grundrechte." In *Handbuch des Staatsrecht der Bundesrepublik - Bd.V : Allgemeine Grundrechtslehren*, organizado por Josef Isensee y Paul Kirchhof. Heidelberg: Müller Juristischer Verlag, 1992, p. 82.

512 DENNINGER, Erhard. "Staaliche Hilfe zur Grundrechtausübung." In Handbuch des Staatsrecht der Bundesrepublik - Bd.V : Allgemeine Grundrechtslehren, organizado por Josef Isensee y Paul Kirchhof. Heidelberg: Müller Juristischer Verlag, 1992, p. 296.

513 CRUZ VILLALÓN, Pedro. "Derechos Fundamentales y Legislación... *cit.*, p. 252.

514 PÉREZ ROYO, Javier. *Curso de derecho constitucional... cit.*, p. 119.

515 MEDINA GUERRERO, Manuel. *La vinculación negativa... cit.*, p. 25.

Esto significa que se puede hablar solamente de *gradación* en la determinación jurídica (*rechtsgeprägt*) o en la determinación material (*sachsgeprägt*), ya que, por un lado, todos los "ámbitos de vida materiales" sólo se *fundamentan bajo* una Constitución Jurídica y, por otro, que inclusive conceptos cuya juridicidad no dependa de una "realidad natural" son tributarios de una evolución histórica. Por eso que en ambos casos hay zonas grises de interpretación, como en las hipótesis de aborto y eutanasia en cuanto al derecho a la vida y del concepto de matrimonio en cuanto a la necesidad de heterogeneidad de género, por ejemplo. Aunque, siempre la adecuada interpretación, tanto a través de leyes o de sentencias, de los comandos contenidos en el orden constitucional debe ser realizada con base a la idea de Derecho de ella advenida, y no a través del orden legal anterior y posterior[516].

De todo modo, la regulación emitida por el legislador no debe resultar en una desvalorización del contenido material del derecho fundamental[517]. La configuración de un derecho fundamental depende, así, de que el carácter prescriptivo de la norma de derecho fundamental sea insuficiente, pero también de que la solución legislativa presentada no entre en conflicto con la Constitución[518].

Bajo esas condiciones, hay, un derecho de menor contraposición con una realidad fáctica o histórica, como la protección de datos, un espacio claro donde el legislador actúa reforzando y actualizando el marco constitucional de los derechos

[516] Sobre el tema, vide REIS NOVAIS, Jorge. *As restrições aos direitos fundamentais não expressamente autorizadas pela constituição*. Coimbra: Coimbra Editora, 2003, p. 163 e sigs, NIERHAUS, Michael. "Grundrechte aus der Hand des Gesetzgebers?." *AöR 116*, 1991, p. 83 y VIEIRA DE ANDRADE, José Carlos. *Os direitos fundamentais na constituição portuguesa de 1976*. Coimbra: Almedina, 2001, p. 214 y sigs.

[517] BVerfGE 63, 131 (143).

[518] GAVARA DE CARA, Juan Carlos. *Derechos fundamentales y desarrollo legislativo: la garantía del contenido esencial de los derechos fundamentales en la Ley fundamental de Bonn*. Madrid: Centro de Estudios Constitucionales, 1994, p. 161.

fundamentales, exigencia que es impuesta por la propia Constitución y en la que funciona como *configurador* de esos derechos, influyendo en titulares, destinatarios, objeto y garantías, y cuyo contrapunto son las posteriores *limitaciones* de esos derechos ya configurados[519].

La *configuración* legislativa de un derecho fundamental consiste, por tanto, en la puesta en práctica de las abstracciones constitucionales, dando lugar a la determinación de facultades y poderes que integran el derecho. El legislador maniobra aquí dentro de los límites que se ajusten dentro del "modelo dogmático construible a partir de la definición abstracta"[520]. Y aquí se debe observar la práctica, la doctrina y, antes que nada, el entendimiento del Tribunal Constitucional[521].

4.1.2- Limitaciones (o Intervenciones) legislativas en los derechos fundamentales.

Las libertades no son absolutas. La convivencia en sociedad exige que haya restricciones en determinadas situaciones en pro de otros derechos individuales o de necesidades del orden público y de bienes de interés colectivo predominante. Ese margen de coordinación es, en primer lugar, atribución del legislador, el cual tiene aquí un amplio margen para tomar las decisiones consecuentes dentro de las urgencias de aquella población, territorio y momento histórico. La existencia de restricciones a

[519] GAVARA DE CARA, Juan Carlos. *Derechos fundamentales y desarrollo legislativo... cit.,* p. 158.
[520] OTTO Y PARDO, Ignacio de. "La regulación del ejercicio de los derechos y libertades. La garantía de su contenido esencial en el artículo 53.1 de la Constitución." In *Derechos fundamentales y Constitución*. Madrid: Civitas, 1988, p. 160.
[521] LERCHE, Peter. "Schutzbereich, Grundrechtsprägung, Grundrechtseingriff... *cit.*, p. 741

derechos es imposición inherente de la obligación de gobernar[522].

Existe así la necesidad de coordinar las posiciones individuales dignas de protección con el bien común, lo que envuelve, como repetidamente veremos, un método explícito de ponderación por parte de la Jurisprudencia, pero también un proceso implícito en las elecciones legislativas y que, bajo el control último de los tribunales con esa competencia, no debe ser meramente menospreciado, bajo pena de no ser consideradas por las mayorías democráticas[523]. En el campo de la defensa del individuo y de la sociedad frente al uso de las nuevas tecnologías hay un inherente estado de duda en la corrección de las elecciones judiciales y legislativas, ya que las respuestas son tomadas en cuanto a fenómenos recientes y, aún cuando las mismas sean adecuadas, corren el riesgo de rápidamente tornarse obsoletas por el progreso continuo de la propia técnica antes regulada[524], aunque ello no puede servir de impedimento para que la jurisdicción verifique, en primer plano, la conformidad o lesión de alguna posición ius-fundamental[525].

La *limitación* (o legítima *intervención*)[526] de un derecho fundamental está en

---

[522] BRAGE CAMAZANO, Joaquín. *Los límites a los derechos fundamentales*. Madrid: Dykinson, 2004, p. 37.

[523] BOROWSKI, Martin. *La estructura de los derechos ... cit.*, p. 60.

[524] LEVY, Joshua S. "Towards a Brighter Fourth Amendment: Privacy and Technological Change". *New York University Law and Economics*, paper 279, p. 38. Un debate que aprehende bien las restricciones que existen de parte a parte en la actuación del Judicial y Legislativo en las nuevas tecnologías ocurre entre ORIN KERR ("The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution". *Michigan Law Review*, marzo 2004) y DANIEL SOLOVE ("Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference". *Fordham Law Review*, Winter 2005.).

[525] Tiene razón SWIRE al declarar que, aunque sea deseable el *diálogo* entre los Poderes cuando entran en conflicto derechos del hombre y nuevas tecnologías, eso no debe significar olvidar el deber de las cortes de impedir la opresión del individuo por las "pasiones de las mayorías" (SWIRE, Peter. "Katz is Dead. Long Live Katz". *Michigan Law Review*, marzo 2004, p. 922).

[526] Términos que se permiten ser usados como sinónimos. Vide BODO PIEROTH, y BERNHARD SCHLINK (*Grundrechte*. Heidelberg: C. F. Müller, 2009, p. 62) y KLAUS STERN (*Das Staatsrecht der Bundesrepublik Deutschland Bd III2*. Vol. 2. München: Beck, 1994, p. 225).

sentido contrario al de su configuración[527]. En la configuración se abren posibilidades de ejercicio por parte del titular, reforzando su alcance sobre el ámbito normativo en la vida real[528]. Ya las normas jurídicas que vehiculan limitaciones son aquellas en que las consecuencias del ámbito normativo total o parcialmente se ven negadas a la persona que la gozaría[529].

La regulación específica del procesamiento de datos en órganos públicos es indudablemente más numerosa y detallada que la referente a emprendimientos privados. Ello se explica, inicialmente, por la necesidad de que la administración pública siempre actúe fundada en una ley, al contrario de la libertad general de acción del particular[530].

En la limitación de los derechos fundamentales, la exigencia de la *reserva de ley parlamentaria*, ante todo, salvaguarda la importancia de las legítimas estructuras democráticas de formación de la voluntad política, resaltando su relevancia para la definición de las decisiones fundamentales de la nación[531]. En ese sentido, en especial cuando no hay expresa reserva de ley en cuanto al derecho fundamental en la Constitución, es necesario investigar cuáles son los otros derechos, bienes y valores constitucionales que puedan constituir *límites inmanentes*[532]. En el caso de la protección de datos y las intervenciones permisibles a la Administración Pública queda clara la preocupación del legislador en brindar al servicio público los medios legales suficientes

[527] STERN, Klaus. *Das Staatsrecht der Bundesrepublik Deutschland Bd III2*. Vol. 2. München: Beck, 1994, p. 17.
[528] BRAGE CAMAZANO, Joaquín. *Los límites ... cit.*, p. 73.
[529] PIEROTH, Bodo, y SCHLINK, Bernhard. *Grundrechte.. cit.,* p. 62.
[530] BVerfGE 6, 32 (36). Esa cuestión de la necesidad de conocimiento por el ciudadano de las hipótesis de limitación de su derecho a la autodeterminación informativa, a propósito, fue particularmente resaltada por el Tribunal Constitucional alemán en la sentencia del Censo - BVerfGE 65, 1 (44).
[531] HESSE, Konrad. *Elementos de derecho constitucional de la República Federal de Alemanha... cit.,* p. 386.
[532] STERN, Klaus. "Die Grundrechte und ihre Schranken". In *Festschrift 50 Jahre Bundesverfassungsgericht II*, organizado por Peter Badura y Horst Dreier. Tübingen: Mohr Siebeck, 2001, p. 15.

para su acción con eficiencia, y así, demarcar los campos legítimos de interferencia en el derecho a la protección de datos, alcanzando especial relieve cuando la actuación es bastante frecuente y pronunciada, como en el derecho de policía[533]. Al mismo tiempo, tal postura demuestra una vez más la inexistencia de relaciones especiales de sujeción privilegiadas al sometimiento de la Administración a la ley[534].

Especialmente en el derecho alemán, la responsabilidad del legislador en esa actividad se ve reforzada por la existencia de la obligación por el Tribunal Constitucional de que todas las decisiones "esenciales" sobre derechos fundamentales deben ser efectivamente tomadas por el Parlamento[535]. Esto no equivale, sin embargo, a la dependencia de un hiper - especificación, de difícil implementación en la práctica y contraproducente al interés de la propia sociedad, sino de la búsqueda de un incremento de la densidad normativa en pro del máximo de clareza y precisión[536]. El uso, bajo esos parámetros, de cláusulas generales y conceptos indeterminados, sin excesos de vaguedad, sirve para permitir que la Administración tenga los subsidios para ejercer sus funciones con la agilidad y adaptabilidad que exige la situación en concreta[537].

Estos límites inmanentes son, finalmente, también sometidos a sus propios límites de intensidad, en sí, la producción de una *concordancia práctica* entre los valores abrigados por la Constitución que concede a cada uno su *optimización*, y lo que

---

533 TINNEFELD, Marie-Therese, EHMANN, Eugen, , y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*, p. 465.

534 HUFEN, Friedhelm. *Staatsrecht II - Grundrechte*. München: Beck, 2009, p. 118.

535 Como es desarrollado en BVerfGE 47, 46 (79). OSSENBÜHL alerta, sin embargo, del equívoco de observar la "Teoría de la esencialidad" (*Wesentlichkeitstheorie)* como dogma, al contrario de un concepto que provee *topoi* que auxilian a encontrar los límites de la reserva legal en la práctica (OSSENBÜHL, Fritz. "§62 Vorrang und Vorbehalt des Gesetzes". In *Handbuch des Staatsrecht der Bundesrepublik - Bd.III*, organizado por Josef Isensee y organizado por Paul Kirchhof. Heidelberg: Müller Juristischer Verlag, 1987, p. 340).

536 PIEROTH, Bodo y SCHLINK, Bernhard. *Grundrechte.. cit.*, p.66.

537 BVerfGE 56, 1 (12).

se alcanza a través de la verificación de la *proporcionalidad* de la limitación[538]. En un escenario constitucional sus requisitos en esa actividad involucran que la limitación se dé en pro de otros bienes también con valor constitucional y que la ponderación de bienes sea realizada con proporcionalidad. Por tanto, se encuentra fundamentalmente en la jurisprudencia de los Tribunales Constitucionales la declaración de la conformación de su *contenido esencial*, entendido aquí en una concepción *relativa*[539]. En otras palabras, podemos expresar que al mismo tiempo que se identifican los contornos básicos de los derechos fundamentales, -función especialmente más importante tratándose de derechos que necesitan bastante complementación legislativa-, el Tribunal también ejerce el control de verificación en cuanto a las intervenciones desproporcionales y que van más allá de los poderes posibles del Parlamento[540].

4.1.3 Garantías otorgadas por el Legislador

Por último, en la legislación encontramos también instrumentos que fortalecen la protección de los derechos. Son todas estas medidas que impiden que el ámbito normativo se torne una mera declaración de buenas intenciones[541]. Se pueden presentar como medios de recursos provistos al afectado y también como instituciones estatales que tienen como finalidad auxiliar la esfera individual. Su sentido común es combatir

---

538 HESSE, Konrad. *Elementos de derecho constitucional de la República Federal da Alemanha... cit.*, p. 255.

539 Al contrario de una concepción absoluta de contenido esencial que pretende encontrar un núcleo inquebrantable resistente anticipadamente a cualquier tipo de ponderación interventiva legislativa (PIEROTH, Bodo, y SCHLINK, Bernhard. *Grundrechte.. cit.*, p. 73). Sobre el debate entre las teorías absolutas y relativas de contenido esencial vide RODRÍGUEZ RUIZ, Blanca. *El secreto de las comunicaciones...cit.*, p. 107 y sigs. y SCHNEIDER, Ludwig. *Der Schutz des Wesensgehalts von Grundrechten nach Art. 19 Abs. 2 GG*. Berlin: Duncker & Humblot, 1983, p. 155 y ssgs.

540 HESSE, Konrad. *Elementos de derecho constitucional da República Federal da Alemanha... cit*., p. 267 y HÄBERLE, Peter "Grundrechte und parlamentarische Gesetzgebung im Verfassungsstaat" *AöR*, 1989, p. 389.

541 RODRÍGUEZ RUIZ, Blanca. *El secreto de las comunicaciones...cit.*, p. 134.

lesiones (o sea, intervenciones ilegítimas) a derechos, sea impidiéndolas, preventivamente, o sanándolas, de manera represiva. Así, en general, en los derechos fundamentales y aquí en el plano específico de la protección de datos, *garantías de organización*, o sea, instituciones fomentadas en pro de la protección del derecho[542] y propios *medios procesales* puestos a disposición del individuo para proteger su derecho.

En este capítulo, por tanto, también observaremos en la protección de datos las garantías otorgadas en la legislación de cada país. Estas se complementan con las *garantías constitucionales generales*, resultantes de la protección como derecho fundamental, y que pueden ser sintetizadas, en el escenario de Alemania, España y Brasil, de manera común, en la existencia de procedimientos reforzados y vedas de reforma de la Constitución, así como en el control de constitucionalidad de las leyes, en la existencia de una reserva legal para la restricción de libertades y, finalmente, en la existencia de una tutela judicial efectiva para impedir que aquel que se sintiera lesionado en sus derechos quede indefenso.

4.2 El Derecho Alemán a la protección de datos

La historia legislativa de la protección de datos (de hecho, no sólo la protección de los datos, sino también de las amenazas al individuo como consecuencia del uso de estos datos) en Alemania, iniciada en la década del 70 del siglo XX, se confunde con la propia historia de protección de datos. Una historia que alcanza un punto fundamental en la sentencia de *Volkszählung*, del 15 de diciembre de 1983, con

[542] MARTINS, Leonardo e DIMOULIS, Dimitri. *Teoria geral dos direitos fundamentais*. São Paulo: Revista dos Tribunais, 2008, p. 75.

su consagración como figura en el derecho general de la personalidad y en la esfera individual de la intimidad, pero que está lejos de ser un momento anterior o desvinculado de los posteriores avances

La formación de esta *cultura de protección de datos*[543] produjo en Alemania, a lo largo de la década del 70, tres ejemplares importantísimos de las denominadas leyes de primera generación, aquellas que apuntaban al alejamiento del mal uso de los datos, que son las leyes de Länder de Hesse (1970) y Rheinland-Pfaz (1974) y la ley federal de 1977.

La actual ley alemana de protección de datos, con sus modificaciones, es la tercera de este género de naturaleza federal en el país. La primera ley, de 1977, poseía un ámbito más relacionado con el mal uso de los datos personales, pero la ley de 1990 ya observaba también prescripciones en cuanto a la recolección y tratamiento de datos. De esta manera, la ley de 2001 debe ser vista en general como una modernización necesaria luego de una década de vigencia de la regulación, pero principalmente como la profundización y endurecimiento de la normalización germánica sobre bases de datos no públicas, como las de origen privado, sobre bases de datos no automatizadas y en la transferencia de datos a terceros países, todas influencias de la directiva 95/46/CE[544].

La segunda ley federal, de 1990, también es el fruto directo de preocupaciones sociales. En cuanto en la Alemania Occidental, a lo largo de la década del 80, hubo un movimiento de desobediencia civil al censo federal (el *Volkszählungsboykott*), que temía la disminución de las libertades democráticas con las informaciones que

[543] DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz*. Frankfurt am Main: Bund-Verl., 2007, p. 70.
[544] BERGMANN, Lutz, MÖHRLE, Roland, y HERB, Armin. *Datenschutzrecht : Handkommentar zum Bundesdatenschutzgesetz, Datenschutzgesetze der Länder und Kirchen, Bereichsspezifischer Datenschutz*. Stuttgart: Boorberg, 2007, p. 2.

llegarían a las manos del servicio de seguridad; la reunificación trajo la realidad del régimen de la Alemania Oriental, en donde el ciudadano no tenía ningún tipo de derecho de esconder nada de su vida ante el Gobierno. De manera que el enfoque ya no es simplemente en el mal uso, sino en regular toda la recolección y tratamiento de datos. Esta norma representa la *segunda generación* en el escenario alemán. Ya la actual ley federal, de 2001, es un reflejo de la directiva europea de 1995 y del establecimiento de una comunicación mundial de datos al alcance del hombre común, a través de la popularización de internet[545].

En el año 2009 esta ley también sufrió algunas modificaciones, para actualizarla en algunas cuestiones peligrosas para el individuo que fueron surgiendo en la primera década del siglo XXI, como la profundización de la evaluación de crédito (*scoring*) de manera automatizada.

Conforme el Tribunal Constitucional Federal , el "derecho a la autodeterminación informativa"[546] está basado en la dignidad de la persona humana (art.1 abs. 1 GG) y en el derecho a la autodeterminación y al libre desarrollo de la personalidad (art. 2 abs. 1 GG), el ser humano que desconoce quién sabe o qué se sabe sobre él, no tiene las condiciones de superar la inhibición en la vida social y desarrollarse y relacionarse adecuadamente con los demás[547]. La decisión de 1983 consagra en las decisiones del Tribunal el uso de la "teoría de las esferas" (*Sphärentheorie*), lo que significa, desde el punto de vista de la protección de datos,

---

545 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 71.

546 Nótese que el Tribunal también menciona el "derecho fundamental a la protección de datos" (*Grundrecht auf Datenschutz*, como en el BVerfG, Urteil vom 27-06-1991 - 2 BvR 1493/89), lo que justifica la opción aquí adoptada de usar los términos como sinónimos.

547 HUFEN, Friedhelm. "Das Volkszählungsurteil des Bundesverfassungsgerichts und das Grundrecht auf informationelle Selbststimmung" *Juristenzeitung*, 1984, p. 1074.

que no hay ninguna información, estando o pudiendo estar o que sea refiera a la esfera íntima, privada o pública, que no esté bajo la dependencia de la autorización del individuo afectado por su uso, tratamiento o transferencia[548].

A pesar de que este derecho no haya ingresado formal y expresamente en la ley fundamental alemana, fue admitido en diversas constituciones estatales, a saber la de Saarland (art. 2), Nordrhein-Westfalen (art. 4.2), en la Constitución de Berlín de 1995 (art. 33), de Brandenburg (art. 11.1), de Mecklenburg-Vorpommern (art. 6.2), de Rheinland-Pfalz (art. 4a), de Sachsen (art. 33), de Sachsen-Anhalt (art. 6.1) y de Thuringen (art. 6.4). Además de esto, mereció tratamiento exclusivo en el artículo 8º de la Carta de Derechos Fundamentales de la Unión Europea[549].

4.2.1 Régimen Jurídico de la ley federal alemana de protección de datos (*Bundesdatenschutzgesetz* - BDSG) de 2001

4.2.1.1 Ámbito de aplicación

El apartado 1 del artículo 1º desde ya observa que el objetivo de la ley es garantizar al individuo que no sufra consecuencias sobre su personalidad por la utilización de sus datos personales. De esta manera, esta primera definición ya parece querer alejar cualquier duda sobre el sentido de "protección de datos", que es la de garantizar la *autodeterminación individual*. También esta preocupación central sobre el tema se encuentra expresada en el art. 1º de la directiva 95/46/CE.

[548] DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 73.
[549] SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 113.

La Bundesdatenschutzgesetz (a partir de ahora utilizaremos la siguiente abreviatura BDSG para referirnos a la misma) debe ser entendida como una ley de protección amplia, cuyos efectos son aplicados sobre diferentes ramas del derecho, especialmente la del derecho del consumidor[550] y en las relaciones laborales. Su aplicación se extiende tanto a las bases de datos públicas como a las privadas (art. 1.2), salvo si el tratamiento se extiende solamente en ámbitos personales o familiares (art. 27 apartado 1 s.2 de la BDSG y art. 3.2. de la directiva).

El apartado 3 del artículo 1º trata sobre la *subsidiariedad* de la BDSG, que ocurre solamente cuando otra ley federal trata específicamente sobre un asunto vinculado a su objeto, independientemente del nivel de complejidad que tenga la regulación[551]. La segunda parte de este apartado mantiene cualquiera de los deberes de secreto de informaciones recibidas que tengan fundamento en otras normativas, como en el caso de los datos fiscales (§ 30 del *Abgabenordnung*), estadísticos (§ 16 del *Bundesstatistikgesetz – BstatG*) o el secreto médico, cuyo deber de silencio está impuesto por el § 203.1 del Código Penal (*Strafgesetzbuch*).

Además hay momentos en que la propia BDSG limita su aplicación, tal como cuando subordina los derechos de rectificación, supresión, bloqueo y oposición en caso de que se pretenda socavar o perjudicar la recepción de documentos para la finalización de la inscripción de los documentos históricos del Archivo Federal (*Bundesarchiv*)[552]. Esto no significa, sin embargo, que este órgano no tenga que observar los intereses de las partes afectadas en los papeles con datos personales que debe recibir (apartado 9 del

[550] WEICHERT, Thilo. "Verbraucher-Scoring meets Datenschutz." *Datenschutz und Datensicherheit - DuD*, 2006, p. 399.
[551] GOLA, Peter, y SCHOMERUS, Rudolf. *Bundesdatenschutzgesetz*. München: Beck, 2005, p. 82.
[552] DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 370.

§ 20 combinado con el apartado 3 del § 2 de la *Bundesarchivgesetz*).

En especial, hay una serie de leyes relativas a los órganos de seguridad que exceptúan la aplicación de la BDSG (§ 12 y siguientes de la BVerfSchG[553], a la cual se remite también el § 7 de la MADG[554] y el § 5 de la BNDG[555], § 32 de la BKAG[556] y § 22 de la SÜG[557]), aunque con apenas una mayor flexibilidad de plazo en cuanto a las situaciones de corrección, eliminación y bloqueo de los datos personales[558].

El criterio de fijación de aplicación de la ley no es territorial en cuanto al lugar del tratamiento de los datos, sino, conforme el artículo 4º de la directiva que es traspasado en el apartado 5 del artículo 1º, de verificación de la ubicación del responsable, aun siendo una filial o agente contratado por otro[559].

Los artículos 2º y 3º de la BDSG se prestan a definir legalmente algunos conceptos necesarios para su interpretación.

Inicialmente el artículo 2º concede su noción de público y privado para los fines de la ley. Esta diferenciación, desde el punto de vista de sus regímenes generales, se convierte paulatinamente más tenue, ya que la visión de que, al referirse a relaciones

---

553 „Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz“ (ley de cooperación entre esfera federal y provincial en la protección constitucional y de la oficina federal).

554 “Gesetz über den militärischen Abschirmdienst“ (ley de la contra inteligencia militar)

555 “Gesetz über den Bundesnachrichtendienst“ (ley del servicio de información federal)

556 “Bundeskriminalamtgesetz“ (ley de la agencia criminal federal).

557 “Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes“ (ley de los chequeos de seguridad federal).

558 También las policías de los estados federados tienen normas de plazo propias en este tema. Sin embargo, existe doctrinariamente la convicción de que ello no significa la permisión del uso por parte de la policía de datos sospechosos fuera de las finalidades con relación a las cuales ellos fueron recogidos (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 956).

559 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 103.

entre dos entes "iguales", las relaciones particulares no deberían estar limitadas por la BDSG, fue superada por la realidad de las grandes fuerzas económicas que manejan datos personales, el endurecimiento del tratamiento que desde hace tiempo era exigido por la doctrina[560]. Esta diferenciación, así y todo, marca además cuáles son bases de datos que, siendo públicas, sufrirán el influjo de las reglas sectoriales de la 2ª Sección de la BDSG (§§ 12 a 26), y cuáles merecerán normas específicas en los §§ 27 a 38a de la 3ª Sección.

Son titulares de bases de datos públicas las consideradas instituciones públicas, en la forma del criterio de otras leyes administrativas alemanas, es decir, por el ejercicio de *Administración Pública*, que se encuentra presente en el apartado 4 del § 1 de la Ley de Proceso Administrativo (*Verwaltungsverfahrensgesetz – VwVfG*) y en el apartado 2 del § 1 del libro X del *Sozialgesetzbuch*; órganos de funciones vinculadas a la Justicia (*rechtspflege*), como los Tribunales y la Procuraduría Pública, sociedades empresariales privadas que desempeñan funciones públicas[561] ("actos de imperio" - "hoheitliche Aufgaben der öffentlichen Verwaltung", 2ª parte del apartado 4 del § 2º); y cualquier otra organización de derecho público como el *Bundesrat*, el *Bundestag*, el *Bundesagentur für Arbeit*, etc., salvo sociedades religiosas, que poseen el privilegio de regulaciones propias de protección de datos[562]. Desde el punto de vista de la BDSG, sólo importan los entes federales ya que los órganos públicos de los *Länder* no se encuentran en su campo de aplicación (art.2 párrafo 2).

Las asociaciones de derecho privado que involucran a órganos públicos (en

[560] Vide SIMITIS, Spiros. "Privatisierung und Datenschutz." *Datenschutz und Datensicherheit - DuD*, 1995, p. 648.

[561] El *Bundespost* no es considerado en ese caso, pero se consideraba como base de datos públicos debido a su ejercicio de monopolio comercial (§2, apartado 1, 2ª parte). Aunque este monopolio fianlizó el 31 de diciembre de 2007, conforme el § 51 del *Postgesetz*.

[562] DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 107.

tareas de administración pública) generalmente son direccionadas para coordinar y efectuar la construcción y el mantenimiento de infraestructuras, como las de tránsito o energéticas, y sólo serán reguladas por la ley federal en caso de que involucren a un territorio más allá de uno de los estados o que tengan capital mayoritariamente federal (art. 2, párrafo 3), pero sus bases de datos también son consideradas como públicas. Los archivos de las demás personas naturales y jurídicas son tratados como privados (art. 2, párrafo 4).

El art. 3 de la ley federal alemana busca establecer una definición modelo de algunos términos que son esenciales para su entendimiento. En primer lugar (en el apartado 1 de este § 3), así como la ley española, define a *dato personal* como aquél que sea determinado o determinable a un individuo[563]. Una imagen o grabación de video que pueda identificar a un ser humano, de esta manera, también puede ser presentado como un *dato individual* y afectar la "autodeterminación informativa"[564]. Por eso, el contenido del monitoreo de áreas accesibles al público por cámaras está regulado en el § 6b[565]. Ya los datos filmados por entes privados estarán regulados por la ley federal de protección

[563] Aunque el concepto de *determinable* sea tal cual en España aquel que pueda ser relacionado con base en otros elementos a cierto ser humano, hay controversia si ello es verificable de manera objetiva (en ese sentido DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 111) o relativamente conforme a las condiciones propias de quien maneja la información (GOLA, Peter, y SCHOMERUS, Rudolf. *Bundesdatenschutzgesetz... cit.*, p. 105). La primera opción parece más acorde con la ley, sea porque aumenta la protección, pero también porque reconoce el natural flujo comunicativo de las informaciones, que aun hoy anónimas, pueden caer en el futuro en las manos de quien pueda identificarlo.

[564] VG Karlsruhe, 10.10.2001, NVwZ 2002, 117.

[565] El uso de cámaras de video en lugares públicos se justifica por el efecto disuasivo sobre la criminalidad y el fortalecimiento de la seguridad del ciudadano que proporciona, lo que explica la necesidad de alertar que hay una cámara en grabación y su controlador (apartado 2 del § 6a de la BDSG). Sin embargo, espacios públicos también son los lugares de mayor interrelación entre los individuos, típicamente adecuados a la expresión de opiniones (Art. 5.1 GG) y a manifestaciones (Art. 8.2 GG). Por esa razón, la Ley Federal de Protección de Datos establece que las causas para ese monitoreo se limitarán a garantizar a los órganos públicos el ejercicio de sus funciones, para proteger que sólo entren y salgan de propiedades aquellos autorizados y a otras concretas finalidades con legítimos intereses de entidades privadas (apartado 1 del § 6b). Esas finalidades son absolutamente vinculantes, con excepción de las imágenes, serán utilizadas para asegurar la paz pública o la persecución de crímenes, y también requisita que haya una ponderación con los intereses del afectado (apartado 3 del mismo artículo).

de datos en caso de que estén sujetos a archivo[566] y no tengan objetivos meramente personales o domésticos (§ 1, apartado 2, núm. 3 de la BDSG).

Al contrario definen los párrafos 6 a 6a del mismo artículo 3 lo que es "*anominizar" y "seudo anonimizar"* En el primero, se separan los campos de identificación del ser humano de las restantes informaciones convirtiendo, al menos, desproporcionalmente difícil su reunión nuevamente. Ya cuando se "seudo anonimiza" hay un reemplazo de la información identificativa real por una falsa, y está implícita en esta técnica la existencia de una tabla que hace posible la reorganización de los datos, lo cual exige obligaciones adicionales al receptor de las informaciones de manera que no convierta el dato nuevamente de naturaleza personal[567]. Ambas son formas de impedir la clasificación del dato como personal y de esta forma son técnicas privilegiadas por el artículo 3a de la ley, que estimula la menor invasión posible en el manejo de los datos, demostrando el sentido general de la BDSG de privilegiar una regulación atenta a las posibles consecuencias maléficas del uso por parte de otros de las informaciones de los individuos.

La dignidad del art. 1 párrafo 1 de la GG no alcanza a personas no naturales, conforme encontramos consolidado en el Tribunal Federal Alemán (BverfGE 67, 142f., 77, 46f.). Hay, de esta forma, protección por la "autodeterminación informativa" solamente para las personas naturales, excluyendo expresamente a las personas jurídicas del concepto de "datos personales" en el apartado 1 del § 3 de la BDSG. Aun así se

[566] Las grabaciones en lugares de trabajo son admisibles en pro de la necesidad de seguridad del establecimiento, como se da en museos o en una usina nuclear. Sin embargo, se impone que haya áreas no sujetas a grabación para que el trabajador pueda aprovechar sus horarios de reposo (DÄUBLER, Wolfgang. *Gläserne Belegschaften? : Datenschutz für Arbeiter, Angestellte und Beamte*. Köln: Bund-Verl., 1987, p. 152).

[567] Vide, en ese sentido el art. 6.3 de la Teledienstedatenschutzgesetz (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 279)

protegen a sus socios[568] y firmas individuales y se presentan categorías de información sobre la empresa que merecen el secreto por parte de quien las trate, como en la hipótesis de la fiscalización tributaria (§ 30 del AO).

En cuanto a los fallecidos, tampoco se encuentran protegidos por la ley, ya que, si el objetivo legal es defender el desarrollo de la personalidad, esta se deshace con la muerte[569]. Esto no impide que los vivos sean afectados por datos relacionados con los muertos (y que de esto surjan posiciones jurídicas) o que, por ejemplo, una gestante no pueda ser lesionada por la divulgación de informaciones sobre su feto, igualmente desprotegido en la BDSG[570].

La BDSG es bastante amplia en la definición del párrafo 2º en lo referente al tratamiento automatizado de cualquier medio electrónico de procesamiento de información. Por otro lado los medios no electrónicos, o sea, no automatizados, dependerán según la misma norma de que la estructura de almacenamiento permita que haya una elección de las características a ser evaluadas.

Los apartados 3, 4 y 5 definen a la recolección de datos, su tratamiento (que comprende almacenamiento, modificación, transferencia, bloqueo o supresión) y su uso en general, cuando el acto no esté incluido dentro del tratamiento. El *responsable* (apartado 7) será quien efectúe dicha recolección, tratamiento o utilización en general, directamente o a través de quien esté sometido a sus órdenes (*terceros*, conforme el apartado 8, 2ª parte). El *receptor* es la persona u organización que posee el archivo que mantiene las informaciones (apartado 8, 1ª parte). Este archivo, evidentemente, sufre

[568] GOLA, Peter, y SCHOMERUS, Rudolf. *Bundesdatenschutzgesetz... cit.*, p. 106.
[569] BVerfGE 30, 194.
[570] SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 232.

también del influjo de la ley en caso de estar en medios móviles de almacenamiento (apartado 10), tales como *chips* (existentes en forma creciente en tarjetas bancarias o de identificación en general) o *pen drives*[571].

4.2.1.2 Principios sobre la Protección de Datos en el Derecho Alemán

4.2.1.2.1 Principio de la Necesidad

El artículo 3a de la BDSG transmite un principio general en la protección de datos en el sentido de recoger la menor cantidad de informaciones del individuo como sea posible y de privilegiar, en la medida de lo razonable, que tan pronto lo permita su necesaria utilización, los datos sean desvinculados del afectado, ya sea convirtiéndolos en anónimos o por medio de pseudónimos. El principio de la necesidad en el derecho alemán es una consecuencia de la recolección estricta conforme la finalidad prevista en el art. 6, apartado 1, letra "c" de la Directiva Europea[572].

Este dispositivo privilegia una técnica de prevención en la defensa del individuo a través de la máxima *restricción y economía* en el volumen de la recolección, uso y tratamiento de los datos. También apunta a la actualización de la protección, al imponer que los sistemas de información estén siempre configurados teniendo en cuenta este objetivo, lo cual provoca constantes adelantos con el avance de la tecnología[573].

Este artículo fue incluido en la ley en la reforma de 2001, inspirado en el § 3.4

[571] En el § 6c de la BDSG se resalta nuevamente la aplicabilidad de las normas de la protección de datos también en estos medios móviles de almacenamiento y procesamiento.
[572] TINNEFELD, Marie-Therese, EHMANN, Eugen, , y GERLING, Rainer W.. *Einführung in das Datenschutzrecht... cit.,* p. 312.
[573] GOLA, Peter, y SCHOMERUS, Rudolf. *Bundesdatenschutzgesetz... cit.,* p. 127.

de la TDDSG (*Teledienstedatenschutzgesetz*) de 1997, considerada una de las primeras leyes de tercera generación en la protección de datos. Fue además uno de los objetos de la reforma de 2009, para aclarar que se aplica también a bases de datos no automatizadas (en papel, por ejemplo) y para facilitar las condiciones que llevan a la tarea de" anonimizar" y de "seudo anonimizar".

4.2.1.2.2 Principio del Consentimiento

Alrededor del consentimiento se desarrollan las reglas centrales de la ley federal alemana de protección de datos. El § 4.1 de la BDSG establece que larecolección, tratamiento o uso de datos de otros depende de la autorización legal[574] o del consentimiento del afectado.

La definición del *consentimiento* que sea capaz de una *producción de efectos*[575] para los fines de la ley está en el artículo 4a párrafo 1. El consentimiento, independientemente de si la base de datos es pública o privada, depende de la certificación *previa* del afectado sobre la finalidad con la cual su dato es recogido, tratado o usado. El concepto de libre consentimiento abarca que el individuo debe comprender, sin dudas, el objetivo específico para el cual será usada la información y quién la usará, incluyendo cesionarios previsibles. Se convierten en especialmente prohibidas las cláusulas redactadas de forma genérica (como, por ejemplo, "con vistas al

[574] Incluyendo en ese concepto determinaciones provenientes de "negociaciones colectivas de trabajo", a través de la fuerza concedida por el § 4 apartado 1 de la *Tarifvertragsgesetz* (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 320.). En el mismo sentido BAG , NJW (1987), 674. Por otro lado, la existencia de "códigos de conducta" propios en determinados campos de actividades, permitidas por el artículo 27 de la Directiva Europea y por el § 38a de la BDSG, desde que la autoridad de control admita como salvaguardados los derechos de los afectados (apartado 2 del § 38a), son de poca realidad práctica en Alemania y en Europa en general (TINNEFELD, Marie-Therese, EHMANN, Eugen, , y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*,p. 332).

[575] DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 138.

tratamiento por parte de otras empresas"[576]) o autorizaciones "en blanco". Este principio de transparencia en la protección de datos (*Grundsatz der Datentransparenz*) del derecho alemán está inspirado en el art. 2 letra "h" de la directiva europea[577].

Además el consentimiento deberá ser siempre por escrito[578], salvo en situaciones en que esté especialmente justificada la preterición de este medio[579], y deberá ser siempre dado en un documento que se destaque de otros eventuales que se celebren entre el responsable y el afectado[580].

El consentimiento para la recolección de información es siempre dado de forma *personalísima* y puede ser revocado, sin ningún tipo de formalidades predefinidas, con efectos futuros (*ex nunc*)[581], sin perjuicio de que esto eventualmente conlleve responsabilidades civiles contractuales para el individuo afectado[582]. Por otro lado, los menores dependen de la autorización legal de sus representantes para dar el consentimiento para que sus datos sean utilizados (§ 107 del Código Civil de Alemania

---

576 GOLA, Peter, y SCHOMERUS, Rudolf. *Bundesdatenschutzgesetz... cit.*, p. 167.

577 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 140.

578 Pero no obligatoriamente en un medio físico, ya que hay los formularios y aceptación electrónicos. Sin embargo, no son *válidos* consentimientos emanados a través del envío de un fax o un e-mail, pero sí una "firma electrónica", en la forma de la *Signaturgesetz*, § 2 y del BGB, § 126a (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 351). Sobre la *Signaturgesetz* de 2001 vide ROßNAGELROßNAGEL, Alexander. "Das neue Recht elektronischer Signaturen." *Neue juristische Wochenschrift*, 2001, p. 1817 y ssgs.).

579 Son esas las situaciones en que el dato será tratado como anónimo, hipótesis de emergencia o cualquier otro tipo de inmediatez y relaciones comerciales de tiempo ya duradero, especialmente cuando se prevén los beneficios a quien tiene el dato recogido (BERGMANN,Lutz, MÖHRLE, Roland, y HERB, Armin. *Datenschutzrecht... cit.*, § 4a, ítem 87.

580 La severidad de la redacción de la norma no impide que los doctrinadores sobre el tema lamenten la fragilidad real de la posición del consumidor, del deudor bancario, del trabajador, etc. en las negociaciones del día a día (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 339 y DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 136).
La ausencia de manifestación por escrito no debe ser confundida con ausencia de manifestación del consentimiento. Esta continuará existiendo, pero será oral o por actos que conclusivamente acrediten la voluntad del afectado. Ya el silencio no es aceptado, por su ausencia de significado legal y porque es incapaz de alcanzar el grado de clareza necesario al consentimiento en la BDSG (DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 139.).

581 Como expresado en el § 4, apartado 3 de la *Teledienstedatenschutzgesetz*, TDDSG.

582 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 146.

- *Bürgerliches Gesetzbuch* o BGB)[583].

Estas condiciones impuestas por la BDSG para la manifestación de voluntad del afectado no impiden que sea alegado que existieron algunas de las hipótesis de "vicio en el consentimiento" presentes en el Código Civil, como un "error" (§ 119 del BGB) o una "coerción" (§ 123 del BGB)[584]. Hay en la dogmática una preocupación especial en observar la autonomía del consentimiento, una hipótesis en que existan relaciones económicas en las cuales una de las partes es más poderosa que la otra, como en el derecho del trabajador[585] y en las concesiones de crédito por agentes financieros, por medio de "cláusulas de adhesión" (AGB – *allgemeine Geschäftsbedingungen*) (§§ 305 y ssgs. del BGB), destacándose cuando involucran textos de difícil comprensión y clareza (§ 307 del BGB), y en negocios en los que se condiciona la venta de un producto o la prestación de un servicio, a la adquisición de otros bienes o servicios que no tienen relación directa con el que se quiere adquirir[586], como en el campo de las telecomunicaciones[587].

La formación de grandes depósitos de registros privados a través de imposiciones en momentos de fragilidad económica del individuo también se refleja en una serie de prohibiciones a la actuación empresarial en el uso de bases de datos, que se encuentran a partir de los §§ 28 y 29 de la BDSG y que continúan implicando actualizaciones, tal como se vio por el cambio de varios dispositivos en las enmiendas

583 TINNEFELD, Marie-Therese, EHMANN, Eugen, , y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.,* p. 319.
584 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.,* p. 346.
585 Vide BetrVG § 94.
586 En ambos casos se exige que siempre el individuo tenga el poder de conformar el formulario a su voluntad, estableciendo con exactitud cuales datos desea revelar. Vide BGH, Urteil vom 19. September 1985 – III ZR 213/83 (CR 1985, 83).
587 TINNEFELD, Marie-Therese, EHMANN, Eugen, , y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.,* p. 320.

efectuadas en 2009 y 2010.

El § 4a.2 de la BDSG trata sobre la especificidad de algunas colectas de material in situ. En el caso de investigaciones *científicas* (no se incluye aquí a ningún otro tipo, como comerciales, por ejemplo[588]) el consentimiento puede ser no escrito, según lo permitido en el párrafo 1 de este artículo 4a, desde que las circunstancias no lo recomienden, como en el caso de trabajos sobre criminalidad en actividad e inmigrantes. Estas razones que perjudicarían el objeto de la investigación, sin embargo, deben ser documentadas por escrito.

No obstante, la importancia de la libertad científica para la sociedad y el individuo[589] pueden justificar que el propio consentimiento pueda ser dispensado en el caso de que conseguirlo exija un esfuerzo desproporcionado y el interés de la investigación supere eventuales objeciones del afectado en incluir informaciones sobre sí mismo. Esto es autorizado por el § 14 apartado 2 número 9, así como por el § 28 apartado 6 núm. 4, § 29 apartado 5 y § 40[590].

Ya para los "datos sensibles" (§ 4a.3), definidos en el § 3 apartado 9 como aquellos que tratan sobre el origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, pertenencia a sindicatos, la salud o la vida sexual, la persona de la cual se recoge dicha información debe ofrecer consentimiento *expreso* sobre los datos *concretos* recogidos. Existe una polémica sobre sí este consentimiento especial referido a los datos sensibles puede ser hecho oralmente, aunque, es verdad, que nunca de

588 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 354.
589 Como expresó el BVerfGE 47, 327 (368).
590 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 355.

manera tácita[591].

Las excepciones al consentimiento en cuanto al uso de datos sensibles para la protección de intereses prioritarios, destacándose el tratamiento médico del afectado, se encuentran en los §§ 13, apartado 2 y 28, apartados 6 y 7.

4.2.1.2.3 Principio de la recolección directa

El apartado 2 del § 4, en su 1ª parte, dice que la información siempre debe ser recogida por el ente privado o público directamente del individuo afectado. Este principio reproduce la idea de *lealtad* en el ámbito general del tratamiento de datos ya previsto en el "Considerando 38" de la Directiva 95/46.

Ya la 2ª parte del apartado 2 del § 4 indican las hipótesis excepcionales de recolección fuera de la persona que es afectada. Esto puede ocurrir por autorización de una ley *específica* (número 1)[592], en el caso de que el cumplimiento de la actividad administrativa o la ejecución de alguna relación comercial previa no puedan ser alcanzadas de otro modo (número 2a)[593] o cuando se exigiese un esfuerzo desproporcionado para que esa información sea recogida del afectado (número 2b)[594].

---

[591] GOLA apunta que, en la práctica, son frecuentes las investigaciones que se valen de los teléfonos para verificar cuestiones de las poblaciones en esas materias, a pesar que frecuentemente anonimización de las mismas alejaría que esos fueran considerados legalmente como datos personales (GOLA, Peter, y SCHOMERUS, Rudolf. *Bundesdatenschutzgesetz... cit.*, p. 169)

[592] La autorización legal puede ser expresa o tácita. Es ejemplo de norma que tácitamente admite la recolección de informaciones fuera de la persona del afectado las investigaciones realizables para deportación de extranjero en razón de comportamiento que amenaza la salud pública (§46.5 de la AuslG), que se dan eminentemente sobre terceros y autoridades sanitarias (TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*, p. 506).

[593] Por ejemplo, para verificar si la persona actúa en consultorio sin autorización para la medicina o para actuar como práctico (TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*, p. 507).

[594] Típico de verificaciones amplias sobre el estado de la fuerza de trabajo del país, que son más ágiles si

En estos últimos dos casos depende además de una evaluación del caso concreto para verificar si el interés del afectado prevalece sobre el del ente recolector para impedir el acto.[595]

Cuando la Administración no recoge el dato directamente del afectado, sino de entes privados que disponen del mismo, y sea indispensable su consentimiento, debe existir un acto administrativo que indique la motivación y los fundamentos legales aplicables (apartado 1a del § 13 de la BDSG combinado con el § 39 del VwVfG)[596].

Hay una intersección entre el deber de información previa al consentimiento y el deber de transparencia previsto en la primera parte (*Satz*) del párrafo 3 del art. 4, inspirado en el artículo 10 de la directiva 95/46, y es que se exige que se asegure a la persona afectada el conocimiento de la cualificación completa del responsable por la recolección, así como el propósito y las identidades exactas de futuros destinatarios[597]. Este requisito es especialmente útil ante la existencia de grandes corporaciones con múltiples actividades económicas. El ciudadano puede de esta manera saber si la información que provee sin pretensiones un día no le cerrará ciertas oportunidades en el futuro con filiales que no imaginaba que existían en el grupo económico.

El interrogado deberá también conocer las consecuencias de su decisión afirmativa o negativa, en especial si existen obligaciones[598] o ventajas dictadas por el ordenamiento jurídico que tengan influencia en su libre voluntad en general (2ª y 3ª

realizadas directamente en los departamentos de personal (TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.,* p. 507).

595 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.,* p. 329.

596 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 308.

597 GOLA, Peter, y SCHOMERUS, Rudolf. *Bundesdatenschutzgesetz... cit.*, p. 153.

598 Las declaraciones por deber legal son típicas del derecho tributario, como el §149.1 del *Abgabeordung, y en la* investigación criminal, vide §161 del *Strafprozeßordnung.* (DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 134).

parte del apartado 3 del § 4).

La recolección directa no impide que ocurran limitaciones especiales. En las relaciones jurídicas laborales, especialmente para aquellos que buscan trabajo, el "derecho de preguntar" por parte del contratante es ceñido en los datos sensibles a los temas que pudieran tener alguna influencia en las condiciones del trabajo pretendido, por la imposibilidad de ser garantizada una libre voluntad[599]. Ante alguna pregunta fuera de lugar, el trabajador puede negarse a responder e incluso mentir, frente a la perspectiva de castigos por parte de la jefatura[600].

Determinadas finalidades también se encuentran prohibidas. La utilización comercial de datos personales, que se limita en la actual redacción al apartado 1 del § 28 de la BDSG a su necesidad para la creación, implementación o finalización de relaciones jurídicas con el afectado, la garantía de intereses legítimos del dueño de la base de datos o por su autorización en publicarlas y por el carácter público de los datos. En estos tres últimos casos se exige además que el afectado no tenga un interés prevaleciente en impedir dicho uso.

4.2.1.3. Principios precautorios especiales en la protección de datos

En la legislación alemana existe una serie de normas que apuntan a garantizar que los objetivos de la protección de datos no se dispersen en la práctica del uso de las informaciones.

---

599 GOLA, Peter, y SCHOMERUS, Rudolf. *Bundesdatenschutzgesetz... cit.*, p. 165.

600 TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*, p. 342.

4.2.1.3.1 Confidencialidad

En el § 5, por inspiración del artículo 16 de la Directiva 95/46, hay una obligación de *confidencialidad* que exige a las personas naturales envueltas en el flujo de datos incluso después del fin de sus vínculos profesionales, ya sean de naturaleza pública o privada al secreto.

El conjunto de personas obligadas por esta norma es mayor que las incluidas como "responsables" por el apartado 7 del § 3, pues involucra a los técnicos y personas contratadas aún en el caso que no recojan, traten o utilicen directamente los datos. Este deber de no revelar se suma a las obligaciones profesionales de sigilo que pudieran existir por acaso (§ 1, apartado 3, 2ª parte).

4.2.1.3.2 Prohibición de decisiones automatizadas

La ley impide que los individuos sufran decisiones sobre sí mismos a través de evaluaciones realizadas exclusivamente por máquinas. Este § 6a fue añadido a partir de abril de 2010 para aclarar que cualquier decisión que no conceda a la persona juzgada la subjetividad de una persona natural debe ser considerada como una "decisión automatizada". O sea, no es suficiente la formalidad de que la decisión sea sancionada por un ser humano para que sea considerada como no automatizada, en el caso de que él no tenga la capacidad o autoridad necesaria para reformar la decisión. El artículo 15.1 de la Directiva Europea es explícito en el sentido de señalar campos especialmente sensibles a la aplicación de esta normativa, como en la concesión de crédito y en la admisión laboral.

Existen solamente dos alternativas en las que se permite una decisión automatizada: en el caso de que la decisión dentro de una relación jurídica sea positiva para el sujeto evaluado o, en el caso de que sea negativa, que él sea concientizado sobre la decisión y le sea otorgada la posibilidad de requerir una nueva evaluación fundamentada, teniendo para tal fin la posibilidad de exponer sus propios argumentos (apartado 2 del § 6a).

Las decisiones automatizadas no son necesariamente injustificables, ya que con ellas es posible reducir el ámbito de investigación a través de criterios predefinidos o incluso encontrar a determinadas personas (como en la búsqueda de sospechosos por huellas digitales). Lo que es realmente nocivo y que la ley busca prohibir es la utilización de técnicas de *scoring* para que, a través de categorías estándar, señalar aspectos de las personas, como forma de controlar su acceso a cualquier tipo de bien de vida, sin que estas fórmulas sean transparentes y abiertas a las argumentaciones que no sean puramente matemáticas y frías[601]. Por ello, existe una gran limitación sobre su propio uso, pudiendo servir a una decisión humana o a las excepciones permitidas de decisiones automatizadas del apartado 2 del § 6a.

La regulación y limitación de las operaciones de *scoring*, o sea, el cálculo y el uso de probabilidades matemáticas, estadísticas para alcanzar predicciones de comportamiento fue el enfoque principal de las enmiendas I y III a la BDSG en 2009, como forma de garantizar transparencia y oportunidad de influencia a los afectados, pero también seguridad jurídica a las empresas involucradas, que se refieren

[601] Vide, en ese sentido, BECKHUSEN, Michael. "Das Scoring-Verfahren der SCHUFA im Wirkungsbereich des Datenschutzrechts". *BKR*, 2005, p. 344.

primordialmente a instituciones de crédito, y afectan también, directa o indirectamente, al mercado de seguros y de venta de inmuebles y automóviles[602].

El § 28a solamente permite el *scoring* con el propósito de establecer, ejecutar o finalizar una relación contractual con el afectado en el caso de que algunas condiciones previas se configuren. Cabe destacar, que la restricción sólo se aplica a los cálculos que dan previsibilidad a futuros *comportamientos* humanos, no sirviendo para establecer condiciones referidas a factores externos naturales, tales como rayos, tornados y enfermedades, o humanos, tales como asaltos. O sea, que no afecte la celebración de seguros de automóviles o de salud[603]. Sin embargo, al intentar utilizarlos, las empresas deberán comprobar, documentalmente, que fueron empleados métodos científicos reconocidos. En el caso de que exista una transferencia de los datos hacia las agencias de *rating*, la transferencia se realizará conforme los §§ 28 y 29. Y, en el caso de que datos referidos a direcciones participen del cálculo, deberá ser realizada conjuntamente con por lo menos otro dato y deberá existir una notificación comprobada al afectado (apartados 1 a 4 del § 28b).

4.2.1.3.3 Seguridad

Ya en el considerando 46 y en el artículo 17.1 de la Directiva Europea el legislador reconocía que cualquier regulación jurídica de protección de datos sería insípida si no obligaba también a los detentores de bases de datos a emprender medidas que apuntasen adecuadamente, dentro de la medida del progreso tecnológico, a impedir

[602] GOLA, Peter. "Die Entwicklung des Datenschutzrechts in den Jahren 2008/2009". *NJW*, 2009, p. 2579.

[603] ROßNAGELROßNAGEL, Alexander. "Die Novellen zum Datenschutzrecht". *Neue juristische Wochenschrift*, 2009, p. 2719.

la destrucción, pérdida, corrupción, acceso y difusión antijurídica de las informaciones. O sea, la protección de los equipamientos contra la acción invasora de *hackers* o de espionaje contra estos sistemas informáticos.

La protección contra estos riesgos en el derecho alemán es exigida no teniendo en cuenta el máximo de la defensa posible, sino dentro de un parámetro de proporcionalidad (§ 9, 2ª parte de la BDSG) a la importancia para el desarrollo del individuo cuyos datos son recogidos[604]. El concepto de *seguridad*, a su vez, no debe ser entendido como dependiente solamente del gasto en equipos adecuados o en medios modernos de cerraduras y codificaciones, sino que también debe involucrar un *diseño organizacional*, en todas las etapas, compatible con un uso sin deslices de los datos (§ 9, 1ª parte). La ley alemana estimula el uso de auditores externos para realizar el estudio de estas estrategias y equipamientos (§ 9a), como forma de impulsar el continuo perfeccionamiento y mantenimiento de la integridad de los sistemas[605].

4.2.1.3.4 Regulación de la transferencia automatizada de datos

Existe en la ley alemana una preocupación bastante peculiar con la transmisión *online* de datos a terceros para su utilización, lo cual ya provocó en tres oportunidades el cambio del § 10[606]. Existe la fijación obligatoria por escrito del destinatario, acerca de las razones de la transferencia, del tipo de datos y de las medidas de seguridad involucradas (apartado 2) y deben haber medios para que sean realizados chequeos ya

[604] TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*, p. 342.

[605] No hay, sin embargo, previsión en la ley federal de certificaciones de calidad por las autoridades de control, como ocurre en el §16 de la ley de firma electrónica (SigG). En el plano de los estados miembro, solamente en **Schleswig-Holstein** hay previsión legal de concesión de sellos de calidad (§43.2 da SH LDSG).

[606] DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 210

sea por muestras o o de manera completa en el caso de la transferencia por lotes (apartado 4)[607]. En el sector público se exige además el conocimiento del Comisario de Protección de Datos y la autorización de la autoridad responsable (apartado 3).

Estas medidas no se aplican en el caso de que los datos personales sean de "acceso general", o sea, aquellos en que la vista no depende de un registro, permiso, o pago de tasa (apartado 5 del § 10).

4.2.1.3.5. Regulación sobre la recolección, tratamiento y uso por encargo de otro

Otra norma en la legislación alemana, ahora con correspondencia en la Directiva Europea (artículo 17.3) y que demuestra la preocupación del legislador para enfrentar las realidades económicas empresariales se encuentra en el § 11 de la BDSG[608]. Aquí se ubica la regulación del *outsourcing* (neologismo de *outside resources using* – uso de recursos externos), o sea, de la contratación de otras personas para realizar, *bajo sus órdenes directas*, cualquiera de las etapas de procesamiento de informaciones individuales, método usual buscado por empresas para la reducción de costos. El *encargado* no es considerado como un tercero, en la definición del apartado 9 del § 3 de la BDSG, pues pertenece internamente como parte de una misma operación[609].

La responsabilidad por el respeto a la ley de protección de datos se mantiene en el controlador (apartado 1 del § 11) y las instrucciones sobre el cumplimiento deben ser realizadas por escrito para el encargado, de manera detallada en los números 1 al 10 del

[607] Y los datos para tanto almacenados sólo pueden ser usados para ese chequeo (§ 31 de la BDSG).
[608] En cuanto a los "datos sociales" la normalización del *outsourcing* está en el § 80 de la SGB X.
[609] DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 287.

apartado 2. El encargado, mientras tanto, debe comunicar inmediatamente a su contratante si considera que alguna orden emitida no cumple con las normas de protección de datos (apartado 3), incluso porque está expresamente obligado a cumplir con el deber de sigilo de los datos a los que tuviera contacto y de respetar las medidas de seguridad, bajo pena de sanciones criminales y administrativas (apartado 4). En la modificación de 2001, se incluyó el apartado 5 en esta sección para definir que también se aplican las reglas de este § 11 a las personas de inspección y mantenimiento que puedan tener acceso a los datos[610].

Este § 11 debe ser interpretado en conjunto con otras disposiciones que exijan el sigilo en determinadas profesiones. De esta forma, el secreto médico (expresado en el § 203 StGB, apartado 1, núm. 1) impide que estos, sin el consentimiento de sus pacientes, por ejemplo, transfieran sus facturas a empresas especializadas en cobranza[611].

4.2.1.4 Derecho de los Afectados

Los derechos individuales básicos a la protección de datos, y por ello indispensables, están detallados en el apartado 1 del § 6 de la BDSG. La esencialidad del derecho de acceso (*Auskunftsrecht*), el cual es secundado por un derecho de notificación, de rectificación, de supresión y de bloqueo explica que la ley prohíba su restricción o eliminación por medio del acuerdo de voluntades. Por influencia del artículo 14 de la Directiva Europea hay también un "derecho de oposición" (en los apartados 5 del § 20, 3 del § 28 y 5 del § 35). El §§ 7 y 8 tratan sobre pretensiones de

[610] *Ibid.*, p. 295.
[611] BGH, Entscheidung vom 10. Juli 1991 - VIII ZR 296/90.

indemnización[612].

4.2.1.4.1 El Derecho de Acceso

La existencia de un derecho de acceso es uno de los núcleos de la "autodeterminación informativa" en la sentencia de la Ley del Censo[613]. Este derecho de acceso posee dos normas básicas, el § 19 de la BDSG, que regula bases de datos públicas, y el § 34, que abarca las bases de datos de personas privadas y empresas sometidas al régimen de la competencia (§27 de la BDSG).

El objeto del derecho de acceso se refiere a informaciones *grabadas* en bases de datos que involucren al que peticiona[614]. La doctrina admite el acceso a informaciones genéticas provistas por ascendentes, ya que se refieren también al interesado, por fuerza de la transmisión de los genes a través del ADN[615]. O sea, son requisitos el almacenamiento y la existencia de una característica referida a una persona. Incluso informaciones que estén registradas bajo nombres en clave de los cuales haga uso el afectado pueden ser buscadas[616].

Cabe destacar, que el almacenamiento, en la forma prevista en el § 3 apartado 2, no se limita a la instalación en equipos (automatización), ya que también archivos de papel (no automatizados) pueden poseer una estructura que haga posible encontrar los

---

612 Hay también un dispositivo propio sobre anexar el contenido de la *respuesta* del afectado en los archivos de la materia periodística del *Deutsche Welle* que la brindó (apartado 2 del § 41). El trabajador también tiene el derecho de anexar declaración suya en su asiento funcional (BetrVG § 83 apartado 2).

613 "Saber quién sabe qué, cuándo y en cuál ocasión" (BVerfGE 65, 1, 43).

614 Terceros no pueden valerse del derecho de acceso, aunque puedan acceder a las informaciones en archivos públicos en las hipótesis del § 16.

615 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 478.

616 *Ibid.*, p. 477.

registros y analizarlos. Aun cuando no exista esta estructura, es posible el acceso a datos que estén guardados, pero en este caso el requirente debe proveer información adicional que sea suficiente para que el controlador del dato alcance el dato perdido sin un esfuerzo desproporcionado (§ 19, 3ª parte).

Aquél que requiera el acceso a su registro debe identificarse[617], pero el pedido no necesita ser por escrito y puede ser realizado repetidas veces e incluso por medio de un procurador[618].

El derecho de acceso garantiza el conocimiento no solamente de las informaciones guardadas y de la finalidad de su registro, sino también de las fuentes que las proporcionó. La respuesta de la Administración no necesita ser por escrito (al contrario, las bases de datos privadas sí tienen que responder de esta manera, con excepción de situaciones especiales que justifiquen otra forma[619] – actual apartado 6 del § 34), pero siempre debe asegurarse la identificación inequívoca de los demandados, lo que justifica métodos de firmas digitales o de otro proceso de certificación de las informaciones por medio electrónico, y que sea comprensible para el requirente[620].

Además el derecho a la información también incluye el conocimiento de la lógica de construcción de los registros de datos (apartado 3 del § 6a). Es una medida más en pro de la *transparencia* en la protección de datos y está inspirada en el artículo

---

617 Para ello, es posible inclusive el suministro de contraseñas previamente definidas, especialmente útiles en comunicaciones sin contacto cara a cara, como el teléfono (DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*., p. 481).

618 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*., p. 347-348.

619 Las evaluaciones de salud por profesionales son usualmente transmitidas al afectado en forma oral, ya que la técnica médica justifica la importancia de la conversación con el paciente como forma de amenizar los resultados diagnosticados y reforzar la relación de confianza (GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 668).

620 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 349.

12 a) de la directiva de la UE[621].

La reforma de la ley de protección de datos en el 2009 tuvo como enfoque una mayor garantía de transparencia en el manejo de los datos personales por parte de controladores privados y para ello fortalecieron el derecho de acceso a través de la inclusión de apartados al § 34. Cuando existen fines de propaganda el nombre de los receptores y los datos enviados deben ser almacenados obligatoriamente durante 2 años posteriores a su transmisión (apartado 1a del § 34). Con base en el actual apartado 2 del artículo 34, las empresas deben proporcionar informaciones sobre las operaciones de *scoring* referidas al que peticiona que comprenda los últimos 6 meses. Las probabilidades alcanzadas deben ser mostradas al individuo y los datos utilizados deben ser explicados, todo de forma inteligible para un hombre común, pero sin que sea necesario exponer sus fórmulas empresariales[622]. En el caso de que la empresa no posea directamente estos datos por haber tercerizado dichos cálculos, total o parcialmente, esta prestadora de servicios deberá proporcionar las informaciones faltantes a su contratante. Las compañías que guardan informaciones de individuos con el fin de transmitirlas comercialmente tienen un deber de información ampliado por el apartado 4 para abarcar a todos los destinatarios y probabilidades remitidos en los últimos 12 meses. Por último, las informaciones que fueren grabadas para formar el contenido de estas respuestas en la forma de estos nuevos apartados 1a a 4 del § 34 están bloqueadas para su uso para cualquier otra finalidad (apartado 5 del § 34).

La respuesta del ente público debe contener también una lista de aquellos a

[621] SIMITIS, Spiros, orgs. *Kommentar zum Bundesdatenschutzgesetz*. Baden-Baden: Nomos-Verlagsgesellschaft, 2003, p. 1230.
[622] ROßNAGEL, Alexander. "Die Novellen zum Datenschutzrecht". *Neue juristische Wochenschrift*, 2009, p. 2719.

quienes fue transferida la información (número 2 del apartado 1 del § 19). No es posible la cobranza de tasas por la Administración por el derecho de acceso a bases de datos públicas (apartado 7 del § 19). En las bases de datos privadas por regla no hay cobranza. Ésta solamente es permitida a partir del segundo derecho de acceso por año en las bases de datos con fines de transmisión comercial, si dicha información sirve en negociaciones directas con terceros, y no podrá exceder el costo de la operación. Además, deberá ser dada como alternativa la posibilidad de consulta directa por el afectado y la cobranza no será admisible si fuese pertinente la rectificación o exclusión legal de los datos o hayan circunstancias que permitan creer que el registro es erróneo o ilegal (apartado 8 del § 34).

Cuando la fuente o un destinatario de la información haya sido un órgano encargado de la protección de la Constitución y de la defensa del Estado, la ley federal alemana, haciendo uso del artículo 13 de la Directiva Europea, impone que exista la concordancia de este órgano como requisito adicional a la posibilidad de derecho de acceso (apartado 3 del § 19 y también § 23 de la *Sicherheitsüberprüfungsgesetz* – SÜG).

También existe un impedimento en el derecho de acceso a los archivos públicos de los registros en la situación expresada en el apartado 4 del § 19, todas trayendo ponderaciones de intereses (*Interessenabwägung*)[623]. Su número 1 se refiere a los perjuicios que puede causar la revelación al ejercicio de su actividad por el titular de la base de datos, lo que sucede especialmente en la persecución penal y en ámbitos de Administración Financiera. Su número 2 apunta a preservar el orden público en general, y recibe interpretación por parte de la doctrina de aplicarse solamente a casos realmente

[623] DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 351.

graves[624]. En su número 3 destaca la peculiar naturaleza secreta que envuelve la información, destacándose en razón de los intereses de terceros, como suele ocurrir en temas de derecho de familia, como adopciones. Estas tres hipótesis, respectivamente, también se presentan como excepción al derecho de acceso a bases de datos privadas, por fuerza de la combinación del § 34, apartado 7 con el § 33, apartado 2, número 7b[625], 6 y 3.

Las demás excepciones al derecho a la información en bases de datos de naturaleza pública están detalladas en el apartado 2 del § 19, el cual tiene el mismo contenido que el § 33, apartado 2 combinado con el § 34, apartado 7[626] para los archivos de entes privados. Estos apartados se aplican a los registros que existen no para el conocimiento de su contenido en sí mismo, sino meramente por obligaciones legales[627] o contractuales de conservación, y para aquellos que buscan solamente el monitoreo de la protección de datos y cuya revelación exigiría un esfuerzo desproporcionado.

En las bases de datos privadas la fuente o los destinatarios pueden también ser protegidos en confidencialidad si el mantenimiento del secreto comercial es superior al interés del afectado por esa información (4ª parte del apartado 1 del § 34) y en caso de esfuerzos desproporcionados cuando fueren investigaciones científicas o fuentes accesibles al público para propósitos propios (apartados 5 y 7a del § 33 combinado con el apartado 7 del § 34). Al contrario, la fuente y los destinatarios deben ser proporcionados aun cuando no fueren grabados si el dato del afectado fue almacenado

624 En ese sentido SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 915.
625 Con el detalle que aquí se refiere a la frustración de interés *comercial* del titular de la base de datos y se asume la posible existencia de interés superior en la divulgación.
626 Antes de abril de 2010 con redacción idéntica en el apartado 4 del mismo §.
627 Como en la conservación de sus libros por los contribuyentes en la forma del AO § 141 (BERGMANN, Lutz, MÖHRLE, Roland, y HERB, Armin. *Datenschutzrecht... cit.*, § 19, punto 25).

comercialmente con el fin de transmisión (3ª parte del mismo apartado).

Existe siempre, en las bases de datos privadas, la *libertad* de informar desde que no haya una falta de respeto a intereses públicos o de terceros más relevantes[628]. La recusación del controlador siempre debe ser motivada con detalles para permitir la verificación por parte del afectado. Pero en la hipótesis del apartado 6 del § 33, en razón del perjuicio que puede causar la revelación a la seguridad pública o a la condición general del estado federado o de la Unión, se justifica que la respuesta se resuma a informar que no hay ningún dato almacenado sobre el requirente[629].

Este contrapeso no es discrecional del agente público y, como acto administrativo, está sujeto a la revisión judicial[630]. Este acto administrativo que vincula la recusación al derecho de acceso deberá tener una motivación informada al que peticiona, salvo si esto perjudicase al propio secreto es que se justifica la no divulgación (apartado 5 del § 19). En cualquier hipótesis negativa, sea o no justificada la recusación, el requirente debe ser informado sobre su posibilidad de contactar al Comisario Federal de Protección de Datos (2ª parte del apartado 5 sumado a la 1ª parte del apartado 6)[631]. Se así lo desea el afectado, la información negada se transmitirá entonces a la Autoridad de Control[632] para verificar el respeto a la ley.

4.2.1.4.2 El Derecho de Notificación

[628] DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 483.
[629] GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 670.
[630] *Ibid.*, p. 470.
[631] BERGMANN, Lutz, MÖHRLE, Roland, y HERB, Armin. *Datenschutzrecht... cit.*, § 19, punto 50.
[632] Excepto si, en situaciones extremas, es amenazado por esta comunicación en el caso concreto a la seguridad de la Unión o de los estados federados (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 920.).

El derecho de notificación al afectado es un reemplazo, en principio necesario, de las hipótesis legales que autorizan una ausencia de recolección directo o de transferencias. Esta es una influencia directa en el derecho alemán del artículo 11 de la Directiva europea, en pro igualmente de una mayor transparencia en el tratamiento de datos[633]. Su contenido es tal cual la información que debe ser proporcionada en la recolección directo, por fuerza del apartado 3 del § 4 de la BDSG (§ 19a, apartado 1).

Tanto en bases de datos públicas como privadas no existenotificación en las hipótesis en las que no exista siquiera el derecho de acceso. En las bases de datos públicas es dispensada igualmente la notificación cuando el afectado tenga conocimiento sobre el hecho a ser notificado, si exigiera un esfuerzo desproporcionado y si fuera exigido el almacenamiento y transferencia por ley (apartados 2 y 3 del § 19a). En las bases de datos privadas hay también una pequeña diferencia en esa exención solamente para la medición de la desproporcionalidad, que sólo será realizable cuando los datos sean almacenados comercialmente para fines de transferencia a través de fuentes accesibles al público o en listas o sumarios (apartado 8 del § 33).

Siempre que la excepción de la notificación no involucre el conocimiento de antemano del afectado las razones debe ser colocadas por escrito, permitiendo la verificación por el órgano que garantiza el control de datos (2ª parte del apartado 2 del § 19ª y apartado 9 del § 33).

4.2.1.4.3 Derechos de Rectificación, de Supresión y de Bloqueo

633 GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 480.

Estos derechos son sucedáneos al derecho de acceso[634], ya que representan que existe realmente un control sobre los datos personales aún después de la retirada de la esfera reservada del individuo. En la ley federal de protección de datos alemana estos derechos están previstos en el § 20 para bases de datos públicas y en el § 35 para bases de datos bajo el régimen privado.

La excepción en la BDSG a la aplicación de estos derechos se encuentra en el apartado 6 del § 35. Pues cuando los datos que no sean "sensibles" estén en bases de datos privadas, con objetivos comerciales de transferencia, y sean adquiridos de fuentes de acceso general y solamente archivados para fines de documentación no habrá necesidad de rectificar, suprimir y bloquear, sino solamente de recoger una contradeclaración del afectado en los archivos y en las transferencias eventuales, siempre tramitando conjuntamente a partir de ese momento. Este apartado es de gran utilización y especial relevancia para las informaciones divulgadas por la prensa[635].

También en el derecho del trabajador hay una pretensión de *contradeclaración* y de *rectificación* de sus archivos personales (apartado 2 del § 83 de la BetrVG). En este caso, sin embargo, la doctrina entiende que debe ser considerada como una disposición adicional en la defensa del empleado, pues la subsidiariedad del apartado 3 del § 1 de la BDSG no puede ser utilizada para debilitar situaciones individuales[636], impidiendo el uso de la supresión y bloqueo de la BDSG.

La procedencia del requerimiento en cuanto a estos derechos impone en diversos

[634] Esta condición queda muy clara en la estructuración de la Directiva europea, que los prevén como una consecuencia dentro del artículo sobre el derecho de acceso (artículo 12 b)).
[635] GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 677.
[636] En ese sentido SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 1258 y DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 498.

casos que sean comunicados sobre la decisión todos aquellos para los que fueron transferidos los datos *para grabación*. Existirá la comunicación de la rectificación de datos equivocados, del bloqueo de informaciones polémicas y del bloqueo y exclusión de grabaciones contrarias a la ley, salvo si esto exigiese un esfuerzo desproporcionado y no fuese contra los intereses del afectado (apartado 8 del § 20 y apartado 7 del § 35). DÄUBLER es bastante crítico de la redacción de estos apartados porque entiende que las limitaciones son bastante rigurosas. Además de que el simple conocimiento de la información por terceros no exige aviso, los casos de datos sensibles polémicos en archivos privados no exigen comunicación y aun así, existe en la práctica una ponderación final de intereses entre los perjuicios al afectado y el trabajo que eso dará al controlador[637]. No obstante, reconoce que igualmente en la práctica muchas veces es mejor para el afectado dejar comunicaciones antiguas inalteradas, sin perturbar el olvido, que revivir antiguos hechos vehiculados erróneamente[638].

Se añade que cuando no es adecuada la aplicación de este apartado 7 del § 35 de la BDSG[639], esto no significa que el individuo se queda sin protección en el tránsito y uso de sus datos, pues la jurisprudencia no impide la aplicación subsidiaria de las reglas generales de protección del Código Civil[640]. Existe una aceptación de una pretensión de "retirada" (*Widerruf*) para la eliminación de los datos individuales que no deberían haber sido transmitidos, que se basa en el § 824 del BGB cuando ocurren específicamente perjuicios en las oportunidades de crédito por la información *falsa* a

[637] DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 497.
[638] También señalando situaciones en que el olvido supera la necesidad de aviso de la corrección, eliminación o bloqueo encontramos GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 685.
[639] Por ejemplo, en la hipótesis del apartado 2 del § 27 de la BDSG.
[640] Como decidió el BGH, 10.06.1986, NJW 1986, 2502. También BAG, 6.6.1984, NJW 1984, 2910.

terceros[641]. En los demás casos se admite la aplicación general por analogía del §§ 12 y 1004 del BGB, fundamentándose en garantizar la ausencia de interferencia en los derechos de la personalidad[642].

4.2.1.4.3.1 Derecho de Rectificación

Es quizás la más importante pretensión del individuo en la protección de datos[643]. Este derecho involucra la *corrección* de registros sobre características personales o sobre eventos pasados que de alguna forma representan falsamente la realidad, lo que permite incluso que se rehaga el *contexto* de ciertas situaciones. Deben ser rectificados los datos aun cuando sean insignificantes o no se refieran a la finalidad central de la base de datos[644]. Los datos rectificables no involucran juicios de valor, en los que se encuentran naturalmente fuera de lugar las evaluaciones de correcto o equivocado[645]. Sin embargo estos deben ser claramente identificados como tales (2ª parte del apartado 1 del § 35, en vigencia a partir del 1º de abril de 2010).

En la Administración Pública esta corrección de datos debe ser realizada *ex officio*, ni bien sea descubierta cualquier falla en el registro[646]. También actos administrativos que transmitan informaciones que no se adecúen al concepto del § 3, apartado 2 de la BDSG deben ser aclarados cuando estuvieren equivocados (2ª parte del

641 Vide OLG Frankfurt, 06.01.1988, NJW-RR 1988, 562.
642 Vide OLG Frankfurt, 06.01.1988, NJW-RR 1988, 562.
643 GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 485.
644 Por ejemplo, el Tribunal Administrativo Federal (*Bundesverwaltungsgericht, - BVerwG*, decisión de 4. 3. 2004 - 1 WB 32. 03 (Lexetius.com/2004,3787)) admitió demanda de un soldado para modificar en la base de datos del Ministerio de Defensa su estado de soltero a la de "unión estable" (*Lebenspartnerschaft*).
645 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 939.
646 BERGMANN, Lutz, MÖHRLE, Roland, y HERB, Armin. *Datenschutzrecht... cit.*, § 20, punto 20. También los entes privados no precisan demanda del afectado, pudiendo rectificar por sí directamente (DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 489.)

apartado 1 del § 20), esto en razón de los principios de claridad y exhaustividad que deben prevalecer en toda manifestación administrativa[647].

Esta rectificación debe estar lista en el menor tiempo posible y los costos son de responsabilidad de la persona responsable por los archivos[648].

4.2.1.4.3.2 Derecho de Supresión

Los datos personales en registros automatizados o no automatizados deben ser inmediatamente eliminados si su tratamiento o recepción fuere contrario a la ley (número 1 del apartado 2 del § 20 y número 1 del apartado 2 del § 35 de la BDSG) o ni bien sean inútiles para servir a los objetivos de tratamiento que sirvieron para su recolección (número 2 del apartado 2 del § 20 y apartado 3 del § 35).

El apartado 2 de este § 35 exige, en las bases de datos bajo régimen privado, que sea borrada cualquier información (legalmente archivada) sobre el origen étnico o racial, las opiniones políticas[649], las convicciones religiosas o filosóficas y lo concerniente a la asociación sindical[650], la salud (independientemente de que se trate de una enfermedad o no), la vida sexual y la ejecución de algún ilícito por parte del

---

647 GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 487.

648 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 1247. Caso haya necesidad de acción judicial para que sea efectuada la rectificación, bloqueo o cancelación, es admisible que exista la concesión de bloqueo de los datos en carácter liminar, en la forma del §123 del *Verwaltungsgerichtsordnung* – VwGO (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 958).

649 Lo que garantiza protección a la afiliación a partidos políticos u otras organizaciones políticas y también a otros auxilios o participaciones sin vinculación formal (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 1251).

650 La doctrina interpreta aquí de la misma forma abarcadora que en las "opiniones políticas", para incluir cualquier tipo de participación (DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 492.).

individuo acerca de las cuales el controlador no pueda probar[651] que sean correctas. Salvo esto último, todas estas características son clasificables como "datos sensibles", en la forma del apartado 9 del § 3. Todas estas informaciones, sin embargo, se destacan por su potencial de provocar discriminaciones sobre la vida del afectado. Por eso pueden ser añadidas otras situaciones concretas al listado, donde el registro de comportamientos cause riesgos al individuo[652].

El apartado 4 trata sobre datos que posean un plazo final para ser borrados. Son los datos procesados comercialmente para fines de transmisión, que deben ser eliminados al final de 4 años desde su grabación inicial, salvo si el tema relacionado a ellos ya estuviere terminado, en este caso el plazo será de tres años.

Existe ahora una parte 3 del apartado 2 del § 35 que prevé un caso adicional de eliminación de datos, en el caso de que estos sean grabados comercialmente para uso o transferencia y el afectado requiera de esto al final de la relación contractual.

4.2.1.4.3.3 Derecho de Bloqueo

El derecho de bloqueo surge como un derecho subsidiario al derecho de supresión. "Bloquear" un registro en una base de datos, definido en el número 4 del apartado 4 del § 3 de la BDSG, involucra realizar una marcación, textual o

[651] No basta que haya una alta probabilidad de ser verdadera, ni afecta que el afectado conteste la veracidad, y los medios de prueba pueden provenir de cualquier fuente, inclusive, la divulgación por la prensa (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 1252 y DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 493).

[652] DÄUBLER cita un ejemplo de un registro de empleo que indicara que determinado empleado es compañero de la hermana de una peligrosa terrorista (DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 493).

técnicamente, de modo que impida su tratamiento o utilización posterior[653].

La transferencia o el uso, sin embargo, pueden ser realizados con el consentimiento del afectado o aún sin consentimiento en las hipótesis legales que sean permitidas para datos no bloqueados (números 2 de los apartados 7 del § 20 y 8 del § 35). Además también puede existir la transferencia o el uso de datos bloqueados si fuere indispensable (*unerlässlich*)[654] para fines científicos, para satisfacer determinada necesidad de prueba y para otras razones de interés superior del controlador o de terceros (número 1 de los mismos apartados).

En el apartado 3 del § 20 (que tiene un texto similar y en el mismo sentido que el apartado 3 del § 35) se indican las tres primeras hipótesis en las que se admite el bloqueo en lugar de la supresión prevista en el apartado anterior: caso la eliminación esté en contradicción con períodos de retención predefinidos en un contrato, regulación o ley, o sea si existe la obligación de archivar por parte del controlador[655]; si la supresión afecta a intereses legítimos del afectado; o si existe la imposibilidad fáctica de borrar o sea desproporcionalmente dificultosa debido al modo de grabación de la información.

Sólo es imaginable que la supresión perjudique a los intereses del afectado cuando la información archivada no pueda ser registrada nuevamente, y esto podría serle ventajoso en el futuro, a pesar de que haya pérdida de contexto (*Kontextverlust*),

---

653 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 120.

654 La indispensabilidad tiene el carácter de ser una forma agravada de necesidad (*erforderlichkeit*), en el sentido estricto de que no serían de cualquier forma alcanzables los propósitos invocados sin el "desbloqueo" de los datos (GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 684.)

655 Como ya se refirió a la ley en el apartado 2 del § 19.

pues los datos restantes pueden generar dudas o confusión sin aquellos anteriores[656]. Ya la imposibilidad o esfuerzo extremo de borrar sólo son concebibles en el actual estado de desarrollo tecnológico en archivos no automatizados, a la luz del constante costo decreciente de las bases físicas de grabación, tales como CDs[657].

El apartado 4 de los §§ 20 y 35 vehicula el denominado caso *non liquet*[658], o sea, cuando hay una disputa por parte del afectado sobre la credibilidad de la información guardada, independientemente que él proporcione o no pruebas[659], y no sea posible concluir por la corrección o no de lo archivado. La carga de la prueba, sin embargo, recae sobre el titular de la base de datos, siendo suficiente para el sujeto al cual los datos se refieren peticionar exponiendo razones que no sean evidentemente incoherentes[660].

No existe en las bases de datos públicas una norma equivalente a la del apartado 2 del § 35, por lo cual también estos "datos sensibles" en estas bases solamente pueden ser bloqueados, mientras que no existe posibilidad de bloqueo en lugar de la supresión en bases de datos privadas[661].

Actos que no se incluyan en sistemas de datos automatizados o no automatizados sólo serán bloqueados cuando, no siendo aplicable su supresión, ya no sean útiles para las tareas de la Administración y su no bloqueo pueda afectar negativamente al individuo (apartado 6 del § 20). Este bloqueo depende del

656 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 948.
657 DÄUBLER, Wolfgang y otros. *Bundesdatenschutzgesetz*. Frankfurt am Main: Bund-Verl., 2007, p. 367.
658 Esa era la fórmula que los jueces medievales utilizaban para expresar que no encontraban una solución al asunto presentado. Tiene el sentido de "me abstengo porque no lo veo claro" (NICOLIELLO, Nelson. *Diccionario del Latín Jurídico*. Buenos Aires: Euros, 2004, p. 211).
659 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 367.
660 GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 683 y DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 495.
661 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 948.

requerimiento del afectado, pues sería impracticable exigir la revisión sistemática de todos los actos administrativos para esta verificación[662].

4.2.1.4.4 Derecho de oposición

El derecho de oposición se encuentra en los apartados 5 de los §§ 20 y 35 y es fruto del artículo 14 de la directiva de la UE, insertado luego de la reforma de 2001. Al mismo tiempo los puntos "e" y "f" del artículo 7 de la directiva no dan suficiente margen para reducir las hipótesis de aceptación de la oposición, lo cual, de esta manera, termina siendo de completa libre configuración por parte de los estados miembros[663].

Este derecho en Alemania se aplica exclusivamente sobre datos *archivados*. La oposición puede ser total o parcial, o sea, abarcar determinados tipos de datos o individual o en combinación con la recolección, tratamiento y uso.

Asimismo, no hay una forma específica en el pedido formulado a la Administración, siendo los únicos requisitos para el aplazamiento, que el particular tenga razones para impedir la recolección, uso y/o tratamiento que superen los del órgano público y que estos no sean impuestos por ley (apartado 5 del § 20). El apartado 5 del § 35 tiene contenido idéntico para las bases de datos privadas. Por lo tanto, en la decisión del derecho de oposición la BDSG impone al controlador que realice una ponderación de intereses en situaciones en las que exista una mera permisibilidad legal para la recolección, uso o tratamiento[664].

---

662 BERGMANN, Lutz, MÖHRLE, Roland, y HERB, Armin.*Datenschutzrecht... cit.*, § 20, punto 66.
663 GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 686.
664 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 369.

4.2.1.4.5 Derecho de Indemnización

El derecho de reparación de los perjuicios sufridos por la persona natural afectada[665] con la recolección o tratamiento o uso indebido (prohibido) o incorrecto (con contenido o procedimiento equivocado) de sus datos personales[666] está previsto en los §§ 7 y 8 de la BDSG.

El responsable por la compensación, cuando esté probado que ocasionó un daño, será en este caso siempre el ente que es dueño de la base de datos[667], independientemente de que otros dispositivos impongan sanciones sobre las autoridades de control de datos o empleados del controlador de los datos[668].

De hecho, sin embargo, el legislador alemán redactó la norma orientada para la limitación de las consecuencias, especialmente en el caso de controladores públicos[669].

Para entes privados existe la exculpación, prevista en la 2ª parte del § 7, si se comprobara en el caso concreto que actuaron con el "debido cuidado" (*gebotene Sorgfallt*), o sea, que su observación sin fallas del comportamiento exigible no fue capaz

---

665 No pueden ser derivadas de aquí pretensiones de terceros o de personas jurídicas, ya que esas no son protegidas en la BDSG (GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 307). Pero la pretensión es pasada a los sucesores (DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 235).

666 La disconformidad puede referirse tanto a una disposición de protección de datos de la BDSG en cuanto a otra ley como la TKG o la TDDSG (GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 307).

667 Si varios entes actuaron de forma que perjudicó al individuo, todos son conjuntamente responsables, por fuerza del § 840 del BGB a los privados y del apartado 4 del § 8 de la BDSG a los públicos.

668 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 231. Inclusive en cuanto al responsable, no hay duda de que otras normas también pueden ser invocables, al contrario del § 7 del BDSG, para justificar la indemnización en la falta de respeto al uso de datos individuales como, por ejemplo, si hay entre afectado y controlador de la base de datos también relaciones contractuales, en las cuales incide el § 280 combinado con § 311, ambos del BGB (DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 236).

669 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 622.

aun así de impedir los perjuicios ocurridos[670]. Este es un concepto flexible, que debe ser analizado con más rigor conforme mayores sean los peligros para el afectado[671].

Los daños inmateriales, ciertamente los más comunes en los perjuicios por la protección de datos personales, no se incluyen en el § 7 de la BDSG, porque el apartado 1 del § 253 del Código Civil de Alemania exige que ellos sean expresamente previstos en la legislación propia[672]. El *quantum* de la indemnización está limitado si hubiera culpa concurrente del afectado (§ 254 del BGB)[673].

Para los entes públicos, sujetos o no a las reglas de competencia, la regulación de la indemnización en sus procesamientos de datos de manera automatizada se encuentra en el § 8 de la BDSG. El apartado 1 define que esta responsabilidad es independiente de la culpa, o sea, tiene naturaleza objetiva. Sólo se exige la prueba por el afectado del acto y de su perjuicio, que puede también ser de naturaleza inmaterial, porque así lo prevé el apartado 2. Existe, sin embargo, la limitación del total de la indemnización a ser pagada en 130.000 euros, la cual debe tener las cuotas que la componen reducidas proporcionalmente si involucrasen en un mismo evento a más de un afectado (apartado 3 del § 8 del BDSG)[674].

4.2.1.5 Reglas especiales de procesamiento de datos en los entes

[670] *Ibid.*, p. 629. Es bastante controvertido si pueden usar también la disculpa de la 2ª parte apartado 1 del § 831 del BGB, para imputar exclusivamente al empleado. A favor, con cautelas, en casos de evidente dolo del empleado, GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 308; contra, SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... cit., p. 629).

[671] DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 233.

[672] *Ibid.*, p. 234 y SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... cit., p. 623.

[673] Hay aplicación de este párrafo tanto para el § 7 como para el § 8 de la BDSG, aunque sólo el apartado 5 de este último lo afirme expresamente.

[674] GOLA afirma que esas limitaciones deben ser alejadas frente al efecto directo que debe tener el artículo 23 de la Directiva 95/46, que no prevé nada en ese sentido (GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 315).

públicos: otras limitaciones del derecho a la autodeterminación informativa en la actuación de la Administración Pública

La segunda parte de la ley federal alemana de protección de datos, en sus §§ 12 a 16, apunta a establecer las especificidades en la recolección, uso y transferencia de datos que son justificadas para el eficaz funcionamiento de la Administración Pública, con esto igualando la aplicación general de la Directiva Europea con las necesidades de acción estatal, admitidas como limitaciones posibles al derecho en la propia norma europea[675].

Por eso las reglas presentes, empezando en el § 13 de la BDSG, sólo han extraído su verdadero sentido cuando son entendidas como una complementación de las excepciones a la regla general del consentimiento presente en el § 4. Por lo tanto, se sabe que, dentro del derecho a la protección de datos, tenemos que el hecho de *recoger* un dato de algún lugar, datos, independientemente si ya conocidos o no[676], sobre un individuo es la actividad del ente responsable de retirar. , (apartado 3 del § 3 de la BDSG). Como tratamos ahora de intervenciones legítimas sobre el derecho fundamental en Alemania, sólo interesan aquellas situaciones en donde es posible la recolección de informaciones sobre el individuo, para el archivo, que no dependan de su consentimiento. Esta recolección de datos de manera *obligatoria*, a su vez, puede ser, sobre el afectado o un tercero y ocurrir con o sin su conocimiento simultáneo[677]. No existe la necesidad de contacto directo, personal, siendo cada vez más usual la obtención de datos por internet y por teléfono. Independientemente del modo, la

675 GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 373.
676 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... cit., p. 783.
677 TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*,p. 499-501.

recolección de una información sobre el individuo contra su voluntad representa una decisiva intervención en el derecho a la autodeterminación informativa, pues la salida del dominio personal incrementa el riesgo de pérdida de control sobre el tráfico y el uso de un detalle de su existencia[678].

Las limitaciones en este capítulo al derecho de protección de datos tiene como autorizados a intervenir a los entes públicos federales no sujetos al régimen de concurrencia (§ 12.1)[679], desde que no se traten de medidas que involucren cualquier relación de contratación de personal (§ 12.4).

El apartado 1 del § 13 autoriza la recolección cuando el ente público la necesite de forma esencial para el cumplimiento de sus funciones. Esta no es una cláusula en blanco para cualquier acción estatal, ya que estos objetivos justificativos deben estar siempre legalmente definidos[680]. Además el análisis debe observar si la información cumple con los límites de responsabilidad del ente recolector dentro de la división de atribuciones territoriales y entre miembros de la federación que el ordenamiento resguarda[681]. Esto no es suficiente. La exigencia de necesidad (*erforderlich*) impone que además de adecuada y conforme al ejercicio de sus atribuciones, aquella información específica sobre el individuo sea también un componente indispensable, no sustituible por ningún otro, para el completo cumplimiento de las obligaciones del órgano en el caso concreto. La necesidad implica igualmente la inadmisibilidad de la recolección de

678 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 781.

679 Aunque el apartado 2 del mismo § se refiera a que entes públicos de los estados miembro en la misma situación podrían utilizar la ley, la existencia de leyes estatales propias en todos tornó letra muerta esa excepción (DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 299).

680 GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 382.

681 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 785.

informaciones para el mero mantenimiento en stock, sin objetivos directos de uso[682], o de la formación de un "registro de sospechosos" de carácter genérico[683].

Son numerosos los ejemplos de aplicación de este apartado en la vida práctica. En las relaciones funcionales, por ejemplo, sólo deben ser mantenidas en los departamentos de recursos humanos aquellas informaciones pertinentes al trabajo ejercido[684]. El Proceso Penal está lleno de hipótesis en las que la ley admite que informaciones sobre personas sean, independientemente de la voluntad del afectado, buscadas sobre su cuerpo[685], a través de terceros, en observaciones escondidas y en documentos, para que sirvan para facilitar el descubrimiento de la verdad sobre actos delictivos ocurridos[686]. El Tribunal Constitucional ha admitido la constitucionalidad de estas normas, incluso en las búsquedas realizadas directamente por policías, desde que sean motivadas por sospechas fundadas de crímenes y con supresión inmediata luego de su uso necesario. Frente al derecho a la autodeterminación informativa estos criterios no son disminuidos ante una supuesta insignificancia del dato recogido[687]. Aún el argumento de "amenaza terrorista" no sensibiliza al Tribunal Constitucional para un relajamiento de estos criterios, lo cual, evidentemente, no niega la justificación, también en razón de motivos fundados, que en una determinada situación pudieran surgir

---

682 *Ibid.*, p. 787.

683 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 318. Por ejemplo, el archivamiento de datos sobre crímenes por la *Bundeskriminalamt* (BKA) siguen ese modelo, al solamente autorizar los hechos criminosos y sospechosos (aun no absueltos) mientras necesario al cumplimiento de las funciones de la agencia y, en cuanto a otros intervinientes en la investigación (víctimas, testigos, informantes), dependiendo de su consentimiento, salvo si ese conocimiento frustra los objetivos de la medida (§ 8 de la BKAG).

684 GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 384.

685 Hoy existe en el StPO normas específicamente para pautar el orden judicial de retirada de ADN de sospechosos contra su voluntad (§81e y siguientes). Se destaca la preocupación demostrada en el §81h de que las muestras sean inmediatamente destruidas tras su utilidad al proceso y no sirvan a la formación de un registro gubernamental.

686 Obsérvese en el StPO los §§ 81, 81a.1, 81b, 131, 161, 100c, 474-478 y 483-495, por ejemplo.

687 BVerfGE120, 378.

también en este tema[688].

Para los "datos sensibles" existe un apartado propio (2) en el § 13. La interpretación de la lista cerrada de hipótesis que permiten el uso debe ser realizada de forma restringida, como forma de no menospreciar el alto deber de protección de esta categoría de datos[689]. Con excepción del número 7 y del número 8 ligeramente modificado para resaltar la ponderación del interés científico específico del proyecto de investigación[690], todos los demás números sirven también como excepciones al principio de la finalidad en el almacenamiento, alteración o utilización de "datos sensibles" (apartado 5 del § 14). E incluso los "datos médicos" en la forma el número 7, sin embargo, pueden ser almacenados, alterados y tratados, respetando la finalidad, pero prescindiendo el consentimiento del afectado (apartado 6 del § 14).

El número 1 de este apartado 2 del § 13 trata sobre la existencia de otra ley estableciendo la autorización o en el caso de urgencia por razones de interés público[691]. Hay en este último caso una necesidad particularmente más exigente de comprobación por parte de la Administración Pública[692]. Igualmente son altas las exigencias en el caso concreto de la prueba de la necesidad de los datos sensibles para la prevención de *considerables* amenazas a la "seguridad pública" [693] (número 5), que es así un bien de

688 Como decidido en BVerfGE 115, 320.

689 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 790.

690 GOLA explica la importancia de esa alteración para impedir modificaciones de finalidad solamente con base en la importancia general de la investigación, debiéndose atener en esa nueva ponderación al beneficio investigativo de los nuevos usos (GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 418).

691 Aunque si otra ley veda la recolección, como en el caso de menores de 14 años el § 11 de la BVerfSchG, entonces esa cláusula no puede ser invocada (*Datenschutzrecht... cit.*, §13, punto 29).

692 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*,p. 791.

693 El concepto de "seguridad pública" proviene del derecho de policía e incluye la inviolabilidad del orden pública, de los bienes y derechos individuales y la protección de la existencia de las instituciones y organizaciones estatales y de las autoridades que la representan (PIEROTH, Bodo, SCHLINK, Bernhard y KNIESEL, Michael. *Polizei- und Ordnungsrecht*. München: Beck, 2008, p. 128).

protección destacado dentro del interés público, o en la defensa de *considerables* desventajas o afectaciones al bien común (número 6) [694].

El número 7 es casi una repetición del apartado 3 del artículo 8 de la directiva europea y se aplica solamente a finalidades relativas a la prestación directa de servicios de tratamiento de salud[695], cuando el personal involucrado, sean administrativos, farmacéuticos, enfermeros o médicos, se sujeta a la obligación de secreto imputable en la forma del § 203 del StGB[696]. El número 8 permite el uso de datos personales para finalidades científicas, cuando estas sean más importantes que eventuales objeciones del interesado y en caso de que la investigación no pueda ser realizada de otra manera o esto exigiera un esfuerzo desproporcionado. Nuevamente ocurre aquí una ponderación de intereses entre los objetivos de la investigación y los del afectado y, caso sea justificado el uso para investigación, esto no permite automáticamente la publicación de lo utilizado[697].

El número 9 exige que la recolección del "dato sensible" sea esencial para la defensa del país, obligaciones internacionales asumidas, prevención de conflictos, gestión de crisis y razones humanitarias en general.

El número 3 se configura cuando por razones físicas el afectado no pueda conceder su consentimiento de manera escrita[698], no cumpliendo los requisitos legales

---

694 La gran amplitud de cláusulas como "desventajas", "afectación" y la propia noción de "bien común" implica que se imponga especialmente alta exigencia para la aceptación del uso en concreto de esa posibilidad (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 793)

695 O sea, no incluye el sector financiero de las Seguradoras de Salud (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 793).

696 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*,p. 313.

697 BVerwG, 23.06.2004, NJW 2004, 2462.

698 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 791.

para el uso de "datos sensibles", y existiendo una amenaza a sus intereses vitales[699]. También el número 4 se basa en el consentimiento del individuo de hacer pública tales informaciones sobre sí, como en una divulgación de candidatura, por lo tanto, no basta que la información se haya vuelto pública[700], y que el uso por el Estado de la información sea realizado exclusivamente de formas que no perjudiquen al individuo, bajo pena de servir como inhibidor de manifestaciones públicas sobre estos temas "sensibles"[701].

El consentimiento en proporcionar la información también es dispensado en lo concerniente al deber de servidores públicos en calificarse con veracidad, previsto en el § 111 de la ley de infracciones administrativas (OWiG), y en cuanto a las medidas coercitivas que pueden ser tomadas por el Ministerio Público y por la Policía para identificar a sospechosos de delitos (§ 162b.1 del Código de Proceso Penal), reglas que tuvieron su constitucionalidad declarada como límites al contenido fundamentado en la jurisprudencia de la autodeterminación informativa[702].

Por otro lado en la decisión de un reclamo constitucional el 2 de marzo de 2010[703] existió la declaración de inconstitucionalidad de la regla de recolección sin anuencia por su desproporcionalidad. Este fallo se trata de una modificación, ocurrida el 21 de diciembre de 2007, que incluyó los § 113a, para determinar el almacenamiento por seis meses por parte de las empresas que prestan servicios públicos de telecomunicación relativos a teléfonos, e-mails y otros servicios de Internet de forma

699 Este apartado repite casi literalmente el artículo 8, apartado 2, letra c de la directiva europea.
700 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 311.
701 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 792. En sentido similar BVerfGE 100, 313 (381).
702 BVerfGE 92, 191 (198).
703 BVerfG, 1 BvR 256/08.

que permita el conocimiento de quién, para quién, por cuánto tiempo y de dónde hubo comunicación, y § 113b, para fijar los propósitos que autorizarían el uso estatal de estas informaciones, en la Ley de Telecomunicaciones (*Telekommunikationsgesetz* – TKG). También fue incluido el § 110g en el Código de Procedimiento Penal (*Strafprozessordnung* – StPO), para especificar más claramente las hipótesis de acceso concedidas por el § 113b, pero igualmente sirviendo para el acceso a cualquier dato de un servicio de telecomunicaciones. Estas modificaciones fueron declaradas nulas pues, aunque en teoría el almacenamiento de todos los datos sin razón previa por seis meses no fuese inconstitucional, el Tribunal entendió que las normas no eran proporcionales a una medida tan gravosa pues no establecían adecuadamente medidas de seguridad de datos; definían de forma muy amplia el rol de delitos que justificaban el acceso directo, además de no establecer ciertas conversaciones que por la inherente confidencialidad deberían estar excluidas del almacenamiento; no aseveraban que los afectados sabrían posteriormente del acceso gubernamental y tendrían consecuencias eventuales ilegales, incluso por no someterse las medidas estatales al control judicial.

Además de comprobar la *necesidad*, el Poder Público está también obligado, en todos los casos en que almacene, modifique o utilice informaciones sobre personas, a respetar de forma estricta la *finalidad* que motivó su acción de conseguir el dato (apartado 1 del § 14 de la BDSG).

En el apartado 2 del § 14 hay una lista cerrada de ocho hipótesis donde puede darse la modificación de la finalidad de origen, exceptuando el consentimiento del afectado. Ellas son: previsión en una ley diversa[704] (número 1), si esto es realizado,

[704] Hay una autorización, por ejemplo, de manera bastante amplia a los órganos de la Administración en compartir los datos recogidos originalmente como registro de extranjeros que vivan en Alemania

justificadamente, para favorecer al afectado y no son conocidos motivos en contrario (número 3) o para comprobar la veracidad del registro, cuando no fue recogido conjuntamente con el afectado[705] (número 4), cuando el dato proviene de "fuentes de acceso general" [706] o el ente tiene el permiso de publicación, salvo si hay un evidente y digno interés de protección del afectado en impedir ese cambio de finalidad (número 5). El número 6 es bastante amplio, admitiendo la alteración de la finalidad con el fin de preservar el bien común, con el destaque principal de protección frente a amenazas a la seguridad pública[707]. El número 7 no se destina al Ministerio Público y a la Policía, que ya están regulados primordialmente por el Código de Procedimiento Penal, sino a los demás órganos del Estado que necesitan del dato para la aplicación de cualquier tipo de pena, incluso sobre menores infractores[708]. En el número 8 se autoriza el cambio de la finalidad si es justificado por la ponderación de intereses que las razones para la protección del derecho de terceros supera, en la existencia de conflicto, a las de la preservación de la "autodeterminación informativa" del afectado. Por último, el número 9 tiene un texto similar al del número 8 del apartado 2 del § 13.

La transferencia de datos entre órganos públicos tiene que ser para las tareas legales del receptor y conforme las condiciones del § 14 (apartado 1 del § 15), o sea, atender a la misma finalidad o encontrarse dentro de sus excepciones estrictas (como está explicitado en el apartado 3 del § 15). El apartado 4 del § 15 aplica las mismas

---

(§76.1 combinado con §75.1 de la AuslG y también §71.2 da SGB X)

705 GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 409.

706 El concepto de "fuente de acceso general", presente en ese apartado 5, está también en el apartado 1 del artículo 5 de la Constitución Alemana, e incluye los medios de comunicación de masa, como películas, radio, televisión y prensa escrita, pero igualmente exposiciones, documentales, folletos, posters en las calles, avisos de neón y hasta las franjas que cargan aviones con fines publicitarios (HERZOG, Roman. "Art. 5". In *Maunz/Dürig, GG*. München: Beck, 2010, puntos 89 a 92).

707 Pero siempre son la atención de que la medida antes debe ser necesaria, en el sentido de única admisible (DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 320.)

708 Como especial atención sobre la *proporcionalidad* de los intereses involucrados (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 822).

reglas a las religiones que sean consideradas corporaciones de derecho público, conforme el artículo 140 GG combinado con el 137 de la Constitución de Weimar, tales como la Asociación de Iglesias Luteranas (VELKD) o las diócesis de la Iglesia Católica, y que tengan medidas suficientes para la protección de datos[709].

Como complemento al apartado 4 del § 10, el apartado 2 del § 15 responsabiliza el ente receptor por la legalidad de la operación, salvo que no haya un pedido de envío, en cuyo caso la responsabilidad es de quien la envía. Con el pedido, basta que el cedente verifique si el ente receptor realmente ejerce las tareas para las cuales alega que necesita los datos.

La existencia de datos físicamente inseparables[710] solamente permite que sea transmitida más información de lo que es necesario, incluso en el ámbito interno de organizaciones, desde que no existan razones *evidentemente*[711] superiores del afectado en mantenerlas en *secreto* y no sean de ninguna manera utilizadas (apartado 5 del § 15).

Solamente hay dos posibilidades de transferencia de datos a entes privados por entes públicos. El apartado 1 del § 16 lo autoriza solamente si, además de enteramente respetados los requisitos del § 14 ya comentados, el órgano público necesita de ellos para cumplir sus funciones. No es, por lo tanto, un apartado que permite indicaciones de fechas conmemorativas del afectado a terceros, sino, por el contrario, involucra situaciones graves que lo involucran y que exigen de la intervención estatal, tales como

709 DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 329.

710 La consecuencia de un esfuerzo desproporcional de separación es típico de archivos no automatizados y con bases de registro no modificables (DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz... cit.*, p. 330).

711 Hay una decisión en pro de la transferencia cuando los intereses públicos y del afectado son equivalentes (GOLA, Peter, y SCHOMERUS, Rudolf. Bundesdatenschutzgesetz... cit., p. 434)

enfermedades o riesgo de muerte para sí mismo o para otros. Además el presupuesto de *necesidad* también controla el número de personas que serán avisadas, lo cual coloca la divulgación a la prensa en el último caso[712].

Ya el apartado 2 del § 16 opone un verdadero conflicto de intereses entre el tercero y el afectado, sobre el cual la Administración está encargada de realizar la ponderación[713]. Exactamente la importancia en este caso de conocer todas las cuestiones involucradas, exige que aquí haya una notificación previa del afectado[714], salvo si este ya sabía o haya algún perjuicio para la seguridad pública o de otra forma a la Unión o a los estados miembros (apartado 3 del § 16). Además de esto, el propósito expuesto por el tercero le es vinculante y él no podrá utilizar la información para ninguna otra finalidad, al contrario de la hipótesis del apartado 1 donde esto es posible con anuencia del ente público transferidor (apartado 4 del § 16).

4.2.1.6 Instancias de control de la Protección de Datos

Existe, sin embargo, el reconocimiento de una inherente debilidad del individuo para ejercer completamente el control de sus datos personales, lo que llevó al consenso en la Unión Europea de que es imprescindible un control interno dotado de autonomía (Considerando 49 y artículo 18.2 de la directiva 95/46) principalmente de una autoridad pública para imponer el respeto a la ley (Considerando 62 y artículo 28 de la directiva). Esta instancia independiente de control, tratada desde el inicio en los fallos del Tribunal Constitucional Alemán, debe ser comprendida como una *garantía* del individuo a la observación de estos derechos, cuando, por cualquier motivo, no busca (por temor a las

712 SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*,p. 869.
713 *Ibid*., p. 870.
714 *Ibid.*, p. 877.

consecuencias, por ejemplo) o no puede procurar (por desconocimiento de su inclusión en la base de datos) por sí mismo[715].

4.2.1.6.1 Comisario Federal para la Protección de Datos (*Bundesbeauftragte für Datenschutz*)

La principal función de esta autoridad es verificar el cumplimiento por los órganos públicos de la Ley Federal de Protección de Datos (Apartado 1 del § 24 de la BDSG), lo cual significa que su actuación es concomitantemente preventiva y represiva. Sin embargo, no funciona como un mero controlador, sino también como consejero, ya que también debe emitir recomendaciones a la Administración Federal con miras a la mejora de la protección de datos y dar pareceres a este cuerpo y al Parlamento Federal (*Bundestag*) cuando así fuese requerido (apartados 3 y 2ª parte del apartado 2 del § 26). Además de esto, cada 2 años remite informes al Parlamento indicando los desarrollos relevantes en la protección de datos en Alemania durante el período (apartado 1 del § 26), lo que lo obliga a observar y también buscar influenciar a los entes privados que manejan datos[716].

Este Comisario es electo por la mayoría de votos del Parlamento, luego de ser indicado por el Gobierno Federal (apartado 1 del § 22) para un mandato de 5 años, con derecho a una reconducción (apartado 3 del mismo § 22). Como es una figura que debe actuar de forma apartidaría, es recomendable que sea ratificado por una amplia coalición[717].

---

[715] BVerfGE 65, 1 (46 e 60) y BVerfGE 67, 157 (185).
[716] TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*, p. 427.
[717] *Ibid.*, p. 428.

El Comisario actúa con independencia (2ª parte del apartado 4 del § 22), lo que coincide con la segunda parte del apartado 1 del artículo 28 de la Directiva Europea. Por eso la supervisión gubernamental prevista en la ley (tercera parte del apartado 4 del § 22) tiene un alcance limitado, solamente la de conseguir una autorización para obtener respuestas sobre el contenido de determinadas decisiones y medidas tomadas por la autoridad de control[718].

Esto es esencial, pues sin esta cierta autonomía no existiría la condición necesaria para analizar y eventualmente cohibir con desenvoltura las demandas de individuos que se consideren lesionados en su derecho a la protección de datos por órganos públicos (§ 21 de la BDSG). Aunque esta decisión administrativa no sea directamente atacable, el inconformismo del peticionario puede desencadenar una acción judicial, teniendo como parte acusada a la República Federativa de Alemania[719].

4.2.1.6.2 Autoridad de Supervisión (*Aufsichtsbehörde*)

El encargado administrativo de controlar al sector privado y garantizar el cumplimiento de las reglas federales de protección de datos es la denominada "autoridad de supervisión", la cual es elegida por los gobiernos de los estados miembro (apartado 6 del § 38). Aunque la ley no imponga directamente mayores instrucciones, la compatibilidad con el artículo 28 de la Directiva de la Unión exige que se garantice la independencia *funcional* de esta persona designada de las influencias externas[720].

[718] SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 970.
[719] *Ibid.*, p. 964.
[720] TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*, p. 429.

Este encargado actúa en la práctica divulgando instrucciones e informes a través de los medios de comunicación, exigiendo esclarecimientos, llevando a cabo inspecciones "in loco" en las empresas[721] y debe tener un registro para archivar todos los tratamientos de datos que legalmente tengan comunicación obligatoria, en la forma del § 4d (apartados 2 a 4 del § 38).

Sin que se exponga ni al afectado ni a las medidas de seguridad empresariales, en este registro formado habrá un "derecho de vista" de cada ciudadano, que deberá ser lo más amplio (incluso con la posibilidad de fotocopias) y facilitado posible[722].

La autoridad de supervisión puede dictar órdenes para corregir cualquier falla que encuentre en la infraestructura organizacional, personal o material de protección de datos, bajo pena de sanción por el incumplimiento y, en casos extremos, hasta puede prohibir la recolección, tratamiento o uso de datos personales por aquél controlador e imponer el despido del responsable interno de la protección de datos si se verifica que es incapaz de ejercer adecuadamente sus funciones (apartado 5 del § 38).

4.2.1.6.3 Autocontrol del establecimiento responsable por la base de datos: el encargado de la protección de datos

Los titulares de las bases de datos, ya sean de naturaleza pública o privada,

[721] Es una limitación a otro derecho fundamental, el de la "inviolabilidad del domicilio" (Art. 13 GG), ya que la sede de empresas también forma parte del concepto de domicilio, conforme la jurisprudencia del BVerfGE, 32, 54.

[722] En ese sentido, ya que no hay mayores reglas para facilitar la transparencia en ese derecho de vista de la BDSG, es apuntado como modelo de aplicación, por analogía, el apartado 5 del § 25 del SGB X (SIMITIS, Spiros (org.). Kommentar zum Bundesdatenschutzgesetz... *cit.*, p. 1271).

pueden tener uno o más empleados o personas designadas externamente como encargados de la protección de datos. Esta nominación es mandataria siempre que estuvieren legalmente obligados a notificar o realizar una verificación previa, o, en cualquier caso, si hay al menos 20 empleados involucrados en la recolección, uso o tratamiento de datos (apartado 1 del § 4f). La existencia de este encargado o consejero de encargados, sin embargo, no exime a la dirección de la persona jurídica de sus responsabilidades legales en el trámite y la seguridad de los datos que utilizan[723].

Además de verificar previamente los tratamientos así definidos legalmente (conforme § 4d), este encargado de la protección debe en primer lugar verificar, con acceso a toda la información necesaria, si el procedimiento de manejo de datos en la persona jurídica que le corresponde atiende las normas de la ley federal, así como debe adoptar medidas para hacer posible la familiarización con el estatuto por parte de los empleados que trabajen en este procedimiento (números 1 y 2 del apartado 1 del § 4g). Es también un elemento de enlace entre los sujetos cuyos datos son tratados y la persona jurídica (2ª parte del apartado 5 del § 4f).

Hay una serie de garantías para asegurarle a este encargado los medios necesarios para practicar adecuadamente sus funciones de supervisión interna. Él debe ser amparado por el personal necesario y asistido materialmente (1ª parte del apartado 5 del § 4f). Desde el punto de vista jerárquico, responde directamente al responsable por la persona jurídica, tiene completa libertad de determinarse en su *expertise*, sin someterse a instrucciones superiores, y no puede sufrir represalias por su actuación (apartado 3 del § 4f).

[723] TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*, p. 444.

Su contratación debe ser realizada por escrito (1ª parte del apartado 1 del § 4f) y tiene como requisitos individuales, analizados en concreto, el conocimiento jurídico y técnico sobre protección de datos y la capacidad de interacción social y comunicacional con la organización en la que irá a actuar[724]. Su despido depende de que su empleador tenga una justa causa para motivarlo (siendo aplicable el § 626 del BGB) o que la autoridad de supervisión justificadamente lo requiera (apartado 3 del § 4f). Es posible aún que en la admisión o en el despido de este encargado se dependa de los testimonios de los empleados, caso haya habido un acuerdo voluntario en este sentido por medio del § 88 de la BetrVG[725].

Por otro lado, están sujetos al deber especial de secreto en cuanto a las informaciones para el desempeño del encargo analizado (apartado 4 y también artículo 28.7 de la directiva europea).

4.2.1.6.4 Funciones adicionales de las instancias de control

4.2.1.6.4.1 La función de archivo de las operaciones avisadas por fuerza de la "obligación de registro" (*Meldepflicht*)

La obligación de registro[726] de determinados tratamientos automatizados está previsto en el considerando 48 y en los artículos 18.1 y 19 de la Directiva Europea y, en

[724] *Ibid.*, p. 448.
[725] LAG Frankfurt/Main, 28. Februar 1989, CR 1990, 342.
[726] Se optó por la traducción por *registro*, al contrario de *notificación*, aunque esta terminología aparezca en la traducción oficial de la directiva europea, para diferenciar del derecho del afectado a su notificación (*Benachrichtigungsrecht*), siendo esta opción conforme a IATE (Inter-Active Terminology for Europe), utilizada por las instituciones y agencias de la Unión Europea.

el derecho alemán, tiene destinatarios distintos conforme se trate de un controlador privado, que avisará a la "autoridad de supervisión", o un órgano federal o compañías postales o de telecomunicaciones, que comunicarán al Comisario de Protección de Datos (apartado 1 del § 4d de la BDSG).

El archivo resultante de este conjunto de notificaciones no pretende reproducir cada operación relativa a cada individuo que haya ocurrido en Alemania. Al contrario, lo que se registra son los procesos completos de operación, detallados conforme los números 1 a 9 del § 4e (lo que incluye, fundamentalmente, la identificación del controlador, los tipos de datos y la finalidad de uso, sus destinatarios y las medidas de seguridad adoptadas), en su inicio, final y eventuales alteraciones (2ª parte del § 4e). Estos procesos suelen, evidentemente, referirse a múltiples sujetos[727].

Esta notificación está exenta si el ente responsable por un encargado de protección de datos o si la recolección, tratamiento y uso no involucra a más de 9 empleados[728] y es el fruto del consentimiento o de la necesidad de obligaciones con el afectado (apartado 3 del § 4d). Al contrario, deben siempre notificar, por exigencia del apartado 4, las empresas que tratan comercialmente informaciones personales con el fin de transferencia identificada (como firmas de propaganda, agencias de *rating* y negocios de venta de direcciones, regulados por el § 29 de la BDSG) o anónima (para investigaciones científicas, por ejemplo, lo cual es tratado en el § 30) o con el objetivo de la realización de investigaciones de mercado y opinión (§ 30a).

4.2.1.6.4.2 La función de pre control

[727] TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.,* p. 438.

[728] O sea, están liberados los pequeños negocios, como farmacias, firmas de arquitectura, médicos, etc.

Las actividades que supongan un riesgo especial a los derechos y libertades de los afectados exigen además un examen previo por una autoridad de control en el derecho europeo (art. 20.1 y Considerandos 53 y 54 de la Directiva), el cual en el derecho alemán es el encargado interno de protección de datos. Sin embargo, en caso de duda, este debe consultar a la autoridad de supervisión o, si es una empresa postal o de telecomunicaciones, al Comisario federal de protección de datos (apartado 6 del § 4d).

Existen dos situaciones que merecen esta pre-verificación, cuando son tratados los "datos sensibles" del ap. 9 del § 3, o cuando el procesamiento involucra informaciones sobre personalidad, habilidades, desempeño o comportamiento del afectado (números 1 y 2 del apartado 5 del §4d). Sin embargo, se exceptúan estos casos de control previo si el tratamiento es fruto de una obligación legal, tiene el consentimiento del afectado o si está dentro de las obligaciones acordadas con él. Así como en el apartado 3 del § 4d, el objetivo de la regla de exclusión es no convertir en demasiado complejo el funcionamiento de personas jurídicas pequeñas, especialmente aquí a consultorios médicos y asociaciones religiosas, cuyo objeto de registro involucra eminentemente "datos sensibles"[729].

4.3. La legislación reguladora del derecho a la autodeterminación informativa en España: Régimen Jurídico de la Ley Orgánica 15/99

[729] TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht... cit.*, p. 442.

4.3.1 Ámbito de aplicación

Ahora analizaremos como se planteó la inserción del contenido esencial del derecho presente en la Directiva 95/46 en el ordenamiento español. Primeramente, se debe resaltar que la modificación fue tan sensible que surgió la necesidad de editar una nueva Ley Orgánica, exactamente esta que recibió el nº15 de 1999, cuando la intención inicial era tan sólo realizar cambios en la Ley Orgánica 5/92. Esta última ley, cuyo origen se debió a la necesidad de inserción por completo de España en el Acuerdo de Schengen sobre la libre circulación de personas, y por consecuencia de sus datos personales, era criticada por establecer un régimen demasiado diferente entre la regulación de archivos públicos y privados, con elevado número de excepcionalidades en pro del primero, por la poca independencia y gran amplitud de poderes del Director de su Agencia de Protección de Datos, nombrado mediante Real Decreto entre los miembros del Consejo Consultivo del órgano y por la normativización de seguridad muy ceñida en los procedimientos internos y poco en el flujo comunicacional[730].

La norma española, en la adaptación proporcionada por el artículo 3º del RD 1720/2007 al contenido del artículo 4º de la Directiva europea, es aplicable cuando el responsable por el tratamiento esté en territorio español o, caso no esté en territorio español, que las normas españolas sean aplicables en la forma del Derecho Internacional Público o, caso no se encuentre el responsable ubicado dentro de la Unión Europea, que al menos parte del tratamiento no incluido el mero tránsito se dé en España.

Es de notar el alcance de la Ley Orgánica 15/99, puesto que su artículo 2 sólo

[730] TÉLLEZ AGUILERA, Abel. *Nuevas tecnologías... cit.*, p. 97.

excluye de su objeto a las bases de datos relativas a actividades exclusivamente domésticas[731], materias clasificadas[732] y combate al terrorismo o a formas graves de delincuencia organizada[733].

El artículo 2.3 de la LOPD permite que determinados archivos se sometan a legislaciones específicas de protección de datos. Así, por ejemplo, los vinculados a la práctica de las elecciones. Ello significa simplemente que hay un doble reglamento, con derogaciones de determinadas normas generales en pro de las especiales. Gran relevancia tiene aquí el artículo 41.3 de la LOREG (Ley Orgánica del Régimen Electoral General), que veda la transmisión de datos constantes del censo electoral para fines distintos del ejercicio de las capacidades políticas activas y pasivas. Con base en éste y en la LOPD, la Agencia de Protección de Datos ha aplicado sanciones en la utilización de esas informaciones para fines de propaganda comercial, y ha encontrado aceptación del Judicial en esta actuación[734].

También los archivos con fines estadísticos poseen sus propias normas, dada por la Ley 12/1989. Hay aquí algunas distinciones con el régimen general, como la

---

[731] El sentido de la exclusividad de aplicación doméstica remite directamente a lo decidido por el TJCE en el caso *Lindqvist.* No es, por tanto, el hecho de ser el archivo creado en el ámbito privado y de forma no profesional que caracteriza esa condición, sino también que no expongan a extraños esas informaciones, como ocurrió en el caso con la publicación de características de los compañeros de la Sra. Lindqvist en la colaboración voluntaria en una parroquia protestante sueca.
Al contrario, cuando una comisión formada por ex integrantes de la Academia Militar de Zaragoza, encargada de organizar la conmemoración del XXV aniversario de la jura a la bandera, entrega informaciones a la agencia de viajes para facilitar el traslado y alojamiento de los interesados, no hay violación a la LOPD (SAN, Sección 1ª , rec. 521/2004). También define "doméstico" en el sentido de privado o familiar el artículo 4a) del RD 1720/2007.

[732] La clasificación como "materia clasificada" en España está sometida al artículo 2º de la "Ley de secretos oficiales" (ley 9/68, modificada por la ley 48/78), admitiendo que pueden ser sometidas a conocimiento restricto datos que afectan la seguridad y la defensa españolas. El art. 3.2 de la Directiva europea también destaca la seguridad y defensa estatales como razones justificables a la exclusión de aplicación de la protección de datos.

[733] Se destacan aquí las leyes 12/2003 y 19/1993, esa específica sobre "blanqueamiento de capitales"(o "lavado de dinero").

[734] Vide, en este sentido, la STS, Sección 6ª , de 23 de septiembre de 2002 (rec. 5654/1998).

imposibilidad absoluta de transferencia de datos a otros sectores de la Administración, a menos que tengan también fines estadísticos, como afirmó el STS, Sección 6ª, en el recurso 5882/1992, y el permiso de un procedimiento especial para su conservación en razón de fines históricos, científicos o propiamente estadísticos (arts. 9, 157 y 158 del "Reglamento de desarrollo de la Ley Orgánica 15/1999" - Real Decreto n. 1720/2007).

Hay dos registros de personal que también se excluyen de la LOPD por sus peculiares estructuras y regímenes: el de los militares (ley 17/99), conteniendo todos los datos de las carreras de los posibles combatientes de las tres fuerzas, y el de los condenados penales, incluido en el Código Penal (ley 10/95). Resáltese que el hecho de no incluir en la regulación de la LOPD no significa que los derechos fundamentales de los sometidos a estos regímenes especiales sean menoscabados por el Poder Público. Ese hecho es especialmente verdadero en lo referente a la divulgación injustificada de hechos que afecten la intimidad y la imagen de los detenidos.

La letra "e" del artículo 2.3 establece una importante restricción al objeto de la LOPD, al excluir de su aplicación las imágenes y sonidos obtenidos a través de las videocámaras de las fuerzas integrantes de la Seguridad Pública del Estado. Esta delimitación es importante porque, para fines legales, imágenes de un individuo también forman parte de sus datos personales, conforme la definición del artículo 3.a de la LOPD. Esa delimitación es importante, pues garantiza una normalización más restricta para un medio bastante intrusivo de la Administración sobre nuestra acción en el espacio público y al mismo tiempo esencial para contener la criminalidad en las grandes ciudades. Ejemplo de ese contraste es el artículo 8º de la ley propia (ley orgánica 4 de 1997), que establece que todas las grabaciones deberán ser destruidas en el plazo

máximo de un mes, salvo las de comprobación de algún crimen o infracción administrativa grave o gravísima, siendo siempre presupuesta la existencia contemporánea de un proceso judicial o administrativo.

En las videocámaras de origen privado, al contrario, no hay razón para ningún distanciamiento del régimen de la LOPD e inclusive, la Agencia Española de Protección de Datos editó Instrucción específica sobre el tema (1 de 2006).

Hay en el artículo 3 algunos conceptos centrales para la correcta interpretación de las normas constantes en la LOPD. La noción de "dato de carácter personal", por ejemplo, involucra la conjugación de tres elementos, que son en primer lugar la información, y que la misma se refiera a una persona física y que ésta sea identificable (art. 3 a))[735].

Esa conceptualización tiene un primer efecto importantísimo, que es confirmado en el art. *3.e*: sólo es titular (y, evidentemente, puede ser "afectado" en lesión a ese derecho o "interesado" en sus facultades) del derecho fundamental a la autodeterminación informativa persona natural, nunca persona jurídica. Se mantiene de esta forma la misma dirección presente desde el Convenio 108 de 1981.

El artículo 1º del Convenio de 1981 auxilia también a remediar una eventual duda de la limitación de la aplicación de la LOPD a españoles, al establecer que su fin es "garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades

[735] REBOLLO DELGADO, Lucrecio. *Derechos fundamentales y protección de datos... cit.*, p. 144.

fundamentales, concretamente su derecho a la vida privada, respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.". No debe ser otro el criterio del intérprete en la LOPD además de preservar el derecho fundamental en el espacio físico español, indistintamente de nacionalidades[736].

Además de la nacionalidad, otra distinción no admisible es en cuanto al ámbito de la vida del individuo a que se refiere el dato, como cuanto a datos personales que involucren actuación profesional. Ello se torna patente por la Agencia de Protección de Datos Española en su Resolución del 27 de febrero de 2001, al decidirse por la aplicación de la LOPD también a profesionales liberales y comerciantes individuales en el trascurso de sus actividades[737].

En cuanto al todavía no nacido, el *nascituro*, aunque no pueda ser titular de derechos fundamentales, como decidió el Tribunal Constitucional en la STC 53/1985, no debe ser rechazada la protección de sus derechos, en especial los de naturaleza genética, como resaltó el Comité de Ministros de los Estados miembro de la Unión Europea en el artículo 4.5 de la Recomendación R (97) 5[738].

De forma consecuente, se considera que el procedimiento de disociación involucra el distanciamiento del dato de la identificación de la persona a la cual él se refiere (art.3 f)). La doctrina distingue la denominada "despersonalización de los datos" del procedimiento, ya que en este todavía es posible la existencia de una "clave de

[736] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 109.
[737] En el mismo sentido SAN, Sección 1a., rec. 348/2004.
[738] "4.5. Medical data concerning unborn children should be considered as personal data and enjoy a protection comparable to the protection of the medical data of a minor." (en una traducción libre: "Datos médicos sobre los fetos deben ser considerados como datos personales y disfrutar de una protección comparable a la protección de los datos médicos de un menor.")

asociación" que le permita al responsable del tratamiento saber a quién se refiere la información, aunque aquellos que consultan los archivos no lo sepan739. La distancia entre los dos conceptos, y la caracterización de "identificable", requiere que no sea posible sin gran esfuerzo individualizar a aquel al que se refiere la información[740].

No importa la trivialidad que pueda tener la información para ser caracterizada como "dato personal". Por tanto, la definición legal abarca tanto el nombre como la dirección del ciudadano, número de documentos de identidad (DNI), número del teléfono[741], dirección de correo electrónico[742] y datos médicos[743].

El criterio de ser el archivo ya automatizado, que se encontraba en la LORTAD, es superado por la inclusión también de bases de datos manuales en la reglamentación[744]. Un buen ejemplo de bases de datos manuales son los seculares libros de bautismo de las iglesias católicas, como decidió la Audiencia Nacional, Sección 1ª, el 17 de enero de 2008.

Hay quien defienda además que la protección de la ley no se refiere solamente a datos incluidos en un "archivo" (o "base de datos"), que es cualquier tipo de conjunto ya *organizado* (o sea, sometido a un criterio de búsqueda) de "datos personales" (art. 3 b)), pero también a cualquier dato susceptible a "tratamiento", que son las operaciones,

739 APARICIO SALOM, Javier . *Estudios sobre la ley orgánica de protección de datos de carácter personal*. Cizur Menor (Navarra) : Aranzadi, D.L., 2002, p. 55.

740 SAN, Sección 1ª , el 8 de marzo de 2002.

741 La Audiencia Nacional, Sección 1ª , en el rec. 1258/2002, mantuvo la sanción a una empresa que comercializaba una base de datos que permitía el descubrimiento de nombre y dirección a partir del teléfono, aun siendo todo constante de la lista telefónica, porque invertía la finalidad de esta fuente de acceso público, que es que una persona descubra el teléfono de otra que ya conoce previamente.

742 SAN, Sección 1ª , rec. 911/2003.

743 La Recomendación R (97) 5, del 13 de Febrero de 1997, del Comité de Ministros del Consejo de Europa incluye en los datos médicos las informaciones genéticas, relativas al ADN. En el mismo sentido el artículo 5.1.g del RD 1720/2007.

744 REBOLLO DELGADO, Lucrecio. *Derechos fundamentales y protección de datos... cit.*, p. 144.

automatizadas o no, que suceden con esos datos, (art. 3 c)), desde que estén esquematizados o en una planilla de tal forma que su posterior inclusión en un archivo sea directa, sin necesitar ningún análisis manual más[745].

Sin embargo, este posicionamiento tiene el inconveniente de tornar usos puntuales de datos punibles, amenazando interacciones sociales inofensivas. Pues, prácticamente cualquier operación imaginable con datos personales puede ser calificada legalmente como un "tratamiento" de este dato. El concepto del artículo 5.1.t del RD 1720/2007 abarca "cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."[746].

La posición que entiende necesaria la posterior existencia de una base de datos no es fruto de una interpretación literal de la legislación española, ya que el artículo 3 c) de la LOPD no contiene la expresión "contenidos en un fichero o a él destinados", presente en la parte final del artículo 3.1 de la Directiva 95/46. Ese requisito se encuentra por la conjugación con el artículo 2º de la LOPD, que habla que el dato debe encontrarse en un "soporte físico, que los haga susceptibles de tratamiento". Ese "soporte físico" es entendido exactamente como la exigencia de una estructura de acceso y logística calificable con una base de datos. También el artículo 19 reforzaría esa conclusión, al presumir en el derecho de indemnización la responsabilidad del titular

[745] APARICIO SALOM, Javier . *Estudios sobre la ley orgánica ... cit.*,, p. 65.

[746] Este texto es más específico que el artículo 3.c de la LOPD, que menciona "recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias", no obstante, menos minucioso que la Directiva Europea, artículo 2.b, que ejemplifica que "cualquier operación" puede consistir en "recolección, registro, organización, conservación, adaptación o alteración, recuperación, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de colocación a disposición, con comparación o interconexión, así como el bloqueo, borrado o destrucción".

del "fichero". De forma idéntica, en cuanto al régimen sancionador, el artículo 43 de la ley[747]. La sentencia de la Audiencia Nacional, Sección 1ª, en el rec. 241 de 2005 parece inclinarse en este sentido, al descalificar la lesividad de la llamada de un hotel ofreciendo oportunidad a un desempleado que había dejado el currículo en otro establecimiento de turismo, cuando, en el desinterés del posible nuevo empleado, fue inmediatamente destruido su currículo de donde se había retirado la información.

La responsabilidad en regla del titular de la base de datos no significa que el *responsable por el tratamiento*, o sea aquel que, por medio de acuerdo, promueve operaciones en bases de datos en que no posee autonomía para definir "finalidad, contenido y uso" (artículo3.d de la LOPD), también no pueda ser imputable. Este fue un importante avance de la LOPD con relación a la LORTAD, al incluir el concepto de "responsable por el tratamiento", en la comparación de sus artículos 3.d y del actual 43.1 y del anterior 42.1.

Se trataba de una hipótesis frecuente en la jurisprudencia española anterior a 1999 que bancos que brindaban a entidades de protección al crédito informaciones equivocadas relativas a débitos ya pagados no fueran, por ello, sancionados. Al contrario, actualmente, ambas empresas son culpables, la que proporciona por la inexactitud de la información; la que recibe y utiliza, por no tener el cuidado necesario de verificación sobre los datos que administra[748]. Lo mismo se aplica a cualquier otra falla en la obtención de los datos, como la falta de consentimiento del afectado.

[747] En el rec. 241/2005, la Sección 1ª de la Audiencia Nacional, expresa la importancia práctica de la cuestión, al rechazar atribuir violación al derecho a la protección de datos la empresa hotelera que, al recibir el currículo por fax, telefonea al trabajador para hablar de empleo y, a seguir, destruye el currículo recibido, sin incluirlo en sus archivos.

[748] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 107.

La identificación del responsable por una base de datos privada es de sobra más sencilla que la de una base de datos pública, ya que mientras que ésta es creada por una "disposición general" publicada por la prensa oficial del Estado en que se indica el *órgano* responsable por el mismo (artículo 20.1 y 20.2.f de la LOPD), en el primer caso se impone solamente la notificación de la Agencia de Protección de Datos (artículo 26.2).

El responsable por el tratamiento actúa sin relación directa de subordinación al titular de la base de datos. Al subordinado, califica la ley como simple *encargado del tratamiento* (art. 3.g).

Los requisitos para la constitución de un "encargado del tratamiento" están en el artículo 12 de la LOPD, en que se destaca que esa persona física o jurídica deberá tener vínculo formal con el responsable del tratamiento, en el cual deberán estar especificadas las instrucciones para el uso. El incumplimiento de dichas instrucciones provocará imputabilidad personal del encargado (art. 12.4). Por último, tras la prestación contractual los datos no podrán quedar en pose del encargado, debiendo ser destruidos o devueltos (art. 12.3).

El cumplimiento del artículo 12 de la LOPD (reglamentado por el RD 1720/2007 en sus artículos 20 a 22) para caracterizar un "encargado por el tratamiento" tiene gran significado práctico, ya que mientras en esa relación de servicios no se exige el consentimiento del afectado, caso ello no se caracterice, estará configurada una cesión o comunicación de datos, punible en la ausencia de anuencia del interesado, como decidió la Audiencia Nacional, Sección 1ª , en los rec. 101/2003 y 380/2003.

El artículo 3º, en su apartado h), aborda la definición de *consentimiento del interesado*. La idea de circulación de informaciones personales eminentemente por fruto de la voluntad del individuo es indudablemente la piedra central que inspiró el derecho en su formulación europea. La importancia de esa definición se refleja por todo sistema de protección de datos europeo y español, como será visto cuando tratemos acerca del principio del consentimiento, en el art. 6º de la LOPD.

El consentimiento, en la forma del apartado, deberá poseer cuatro requisitos. Primeramente, debe ser libre, o sea, no dominado por ningún factor externo, como violencia, error o intimidación[749]. También debe ser informado, en la forma prescripta por el art. 5º de la LOPD, que trata del "derecho a la información"; específico, por tanto, están vedadas autorizaciones genéricas; e inequívoco, lo que impide consentimientos presumidos.

Esta última exigencia significa que hay tres formas básicas de proveer consentimiento en la legislación española: por escrito, verbalmente (en ambas el individuo demuestra su voluntad *expresamente*) o por comportamientos (*tácitamente*). Ello, porque la ley reserva el consentimiento expreso (y en el primer caso en la forma escrita) solamente a determinadas categorías de datos (artículos 7.2. y 7.3).

Menores de edad también podrán dar consentimiento para la recolección de sus datos, pero poseen un reglamento propio, conforme el artículo 13 del RD 1720/2007. El "derecho de información" para ellos deberá ser como un lenguaje más simplificado y

[749] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 118.

solamente para menores de 14 años se exige también el consentimiento de padres y tutores; para los demás menores de edad está la *asistencia* de estos exclusivamente cuando es exigido por ley (art. 13.1).

Dice el artículo 3.i) que debe ser considerada cesión o comunicación de datos "toda revelación de datos realizada a una persona distinta del interesado". A pesar de que su régimen sea disciplinado más adelante, en el artículo 11 de la LOPD, hay una importante conclusión jurisprudencial, vehiculada en el rec. 132/2002 de la Sección 1ª de la Audiencia Nacional, sobre esa sencilla definición: la cesión de datos depende de que se realice el verbo "revelar" y, en la acepción del vocablo, sólo "revela" quien expone a terceros hecho secreto o desconocido que antes no podría saber. Así, concluye la sentencia, "la restitución o devolución de los datos previamente cedidos por el cedente al cesionario no puede ser sancionada pues el cesionario se limita a restituir al cedente lo previamente cedido".

Ello explica también porque escapa del régimen general que exige el consentimiento del dato cedido que se encuentra en *fuente accesible al público* (arts. 3.j), 11.2.b) y 28). Si no hay ninguna limitación legal que cualquiera del pueblo, aun pagando por el acceso, tenga acceso a alguna información no hay de hecho desconocimiento o secreto a revelar.

Más difícil es la identificación en la práctica de cuáles exactamente son esas "fuentes accesibles al público", aunque el legislador en la parte final del artículo 3.j) de la LOPD haya tenido la preocupación de establecer una relación que se pretendía

numerus clausus[750]. La tendencia de los tribunales españoles fue también interpretar restrictivamente la clasificación como "fuente accesible al público"[751], como forma de reforzar la protección ciudadana. Ejemplificativamente, no fueron incluidas en el concepto del art. 3.j) : archivos de datos de ciudadanos simplemente por provenir de la Administración Pública (rec. 321 de 2003 y 265 de 2005 de la 1ª Sección de la Audiencia Nacional); archivos del Registro Mercantil (rec. 621 de 2004 del mismo juicio); datos de procesos judiciales, aun con el "principio de la publicidad de los actos judiciales" estando en la CE (art. 120.1) y en la Ley Orgánica del Poder Judicial (LOPD, arts. 232, 234, 235 y 266.1), ya que sólo abarca a aquellos comprendidos como legítimos interesados en el asunto, (STS del 3 de marzo de 1995, rec. 1218 de 1991 y SAN, Sección 1ª, rec. 554 de 2004) e informaciones sobre domicilios de individuos resultantes de la observación de los nombres constantes en cajas del correo (rec. 35/2005 de la Sección 1ª de la Audiencia Nacional).

Por último, apúntese que inclusive el tratamiento autorizado del dato proveniente de "fuente accesible al público" no debe subvertir la lógica de aquella existencia (así, por ejemplo, es ilícita la organización por empresa comercial que permita que la lista telefónica sea consultada por número de teléfono y no por el nombre del suscriptor – rec.1258 de 2002 de la Sección 1ª de la Audiencia Nacional) y no agregar nuevas informaciones sin consentimiento de los interesados (como su correo electrónico – rec. 319 de 2005 del mismo tribunal).

---

[750] "j. Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. *Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.*" (cursivo nuestro). Listado semejante se encuentra en el artículo 7 de la RD 1720/2007.

[751] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 124.

4.3.2 Principios

La LOPD, en su título II, que inscribe los principios relativos a la protección de datos, por los cuales el legislador busca establecer un sistema al responsable por la base de datos donde sea observado un adecuado equilibrio entre la libertad ciudadana y los avances inherentes a la sociedad de información[752]. Los denominados principios en la ley de protección de datos son en verdad vertientes que derivan del contenido del "derecho a la autodeterminación informativa"[753]. Los contornos de este nuevo derecho fundamental sólo se tornan suficientemente claros con la conjunción práctica de las normas intituladas "principios" que a continuación serán discriminadas[754].

Cabe recordar que la técnica de legislar la protección de datos por medio de la enumeración de un rol de principios, que en verdad, constituyen guías maestras de las actuaciones que incidan sobre el cuerpo digital de los afectados, ya se encuentra en el Convenio del 28 de enero de 1981 del Consejo de Europa, lo que también se repite en la Directiva 95/46/CE. La Directiva europea, a propósito, posee, en su Considerando 25[755] una indicación sobre la clasificación de los principios de la protección de datos como, por un lado, obligaciones a los responsables por el uso de los datos y, por el otro,

---

[752] HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales … cit.*,p. 53.

[753] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 138.

[754] De forma muy clara se expresó el relator (*ponente*) Carlos Lesmes Serrano en el rec. 210/2005 de la Sección 1ª de la Audiencia Nacional sobre el significado jurídico efectivo en el derecho español de aquello que la LOPD llama principios: "sirven para delimitar el *marco* en el que debe desarrollarse cualquier uso o cesión de los datos de carácter personal y para integrar la definición de los tipos de infracción definidos en el artículo44 LOPD (...)" (cursiva nuestra).

[755] "(25) Considerando que los principios de protección deben encontrar expresión, por un lado, en las obligaciones que recaen sobre las personas, las autoridades públicas, las empresas, los servicios u otros organismos responsables por el tratamiento de datos, en especial en lo que respecta a la calidad de los datos, a la seguridad técnica, a la notificación a la autoridad de control, a las circunstancias en que el tratamiento puede ser efectuado, y, por otro, en los derechos de las personas cuyos datos son tratados ser informadas sobre ese tratamiento, poder tener acceso a los datos, poder solicitar su rectificación y aun, en ciertas circunstancias, poder oponerse al tratamiento;"

derechos de los afectados.

4.3.2.1 Principio de la Calidad y sus sub-principios

Por la representatividad del carácter preventivo de la ley de protección de datos, el "*principio de la calidad*" adquiere prevalencia, de la misma forma que el "principio del consentimiento" es relevante al contenido sancionador de la LOPD.

El legislador español, en el artículo 4º de la ley, aborda la cuestión de la *calidad* de los datos desde una doble perspectiva, que involucra la *exactitud* de los datos recogidos y almacenados. Así, se exige que el responsable por el tratamiento se esmere en mantener la veracidad de las informaciones, independientemente de las facultades otorgadas al interesado (art. 4.3 y 4.4).

Además, se impone, a través de las obligaciones de *pertinencia, adecuación y no excesos*[756], que la recolección y utilización sean limitados a su consonancia con la *finalidad explícita*, *determinada* y *legítima*[757] de las bases de datos (art. 4.1 y 4.2) y que el dato sea mantenido tan solamente en el período necesario para aquel objetivo específico (art. 4.5).

El *sub-principio de la veracidad* o *exactitud* involucra, en el derecho comparado, la veda de dos tipos de equívoco, el del dato *erróneo* (*incorrect*) y el del dato *engañoso (misleading)*[758]. No hay en la ley española, sin embargo, mayores consideraciones sobre

[756] REBOLLO DELGADO, Lucrecio. *Derechos fundamentales y protección de datos... cit.*, p. 146.
[757] La protección al ciudadano es aquí ampliada, pues la LORTAD (art. 4.1) sólo hablaba de finalidades *legítimas*.
[758] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 155.

una diferenciación en este sentido. Se considera verdadero todo dato brindado por el ciudadano (art. 8.5 del RD 1720), sin exigir ninguna verificación posterior salvo por discrecionalidad de la Administración Pública dueña de la base de datos (art. 11 del mismo RD).

Parece ser la cuestión central aquí el intercambio por el art. 4.3 de la LOPD (con relación al texto del mismo artículo de la LORTAD) del parámetro de veracidad del dato archivado de *real* para *actual*. Esta norma exige un cuidado redoblado por organizaciones de protección de crédito, ya que sus informaciones deberán estar a todo instante condecentes con el carácter dinámico de la situación patrimonial del ciudadano. Sobre este tema hay artículo propio en la LOPD, el de número 28.

Del principio de la veracidad deriva el *derecho de cancelación* por el afectado del dato erróneo, pero principalmente, el *deber de cancelar* dichos datos por el dueño de la base de datos, el que aparece también en el archivamiento de informaciones por tiempo que excede la finalidad de recolección. El uso de la forma verbal "serán cancelados" en los apartados 4.4 y 4.5 justifica esta interpretación[759].

Hay, sin embargo, en el artículo 8.6 del RD 1720/2007 dos importantes excepciones al deber de cancelar. La primera se refiere a la preservación de los datos por el tiempo necesario a la posibilidad de exigencia de alguna responsabilidad civil del dueño de la base de datos o durante ejecución contractual que los utilice y la segunda ocurre cuando ellos son mantenidos de forma *desasociada*.

[759] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 159.

El deber de cancelación, o al menos, la disociación del dato, en razón de la superación del período adecuado a su utilización de forma condecente con la finalidad de la recolección se repite en varias normas sectoriales, como en la Ley General de Telecomunicaciones (Ley 32/2003, art. 38.3), en la Ley de Comercio Electrónico (Ley 34/2002, art. 12.1) y en cuanto a la historia clínica de pacientes médicos (Ley 41/2002, apartados 17.1 y 17.2).

La limitación de la amplitud de la recolección de datos de los ciudadanos para la formación de archivos es centro frecuente de preocupación e informes de la Agencia de Protección de Datos de España (AEPD), de forma que evite sanear situaciones ya iniciadas de forma equivocada. Por ejemplo, en el informe 161/2003/AEPD se alertó que la identificación del domicilio y teléfonos particulares de los trabajadores participantes de los cursos de perfeccionamiento profesional, con relación a los cuales sus empresas empleadoras buscaban ayuda o subvenciones de la "Fundación Tripartita para la Formación en el Empleo", era excesivo, pues se trataban de actividades de naturaleza exclusivamente profesional.

Otra importante cuestión tratada por la Agencia española es cuando junto a la obtención de crédito en instituciones bancarias, como, por ejemplo, en el contrato mutuo para la compra de inmueble, está adjunta la exigencia de celebración de un seguro de vida. En ese caso es exigido por la administración española, por medio de la Instrucción 2/1995, que encuentra una separación estricta entre la colocación de los datos de salud necesarios al seguro de vida y los archivos que almacenan el historial de crédito del individuo, de modo que no haya ningún intercambio entre ellos, aun siendo celebrados ambos instrumentos en la misma fecha, lo que inclusive, deberá ser firmado

expresamente por la entidad financiera.

El aspecto de la finalidad para fines de utilización posee un importante precedente en la sentencia 11/1998[760] del Tribunal Constitucional. En este "leading case", es concedido el amparo al trabajador I.C.N., contra la Sentencia de la Sala de lo Social del Tribunal de Justicia de Madrid, del 30 de junio de 1995, ya que este tuvo su salario descontado en razón de una huelga realizada por el sindicato al cual era afiliado. Sin embargo, el recurrente no había participado de la paralización, ya que su horario de trabajo se lo impedía, y por tanto, la disminución del salario ocurrió solamente porque la empresa pública contratante RENFE utilizó su conocimiento de la afiliación sindical del mismo (y de otros), lo cual se daba solamente para permitir el descuento de la cuota sindical, para introducir un mando automático en el sistema de pago para poder reembolsar con más facilidad los días parados. En sentido similar, decide el Tribunal en la STC 202/1999, del 8 de noviembre. Aquí es utilizada la *finalidad* para entender que viola derechos fundamentales de la persona humana la realización de tratamientos de datos en que exista la acumulación en un archivo de faltas por razones médicas con datos sobre la salud de los empleados.

No obstante, ni siempre la violación de los requisitos a la *finalidad* de la recolección es tan evidente. En cuanto a su carácter de *determinación*, es importante la decisión emitida por la Sección 1ª de la Audiencia Nacional en el recurso 565/2004, del 27 de abril de 2006, en que el Tribunal afirmó que un club infantil que obtiene datos de los padres e hijos para "comunicarles actividades culturales, formativas, deportivas y de ocio, y para el envío de promociones comerciales de productos y servicios que pueden

[760] Son en el mismo sentido las SSTC 33, 35 y 94/1998.

resultar de su interés", no queda autorizado a mandarles propagandas de servicios de proveedores de Internet y *videogames*, pues no hay forma de aceptar la desvinculación entre los propósitos lúdicos del club de convivencia al aire libre con las propagandas que él se disponía a enviar.

Hay una leve facilitación legal a la utilización de datos tras su recolección, pues mientras, en este, el análisis de la finalidad es estricto en cuanto a la explicitación, determinación y legitimidad, en aquella el tratamiento es posible desde que no sea *incompatible* con el motivo inicial. La LORTAD, en su artículo 4.2, presentaba un mayor rigor, al vedar el uso para finalidades *distintas*.

La jurisprudencia de la Audiencia Nacional (rec. 1067/2000, 650/2001 y 119/2002) aunque tiende a desconsiderar el cambio terminológico, argumentando que, desde el punto de vista de una interpretación sistemática, el cambio no tiene sentido, vaciando la protección de la recolección con fin "determinado". Así, el adjetivo "incompatible" funciona en la práctica vedando cualquier uso para finalidad "distinta"[761].

El estudio de las decisiones sobre finalidades incompatibles demuestra la intención de la jurisprudencia en sancionar prácticas antes consideradas comunes. Son prácticas vedadas: compañía telefónica que franquea a otra empresa datos de sus clientes para promoción comercial de ésta de servicios de telecomunicaciones[762]; utilizar las bases de datos de los colegiados para enviar carta pidiendo voto para

[761] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 147.
[762] SAN, Sección 1ª , 11 de febrero de 2004, rec. 119/2002.

elección en el "Colegio Oficial de Agentes Comerciales"[763]; e igualmente cuando la empresa se aprovecha de la publicidad exigida de los nombres de los propietarios afectados por proyecto de desarrollo urbanístico del *ayuntamiento* para declarar que el plano contiene errores y pone a disposición a sus abogados y arquitectos. Aquí es relevante notar que la recolección legítima (pues las informaciones fueron y estaban en proceso administrativo abierto a consulta y forma publicadas en *boletín oficial*) no equivale a un uso legítimo, ya que la divulgación pretendía solamente la participación ciudadana en la defensa de los intereses afectados[764]. Por otro lado, las hipótesis de *fin compatible*, exigen una intención de protección del bien común, sea del alcalde que envía cartas a los pobladores nacidos en otra localidad anunciando la llegada del alcalde a la ciudad natal, lo que favorecería la integración social de la localidad[765], o cuando la empresa protege la confianza a sus antiguos clientes al informar que no posee vínculo con su sucesora[766].

Hay, sin embargo, una presunción absoluta de compatibilidad en los tratamientos para fines históricos, estadísticos o científicos (LOPD, art. 4.2 y RD 1720/2007, art. 9.1[767]). El denominador común en esas hipótesis es una utilización desvinculada de la afectación a los individuos sobre los cuales hubo recolección de datos, pero objetivando primordialmente alcanzar conclusiones en un estudio relativo a cualquier ramo del

[763] SAN, Sección 1ª , 29 de marzo de 2006, rec. 48/2006.
[764] SAN, Sección 1ª , 21 de diciembre de 2006,, rec. 265/2005.
[765] SAN, Sección 1ª , 21 de abril de 2004, rec. 637/2002.
[766] SAN, Sección 1ª , 15 de junio de 2005, rec. 669/2003.
[767] "Artículo 9. Tratamiento con fines estadísticos, históricos o científicos.
1. No se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.
2. Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias."

conocimiento, abarcando ciencias exactas, naturales y sociales[768].

Ello se confirma en el art. 17.2 de la Ley 41/2002[769], que permite investigación desde que sea evitado que el paciente no esté identificado, y las Leyes 12/1989 (art. 19[770]) y 16/1985 (art. 57.1.c[771]) entienden que la información personal de carácter estadístico e histórico depende de transcurridos 25 años tras la muerte del afectado, caso esta fecha sea conocida, o entonces 50 años tras la producción del documento para ser permitida su divulgación sin consentimiento a terceros sin intereses legítimos. O sea, tiempo bien condecente para que la información revelada sea inocua a la vida del

[768] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 186.

[769] "Artículo 17. La conservación de la documentación clínica.
1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aun que no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.
2. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas.
3. Los profesionales sanitarios tienen el deber de cooperar en la creación y el mantenimiento de una documentación clínica ordenada y secuencial del proceso asistencial de los pacientes.
4. La gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la unidad de admisión y documentación clínica, encargada de integrar en un solo archivo las historias clínicas. La custodia de dichas historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario.
5. Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen.
6: Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal."

[770] "Artículo 19.
1. La obligación de guardar el secreto estadístico se iniciará desde el momento en que se obtenga la información por él amparada.
2. La información a que se refiere el apartado anterior no podrá ser públicamente consultada sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida o, en otro caso, de cincuenta años a partir de la fecha de su obtención."

[771] "art. 57.1.c Los documentos que contengan datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida, o, en otro caso, de cincuenta años, a partir de la fecha de los documentos."

individuo referido[772].

4.3.2.2 Principio de la Información

También es tratada en la legislación española la hipótesis de *información*, ya presente, como es visto, en la Directiva 95/46/CE, lo que permite que la doctrina española hable de un "principio de transparencia del tratamiento"[773] o "deber de información sobre el tratamiento"[774], que sería la publicidad del tratamiento al interesado de forma que, en la mayor parte de los casos, se aplique el sistema de carácter preventivo en su totalidad. Sólo puede haber verdadero e íntegro consentimiento del afectado si él fue adecuadamente informado.

Ese derecho a la información viene regulado en el derecho español en el artículo 5 de la LOPD, cuyos apartados 1,2 y 3 corresponden al art. 10 de la Directiva 95/46/CE y cuyos apartados 4 y 5 tratan de la misma materia del art. 11 de la Directiva Europea. Tenemos aquí, por tanto, desde el punto de vista de la regulación dos tipos de obligación de informar, cuando los datos son recogidos del afectado y cuando no.

Ese deber de informar existe para el responsable por la base de datos o por el tratamiento (RD 1720/2007, art. 18) inclusive cuando el interesado voluntariamente provee sus informaciones personales, como cuando busca un empleo o crédito para la

[772] Esta definición de la naturaleza científica, histórica o estadística de determinado dato tendrá aplicación en cualquier momento que la LOPD se refiera a esta terminología.
[773] HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales … cit.*, p. 55.
[774] REBOLLO DELGADO, Lucrecio. *Derechos fundamentales y protección de datos... cit.*, p. 148.

compra de bienes[775]. Igualmente no se exime de ese deber cuando subcontrata el levantamiento de datos[776]. Y esta obligación se renueva cuando hay cualquier cambio del grupo que dirige la empresa responsable por la base de datos, por estar configurada, por el derecho español, verdadera cesión de datos, en la forma del artículo 19 del RD 1720/2007[777].

La información debe ser dada de forma *expresa*, por lo general puede darse indistintamente por medio oral o de escrita legible (tanto en claridad de la grafía como en el tamaño de la fuente)[778], pero así obligatoriamente cuando los datos sean recogidos por medio de formulario (art. 5.2), y de manera *precisa* e *inequívoca* (art. 5.1, "caput").

Ello significa decir, según el entender de la jurisprudencia, que no debe permitir dudas razonables o conformarse en términos genéricos. Por ello, ya fueron judicialmente confirmadas sanciones administrativas relativas a expresiones contractuales como "autoriza (…) su cesión a otras empresas del grupo"[779], pues no es claro quiénes son estas, o en la determinación de la finalidad amplísimamente como "proporcionarle los mejores servicios"[780]. También no son admitidas deducciones de que el afectado sabría de la base de datos independientemente, por constar tal información en otros documentos y comunicados de la empresa que sometía ficha de

[775] SAN, Sección 1ª , 31 de enero de 2003, rec. 534/2001.
[776] STS, Sala 3ª , 17 de abril de 2007, rec. 3755/2003.
[777] "Artículo 19. Supuestos especiales : En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre."
[778] Inclusive por medio de carteles en locales visibles, como aclara el Informe 304/2005 de la AEPD.
[779] SAN, Sección 1ª , 21 de abril de 2004, rec. 488/2002.
[780] STS, Sala 3ª , Sección 6ª , 11 de abril de 2005, rec. 4209/2001.

registro a sus empleados, autónomos y franqueados[781].

Específicamente en sus letras el art. 5.1 impone que aquel al que se solicitan datos sea avisado de la existencia y finalidad de la eventual base de datos o tratamiento de la información y de sus destinatarios, con identidad y dirección del responsable por el tratamiento y de su representante (letras "a" y "e"). De orden práctica, nótese, por ejemplo, que hay una diferencia significativa en la utilización de elementos brindados relativos a su salud por un médico y por un programa de televisión[782].

Debe ser igualmente alertado en cuanto al carácter obligatorio o facultativo de las respuestas y de las consecuencias de la decisión positiva o negativa en proveer los datos y en cuanto a los inherentes derechos de acceso, rectificación, cancelación y oposición (art. 5.1. b), c) y d)), aunque haya dispensa en la explicación de cualquiera de estas hipótesis, cuando se tornen evidentes las circunstancias (art. 5.3).

El principal efecto que se debe destacar, en la negativa de informar, es la imposibilidad de la celebración de contrato con persona que se niega a identificar, pero esa cláusula del artículo 5.3 también puede ser aplicada en otras situaciones, como en cuanto a las relaciones jerárquicas en que servidores públicos se recusan a prestar las informaciones necesarias para la puesta en marcha de "sistema de punto". En este caso, afirmó la sentencia del Tribunal Superior de Justicia de Cantabria, del 16 de mayo de 2003 (rec. 630/2002), que obviamente es de aplicación el régimen disciplinario autonómico.

[781] SAN, Sección 1ª , 30 de noviembre de 2001, rec. 417/2000.
[782] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 171.

Hay obligatoriedad de "transparencia", también de forma precisa, expresa e inequívoca, aun cuando el afectado no ayuda en la recolección. Ello sólo se excluye cuando el interesado ya fue previamente informado y en cuanto a las letras "b" y "c" del art. 5.1, que tratan de la voluntariedad del sometimiento del dato y, por tanto, son incompatibles con esta hipótesis (LOPD, art. 5.4). Aunque, aquí la normalización española presenta una importante diferencia con relación a los términos de la Directiva 95/46/CE, pues, mientras en esta, en el artículo 11 exige que la información se dé en el momento del registro o de la primera utilización, la ley española garantiza un plazo de 3 meses para hacerlo[783].

Se exceptúa la obligatoriedad de información al afectado cuando exista la regulación de la cesión por ley especial y esta no la prevea[784], en cuanto a los datos para fines históricos, estadísticos o científicos o cuando el aviso al interesado sea imposible o exija esfuerzo desproporcionado (art. 5.5 de la LOPD). En este último caso la decisión en cuanto a la adecuación del caso concreto a esos conceptos jurídicos indeterminados se da a juicio de la Agencia Española de Protección de Datos, por medio de un procedimiento administrativo en la forma de los artículos 153 a 156 del RD 1720/2007, y ponderado con posibles medidas compensatorias del no seguimiento estricto del artículo 5.4.

También es dispensable la comunicación cuando la recolección se dio en fuente accesible al público para publicidad o prospección comercial, pero al menos debe ser

[783] Hay regla especial a este plazo en el art. 29.2 de la LOPD, que habla en notificación en 30 días en lo que respecta a obligaciones crediticias.

[784] Como admitió la AEPD en cuanto a la disposición adicional 7ª. a la ley 7/1985, que permite que la Dirección General de la Policía conozca extranjeros *empadronados* en los municipios (Informe 60/2007), y para la comunicación de operación financiera por banco a la "Comisión de Vigilancia" en razón de la ley de prevención y bloqueo de la financiación al Terrorismo – ley 12/2003 (Informe 290/2005).

manifestada al afectado el origen del dato, el responsable por el tratamiento y sus derechos (art. 30.2 de la misma ley).

4.3.2.3 Principio del Consentimiento

La idea de *consentimiento* del afectado, cuyo estadio temporal es necesariamente tras la noción de *información* anteriormente tratada, es tan central al modelo europeo de protección de datos que uno de los mayores y más antiguos estudiosos españoles sobre el tema afirmó en una de sus obras que este "es la piedra angular a partir del cual se construye el sistema de protección de datos personales."[785]. Ya SERRANO PÉREZ se refiere al consentimiento como el primer pilar del derecho fundamental sobre la protección de datos, donde la libertad y dignidad humana se presentan en ese espacio de nuestra existencia (siendo el segundo pilar compuesto por los derechos que favorecen su protección)[786].

El "*principio del consentimiento*" es regulado en el artículo 6º de la ley orgánica 15/99 en condiciones semejantes a la del artículo 7º de la Directiva, o sea, estipulando como regla general la característica de un consentimiento "inequívoco". Es entendido que ese vocablo debe ser interpretado conforme su definición en el diccionario, o sea, que no debe haber ninguna duda en cuanto a la voluntad asentida, pero que no hay forma ni momento preestablecido, pues cuando la ley quiso tornar el consentimiento obligatoriamente expresado, escrito o previo así lo hizo (en el artículo 7.2)[787].

---

[785] MURILLO DE LA CUEVA, Pablo Lucas. Informática y protección de datos personales: estudio sobre la ley orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal. Madrid: Centro de Estudios Constitucionales, 1993.

[786] SERRANO PÉREZ, María Mercedes. "El derecho fundamental a la Protección de Datos... *cit.*, , p. 255.

[787] VIZCAÍNO CALDERÓN, Miguel. *Comentarios a la ley orgánica de protección de datos de carácter*

O sea, en cuanto a la forma no hay en la regla general del art. 6.1 del "consentimiento inequívoco" cualquier requisito legal, siendo posible inferir la manifestación de voluntad favorable a la utilización del dato a través de actitudes claras del afectado que no dejen dudas, como, por ejemplo, cuando estando informado de que el dato será utilizado, completa y entrega el formulario sobre sí, o cuando mantiene pagos inclusive con sus datos modificados sin su actuación, demostrando su no molestia[788], o inclusive, cuando entregó voluntariamente su tarjeta de visita con e-mail electrónico en stand comercial[789].

Esa posibilidad amplia de un "consentimiento tácito" no debe ser confundida con una autorización en el mismo sentido para el "consentimiento presumido", o sea, aquel que, al contrario, se cree en el consentimiento por la ausencia de actos, por el silencio del afectado[790]. En este caso la interpretación de la ley orgánica 15/99 debe ser conjugada con la jurisprudencia más general sobre el tema del Tribunal Supremo, que afirma que:

> "A tenor de las Sentencias de 24 noviembre 1943 (RJ 1943\1292); 11 noviembre 1958 (RJ 1958\3442); 3 enero 1964 (RJ 1964\116); 29 enero 1965 (RJ 1965\262) y 10 junio 1966 (RJ 1966\3028), el consentimiento tácito ha de resultar de actos inequívocos que demuestren de manera segura el pensamiento de conformidad del agente, sin que se pueda atribuir esa aceptación al mero conocimiento, por requerirse actos de positivo valor demostrativo de una voluntad determinada en tal sentido, exigiendo el consentimiento tácito la realidad de un acto

personal. Madrid: Civitas, 2001, p. 115.

788 SAN, Sección 1ª , 20 de septiembre de 2006, rec. 626/2004.

789 SAN, Sección 1ª , 17 de mayo de 2007, rec. 157/2005.

790 APARÍCIO SALOM utiliza esos términos en el sentido contrario al optado por el texto, como se ve de este pasaje: "el consentimiento tácito es más una forma de consentimiento presunto o implícito, que se diferencia por el hecho de que la deducción del contenido de la voluntad no se obtiene de actos del interesado, sino de su falta de actuación, de su silencio." (APARICIO SALOM, Javier. *Estudios sobre la ley orgánica ... cit.*,, p. 71). Sin embargo, a pesar de ser un autor con notable influencia en el tema en el derecho español, esa definición suya vaen el sentido contrario a lo que se encuentra en la jurisprudencia española, en el derecho brasileño e inclusive, en otros autores ibéricos. Así, se optó por mantener el sentido de acto tácito aquel que proviene de comportamientos y no de la declaración de voluntad, manteniendo la idea de presunción para los silencios de que la ley extraye efectos.

> que ponga de relieve el deseo o voluntad del agente, sin que ofrezca la posibilidad de diversas interpretaciones, insistiéndose en que el silencio absoluto no es productor de efectos jurídicos mas que en el caso de que la ley o la voluntad de las partes se le reconozca o conceda previamente"[791]

APARÍCIO SALOM, en sentido contrario, trataba como hipótesis admisibles de "consentimiento presumido" aquellas existentes en el texto de la LOPD en que no exige el consentimiento del interesado, pero se requiere su información, como ocurre en los artículos 5.4, 5.5, 6.2, inciso tercero, 11.2 b) y 30[792]. Es una posición con la cual no es posible concordar, pues la ley en estos casos exactamente dice que no existe el consentimiento La información simplemente abre la posibilidad del derecho de oposición por el interesado al tratamiento (advenida del artículo 14 de la directiva europea) en un segundo instante, no negando que la recolección inicial sin consentimiento por el responsable por la base de datos ocurrió de manera legal.

No hay, por tanto, en la LOPD cualquier hipótesis legal de valoración del puro silencio, de la sencilla inacción, al consentimiento. Sin embargo, en el RD 1720/2007, artículo 14, hay una posibilidad de iniciar el tratamiento de algún dato que exija consentimiento expreso del interesado caso este se mantenga sin negarlo tras 30 días de tomar conocimiento. Ese silencio productor de consentimiento por fuerza legal puede ahora ser considerado el único "consentimiento presumido" en la protección de datos en el derecho español.

La "revocación de consentimiento" está prevista en el artículo 6.3 de la LOPD y en el artículo 17 del Real Decreto de reglamentación, la cual torna un uso y divulgación antes legítima en ilegal. El Decreto habla en un medio de revocación simple y gratuito,

---

[791] Sentencia de la Sala de lo Civil, del 23 de julio de 1998 (RJ 1998, 6137), FJ 2.
[792] APARICIO SALOM, Javier. *Estudios sobre la ley orgánica ... cit.*,, p. 76.

como a través de servicio de atención al público, y que la interrupción de utilización por el que recoge y por sus cesionarios debe ocurrir en un plazo máximo de 10 días, lo que tiene especial efectividad sobre servicios de guía telefónica, publicadas en papel o por medio de Internet, ya que aquí el deseo de la no divulgación exactamente se confunde con el derecho a la no publicación[793]. Ello no se confunde con el "derecho de oposición" de tratamiento de los datos (art. 6.4 de la LOPD), porque mientras en el anterior hubo consentimiento, en este ocurrió una de las situaciones de dispensa legal del consentimiento.

La ley, en el apartado 2 del artículo 6, exceptúa la necesidad del consentimiento en cuatro casos: cuando el tratamiento sea necesario al cumplimiento de un acuerdo contractual o precontractual laboral o de naturaleza administrativa realizado por el afectado; cuando se proteja un "interés vital"[794] su, concepto que adquiere contornos semejantes a la de un específico "estado de necesidad"[795]; en el caso de informaciones adquiridas en fuentes accesibles al público[796], pero bajo la condición de que haya un "interés legítimo" de quien recoge y que no se violen libertades y derechos del afectado; y finalmente por el interés público existente en alguna de las funciones propias de la Administración Pública (art. 6.2), lo que debe ser contrastable frente a las finalidades del fichero constituido conforme el artículo 20 de la LOPD. Ese último caso incluye la

[793] Hay frecuentes juzgados sobre el tema, vide SAN, Sección 1ª , 10 de mayo de 2006, rec. 528/2004, SAN, Sección 1ª , 23 de marzo de 2006, rec. 434/2004 y SAN, Sección 1ª , 10 de mayo de 2006, rec. 528/2004.

[794] Definidas como las situaciones de urgencia en los términos del art. 7.6 de la misma ley, como aquel que "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 se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.".

[795] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 234.

[796] La Audiencia Nacional, en el fundamento jurídico 4 del juzgado relativo al recurso contencioso administrativo n. 3517/2000, del 28 de septiembre de 2001, presenta la importante distinción entre "fuente accesible al público" y hecho notorio y de dominio público, al mantener sanción a la empresa turística que se utiliza de información sobre filiación a partido político de ciudadano que, aunque de conocimiento general, no se encontraba en la primera.

formación de registros en cuanto a las personas involucradas en relaciones de trabajo junto al Estado y no solamente en lo que respecta a la actividad fin[797].

El "principio del consentimiento" es de aplicación también en cualquier revelación de datos del responsable de la base de datos a terceros que no sea el afectado con vistas a nuevas especies de tratamiento[798].

Esa cesión (o transferencia) puede ocurrir a través del pasaje material del dato o con la disponibilidad del acceso al sistema[799]. En la cesión de datos el consentimiento debe ser *previo* (art. 11.1), sin perjuicio de ser inequívoco siempre y expresado y escrito conforme la naturaleza de los datos[800]. La jurisprudencia de la Audiencia Nacional viene entendiendo que la anuencia posterior no remedia el vicio del pasaje del dato antes del consentimiento, persistiendo la infracción administrativa[801].

Aunque este apartado 1 del artículo 11 enumere tres requisitos para la cesión, cuáles sean atender a los fines legítimos de cedente y cesionario y tener el consentimiento del afectado, VIZCAÍNO CALDERÓN adopta aquí una "interpretación flexible", sólo entendiendo imprescindibles los dos últimos, lo que se conformaría mejor a la idea de *autodeterminación* presente en la protección de datos y también en

---

797 STS, Sala 3ª, Sección 3ª, 14 de diciembre de 2005, rec. 7/2005.

798 Este trazo final, de mantenimiento del vínculo original (RD 1720, art. 20.1), diferencia un mero encargado del tratamiento (art. 12 de la LOPD), que es un prestador de servicios para el responsable por la base de datos, de un cesionario de datos.
La AEPD y la doctrina española vedan que haya subcontratación por el encargado del tratamiento, "dado el riesgo que, frente al interesado, implica la ausencia de conocimiento de la localización y alcance del tratamiento de sus datos de carácter personal, y ello en aras a no vaciar de contenido el concepto de autodeterminación informativa, base la vigente LOPD" (BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 321).

799 SAN, Sección 1ª , 9 de noviembre de 2001, rec. 565/2000.

800 BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 292.

801 SSAN, Sección 1ª, 25 de junio de 2003 (rec. 1099/2000), Sección 1ª, 21 de junio de 2002 (rec. 1064/2000) y Sección 1ª , 11 de octubre de 2002 (rec. 1115/2000).

una visión lógica de la LOPD, ya que para flujos transfronterizos de datos basta este consentimiento, en la forma del artículo 34.e)[802].

La ley española admite, sin embargo, una serie de excepciones a la necesidad del consentimiento del afectado para la cesión (art. 11.2, letras "a" a "f"). Puede ocurrir autorización en otra ley, como en lo que respecta a la "Comisión Nacional de Mercado de Valores" (CNMV), que posee, por fuerza del artículo 85 de la ley 24/1988 el poder de requerir las informaciones necesarias al cumplimiento de sus fines; pueden los datos ser recogidos de "fuentes accesibles al público"; la transmisión también se autoriza si inherente a otra relación jurídica libremente aceptada; cuando tenga como destinatario el Defensor del Pueblo, el Ministerio Público, el Poder Judicial[803] o el Tribunal de Cuentas u órganos con funciones análogas, sean estatales o autonómicos, dentro del ejercicio de las funciones que le son atribuidas; cuando se dé entre Administraciones Públicas y con miras a fines históricos, estadísticos o científicos; y, en cuanto a datos de salud, para solucionar alguna urgencia o para realizar estudios epidemiológicos establecidos en la legislación sanitaria[804].

En la penúltima hipótesis de cesión sin consentimiento, en el ámbito de Administraciones Públicas, el art. 10.4.c) del RD 1720 desarrolló dos posibilidades más, que el dato sea producido por una con destino a otra o que la comunicación pretenda el ejercicio de competencias idénticas o tengan ellas por objeto las mismas materias. Esta

802 VIZCAÍNO CALDERÓN, Miguel. *Comentarios a la ley orgánica... cit.*, p. 160.

803 Aunque el Tribunal Supremo veda que particular traiga a los autos en proceso civil documento que contenga dato de tercero que a él no podría haber sido cedido, el pedido y la entrega deben ser directo al juicio (STS, Sala 3ª , 12 de abril de 2005, rec. 664/2001).

804 El Informe 381/2003 de la AEPD concluye, analizando las disposiciones sobre mantenimiento de datos sobre la salud de pacientes en la LOPD y en el artículo 17 de la Ley 41/2002, que no hay disposición del legislador en pro de la destrucción inmediata de eses datos tras el tratamiento; al contrario, usos posteriores pueden salvaguardar la integridad física y la sobrevivencia de este individuo. Aunque el uso para otros fines debe preservar la confidencialidad de la relación o conseguir su consentimiento.

inclusión simplemente une lo previsto en el artículo 11 de la LOPD con lo que ya constaba en el artículo 21 de la misma ley sobre el título "Comunicación de Datos entre Administraciones Públicas".

El interesado debe ser previamente informado por el cedente sobre la finalidad exacta a la que se destinan los datos y la actividad de quien se pretende comunicar, bajo pena de nulidad (art. 11.3). Además en los juzgados se verifica que el consentimiento no es admitido cuando está basado en cláusulas amplias o genéricas de contratos[805], siendo que hay habitual inversión de la carga de la prueba en favor del afectado[806]. Tal como el consentimiento para la recolección, este también es revocable (art. 11.4).

Ello no significa ausencia de responsabilidad del cesionario, que deberá, evidentemente, respetar las disposiciones de la LOPD (art. 11.5), y también verificar diligentemente si los datos que recibieron tuvo un consentimiento adecuado en la transmisión, bajo pena de sanción[807].

No son consideradas "cesiones de datos personales" aquellas en que los datos son previamente "disociados" (art. 11.6), pues entonces los datos dejan de entrar en la clasificación de personales, ya que se tornan impracticables para identificar al individuo, y cuando el acceso por terceros se da tan solo para la prestación de servicios al responsable por el tratamiento, siempre serán respetadas las medidas adecuadas de seguridad (art. 12).

[805] SSAN, Sección 1ª , 29 de abril de 2005 (rec. 259/2003), 30 de noviembre de 2005 (rec. 133/2004) y 18 de mayo de 2006 (rec. 429/2004).
[806] Vide STS, Sala 3ª , 4 de abril de 2002(rec. 8065/1995).
[807] SSAN, Sección 1ª , 30 de junio de 2004 (rec. 619/2002) y 2 de marzo de 2006 (rec. 355/2004).

4.3.2.4 Datos especialmente protegidos

También aparece en la Ley Orgánica de Protección de Datos una categoría en la que hay una *protección reforzada*, en el mismo sentido de los "datos sensibles" de la legislación europea precedente. No se brinda una definición exacta de lo que sean eses datos, sino una enumeración de cuáles sean, que magnifica los cuidados en su utilización independientemente del contexto en que esta ocurra[808].

Se infiere en la interpretación sistemática de este artículo que en la legislación española hay una gradación dentro de la categoría de los datos sensibles que no encuentra paralelo en el artículo 8º de la Directiva 95/46/CE. Por ello, informaciones relativas a ideología, religión y creencias (valores expresamente listados también en el artículo 16.2 de la Constitución Española[809]) y la filiación sindical encuentran su reglamentación en los apartados 1 y 2 del artículo 7 y otras, como origen racial, orientación sexual y salud son tratadas a partir del apartado 3.

El apartado 1 repite el apartado 2 del artículo 16 de la Constitución Española, al vedar la obligación en la declaración sobre elecciones de religión, ideología y creencias. Obsérvese que eso no puede ser considerado como una protección menor a la afiliación sindical con relación a estas, pues el Tribunal Constitucional Español, en la STC 292/1993, decidió que también la afiliación sindical puede ser considerada una forma de ideología y por lo tanto, está protegida por el artículo 16 de la Constitución. Se encuentra así en el FJ 5 de este fallo la siguiente declaración: **"Siendo los sindicatos**

[808] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 216.
[809] "Art. 16.2. Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias."

formaciones con relevancia social, integrantes de la estructura pluralista de la Sociedad democrática, no puede abrigarse duda alguna que la afiliación a un sindicato es una opción ideológica protegida por el art. 16 de la CE, que garantiza al ciudadano el derecho a negarse a declarar sobre ella"[810].

En el art. 7.2 hay un aumento en el "consentimiento", que pasa de "inequívoco" para "expreso y por escrito", en estos casos y para la afiliación sindical.

Ese *plus* de requisito para el consentimiento en esa gestión de datos sólo es excluido cuando se trata de archivos propios de partidos políticos, sindicatos, iglesias y asociaciones en general sin fines de lucro y con finalidades de carácter político, filosófico, religioso o sindical y no incluye la permisión a la cesión de esos datos (art. 7.2)[811]. Esta parte final del apartado adopta una solución semejante a la del artículo 8.2.d) de la directiva.

Hay informes de la AEPD y fallos que exponen soluciones de conflictos en este tema. En el informe 382/2005 se entiende que la filiación partidaria (ideología) no puede ser divulgada por el partido a terceros, sino que puede ser gestionada incluso, por órganos de gobierno y representación en un sistema parlamentarista como el español. Tampoco los sindicatos pueden revelar sus listas de asociados[812].

---

[810] Cursiva en el original.

[811] "7.2. 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."

[812] STS, Sala 3ª , Sección 7ª , 30 de marzo de 2001, rec. 6153/1996.

En la decisión de la Audiencia Nacional, Sección 1ª, del 31 de enero de 2003 (rec. 534/2001), se confirmó la grave infracción contra un programa de televisión que impuso un cuestionario con preguntas sobre opción política, religiosa y sexual a participantes del programa sin dejar clara la posibilidad de no responder, lo que no es sustituible por el relleno voluntario. Sin embargo, la negativa o aceptación de cursar disciplina vinculada a la religión en la escuela no equivale a la declaración del apartado 1, pues es una simple declaración de preferencia con el fin de conformar el plan de estudios (STS, Sala 3, Sección 7ª, 25 de enero de 2005 – rec. 119/2003).

En la segunda clase de datos especialmente protegidos (origen racial, salud y vida sexual) el consentimiento pasa a ser expresado (ya no escrito obligatoriamente) y puede ser prescindido habiendo ley que indique el interés general que ello justifique (art. 7.3 de la LOPD). En ese sentido la policía local del *Ayuntamiento* de Alcobendas fue impedida de recoger datos de etnia, vida sexual y vicio en estupefacientes (salud) en sus archivos porque no había consentimiento de los afectados, ley de permisión o infracción concreta a ser evitada[813], y cuyo uso tendría carácter posiblemente discriminatorio. Por otro lado, registro de pacientes portadores del HIV creado por ley y con las medidas de seguridad necesarias para preservar a los infectados sería justificable por el interés público en la prevención de epidemias[814].

En el derecho español, la definición de dato personal relativo a la salud es dado por el artículo 5.1.g) del RD 1720, que adopta en líneas generales la definición constante del ítem 1 del apéndice de la Recomendación n. R 97 (5) del Comité de

[813] SAN, Sección 1ª , 8 de junio de 2001, rec. 1133/1999.
[814] MIGUEL SÁNCHEZ, Noelia de. "Análisis de la sentencia del Tribunal Supremo de 9 de julio de 2007, relativa al fichero Sistema de Información sobre Nuevas Infecciones (SINIVIH): una obligada reflexión en torno al principio de seguridad." Revista jurídica de Castilla y León, n. 16, 2008, p. 311.

Ministros del Consejo de Europa: son "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.". Conforme el informe 129/2005 de la AEPD también se incluye en el concepto de salud informaciones sobre consumo de estupefacientes, pero no la sencilla anotación del uso de alcohol y nicotina sino referencia a la cantidad (un campo "fumador", por ejemplo).

Está vedada la creación de bases de datos cuyo propósito exclusivo sea guardar datos personales relativos a las convicciones ideológicas o religiosas, de afiliación sindical y de origen étnico, racial o sobre la vida sexual (art. 7.4). Es de admitir, no obstante, que sean los datos que involucren, especialmente, cuestiones referentes a la salud de los individuos los que puedan ser utilizados cuando es necesario para el diagnóstico médico[815] y la gestión y prevención sanitaria, siempre con la observancia de la seguridad inherente al tratamiento debe ser realizado por los profesionales sujetos al secreto profesional (art. 7.6)[816]. La confidencialidad de los datos relativos a la salud se ve reforzada también por las medidas de seguridad previstas en los artículos 14 al 17 de la Ley 41/2002.

Las condenaciones relativas a infracciones penales y administrativas son tratadas de la misma forma como "datos sensibles", con archivamiento solamente mediante norma reguladora (art. 7.5). Sin embargo, el texto español difiere del art. 8.5 de la

[815] También art. 8, LOPD.

[816] Nótese, sin embargo, que "Siendo así que es regla general la exigencia del consentimiento inequívoco del afectado para el tratamiento de datos de carácter personal (artículo6.1 Ley Orgánica 15/99)-y sabemos que el legislador ha querido reforzar esta exigencia cuando se trata de datos especialmente protegidos (artículo7.2y7.3)-las excepciones a dicha norma general, como la prevista en el artículo 7.6, deben ser *interpretadas de modo estricto* sin que quepa admitir otros casos de dispensa del consentimiento distintos al que aparece expresamente contemplado en la norma." (SAN, Sección 1ª , 26 de septiembre de 2002, rec. 581/2001). (cursiva nuestra).

Directiva al sólo exigir que la titularidad de la base de datos sea pública, sin incluir también el control o gestión, y por no tratar sobre la gestión de los datos de los procesos de naturaleza civil[817]. De todas formas, el tratamiento de ese tipo de dato no puede ser efectuado por asociaciones de derecho privado, aun siendo su finalidad exponer a la sociedad crímenes cometidos, como casos de torturas y maltratos, y cuyo conocimiento se efectuó por medio de petición en los propios procesos judiciales[818].

4.3.2.5 Principio de la Seguridad

La protección de datos personales se completa con el "*principio de seguridad*", que no se refiere a licitud del tratamiento, como los demás, sino a los riesgos del tratamiento. El Tribunal Constitucional español ya en el comienzo de la década del 90 comprendió que, en la protección a datos personales, la defensa de los sistemas informatizados contra agentes externos (*hackers*) tiene tanto significado como establecimiento jurídico de normas bien ponderadas. Afirmó el TC, en el fundamento jurídico 7 de la sentencia 143/1994, que "(...) un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta.".

El "principio de la seguridad" es concretizado en reglas que establecen

[817] HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales … cit.*,p. 60.
[818] SAN, Sección 1ª , 28 de febrero de 2003, rec. 1062/2000.

comportamientos activos exigibles del responsable y del encargado del tratamiento consistente en medidas de carácter técnico y de organización necesarias para evitar la alteración, pérdida o acceso no autorizado a los datos almacenados[819] (art. 9). Así, complementado el nivel de reglamento, se establecen niveles de seguridad en básico, mediano y alto, conforme el tipo de dato almacenado, y controles clasificables como *directivos*, que son los que establecen las bases o políticas de protección, *preventivos*, para evitar intromisiones de terceros, correctivos, para rectificar errores intencionales o por negligencia o impericia, y de *recuperación*, que pretendan restablecer la situación anterior al eventual accidente o invasión que ocurra[820].

Las medidas de seguridad desde el punto de vista técnico son tratadas en los artículos 79 al 114 del Real Decreto 1720/2007. Todos aquellos que gestionan archivos deben adoptar las medidas de seguridad de nivel básico, siendo que, en cuanto a la Administración Pública, las fiscalizaciones tributarias, de entidades financieras, la Seguridad Social y órganos que controlan condenas penales y administrativas deberán también adoptar las prevenciones de nivel medio (artículo 81.2). Por último, datos en cuanto a violencia de género y de naturaleza "sensible", independientemente del titular de la base de datos, y cualquier otro cuyas Fuerzas Policiales gestionan sin el consentimiento del interesado también necesitan medidas de nivel alto (art. 81.3).

Una gran cantidad de casos en que los Tribunales mantienen sanciones en razón del incumplimiento del "principio de seguridad" se refiere a empresas dueñas de bases de datos que permitieron que fuesen expuestas al público informaciones que deberían

[819] La seguridad de la privacidad en las comunicaciones electrónicas es tratada en el derecho español por la ley 32/2003 ("*General de Telecomunicaciones"*), que hizo ingresar las normas de la Directiva 2002/58/CE ("Directiva sobre la privacidad y las comunicaciones electrónicas").

[820] HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales … cit.*, p. 65.

resguardar para uso interno[821]. Además de vincular a los responsables por las bases de datos, impidiéndoles divulgar informaciones más allá de que los permisos legales abarquen también a sus empleados, ya que la LOPD crea un secreto profesional general, que se sobrepone a las categorías anteriormente existentes (art. 10). Excepcionalmente, sin embargo, esos deberes de confidencialidad impuestos por el derecho a la protección de datos pueden ser sopesados con la libertad de información, del artículo 20 de la Constitución Española, justificando la divulgación de dato personal que constituya noticia veraz y de transcendencia social[822].

4.3.3 Derechos de los Afectados

La efectividad de los principios relativos a la protección de datos se alcanza principalmente a través de los *derechos, inmunidades* y *poderes* otorgados a los afectados para defensa concreta de sus intereses, conformados a través de las facultades de oposición, de no soportar valoraciones automáticas, de consulta, acceso, rectificación y cancelación[823]. Los mismos serán objeto de nuestro estudio en la Ley Orgánica 15/99. Estos derechos son *personalísimos*[824], sólo pudiendo ser ejercidos por otros en caso de incapacidad o minoridad[825](RD 1720, art. 23), e *independientes* entre sí, no habiendo

[821] Vide SAN, Sección 1ª , 25 de enero de 2006, rec. 227/2004, SAN, Sección 1ª , 10 de noviembre de 2006, rec. 119/2005, SAN, Sección 1ª , 15 de octubre de 2003, rec. 1517/2001, entre otras.

[822] Vide, sobre este tema, la extensa fundamentación y precedentes jurisprudenciales presentes en la sentencia de la Sala del Contencioso de la Audiencia Nacional de 23 de noviembre de 2005 (rec. 109/2004).

[823] Aunque el artículo 19 de la LOPD trate del "derecho a la indemnización", esta posición jurídica no es derivada exactamente del derecho a la protección de datos, sino, en verdad, de su lesión gravosa a algún patrimonio material o moral del afectado que hace surgir el deber de recomponer pecuniariamente el daño.

[824] Lo que no significa la imposibilidad de constituir mandatario, desde que esté "expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél." (RD 1720, art. 23.2.c)).

[825] En los mismos términos de aquellos que no pueden dar consentimiento en la recolección de sus datos,

ninguna jerarquía o precedencia entre ellos (RD 1720, art. 24).

Personas fallecidas no pueden valerse de los derechos referentes a protección de datos, por medio de sus herederos, los cuales podrán solamente llevar el certificado de defunción al titular de la base de datos para fines de cancelación (RD 1720, art.2.4). Sin embargo, los herederos podrán conocer los datos del *de cujus* para facilitar su condición de sucesor (por ejemplo, para saber la ubicación de bienes) o en nombre de las finalidades de protección de la honra, intimidad e imagen del muerto, pero con base en la Ley Orgánica 1/1982, nunca de la LOPD[826].

4.3.3.1 Derecho de oposición

La primera facultad a aparecer en la ley española, ya en el artículo 6.4, es el de "*oposición*" al tratamiento. Su inclusión en el ordenamiento español sólo ocurre con la LOPD, y se basa en el artículo 14 de la Directiva europea.

Esto ocurrirá cuando el interesado posea motivos legítimos para reclamar contra una concreta situación en que haya permisión en la LOPD de utilizar sus datos sin su consentimiento, salvo, si hay otra ley que excluya, en la hipótesis, ese derecho suyo de oponerse. Esa facultad tiene el don de impedir que el tratamiento ni siquiera ocurra, o sea, tiene un carácter eminentemente previo, aunque pueda ser realizado a cualquier momento.

La respuesta del responsable por la base de datos al pedido será en el plazo

o sea, menores de 14 años, desde que otra causa que no les haya concedido madurez plena (Informe AEPD 466/2004).

826 BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 329.

máximo de 10 días (artículo 35.2 del RD 1720).

4.3.3.2 Derecho a no soportar valoraciones automatizadas

En el artículo 13 de la LOPD aparece un "*derecho a no soportar valoraciones automáticas*" basadas exclusivamente en tratamientos de datos. Verdaderamente se busca evitar la deshumanización de las interacciones sociales, manteniéndose contacto directo como la principal fuente de evaluación sobre el próximo. La preocupación del legislador español en este tema fue bien definida en la exposición de motivos de la LO 5/1992:

> "Los más diversos datos -sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado <dinero plástico>, sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideologías, por poner solo algunos ejemplos- relativos a las personas podrían ser, así, compilados y obtenidos sin dificultad. Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo deben tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que él autorice. Aún más: 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; 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."

Hay innovaciones frente a la directiva comunitaria que merecen evaluaciones distintas de la doctrina. Por un lado, se elimina la veda solamente de "tratamientos automatizados", como en la Directiva 95/46/CE, y sí, prohibir cualquier evaluación basada exclusivamente en tratamientos, inclusive manualmente. Por otro, los términos del apartado 13.3 permiten al responsable por el tratamiento proveer como información solamente criterios o programas sobre el cual se basó y no apenas una argumentación

comprensiva de todas las bases utilizadas[827].

Al mismo tiempo no puede negarse el amplio campo de aplicación de los análisis económicos computadorizados, especialmente en el sector de préstamos bancarios, que eliminan subjetivismos que violan el tratamiento igual, a pesar de su desvirtuación por las prácticas especulativas que condujeron a las recientes crisis financieras. El reglamento de *desarrollo* de la LOPD, pre crisis, admite esa realidad económica, al matizar el contenido del artículo 13 de la LO 15/1999 con la posibilidad de tratamientos automatizados desde que sea garantizada la posibilidad de defensa adecuada del interés del afectado (art. 36 del RD 1720).

De manera contraria, en el derecho penitenciario, su reglamento (RD 190/1996), en el artículo 6.1, veda de manera total que los apenados sufran evaluaciones exclusivamente automatizadas.

4.3.3.3 Derecho de Consulta

El artículo 14 de la LOPD trata del "derecho de consulta", que se refiere a la posibilidad de que gratuitamente cualquier persona sepa sobre la existencia de tratamientos de datos personales, de sus finalidades y de la identidad de sus responsables. El "derecho de consulta" ganó una fuerte efectividad en el derecho español a través del artículo 7º del estatuto de la Agencia Española de Protección de Datos (Real Decreto 428/1993), que determinó la AEPD que publicase anualmente una

[827] HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales … cit.*, p. 68.

lista completa de todos los *ficheros* inscriptos en el "Registro General de Protección de Datos". Hoy, esa posibilidad ciudadana se ve aun más facilitada, pues la Resolución de la Agencia de 1º de septiembre de 2006 determina que esta relación constará en su página (www.agpd.es), con actualización diaria.

Como establece con claridad la primera disposición de esa resolución de 1º de septiembre, el "derecho de consulta" tiene carácter eminentemente instrumental al proporcionar la realización de los derechos de acceso, rectificación, cancelación y oposición.

4.3.3.4 Derecho de Acceso

El artículo 15 aborda el "derecho de acceso"[828]. Es la facultad dada al individuo de solicitar y obtener información sobre sus datos sometidos a tratamiento. Nótese que la propia organización de las bases de datos debe facilitar el acceso de los interesados (artículo 4.6 de la LOPD).

Ese "derecho de acceso" integrante del derecho fundamental a la autodeterminación informativa no excluye otros derechos de acceder a informaciones (art. 27.3 del RD 1720). Especial interés para este tema tiene el expreso mantenimiento en este apartado del derecho de acceso previsto en el "Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común" (ley 30/1992).

[828] HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales … cit.*, p. 68. La autora afirma que este derecho también es conocido como *Habeas Data*. Es la misma denominación que la SAN del 9 de febrero de 2006 utiliza (anotando también como un sinónimo *Habeas Scriptum*). Sin embargo, desde el punto de vista del abordaje en este trabajo, no debe ser admitido ese posicionamiento, al mezclar el derecho subjetivo al medio procesal utilizado para su defensa.

El contenido de la atención al derecho de acceso puede ser realizado con la misma amplitud prevista por el "principio de la información"[829], inclusive con la determinación de las comunicaciones realizadas (RD 1720, art. 27.1). Sin embargo, también puede ser limitada en razón de la voluntad del afectado en su inquisición sobre punto específico o justificada por el nivel de complejidad en la atención por completo por el titular de la base de datos, cuando entonces el pedido debe ser completado por el interesado (art. 27.2).

El pedido de solicitud de acceso debe ser decidido por el responsable del fichero y respondido, positiva o negativamente, en cuanto a la posesión de datos, como máximo en 30 días (RD 1720/2007, artículo 29.1) a través del medio elegido por el afectado (carta, e-mail, tele copia o mera visualización en pantalla), salvo cuando la limitación se justifique en función de las condiciones de implantación material de la base de datos, desde que la forma ofrecida de atención sea siempre gratuita (art. 28 del RD y art. 15.2 de la LOPD).

En caso que la respuesta del responsable por la base de datos de que posee datos del solicitante no esté acompañada por los datos en concreto, el ordenamiento español todavía concede 10 días más para este envío (artículo 29.2 del RD). De toda forma, debe ser redactada de forma que sea comprensible al solicitante y no dependiente de algún mecanismo para su lectura (art. 29.3).

Comparando la legislación de la Unión Europea con la LOPD, se ve que el

829 BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 345.

legislador español incluyó también un plazo de intervalo para el ejercicio del derecho de acceso, salvo interés legítimo, de 12 (doce) meses entre uno y otro pedido (art. 15.3), lo que no estaba previsto ni en el Convenio n. 108 del Consejo de Europa, ni en la Directiva 95/46/CE, que meramente se refería en su artículo 12.a) de una "periodicidad razonable", con el fin meramente de evitar que el funcionamiento de la base de datos se vea inviabilizada por la reiteración caprichosa de pedidos ya atendidos[830]. Al mismo tiempo, como ya fue dicho, fue satisfactoria al garantizar la gratuidad del acceso (art. 15.1 de la LOPD) cuando la legislación europea aseveraba solamente el acceso "sin gastos excesivos"[831].

Señálese que la centralidad del derecho de acceso en la autodeterminación informativa puede ser verificada por la propia cuestión de fondo en la STC 254/1993. Se trata de un recurso de amparo basado en la negativa de entrega por parte de la Administración Pública, en la figura del Gobernador Civil de Guipúzcoa y del Ministro del Interior, de toda la información sobre los datos recogidos de un ciudadano. Así, en el FJ 9, el Tribunal Constitucional presenta una preciosa síntesis de la importancia del "derecho de acceso" en la protección de datos personales:

> "No es ocioso advertir que la reciente aprobación de la Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal [LO 5/1992, de 29 de octubre (RCL 1992\2347)] no hace más que reforzar las conclusiones alcanzadas con anterioridad. La creación del Registro General de Protección de Datos, y el establecimiento de la Agencia de Protección de Datos, facilitarán y garantizarán el ejercicio de los derechos de información y acceso de los ciudadanos a los ficheros de titularidad pública, y además extienden su alcance a los ficheros de titularidad privada. Pero ello no desvirtúa el fundamento constitucional de tales derechos, en cuanto imprescindibles para proteger el derecho fundamental a la intimidad en relación con los ficheros automatizados que dependen de los poderes públicos. Ni tampoco exonera a las autoridades administrativas del deber de respetar ese derecho de los ciudadanos, al formar y utilizar los ficheros que albergan datos personales de éstos, ni del deber de satisfacer las

[830] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 349.

[831] HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales … cit.,* p. 70. La autora escribe que el texto del art. 12.1 de la Directiva 95/46/CE y del art. 8.b) del Convenio del Consejo de Europa significa que los Estados pueden establecer una contraprestación del acceso desde que ésta no obstaculice el mismo.

peticiones de información deducidas por las personas físicas en el círculo de las competencias propias de tales autoridades.

Por consiguiente, el otorgamiento del presente amparo implica el reconocimiento del derecho que asiste al Sr. Olaverri que el Gobernador Civil le comunique sin demora la existencia de los ficheros automatizados de datos de carácter personal que dependen de la Administración Civil del Estado, sus finalidades, y la identidad y domicilio de la autoridad responsable del fichero. Igualmente, deberá comunicarle en forma inteligible aquellos datos personales que le conciernen, pero tan sólo los que obren en aquellos ficheros sobre los que el Gobernador Civil ostente las necesarias facultades.

Finalmente, el reconocimiento de estos derechos, derivados del art. 18 CE de conformidad con el Convenio del Consejo de Europa a la protección de datos personales de 1981, no obsta a que la autoridad administrativa deniegue, mediante resolución motivada, algún extremo de la información solicitada, siempre que dicha negativa se encuentre justificada por alguna excepción prevista por la Ley, incluido el propio Convenio europeo de 1981."

Desde el punto de vista lógico[832], tras haber utilizado el afectado de su derecho de acceso, se abre a él la posibilidad de utilizar los derechos de *rectificación*, *cancelación y bloqueo* de sus datos, entonces completándose una efectiva defensa contra la utilización abusiva de sus datos.

4.3.3.5 Derechos de rectificación y cancelación

Los derechos de rectificación y cancelación, aunque sean tratados conjuntamente en el artículo 16.2 de la LOPD, se basan en hipótesis distintas. La doctrina esclarece que la *rectificación*, que es el mero reemplazo de los datos almacenados, ocurre cuando estos sean incorrectos o inexactos, mientras la cancelación, o sea, su destrucción física o digital, se da cuando estos sean inadecuados o desproporcionales con relación al objetivo del tratamiento, o cuando el consentimiento sea revocado[833].

[832] En la práctica española, sin embargo, el derecho de cancelación es más utilizado que el derecho de acceso, ´se estima porque el individuo ya sabe donde consintió la entrega de su dato y ahora quiere simplemente borrarlo. Así, en el año 2005, hubo, entre todos los pedidos entregados en la AEPD, 53% referentes a cancelaciones y 42% de acceso (datos constantes de la *Memoria* de la Agencia del año 2005).

[833] HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales … cit.*, p. 70.

El responsable por el tratamiento debe hacer efectivo el derecho de cancelación o rectificación, o denegar el pedido motivadamente, en el plazo de 10 (diez) días (art. 16.1), que sirven también para informar el resultado al interesado[834], contados a partir del momento que reciba la solicitación (art. 32.2 del RD), y notificar a terceros cesionarios para que realicen el mismo cuando todavía estén utilizando aquellos datos (art. 16.4).

El pedido de cancelación puede ser rechazado por el titular de la base de datos cuando haya todavía una relación entre él y el afectado que justifique el mantenimiento del registro o cuando el almacenamiento se dé en razón de cumplimiento de disposición legal (RD 1720, art. 33). Por ejemplo, un *Colegio Profesional* puede mantener los datos de uno de sus inscriptos aun después de él haber pedido "baja" pues, está dentro de sus obligaciones mantener un registro de todos los profesionales..

Podemos destacar que el derecho de cancelación se transmuta en mero *bloqueo* mientras sea necesario a las Administraciones o al Poder Judicial para observar eventuales responsabilidades en razón del tratamiento ilegítimo (art. 16.3 de la LOPD y art. 5.1.b) del RD 1720), inclusive para verificar si el afectado tiene derecho a ser indemnizado por daño o lesión causado por el responsable por la base de datos. La responsabilidad civil en este caso puede ser de naturaleza pública o privada, conforme quien sea el responsable por el archivo de los datos (art. 19 de la LOPD).

El bloqueo debe ocurrir por medio de un aislamiento de la información, de

[834] STSJ de Madrid, Sala de lo Contencioso administrativo, 4 de junio de 2001 (rec. 1248/1998), teniendo en cuenta que en la ausencia de respuesta puede el interesado interponer el reclamo del artículo 18 de la LOPD por permisión del artículo 32.2 de la LOPD.

forma que torne imposible su utilización[835]. Tras ese plazo de prescripciones, sin embargo, es muy claro el posicionamiento de la Agencia española, constante en la norma tercera.8 del Informe 1/1998, de que "la cancelación exige el borrado físico de los datos, sin que sea suficiente a estos efectos una marca lógica o el mantenimiento de un fichero alternativo en el que se registren las bajas producidas.".

La cancelación es entendida efectivamente cumplida si la empresa retira los datos de sus archivos y, eventualmente, de Internet y si no envía ninguna correspondencia o emite publicación utilizándolos[836].

Hubo en esta década en España una serie de casos involucrando a la Iglesia Católica e individuos que deseaban la cancelación de sus inscripciones en los libros de bautismo. Los Arzobispados alegaban que estos asientos no podían ser considerados "bases de datos", lo que no fue aceptado, inicialmente, por la Agencia Española de Protección de Datos. La jurisprudencia, como se ve, por ejemplo, en el rec. 237/2007, del 17 de enero de 2008 de la Sección 1ª de la Audiencia Nacional, entendió que acertadamente la Agencia rechazó la distinción de los clérigos, y que ese rechazo violaba tanto la libertad religiosa como el derecho a la protección de datos de los afectados.

4.3.4 Límites al derecho a la protección de datos en la Administración Pública española

[835] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 370.
[836] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 364.

La descripción de facultades y principios del régimen general español del "derecho a la autodeterminación informativa" sería incompleta si no se agregara al análisis la verificación de las restricciones y límites previstos legalmente, ya que representan el evidente reconocimiento del no carácter absoluto del derecho fundamental y a *contrario sensu* demuestran el núcleo inquebrantable del mismo, ayudando a definir los contornos de ese propio *contenido esencial*[837]. En este sentido el FJ 11 de la STC 292/2000:

> "Más concretamente, en las Sentencias mencionadas relativas a la protección de datos, este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, F. 7; 196/1987, de 11 de diciembre [RTC 1987, 196] , F. 6; y respecto del art. 18, la STC 110/1984, F. 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, puedan fijar los límites a un derecho fundamental. Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero [RTC 1994, 57] , F. 6; 18/1999, de 22 de febrero [RTC 1999, 18] , F. 2). "

Se concluye entonces que hay un triple condicionamiento impuesto por el TC para efectuar restricciones a los derechos fundamentales, lo que auxilia a entender las propias inconstitucionalidades declaradas por la STC 292/2000. Primero que deben ser vehiculados por medio de norma creada por el legislador, o sea, se encuentran sometidas a la reserva de ley del artículo 53.1 de la Constitución Española. Ello ayuda a explicar la inconstitucionalidad declarada en la propia sentencia 292 de 2000 con relación al

[837] SERRANO PÉREZ, María Mercedes. "El derecho fundamental a la Protección de Datos... *cit.*, ,p. 255.

artículo 21.1 de la Ley Orgánica 15/1999, ya que esta terminaba por dar un margen tan amplio de discrecionalidad a la regulación por norma inferior a la ley de la cesión de datos sin consentimiento del afectado dentro de la Administración Pública que negaba la idea en sí de reserva legal (FJ 14). El segundo requisito para la limitación del derecho fundamental es que esa sea justificada en razón de la protección de otros valores constitucionales. Por esa razón, también se declaró la inconstitucionalidad de parte del artículo 24.1 de la LOPD, que admitía como excepción el "principio de la información" por las Administraciones Públicas la persecución de infracciones de naturaleza administrativa, pues el legislador constituyente, en el art. 105.b) de la CE sólo resguardó al derecho de acceso correlacionado a la transparencia administrativa bienes jurídicos como la seguridad del Estado, la intimidad de los individuos y la averiguación de delitos de orden penal, sin manifestar la necesidad de consagrar en la carta magna la persecución de faltas administrativas.

Y, por último, es necesario que los límites establecidos respeten exactamente ese conjunto de garantías y facultades que forman ese contenido esencial del derecho a la protección de datos, para que este no sea vaciado por desnecesarias restricciones[838]. En la LOPD original, continua la decisión del TC, ese contenido esencial era violado por una serie de cláusulas de excepción de sentido genérico, como "interés público", "funciones de control y verificación" y "garantía de intereses de terceros más dignos de protección" que impedían en la práctica la verificación del adecuado ejercicio del derecho, más allá de la propia seguridad jurídica (FFJJ 15 a 18)[839].

[838] TRONCOSO REIGADA, Antonio."La protección de datos personales... *cit*., ,p. 320.

[839] Resáltese que el análisis de las limitaciones legales al derecho fundamental a la protección de datos fue propositivamente resumida, solamente como forma de ilustrar el contenido esencial del derecho en el entendimiento del Tribunal Constitucional Español, con miras solamente a auxiliar en el propósito de este trabajo, que es el análisis de la configuración de este derecho fundamental en el derecho español.

4.3.4.1 Régimen jurídico de las bases de datos públicos

El contenido de los artículos 20 al 24 posee las normas específicas generales de la LOPD para la organización de la Administración Pública. Esa regulación no inhibe, como ya dicho, los normativos específicos de los archivos en algunos campos más sensibles a la Administración citados en el artículo 2.3 de la LOPD (a saber, elecciones, funciones estadísticas, archivos del personal de las fuerzas armadas, registro civil, "registro de penados y rebeldes" y grabaciones provenientes de las videocámaras de las Fuerzas de Seguridad).

Los archivos del Poder Judicial no poseen un reglamento específico que les desvincule de la regla general de la LOPD. De esta forma, la jurisprudencia del Tribunal Supremo reconoce que la publicidad de sus actos (a su vez reglamentada en los artículos 234 y 266 de la ley 6/1985, LOPJ) está limitada por la protección de los datos de aquellos involucrados en los asuntos judiciales. Hay una sentencia en particular, dictada por el ponente PABLO MURILLO DE LA CUEVA, que expone con claridad esa limitación de divulgación a terceros:

> "(...) no comporta la incompetencia del Juez para adoptar una resolución como la que ha dado lugar a este proceso porque a él corresponde decidir en qué casos procede limitar la publicidad de las actuaciones judiciales (artículo 232.2 de la Ley Orgánica del Poder Judicial), entre las que se incluye su plasmación documental (artículo 234) (…)
>
> (…) conviene precisar el alcance de lo que se discute en este proceso. En realidad, lo que el recurrente pretendía es que por el Juzgado Decano se le comunicaran unos datos de carácter personal contenidos en los registros de dicho órgano jurisdiccional. Según el artículo 3a) de la Ley Orgánica 15/1999 así han de ser calificados los pedidos por el Sr. Armando. Y la protección de los datos de ese carácter es el objeto de un derecho fundamental autónomo, fundamentado en el artículo 18.4 de la Constitución y distinto de los que enuncia su apartado primero .Derecho fundamental que se proyecta también sobre aquellas informaciones que no forman parte del honor ,la intimidad personal o familiar o la propia imagen. Y la protección que comporta

descansa, entre otros principios básicos, en la exigencia del consentimiento del interesado para ceder o comunicar sus datos a terceros, salvo que lo autorice la ley o se dé alguno de los supuestos enunciados en el artículo 11.2 de la Ley Orgánica 15/1999 . El Tribunal Constitucional ha tenido ocasión de perfilar los rasgos de este derecho fundamental en sus Sentencias 292 y 290 ,ambas de 30 de noviembre de 2000. Y no está de más recordar que también ha sido enunciado con autonomía respecto del derecho a la vida privada por la Carta de los Derechos Fundamentales de la Unión Europea y por el Tratado por el que se establece una Constitución para Europa.

Así, pues, lo primero que debe señalarse es que está en juego un derecho fundamental, vinculado a todos los poderes públicos, incluidos los Juzgados y Tribunales. Precisamente, por eso, el artículo 230.5 de la Ley Orgánica del Poder Judicial recuerda que las garantías y derechos que protegen los datos de carácter personal han de ser observados también ante los ficheros automatizados de los órganos jurisdiccionales. Eso quiere decir, en lo que ahora importa, que no estamos ante un simple principio que se contrapone al de publicidad de las actuaciones judiciales, sino frente a un derecho fundamental que limita las posibilidades de acceso por parte de terceros a datos personales ajenos y obliga a los órganos que los custodian a no facilitarlo aquí en es no cuentan con el consentimiento del afectado o no se hallan en alguna de las posiciones en que la Ley Orgánica 15/1999 lo autoriza.

Es preciso observar, por otra parte, que los registros de los Juzgados no son fuentes accesibles al público en el sentido en que los define el artículo 3j) de la Ley Orgánica 15/1999.Y que la Ley Orgánica del Poder Judicial explícitamente erige en límite al acceso a las actuaciones judiciales la protección de los derechos y libertades y, en todo caso, requiere la condición de interesado para acceder a los libros, archivos y registros (artículo235).”[840]

Como bien observa ÁLVAREZ-CIENFUEGOS, el sentido de la transparencia de las decisiones judiciales y de un proceso público, consagrada en el artículo 120.1 de la Constitución Española y en el art. 6.1 del Convenio Europeo de Derechos Humanos, pretende que el ciudadano alejado del conflicto pueda controlar al Poder Judicial a través del conocimiento y posible crítica de sus decisiones emitidas en cuanto a sus fundamentos jurídicos independientemente de los involucrados y no tiene el contenido de permitir la exposición de las cuestiones personales de otros[841].

Dentro de las “disposiciones sectoriales” de la LOPD, en los artículos 20 al 24 se establecen las normas generales que se aplicarán solamente a archivos cuando el titular sea un ente público, sea del Estado, de las Comunidades Autonómicas o de naturaleza local. Desde el punto de vista doctrinario, ello incluye a la “Administración

[840] STS, Sección 7ª , 18 de septiembre de 2006 (rec. 274/2002).

[841] ALVAREZ-CIENFUEGOS SUÁREZ, José María. *La defensa de la intimidad de los ciudadanos... cit.*,, p. 94. En el mismo sentido las sentencias de 8 de diciembre de 1983 (caso Pretto y otros) y de 22 de febrero de 1984 (caso Sutter) del TEDH.

Corporativa", aquella referente a los colegios profesionales, y a la "Administración Institucional" sometida al Derecho Administrativo, o sea, aquellos denominados por la Ley 6/1997 (arts. 43 y 52) de "Organismos Autónomos", quedando así, fuera de las llamadas "Entidades Públicas Empresariales" (art. 53), que son caracterizadas por actuar en el mercado contra remunerado de bienes o servicios y cuyo funcionamiento es, por ello, regido por el derecho privado[842].

Pero no solamente. Existe además una vinculación entre la base de datos para que sirva como instrumento para ejercicios de "poderes de derecho público" y ser clasificado como de naturaleza "pública"[843], lo que también se encuentra expresado en el final de la definición que concede el artículo 5.1.m) del RD 1720. En ese sentido, la SSTJ de Valencia, Sección 1ª, de 1º de junio de 1998 (rec. 45/1996) entendió que también los archivos de las Cámaras de Comercio son regulados por estos artículos 20 al 24 de la LOPD.

Ese fin eminentemente público justifica que ya el apartado 1 del artículo 20 declare que la creación, modificación o extinción de esas bases de datos públicos dependen de una "disposición general" que sea pública en el "Boletín Oficial del Estado" o en el Diario Oficial correspondiente. Esa publicidad no dispensa que exista la notificación de la Agencia Española de Protección de Datos para que haya una adecuada inscripción también de este en el "Registro General de Protección de Datos" (art. 55.1 y 60.2 del RD 1720/2007).

El acto de creación y modificación es necesariamente amplio, indicando la

[842] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 401.
[843] VIZCAÍNO CALDERÓN, Miguel. *Comentarios a la ley orgánica... cit.*, p. 228.

finalidad del *fichero*, de donde vendrán sus datos, cómo será estructurado y cuáles son sus medidas de seguridad, quién irá a gestionarlo, quién podrá previsiblemente recibir por cesión sus datos (incluso terceros países) y frente a quién los afectados podrán ejercer sus derechos de la LOPD (art. 20.2 de la LOPD). Para el acto de destrucción de esas bases de datos, naturalmente, no son necesarias tantas informaciones, pero la ley 15/1999 aduce la necesidad de dos bastante relevantes: cómo será hecha la supresión y cuál será el destino del material (apartado 3 del artículo 20).

Los apartados 1 y 3, combinados con el 4, del artículo 21 pretenden crear hipótesis en que la comunicación de datos entre las Administraciones Públicas dispensará el consentimiento del interesado. La STC 292/2000 declaró la nulidad de una de las posibilidades originalmente previstas por la ley, que era la creación de nuevas formas de cesión sin consentimiento con base solamente en la disposición de creación del nuevo *fichero*. El Tribunal Constitucional entendió, acertadamente, que ello permitiría la vulneración de derecho fundamental con base en norma sin el nivel jerárquico de ley. La LOPD debe establecer claramente las condiciones para exclusión de la indispensabilidad del consentimiento, y no pasar la normativa reglamentaria esa atribución.

Esta fijación legal de parámetros en el alejamiento del consentimiento para la formación de bases de datos públicos se refleja también en el artículo 10.3.a) del RD 1720, que permite la recolección sin intervención del afectado para el cumplimiento de atribuciones administrativas, desde que estas hayan sido definidas por ley española o de derecho comunitario[844].

[844] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 427.

Sin embargo, se mantuvieron las demás excepciones.

En la primera de ellas, bien al inicio del apartado 1, se permiten comunicaciones entre Administración cuyas competencias sean iguales o de mismas materias. La lógica de esta norma se basa en el argumento de que, sí el artículo 6.2 de la LOPD facilita la recolección de datos por parte de la Administración sin consentimiento, no hay cabida de que ella no lo utilice y se ampare en el trabajo de otra para el cumplimiento de sus atribuciones. No se exige repetición de esfuerzos, por ello, por ejemplo, no hay veda de la Administración Tributaria al enviar información de persona física que facilita la recaudación de la Cámara de Comercio[845].

Hay una importante excepción a esa regla general, lo que para la doctrina que simboliza la amplitud de esa restricción también las mismas Administraciones[846], permitiendo solamente para auxiliar la fiscalización tributaria que una serie de entes le provean datos, lo que está en el artículo 94.5 de la ley 58/2003, actual Ley General Tributaria de España (LGT), cuya redacción repite de forma absolutamente idéntica el artículo 112.4 de la antigua LGT, que había sido modificado por la disposición adicional cuarta de la LOPD. Al mismo tiempo, la jurisprudencia ve la limitación *numerus clausus* de las hipótesis y del rol de entes que reciben informaciones de la Administración Tributaria (art. 95.1 de la actual LGT) como "uno de los derechos generales de los contribuyentes"[847] y el Ministerio de Hacienda reguló, por medio de la orden del 18 de noviembre de 1999, que sólo se autoriza el trámite de esos datos

[845] STSJ de Valencia, Sección 1ª , 1º de junio de 1998 (rec. 45/1996).
[846] VIZCAÍNO CALDERÓN, Miguel. *Comentarios a la ley orgánica... cit.*, p. 238.
[847] SAN, Sección 1ª , 18 de mayo de 2005 (rec. 484/2003).

reservados identificado el recibidor y la situación en concreto de la solicitud[848].

La asignación de permisos de cesión sin el consentimiento del afectado entre Administraciones Públicas son las que tratan de fines históricos, estadísticos y científicos y cuando la información se recoge en uno, pero tenga destino competencial a otra, como cuando el ciudadano yerra el destinatario de su derecho de petición.

El apartado 3 del artículo 21, que veda pasajes sin consentimiento de fuentes de acceso público de naturaleza pública a entes privados sin consentimiento es de poca aplicación práctica, ya que importantes registros, como el de vehículos o el electoral, que interesarían a personas jurídicas comerciales no tienen la naturaleza de "fuentes accesibles al público". De todo modo, la veda no impide que la persona jurídica privada busque la información directamente en la fuente o que entes públicos distintos intercambien informaciones provenientes de ese origen.

El artículo 22 trata de un tema que se destaca por su peculiaridad entre los demás en la protección de datos personales: la de las bases de datos de Fuerzas y Cuerpos que actúan en la Seguridad Pública, o sea, los archivos para "fines policiales"[849]. La fuente de inspiración para este artículo 22 está en el artículo 13 de la Directiva Europea, la de que la protección de los derechos fundamentales no puede olvidar el mantenimiento de las condiciones para alejar las amenazas a la seguridad de la sociedad.

Los apartados del artículo 22 se equilibran entre la redundancia de afirmar la aplicación de la LOPD a los archivos de las Fuerzas de Seguridad (apartado 1), lo que

[848] VIZCAÍNO CALDERÓN, Miguel. *Comentarios a la ley orgánica... cit.*, p. 239.
[849] ALVAREZ-CIENFUEGOS SUÁREZ, José María. *La defensa de la intimidad de los ciudadanos... cit.*,,p. 64.

ya se debería deducir al no encontrar esa opción en las excepciones del artículo 2, y el establecimiento de modelo amplio de exclusión del consentimiento del afectado en la recolección de sus datos, inclusive si son "sensibles"[850], para este fin, siempre desde que haya una investigación en concreto siendo ejercida y solamente mientras sean *necesarios* (apartados 2, 3 y 4).

Ello significa un control especial de la *motivación* de los actos administrativos de recolección sin consentimiento por las Fuerzas de Seguridad, como expresa la AEPD en el Informe 213/2004 (que trata de la identificación del usuario de Internet a través del suministro por la empresa de telecomunicaciones de la dirección IP – *Internet Protocol Acess*, fechas y hora de la conexión de uso de determinado paquete de información) y la STC n. 14/2003. En esta Sala Segunda del TC brindó recurso de amparo en favor de una persona que tuvo su foto sacada en las dependencias de la Policía en su día de prisión, 26 de febrero de 1994, divulgada por la "Jefatura Superior de la Policía de Valladolid" a dos grandes periódicos regionales. Argumentó inicialmente el fallo (FJ 7), que:

> "(...) aun cuando en la demanda de amparo no se ha invocado la posible vulneración del art. 18.4 CE, en modo alguno resulta ocioso resaltar que, según se señala en el informe del Jefe de la Brigada de la Policía Judicial de Valladolid, la reseña fotográfica del recurrente en amparo conforma el archivo "reseña de filiación", y que, de conformidad con la legislación en aquel momento vigente, "la recogida y tratamiento automatizado 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" (art. 20.2 Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal -LORTAD-; también art. 22 de la actualmente vigente Ley Orgánica 15/1999, de 14 de diciembre, de protección de datos de carácter personal -LOPD). Tales datos, además, de acuerdo con los principios de protección de datos recogidos en el Título II de la mencionada Ley, "no podrán usarse para finalidades distintas a aquellas para las que los datos hubieran sido recogidos" (art. 4.2 LORTAD; también art. 4 LOPD), estando obligados el responsable del fichero automatizado y quienes interviniesen en cualquier fase del tratamiento de los datos de carácter personal "al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar las relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo" (art. 10 LORTAD; también art. 10 LOPD). Finalmente, únicamente estaba autorizada su cesión, sin el previo consentimiento del afectado, en los tasados supuestos del art. 11.2 LORTAD, entre los que no se contempla la

[850] Debiendo en ese caso el dato ser "absolutamente necesario" (art. 22.3).

> cesión a los medios de comunicación de datos personales que figuren en los ficheros de las fuerzas y cuerpos de seguridad (en el mismo sentido, art. 11.2 LOPD).”

Por otro lado, el Tribunal Constitucional no rechaza que otros bienes constitucionales puedan ser proporcionalmente ponderados en las situaciones en concreto durante las investigaciones en perjuicio de la protección de datos. En el caso, frecuente, aducen en sus pareceres la Abogacía del Estado y el Ministerio Público, que debe prevalecer la “libertad de información” a la sociedad sobre la resolución investigativa del crimen que causó grave conmoción social, que en el caso se sumaba a la importancia de la participación ciudadana para encontrar al cómplice fugitivo. Sin embargo, más allá de esa última fundamentación no haber sido emanada en el momento de la liberación de la fotografía, sólo surgiendo durante la acción de responsabilidad civil propuesta por el preso, ambos objetivos, entendió el TC, no dependían de medida tan gravosa como exponer la imagen oficial del indiciado, siendo alcanzadas por la simple divulgación oficial de su captura. El análisis de los motivos para el acto realizado por la Policía de Valladolid, al final de este FJ 11, es completamente negativa:

> “En este caso, dadas sus circunstancias, tales bienes o intereses en modo alguno requerían para su consecución y satisfacción la difusión por parte de la policía de la reseña fotográfica policial obtenida del demandante de amparo a los fines de la investigación y esclarecimiento de los hechos investigados, pues, identificados los presuntos autores de los hechos delictivos, y encontrándose detenido el demandante de amparo, su satisfacción se alcanzaba perfectamente, sin merma alguna, informando a la opinión pública sobre las investigaciones policiales llevadas a cabo, sus resultados positivos, la detención de dos de las personas presuntamente implicadas en los hechos investigados y la búsqueda de la tercera que se encontraba huida e identificada por su propia reseña fotográfica.”

Si los artículos 21 y 22 alejan en algunos casos el “principio del consentimiento”, los artículos 23 y 24 de la LOPD permiten que también las facultades individuales sean afectadas en las bases de datos públicos.

En su apartado 1 sigue la materia del artículo anterior, al permitir que se denieguen peticiones que pretendan el ejercicio de estos derechos siempre que ello pueda afectar la seguridad pública o la defensa del Estado, derechos o intereses de terceros, o la propia efectividad de la investigación en la que se está trabajando. Por otro lado, el apartado 2 permite la misma denegación por parte de la Hacienda Pública cuando ello obstaculice la recaudación por la fiscalización tributaria. Estos dos apartados reproducen básicamente los párrafos del artículo 13.1 de la directiva europea.

Estas denegaciones, sin embargo, poseen un control de legalidad creado en el apartado 3 del artículo 23 de la LOPD, que faculta al afectado que tenga su pedido recusado a poner dichos hechos en conocimiento de los Directores de las Agencias de Protección de Datos (autonómicas para actos de las policías y administraciones tributarias de estas Comunidades y nacional en los demás casos) para que ellos evalúen la procedencia de la denegación e impongan la corrección del cumplimiento de la ley de protección de datos, cuando sea el caso (atribución constante del art. 37.f) de la LOPD)[851]. También en ese caso el elemento esencial de análisis de la Agencia y, eventualmente, tras los Tribunales, será la adecuada y suficiente motivación de los actos administrativos, basada en concretas razones y no en meros alegatos jurídicos de peligros en abstracto[852].

Por otro lado, aseveran los Tribunales españoles, y especialmente la SAN, Sección 1ª, del 13 de noviembre de 1998 (rec. 51/1998), "que el "derecho de acceso de los ciudadanos a los archivos y registros públicos", previsto en el artículo 105.b) de la Constitución Española, es un derecho *subjetivo* de configuración legal, en el caso

[851] VIZCAÍNO CALDERÓN, Miguel. *Comentarios a la ley orgánica... cit.*, p. 260.
[852] SAN, Sección 1ª , 18 de mayo de 2005 (rec. 484/2003).

regulado por el artículo 37 de la "Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común" (LRJAP-PAC, ley 30/1992). Ello significa decir que el "derecho de acceso" se constituye como derecho fundamental y consecuentemente no se confunde con el derecho fundamental a la libre información (art. 20.1 de la Constitución Española). Por ello, terceros están sometidos a los límites de este artículo 37, notoriamente la individualización de lo que desean, con excepción en temas relacionados con investigaciones históricas, científicas o culturalmente relevantes (apartado 7) y la posibilidad de denegación de su pedido cuando este acceso afecte la seguridad del Estado o los derechos y libertades de otras personas (apartado 5)[853].

El artículo 24 fue prácticamente anulado en su totalidad por la STC 292/2000 en razón de la utilización de expresiones tan imprecisas que podían significar restricciones al derecho fundamental en pro de cualquier órgano administrativo o fundamentados en cualquier interés[854].

El apartado 2 fue completamente excluido, por conceder una autorización genérica para que la Administración niegue derechos de acceso, rectificación y cancelación en pro de indeterminados intereses públicos o de terceros "más dignos de protección". También la incertidumbre de la cláusula creada por el legislador en el primer inciso del apartado 1 ("cumplimiento de las funciones de control y verificación") es la razón porque el TC anula la posibilidad de que la Administración no respete el derecho a la protección de datos cuando este impidiera o dificultara a aquel. Por último, también la persecución de infracciones administrativas (final del apartado 1) no permite,

[853] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 455.
[854] VIZCAÍNO CALDERÓN, Miguel. *Comentarios a la ley orgánica... cit.*, p. 264.

según la sentencia del TC, la exclusión del derecho teniendo en cuenta que ello puede producir al ciudadano su completa indefensión en un proceso administrativo sancionador, siendo acusado kafkianamente sin poder tener acceso a los datos en que se basa su posible infracción.

Son mantenidas en el artículo 24, por tanto, como exclusiones del principio de la información solamente hipótesis semejantes a las que en el artículo 23 exceptuaban derechos de la protección de datos: Defesa Nacional, Seguridad Pública y persecución de infracciones penales.

4.3.5 Las garantías en el derecho español de la protección de datos

4.3.5.1 La Agencia de Protección de Datos

Ningún estudio de la legislación europea estaría completo sin la observación del órgano que sirve de guardián del derecho fundamental a la protección de datos, a sus Agencias Reguladoras. El artículo 28 de la Directiva 95/46/CE no se refiere propiamente a una institución con esa naturaleza, pero sí de la indispensabilidad de que cada país determine una o más autoridades públicas dotadas de *independencia* a la vigilancia del cumplimiento de la norma de la UE. Aunque esa estructura de agencia, tiene influencia del derecho estadounidense[855], se popularizó como la más común entre las naciones del continente.

[855] VIZCAÍNO CALDERÓN, Miguel. *Comentarios a la ley orgánica... cit.*, p. 388.

En el caso español, el artículo 35.1 de la LOPD prevé que la "Agencia de Protección de Datos" es un ente de derecho público y personalidad jurídica propia, regida por un estatuto específico (que es, en el caso de la Agencia Española de Protección de Datos, el Real Decreto 428/1993).

La independencia de la AEPD no es, total, sino relativizada dentro del marco legal. En estos términos ella es claramente garantizada en el caso español. Desde el punto de vista presupuestario, la Agencia elabora su propio presupuesto, el cual envía al Gobierno para ser agregado al "Presupuesto General del Estado" (apartado 5 del artículo 35 de la LOPD), lo que dificulta maniobras de asfixia económica por parte de gobernantes incomodados.

En su estructura, aunque el consejo consultivo contenga una fuerte composición proveniente de los órganos políticos (art. 38 de la LOPD), este órgano presta mera asesoría al Director de la Agencia, que es quien efectivamente toma las decisiones y representa la autoridad dentro de la AEPD, sin sometimiento a nadie más (art. 36.2 de la LOPD y artículo 16 del RD 428). Siendo así, constituye la última instancia de recursos administrativos tratándose de Protección de Datos (art. 109.c) de la ley 30/1992), sólo restando al interesado insatisfecho con su decisión apelar al recurso contencioso administrativo direccionado a la Sala de lo Contencioso de la Audiencia Nacional (disposición adicional cuarta, apartado 5 de la ley 29/1998, reguladora de la Jurisdicción Contencioso Administrativa)[856].

Él es nombrado para un mandato de 4 años, elegido por el Gobierno, bajo

[856] VIZCAÍNO CALDERÓN, Miguel. *Comentarios a la ley orgánica... cit.*, p. 401.

propuesta del Ministro de Justicia, entre los propios miembros del Consejo Consultivo (art. 36.1 de la LOPD y art. 14 del RD 428). Su cese del cargo depende de manifestación voluntaria o de iniciativa del Gobierno por "incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso" (art. 36.3 de la LOPD).

El artículo 37 de la LOPD enuncia las funciones ejercidas por el Director que corresponden exactamente a los *poderes de control* de la Agencia para el cumplimiento de la legislación de protección de datos dentro de España. Así, en verdad, todos los párrafos de este artículo 37 son repeticiones en concreto de la letra "a": "velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos."[857].

Se destaca el epígrafe "c" que concede poder normativo de dictar *instrucciones*, que, conforme la jurisprudencia del Tribunal Supremo[858], no involucren la reglamentación de la LOPD, esta reservada al Gobierno y sometida a reglas procedimentales previstas en la ley 50/1997("Ley del Gobierno"), pero sí, la posibilidad de conformar la actividad de aquellos que tratan datos a los exactos principios de la LOPD. Además, recibe peticiones y reclamos de afectados (párrafo "d"), determina a los responsables, bajo previa audiencia, adecuación o cese de conductas inadecuadas ("f") y ejerce el poder sancionatorio sobre los reincidentes ("g"). También elabora una *memoria* sobre la situación general de la protección de datos en cada año (párrafo "k" y artículo 8 del RD 428).

[857] *Ibid.,* p. 404.
[858] STS, Sección 6ª , 16 de febrero de 2007 (rec. 220/2003).

La letra "j" del artículo 37, que se refiere a cuidar la publicidad de las bases de datos existentes tiene una íntima relación con la divulgación del contenido inscripto "Registro General de Protección de Datos" (art. 39 de la LOPD y 23 del RD 428), que corresponde a todas las informaciones actualizadas sobre las bases de datos públicas y privadas del país, "códigos tipo"[859], que son fallos sectoriales o decisiones de empresa que complementan las lagunas del régimen legal de tratamiento de datos y las *autorizaciones* que hayan sido concedidas para el envío de datos a países que no posean nivel de protección semejante al europeo.

El artículo 40 de la LOPD trata sobre los "poderes de inspección" de la Agencia (denominados en la versión portuguesa del art. 28.3 de la directiva 95/46/CE como "poderes de inquérito"), que permiten que sean analizados todos los repositorios de datos y requerido el envío de cualquier documento de modo que sea útil al control por ella ejercido. El art. 12.k) del RD 428 permite hasta que el Director de la AEPD autorice la entrada a cualquier establecimiento, respetada la inviolabilidad de los domicilios[860]. Toda documentación formada de la acción del órgano de "Inspección de Datos" de la AEPD posee presunción *iuris tantum* de veracidad (art. 40.2 de la LOPD combinado con art. 137.3 de la LRJAP-PAC).

Los artículos 41 y 42 de la LOPD tratan sintéticamente de la repartición de competencias entre Estado y Comunidades Autónomas en el ámbito competencial de la protección de datos. En el caso español, y ello fue confirmado por el Tribunal Constitucional en el juzgamiento de la STC 290/2000, fue concedido un espacio

[859] Vide artículo 32 de la LOPD.
[860] VIZCAÍNO CALDERÓN, Miguel. *Comentarios a la ley orgánica... cit.*, p. 426.

diminuto a las Comunidades, que sólo pueden ejercer control de las bases de datos públicas creadas por sí mismas (art. 41.1).Por lo que el tema se desarrolló poco cuantitativamente en este ámbito, siendo las pioneras las Agencias de Protección de Datos de Madrid, Cataluña y País Vasco[861].

4.3.5.2 La tutela de los derechos de acceso, oposición, rectificación y cancelación

La petición de acceso, rectificación, oposición o cancelación debe ser direccionada por el interesado o su representante al responsable por la base de datos. Como asevera el artículo 24.5 del RD 1720, hay una intención en la norma por el *antiformalismo,* debiendo ocurrir el análisis de la solicitud siempre que sea posible verificarse su contenido y envío e identificarse al solicitante y su dirección para notificaciones (artículo 25.1 del RD), inclusive, si el procedimiento previamente establecido no fue fielmente seguido.

Esta facilitación del uso de los derechos referentes a la protección de datos (acceso, cancelación, rectificación y oposición) se encuentra igualmente por la determinación de su procesamiento *gratuito,* en el artículo 24.2 del RD, lo que es reiterado en lo que respecta al derecho de acceso en el artículo 28.2. En la LOPD, el artículo 17.2 tiene el mismo sentido al referirse que los derechos serán ejercidos sin exigencia de contraprestación.

[861] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 618.

Cualquier incumplimiento a la LOPD que afecte determinada persona física o la negativa en implementación de los derechos de acceso, oposición, rectificación y cancelación por el titular de la base de datos, tornan admisible un "reclamo" ante la Agencia de Protección de Datos española (art. 18.1 y 18.2 de la LOPD), órgano de control de la aplicación regular de la legislación sobre el tema. Este derecho a la instancia administrativa, evidentemente, no retira la posibilidad de apelar a la jurisdicción ordinaria[862].

Recibido el reclamo exponiendo con claridad los dispositivos de la LOPD violados, la Agencia concederá 15 días al responsable por la base de datos para que pueda exponer sus alegatos y decidirá la cuestión expuesta en el plazo máximo de 6 meses (arts. 117 y 118 del RD 1720 y art. 18.3 de la LOPD). Conforme el artículo 118.2 del RD, en la superación de este plazo sin manifestación de la Agencia, se deberá considerar el *silencio* administrativo *con efectos positivos*, o sea, estimatorio de la demanda[863].

El artículo 18.4 de la LOPD (en repetición al artículo 22 de la Directiva 95/46/CE) concede al afectado también la posibilidad de apelar a la Jurisdicción, a través del denominado *recurso contencioso administrativo* contra resolución de la Agencia. Además, frente a la aplicación suplementaria de la ley 30/1992, expuesta por el artículo 115 del RD 1720, cabrá cualquiera que sea el contenido de la resolución de la Agencia el *recurso de reposición*, previsto en los actuales artículos 116 y 117 de la

[862] HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales … cit.*, p. 72.

[863] O sea, en el mismo sentido regla general en el derecho español, fruto de la actual redacción del artículo 43.2 de la ley 30/1992 (*Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común*), dada por el artículo 11 de la ley 4/1999.

citada ley 30 [864]. Para el afectado que tenga interés, la elección entre los dos recursos está limitada por las diferentes coyunturas: mientras el *recurso de reposición* debe ser interpuesto en el plazo de un mes de la notificación de la decisión administrativa, el recurso judicial puede dar hasta 2 meses (artículo 46 de la ley 29/1998, que regula la Jurisdicción Contencioso Administrativa).

Ese reclamo igualmente, y su eventual resultado sanador de la lesión al ciudadano, no se confunde con la posibilidad de que la Agencia instaure, inclusive de oficio, cualquier procedimiento sancionador por infracción a la LOPD[865]. Los reclamos pretenden la tutela de derechos, mientras las sanciones son impuestas en razón del Poder de Policía de la AEPD, aunque, claro, hechos aducidos en reclamo puedan justificar aplicación de penas administrativas.

4.4. La legislación de protección de datos en Brasil

También en Brasil, a partir de la década del '90 del siglo pasado, se intensifica una preocupación sobre los peligros de ciertas informaciones archivadas sobre la integridad de la esfera individual del ser humano, igualmente influenciada por la terrible reducción de los equipos combinada con un equivalente aumento de sus capacidades, como se ve en los aparatos de captación de imagen y procesamiento de datos. La idea central de esta nueva doctrina es marcada en la afirmación del profesor CELSO RIBEIRO BASTOS: "A evolução tecnológica torna possível uma devassa da vida

[864] BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos... cit.*, p. 392.
[865] SAN, Sección 1ª , 11 de mayo de 2001 (rec. 12/2000).

íntima das pessoas, insuspeitada por ocasião das primeiras declarações de direitos."[866]

La protección de los datos personales en Brasil se realiza en la legislación infra constitucional de una forma breve y fragmentaria, lo que se refleja en una incipiente jurisprudencia, donde solamente se destaca la creciente preservación del secreto de tipos puntuales de informaciones, como las bancarias y fiscales, con base primordial en el derecho fundamental individual a la vida privada y a la intimidad del inciso X del artículo 5º de la Constitución Federal Brasileña[867].

En ese sentido abordaremos las principales regulaciones legales en cuanto a los derechos individuales en lo que respecta a sus informaciones en bases de datos de otros. Esta protección a los datos personales en Brasil está permanentemente vinculada al derecho a la intimidad, o sea, con un sentido de resguardo de sus informaciones a los ojos y usos de otros, eminentemente como libertad negativa. Las facultades del individuo en exigir *obligaciones de hacer* a los responsables por bases de datos surgen principalmente alrededor de la regulación legal de la acción constitucional del "Habeas Data" y de la jurisprudencia relacionada.

4.4.1 La protección de datos como libertad negativa

866 RIBEIRO BASTOS, Celso. *Curso de direito constitucional. cit.*, p. 194.

867 En la jurisprudencia del Supremo Tribunal Federal (STF) sobresalen en ese sentido los MS 22.801-6/DF, Inq 2245/MG, Pet QO 577/DF, Pet-AgR 1564-5/RJ, MS 21729/DF, AI-AgR 541265/SC y RE 219780/PE. Por otro lado, se resalta que en el juzgamiento de este último asentó el Supremo Tribunal Federal (STF) brasileño que el secreto previsto en el inciso XII del mismo artículo 5º constitucional no se refería al contenido de datos, sino solamente a la interceptación de la comunicación de los mismos. Defendiendo la posición del STF: FERRAZ JUNIOR, Tercio Sampaio. "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado... *cit.*. En sentido contrario: LEITE SAMPAIO, José Adércio. *Direito à intimidade e a vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte*. Belo Horizonte: Del Rey, 1998.

4.4.1.1 Los objetos protegidos y sus titulares

Por la ausencia de una legislación propia, así como del reconocimiento por parte del Supremo Tribunal Federal de un derecho a la protección de datos autónomo con substrato constitucional, hay bastante inseguridad jurídica en la protección general de datos en Brasil, o sea, relativamente a aquellos donde no hay disposiciones específicas que determinen el secreto en relación a los terceros que de ellos tomen conocimiento. No es suficiente la indicación de que hay un derecho a la intimidad también en informaciones personales registradas[868], si no quedan claros cuales son exactamente esos datos íntimos y mientras la legislación no estipule las situaciones de necesaria limitación.

Por tanto, los datos que son inequívocamente protegidos son aquellos que se encuentran cubiertos legislativamente por específicos *secretos*, situaciones en que se determina a los profesionales que guarden secreto sobre informaciones que recibieron en función de su empleo. Se encuentran situaciones concretas de sigilo, inclusive para fines de sanción penal en caso de incumplimiento[869], en las informaciones recibidas por médicos, abogados, bancos y fiscales de tributación. Solamente los dos últimos casos, sin embargo, tienen una normalización más pormenorizada, ya que los artículos 73 al 79 del Código de Ética Médica (Resolución CFM Nº 1931/2009) y el inciso VII del art. 34 del Estatuto del Abogado (Ley 8.906/94)[870] simplemente prohíben de manera

[868] Como enuncia, por ejemplo, como regla de veda de acceso a consulta de documentos públicos el art. 7 º de la ley 11.111/2005.

[869] Art. 154 del Código Penal.

[870] Además hay acciones judiciales en que igualmente es vedada cualquier divulgación por quien tome conocimiento del proceso, como forma de preservar las partes:

"Código de Proceso Civil, Art.155. Los actos procesales son públicos. Corren, incluso, en secreto de justicia los procesos:

I - en que exigir el interés público;

Il - que respectan al casamiento, filiación, separación de los cónyuges, conversión de esta en

prácticamente absoluta la revelación de cualquier información a terceros[871].

Al mismo tiempo las inconsistencias de la fórmula de esa simple protección objetiva de los datos por medio de la intimidad aparecen de forma clara y frecuente en el campo relativo a las informaciones almacenadas en empresas de telecomunicaciones, donde hay más resistencia a la aplicación de la idea de secreto, hasta por la tradicional divulgación de una "lista de suscriptores", y en una actividad que abarca casi la totalidad de la población, teniendo así una fuente cuantitativamente muy amplia de intereses a ser afectados. Las soluciones encontradas en ese campo para la composición de conflictos, en etapa de alguna densidad normativa, aunque insuficiente, merecerán así una mirada por separado.

No hay duda, sin embargo, que ningún secreto en Brasil configure derecho impenetrable, que no comportase divulgaciones, siempre que el Poder Judicial observase interés superior. Como ya afirmaba el relator del STF, Ministro Ribeiro da Costa, en el RMS 1047, del 6 de septiembre de 1949, en un caso justamente relativo a las informaciones bancarias "(...) este [secreto profesional] no puede, de ningún modo, ser absoluto. Debe ceder, cuando se trata de ayudar a la Justicia, pues el interés de la sociedad prima sobre el de los individuos (...)". Y completaba, de forma perentoria, que "la universalidad de los tratadistas, que cuidan de la materia, se dirige a un único punto – el banco no puede rechazar informaciones que le son requeridas por el juez de

---

divorcio, alimentos y guarda de menores.

Párrafo único. El derecho de consultar los autos y de pedir certificados de sus actos es restricto a las partes y sus procuradores. El tercero, que demostrar interés jurídico, puede requerir al juez certificado del dispositivo de la sentencia, así como, de inventario y división resultante del divorcio."

871 Las únicas excepciones legales, para el médico, involucran el peligro a la salud de los compañeros de trabajo y de las comunidades, en cuanto a exámenes laborales y a la información a padres del menor examinado si no puede ello causar daño al paciente. Ello no significa, sin embargo, que el Poder Judicial no pueda, excepcionalmente, decidir otros conflictos de intereses (como afirmó el STF en los juzgamientos RE 60176 / GB, el 17 de junio de 1966, y RE 91218 / SP, el 10 de noviembre de **1981).**

instrucción."Agregando a la evaluación casuística del Judicial, la legislación brasileña, progresivamente, fue admitiendo otras excepciones, especialmente en el secreto bancario y fiscal.

Esta protección de datos que básicamente garantiza la defensa de secretos legales íntimos provoca también dos importantes consecuencias. Primero la exclusión del objeto de datos meramente calificativos, los denominados "datos de registros", pues no serían íntimos, ya que son provistos en relaciones usuales del día a día[872].

Y, aunque la doctrina acepte que algunos derechos fundamentales sean aplicables, cuando consistentes con su estructura e inexistencia biológica, también a personas jurídicas[873], la idea de intimidad y privacidad viene usualmente con su justificación vinculada al concepto de personas naturales y relaciones humanas[874].

En lo que respecta a los "sigilos", eso fue afirmado por el STF al permitir el acceso a determinadas operaciones bancarias meramente por medio de la requisición por el Ministerio Público. Como primero dice el Min. Maurício Corrêa en su voto en el Mandado de segurança 21.729, del 7 de abril de 1995, siendo el secreto bancario

---

872 En ese sentido, excluyendo datos de registro en los "relevantes" secreto bancario y fiscal encontramos expresamente el STJ, 5ª. Grupo, EDcl en el Recurso em Mandado de Segurança Nº 25.375 – PA, rel. Min. Felix Fischer, juzgado en 18 de noviembre de 2008.

873 MARTINS, Leonardo e DIMOULIS, Dimitri. *Teoria geral dos direitos fundamentais... cit.,* p. 97 e FERREIRA MENDES, Gilmar, MARTIRES COELHO, Inocêncio, y GONET BRANCO, Paulo Gustavo o. *Curso de direito constitucional... cit.,* p. 305.

En sentido contrario, defendiendo la aplicación de un derecho a la privada para personas jurídicas, frente a su igual necesidad de poseer una esfera protegida para "evaluar lo que está ocurriendo con la empresa y decidir cómo responder a las situaciones" ROSCOE BESSA, Leonardo. Para este autor, además, sería adecuado, en el campo de la protección de datos, verificar un derecho de rectificación a las personas jurídicas como forma de preservar su honra de informaciones falsas (*O consumidor e os limites dos bancos de dados de proteção ao crédito*. São Paulo: Revista dos Tribunais, 2003, p. 102).

874 Vide en ese sentido FERREIRA MENDES, Gilmar, MARTIRES COELHO, Inocêncio, y GONET BRANCO, Paulo Gustavo o. *Curso de direito constitucional... cit.,* p. 433 y RIBEIRO BASTOS, Celso. *Curso de direito constitucional. cit.,* p. 158.

fundado en el derecho a la intimidad de los individuos, no están incluidas en él, las cuentas operadas por persona ficticia[875]. Igualmente, como al final afirma la decisión que prevaleció por la mayoría mínima, el secreto bancario tampoco engloba operaciones que involucran verbas del Erario público, porque, de la misma forma, "(...) en materia que involucra gestión de dinero público, no hay secreto privado, sea él de *status* constitucional o meramente legal, a oponerse al principio básico de la administración republicana."[876].

O sea, el STF define como *titulares* de secreto bancario a las personas físicas[877]. La verificación de la intensidad de la afectación, así, debe siempre tener como parámetro al individuo[878]. Así, cuando encontramos fallos que protegen sigilos relativos a informaciones de empresas[879], en verdad lo que se está protegiendo son las informaciones que relativamente a actuación de los socios (y eventualmente empleados con poder de mando) puedan provocarles consecuencias graves.

4.4.1.1.1 La protección de datos en el secreto bancario

El sigilo de dados más tradicional en Brasil es el denominado "sigilo bancario". La historia de la positivización de la anterior costumbre del derecho real lusitano en el

875 MS 21729 (Supremo Tribunal Federal 1995), voto do Ministro Maurício Corrêa, p. 29.
876 MS 21729 (Supremo Tribunal Federal 1995), voto do Ministro Sepúlveda Pertence, p. 104.
877 Aunque ese caso tenga la peculiaridad de haber tratado de persona jurídica de *derecho público*.
878 En ese sentido dice el Min. Joaquim Barbosa que la "quebra" de sigilo de empresa para el "rastreamento dos recursos públicos que (...) teriam sido desviados em proveito próprio do acusado (...) foi medida menos gravosa do que a quebra do sigilo bancário do acusado e não representou invasão do seu sigilo de dados." (Inq. 2250/RR del STF, juzgamiento por el pleno el 11/02/2010, p. 29)
879 Como en el RECURSO EN HABEAS CORPUS Nº 25.789 – SP de la 5ª. Grupo del STJ que se refiere en su enmienda expresamente de la "quebra do sigilo bancário da empresa" (rel. Min. Napoleão Nunes Maia Filho, juzgamiento el 20/08/2009).

sentido de un "secreto bancario" se inicia en Brasil con el Código Comercial de 1850, que otorga a los *accionistas*, en su artículo 120, los mismos derechos de los demás comerciantes, dentro los cuales, en el artículo 17 del mismo Código, el de mantener sus libros mercantiles lejos de la verificación de otros, aún autoridades públicas, salvo mediante orden judicial (arts. 18 a 20)[880]. En la década del '40 del siglo XX, los Códigos, editados bajo régimen dictatorial en Brasil y también vigentes, Penal (artículo 154) y de Proceso Penal (artículo 207), reproducen, respectivamente, la criminalización de la conducta de quien revela secreto profesional y la prohibición del testimonio de quien posee el "secreto".

La definición actual de secreto bancario en Brasil está en el artículo 1º de la ley complementaria Nº 105/2001[881], la cual revocó expresamente la disciplina anterior, que era por medio del artículo 38 de la ley 4.595 de 1964. Él impone que todas las instituciones financieras (relacionadas en el §1 º del mismo artículo de forma bastante amplia, incluyendo todos los tipos de banco, casas de cambio y valores mobiliarios, todas las personas jurídicas que conceden crédito o préstamos a terceros, bolsas de valores y todas las otras que así define el Consejo Monetario Nacional) deberán conservar secreto de cualquier hecho que tomen conocimiento en razón de su actividad[882]. Jurídicamente estamos ante una obligación de no hacer, los bancos y afines no pueden revelar lo que tiene conocimiento en razón de la confianza depositada[883].

El titular de derecho no son solo los clientes habituales, sino cualquier persona

---

880 *MS 21729* (Supremo Tribunal Federal 1995), voto del Ministro Mauricio Corrêa, p. 4.

881 La cual, frente a las presiones del poderoso sector bancario contra esas normas causaron que el proceso legislativo de esta norma quedara por seis años parada en el Senado, siendo al fin conseguida la aprobación por el Gobierno Federal como condición a un aumento sustancial en el salario mínimo brasileño (TERRIGNO BARBEITAS, André. *O sigilo bancário... cit.*, p. 115).

882 TERRIGNO BARBEITAS, André. *O sigilo bancário... cit.*, p. 15.

883 En ese aspecto no se innova con relación al "caput" del artículo 38 de la ley 4.595 de 1964.

que revele informaciones por causa de las actividades profesionales que ejercen las instituciones financieras[884].

El Supremo Tribunal Federal, en varios momentos ya bajo la égida de la "Carta ciudadana" de 1988[885], no tuvo dudas en justificar ese secreto dentro del "derecho a la intimidad" (inciso X). También en la doctrina no hay grandes discusiones en el continuar de este posicionamiento, de que el secreto bancario estaría incrustado en el "derecho a la intimidad". En ese sentido se posicionan algunos de los más influyentes autores de Derecho Tributario y Civil[886].

El deber de secreto, evidentemente, no existe cuando el afectado *consiente* en el uso de sus informaciones (LC Nº 105, art. 1º, § 3º, inciso V), ya que la obligación de secreto solo se justifica cuando la persona afectada no desea que esa información se haga pública. La esfera del "íntimo" es naturalmente conforme a las voluntades de exponerse más o menos de cada individuo.

El secreto bancario no deja de producir efectos aún cuando hay alguna hipótesis legal de transmisión sin consentimiento, porque el empleado que recibe esa información también se ve obligado a continuar manteniendo el secreto, no pudiendo, en regla, pasar a otro (arts. 2º, §5º, 5º, §5º, y 11 de la LC Nº 105 y los tipos penales del art. 18 de la ley

884 OLIVEIRA LIMA ROQUE, Maria José. *Sigilo bancário e direito à intimidade*. Curitiba: Juruá, 2001, p. 86.

885 Cítese la Pet QO 577, el Ag Reg en el Inquérito 897, el Rec 511, el Recurso Extraordinario 215.301-0 y el Mandado de Segurança 21.729-4, entre otros.

886 Vide DERZI, Misabel de Abreu Machado. "O sigilo bancário, a Lei 9.613/98 e a intributabilidade do ilícito." *Repertório IOB de jurisprudência: civil processual penal e comercial*, Julho 1998, MARTINS, Ives Gandra da Silva, y REALE, Miguel. "Sigilo bancário. Inconstitucionalidade do Decreto n. 4.489 de 28/11/2002 por macular o processo legislativo plasmado na Lei Suprema e infringir direitos fundamentais do cidadão." In *Sigilo fiscal e bancário*. São Paulo: Quartier Latin, 2005 y WALD, Arnoldo. "O sigilo bancário no projeto de Lei Complementar de reforma do sistema financeiro e na lei complementar nº 70." *Revista de información legislativa*, 1992.

7.492/86 y art. 10 de la LC Nº 105).

4.4.1.1.2 La protección de datos en el secreto fiscal

Inicialmente cabe reconocer que el modo de constitución de informaciones fiscales (y tributos) por parte de las Administraciones Tributarias (el denominado "Ingreso" de cada ente federativo) es una actividad constitucional que envuelve normalmente, por sí sola, con datos personales íntimos o privados. Reconociendo la afectación de acceso inherente a las informaciones individuales sedestacan en el Código Tributario Nacional (CTN) la existencia de *poderes* atribuidos a la Administración Tributaria en Brasil[887].

Además de que los libros comerciales son accesibles para los fiscales en el interés de su actividad pública (art. 195 del Código Tributario Nacional y sumario 439 del Supremo Tribunal Federal[888]), también terceros, como notarios, administradores de bienes y agentes, entre otros, definidos en ley[889], deben prestar las informaciones que

[887] La grandeza de los poderes de la fiscalización tributaria en Brasil, con tradición desde la época colonial, se nota inclusive por la preocupación del constituyente originario en salvaguardar expresamente los derechos individuales y limitar a los términos de la ley la amplitud de esa fuerza, como se ve en la redacción del § 1 º del artículo 145 de la CF ("§ 1º - Siempre que sea posible, los impuestos tendrán carácter personal y serán graduados según la capacidad económica del contribuyente, facultando a la administración tributaria, especialmente para verificar efectividad a esos objetivos, identificar, respetados los derechos individuales y en los términos de la ley, el patrimonio, los rendimientos y las actividades económicas del contribuyente").

[888] STF Súmula nº 439: "Estão sujeitos a fiscalização tributária ou previdenciária quaisquer livros comerciais, limitado o exame aos pontos objeto da investigação." (*DJ de 8/10/1964, p. 3645; DJ de 9/10/1964, p. 3665; DJ de 12/10/1964, p. 3697).*Por esto no se permite la fiscalización tributaria invadir espacios privados de contabilidad empresarial fuera de las hipótesis que exceptúan en la Constitución, la inviolabilidad del domicilio (inciso XI del artículo 5º: *"a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;"), conforme decidió el Supremo Tribunal Federal en el HC n º 82.788-8, de 12 de abril de 2005.*

[889] „Art. 197. Mediante intimação escrita, são obrigados a prestar à autoridade administrativa todas as informações de que disponham com relação aos bens, negócios ou atividades de terceiros:

posean sobre los "bienes, negocios y actividades" que conozcan de los sujetos pasivos de las obligaciones tributarias (art. 197 del CTN).

Los "secretos profesionales" propios son eliminados de la aplicación del deber de revelar al Fisco (párrafo único del art. 197 del CTN[890]), como forma de preservar la confianza que exige la actuación de determinados profesionales. Se destacan aquí, nuevamente, el secreto en el trato médico y paciente y lo que debe existir sobre lo que es revelado en la relación entre cliente y su abogado (arts. 25 a 27 del Código de Ética y Disciplina de la OAB y arts. 7º, inciso XIX y 34, inciso VII de la ley 8.906/94 - "Estatuto de Abogacía")[891].

Sin embargo, en cuanto a los agentes públicos de la Administración Tributaria y a los organismos que reciben esas informaciones hay una advertencia de que esa comunicación no las vuelve públicas (art. 198, "caput" del Código Tributario Nacional), aun existiendo el deber de sigilo (ahora denominado *fiscal*[892]) en cuanto a terceros.

4.4.1.1.3 La protección de datos por parte de las empresas concesionarias

---

I - os tabeliães, escrivães e demais serventuários de ofício;
II - os bancos, casas bancárias, Caixas Econômicas e demais instituições financeiras;
III - as empresas de administração de bens;
IV - os corretores, leiloeiros e despachantes oficiais;
V - os inventariantes;
VI - os síndicos, comissários e liquidatários;
VII - quaisquer outras entidades ou pessoas que a lei designe, em razão de seu cargo, ofício, função, ministério, atividade ou profissão."

890 "Parágrafo único. A obrigação prevista neste artigo não abrange a prestação de informações quanto a fatos sobre os quais o informante esteja legalmente obrigado a observar segredo em razão de cargo, ofício, função, ministério, atividade ou profissão.".

891 SILVEIRA DIFINI, Luiz Felipe. *Manual de Direito Tributário*. São Paulo: Saraiva, 2005, p. 347. HUGO DE BRITTO MACHADO dice que el secreto profesional es derecho y deber del abogado (*Curso de direito tributário*. São Paulo: Malheiros, 2004, p. 237).

892 Ello se repite cuando se tratan las informaciones bancarias recibidas en la LC nº 105: "Art. 5º. § 5º. As informações a que refere este artigo serão conservadas sob sigilo fiscal, na forma da legislação em vigor.".

de telecomunicaciones

En la prestación de servicio público de telefonía, que incluye llamadas habladas y también internet, se pone en poder de las empresas concesionarias un amplio espectro de informaciones del individuo necesarios para el cumplimiento de una específica relación jurídica, como nombre, CPF (*Cadastro de Pessoa Física* - Registro de Persona Física), dirección, número de teléfono, llamadas realizadas y recibidas, eventualmente cuenta corriente para descuento bancario. Como se ve, algunas de carácter típicamente más reservado que otras, pero todas pudiendo ser útiles para algunas de las funciones públicas, sea tan sólo para encontrar la dirección de alguien, o para un mayor conocimiento de actividades con fines de investigación policial, especialmente como medida previa a interceptaciones telefónicas, o hasta para la realización de la fiscalización que emprende en este servicio la "Agencia Nacional de Telecomunicaciones" (ANATEL).

Se suma que las informaciones calificativas del usuario de telefonía *fija*[893] son objeto de una lista general de suscriptores que es de obligatoria confección por parte de la concesionaria brasileña del servicio público de telefonía (art. 96, inciso IV de la LGTel – Ley Nº 9.472, del 16 de julio de 1997) y de gratuito suministro al usuario y por precio razonable, no discriminatorio a otros que quieran divulgarla (art. 213 de la LGTel). La divulgación de nombre, dirección y código de acceso[894], sin embargo, se somete a la manifestación de voluntad en sentido contrario (art. 3º, inciso VI de la

[893] O sea, no incluye los subscriptores usuarios del sector de telefonía que más crece en Brasil, que es la de naturaleza *móvil*. Sin embargo, la no divulgación en lista no significa la inexistencia de base de datos de registro de los clientes de la telefonía móvil, que es inclusive obligatorio aun en la ausencia de contrato, en el llamado sistema de "prepago" (art. 1º de la ley 10.703/2003).

[894] Que es el contenido de la "lista de subscriptores", conforme inciso XXIII del artículo 1º del anexo de la Resolución n º 66/1998 de ANATEL que regula la "divulgação de listas de assinantes e de edição e distribuição de lista telefônica obrigatória gratuita".

LGTel), o sea, al descontento expreso con la divulgación. Por lo tanto, es común la comprensión de que estos datos tienen carácter *público*, y ende son accesibles para todos[895].

En las demás situaciones, afectando en especial a los usuarios de telefonía móvil, dice solamente la ley que es derecho del usuario la *privacidad* de su factura de cobro y de los *datos personales* en su utilización por parte de la concesionaria (inciso IX del artículo 3º de la LGTel). Eso significa, en el propio entender de la agencia reguladora, diez años después de la edición de la ley, que "ni la reglamentación de ANATEL ni la legislación traen directivas claras en cuanto a los requisitos para suministro de datos de registro de los suscriptores del STFC[896] que hayan requerido la no divulgación de sus datos en listas telefónicas o de usuarios de otros servicios de telecomunicaciones cuando no haya listas de suscriptores/usuarios"[897].

Para el suministro de datos a terceros, ANATEL tiene que *parecer* en el sentido de adoptar como parámetro para la configuración de "datos no sensibles", y así de una menor protección, la Ley 6.015/73 – Ley de Registros Públicos (LRP). Pues en su artículo 176, § 1º indica que obligatoriamente deberán constar en los *Registros públicos de inmuebles* en el campo del propietario el nombre, domicilio, nacionalidad, estado civil, profesión y número de registro de personas físicas, si es persona natural, o la sede social y número de inscripción en el registro general de contribuyentes, si es persona

[895] Como expresado en el ítem 19 del Parecer n º 105-2007/PGF/PFE/MW/ANATEL. Agréguese que la Agencia no encuentra como limitación que la *finalidad* sea el conocimiento del número de teléfono del usuario, admitiendo combinaciones para el descubrimiento de cualquier dato de este registro (ítem 21 del Parecer n º 105-2007/PGF/PFE/MW/ANATEL).

[896] "Servicio Telefónico Fijo Conmutado".

[897] Ítem 23 del Parecer n º 105-2007/PGF/PFE/MW/ANATEL.

jurídica[898]. De forma similar el Ingreso Federal considera esos datos de "dominio público", salvo cuando informen la situación económica o financiera de los contribuyentes constantes de su registro[899]. En la práctica tales interpretaciones eliminan del campo de la intimidad los datos calificativos y la dirección de personas físicas y jurídicas. En verdad, un vez más la interpretación de la legislación se ve presa a los parámetros de solo protegerse datos íntimos con que opera el STF[900].

Por lo tanto solo hay secreto en cuanto a los registros telefónicos junto a las empresas de telefonía, pues hay también en la LGTel o "caput" y § 1 º del artículo 72, en que consta:

> "Art. 72. Apenas na execução de sua atividade, a prestadora poderá valer-se de informações relativas à utilização individual do serviço pelo usuário.
> § 1° A divulgação das informações individuais dependerá da anuência expressa e específica do usuário."

Aquí se ve que la ley protege las informaciones individuales como un todo, sometiendo su transferencia siempre al consentimiento del afectado (§ 1º) y su uso al objeto contractual ("caput"). Se destaca también que el § 2º explicita un típico uso estadístico, permitido por medio del uso de técnicas *anónimas*[901].

4.4.1.2 Límites al sigilo de datos en Brasil

898 Ítem 85 del Parecer nº 1314/2009/LBC/PGF/PFE-ANATEL.

899 Art. 2 º de la Instrucción Normativa SRF n º 19, del 17 de febrero de 1998.

900 Señálese también que esos reglamentos internos no consideran la propia incompatibilidad de la LRP, anterior a la redemocratización brasileña, con el concepto de protección de datos personales, ya que torna accesibles a todos, informaciones que deberían tener en regla reserva al titular. Además, la terminología utilizada en el parecer de ANATEL es errónea, ya que no es posible que todas las demás informaciones individuales no incluidas en ese registro merezcan la protección reforzada como "datos sensibles".

901 "§ 2° A prestadora poderá divulgar a terceiros informações agregadas sobre o uso de seus serviços, desde que elas não permitam a identificação, direta ou indireta, do usuário, ou a violação de sua intimidade."

4.4.1.2.1 Límites al secreto bancario

Al principio, se admitió la limitación del secreto bancario para la fiscalización de la actividad de los bancos, por medio del artículo 3º del Decreto ley Nº 8.495, del 28 de diciembre de 1945[902] y, a continuación, para viabilizar la actuación del Estado en la verificación y recaudación de tributos, según el inciso II del artículo 197 del Código Tributario Nacional, originalmente del 25 de octubre de 1966.

La ley complementaria Nº 105 lista diversas situaciones en que hay otros intereses que no justifican el secreto bancario. Aunque la técnica legislativa haya separado entre ausencia de violación del deber de secreto (§ 3º del artículo 1º) y obligación de prestación de información por parte de las instituciones financieras (arts. 3º, 4º y 5º) o imposibilidad de oposición del deber de secreto (§ 1º del artículo 2º), no hay base para diferenciar situaciones en que igualmente podemos decir que hay intervención justificada en un ámbito de intimidad del individuo.

En la LC 105, en general, las limitaciones al secreto bancario no dependen de intervención del Poder Judicial. Pueden ocurrir directamente revelaciones de datos bancarios que tienen por fin: la *preservación del sistema crediticio*[903], por medio de las informaciones que ayuden en análisis de riesgo (ver art. 1º, § 3º, incisos I[904] y II[905]); la

[902] Curiosamente entendió el Supremo Tribunal Federal, en el MS 1959, del 23 de enero de 1953, que sólo la autoridad administrativa expresamente sometida al sigilo de la información recibida en el ámbito de sus funciones quedaba impedida de la divulgación.

[903] Este fin ya era admitido por la doctrina aun antes de esa norma legal (Vide OLIVEIRA LIMA ROQUE, Maria José. *Sigilo bancário e direito à intimidade... cit.*, p. 86, 112 y 113).

[904] "a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de

realización del *poder de policía de los órganos de fiscalización del sistema financiero* (art. 2º, §§ 1º y 3º[906]); y en la comunicación de la práctica de ilícitos penales y administrativos (art. 1º, § 3º , IV)[907].

Existe una especial preocupación con el crimen del "lavado de dinero" proveniente de las ganancias de operaciones delictivas (art. 1º, § 3º, IV, parte final). En este caso la limitación al secreto bancario viene prevista más detalladamente en la ley 9.613/98 y se hace posible la comunicación de meros indicios (art. 11 de la ley 9.613/98) a un órgano propio especialmente diseñado para centralizar este tipo de información, el COAF – Consejo de Control de Actividades Financieras, el cual comunica a las instituciones de persecución penal las sospechas fundadas (arts. 14 y 15 de la ley 9.613). Los órganos fiscalizadores también deben enviar al COAF las informaciones bancarias que tuvieran conocimiento o existiesen indicios de lavado de dinero, lo que es una excepción a su propio deber de secreto (LC N º 105, art. 2º, § 6º).

Aunque estas hipótesis de límites al secreto de datos bancarios ocurran sin grandes problemáticas diurnamente en la práctica administrativa brasileña, hay una serie

---

centrais de risco". La intención aquí es reforzar el intercambio de informaciones positivas sobre el consumidor (ROSCOE BESSA, Leonardo. *O consumidor e os limites dos bancos de dados... cit.*,p. 270).

905 "o fornecimento de informações constantes de cadastro de emitentes de cheques sem provisão de fundos e de devedores inadimplentes, a entidades de proteção ao crédito"

906 "§1º. O sigilo, inclusive quanto a contas de depósitos, aplicações e investimentos mantidos em instituições financeiras, não pode ser oposto ao Banco Central do Brasil:
I – no desempenho de suas funções de fiscalização, compreendendo a apuração, a qualquer tempo, de ilícitos praticados por controladores, administradores, membros de conselhos estatutários, gerentes, mandatários e prepostos de instituições financeiras; (…)
§3º. O disposto neste artigo aplica-se à Comissão de Valores Mobiliários, quando se tratar de fiscalização de operações e serviços no mercado de valores mobiliários, inclusive nas instituições financeiras que sejam companhias abertas."

907 Además, la regla del artículo 9º de la LC n.º 105/2001, dispone expresamente que, , "quando, no exercício de suas atribuições, o Banco Central do Brasil e a Comissão de Valores Mobiliários verificarem a ocorrência de crime definido em lei como de ação pública, ou indícios da prática de tais crimes, informarão ao Ministério Público, juntando à comunicação os documentos necessários à apuração ou comprovação dos fatos."

de impugnaciones recientes al acceso directo de datos bancarios por el Ingreso Federal para fines de recaudación.

4.4.1.2.1.1 Acceso directo del secreto bancario por el Fisco

En la vigencia de la ley 4.595, del 31 de diciembre de 1964, no había derecho al quiebre directo del secreto bancario por parte de la autoridad fiscal, pues el artículo 38 establecía que "las instituciones financieras conservarán en secreto sus operaciones activas y pasivas y servicios prestados" y porque el párrafo único del artículo 197 del CTN[908] habría revocado tácitamente los párrafos 5º y 6º del artículo 38 de la ley 4.595[909].

Este escenario comienza a cambiar con el artículo 8º de la ley 8.021 de 1990[910], que permite los lanzamientos tributarios de oficio con relación a contribuyentes con "señales exteriores de riqueza", o sea, indicaciones de patrimonio no compatible con el ingreso por ellos declarado, admitiendo de este modo que esto se configuraría como una

[908] "Art. 197. Mediante intimação escrita, são obrigados a prestar à autoridade administrativa todas as informações de que disponham com relação aos bens, negócios ou atividades de terceiros:
(…) II - os bancos, casas bancárias, Caixas Econômicas e demais instituições financeiras;
(…) Parágrafo único. A obrigação prevista neste artigo não abrange a prestação de informações quanto a fatos sobre os quais o informante esteja legalmente obrigado a observar segredo em razão de cargo, ofício, função, ministério, atividade ou profissão."

[909] "Art. 38. As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados.
(…) § 5º Os agentes fiscais tributários do Ministério da Fazenda e dos Estados somente poderão proceder a exames de documentos, livros e registros de contas de depósitos, quando houver processo instaurado e os mesmos forem considerados indispensáveis pela autoridade competente.
§ 6º O disposto no parágrafo anterior se aplica igualmente à prestação de esclarecimentos e informes pelas instituições financeiras às autoridades fiscais, devendo sempre estas e os exames serem conservados em sigilo, não podendo ser utilizados senão reservadamente."

[910] "Art. 8° Iniciado o procedimento fiscal, a autoridade fiscal poderá solicitar informações sobre operações realizadas pelo contribuinte em instituições financeiras, inclusive extratos de contas bancárias, não se aplicando, nesta hipótese, o disposto no art. 38 da Lei n° 4.595, de 31 de dezembro de 1964."

excepción a lo dispuesto por el artículo 38 de la ley de 1964, permitiendo la solicitud sin intermediarios del Fisco a las instituciones financieras.

Pero esa ley encontró poca aplicación práctica y observación en la jurisprudencia. Así, por ejemplo, en la Pet QO Nº 577, del 25 de marzo de 1992, en que el relator, Ministro Carlos Veloso, entendió que el encontrar "fajas de dinero" en los residuos del ministro de Estado no era razón suficiente para que el Judicial apartase ese "secreto" en pro del interés público. Básicamente el Supremo no se apartaba de la jurisprudencia anterior a la Constitución de 1988[911], que admitía el "quiebre" del secreto bancario solamente en las hipótesis de los párrafos del artículo 38 de la ley 4.595, o sea, por medio de autorización judicial, o determinación de Comisión Parlamentaria de Investigación[912].

En 1996 se instituyó un tributo en Brasil (ley Nº 9.311/1996) cuyo hecho generador era exactamente los movimientos financieros (Contribución Provisoria sobre Movimiento o Transmisión de Valores y de Créditos y Derechos de Naturaleza Financiera – CPMF), lo que, claro, permitía a las Haciendas el acceso a las informaciones bancarias de los contribuyentes. La extinción de ese tributo en 2007, sin embargo, no ocasionó la disminución legal de los poderes del Fisco.

---

911 Vide RMS 15.925, Recurso Extraordinario 71.640, Mandado de segurança 1.047, Mandado de segurança 2.172 y Recurso Extraordinario 94.608. Aun merecen destaque casi 40 años de juzgados del STF, hasta la CF de 88, sobre el tema, y en la formación de este posicionamiento que siempre admitió el alejamiento del sigilo bancario en pro de interés público superior, el RHC 31.611, el MS 2.172, el RMS 2.574, el RMS 9.057, el AG 40.883, el RE 82.700, el RE 94.608, el AG (AgRg) 115.469 y el HC 66.284.

912 Que, conviene recordar, posee poderes propios de autoridad judicial, por fuerza del artículo 58, § 3º de la Constitución ("As comissões parlamentares de inquérito, que terão poderes de investigação próprios das autoridades judiciais, além de outros previstos nos regimentos das respectivas Casas, serão criadas pela Câmara dos Deputados e pelo Senado Federal, em conjunto ou separadamente, mediante requerimento de um terço de seus membros, para a apuração de fato determinado e por prazo certo(...)").

Pues en 2001, al ser modificado el párrafo 3º del artículo 11 de esa ley 9.311 (por la ley 10.174/2001, sancionada un día antes de la LC Nº 105), el Congreso Nacional autorizó la utilización de estos datos inherentes al cálculo del tributo debido para cada ciudadano para lanzamientos de otros impuestos[913]. Por fin el art. 6º[914] de la LC Nº 105/2001, expresamente permite el acceso a informaciones bancarias por los agentes de fiscalización tributaria de la Unión, de los Estados, Distrito Federal y Municipios.

El art. 5º de la LC Nº 105 establece también que habrá informaciones sobre operaciones financieras de clientes del banco que serán dadas de manera automática, bajo criterios definidos exclusivamente por el Poder Ejecutivo por medio de su poder reglamentario[915]. Aunque al principio estos datos solo contengan la identificación del titular de la cuenta y el total mensual de las transacciones (§ 2º de ese artículo), el párrafo 4º a continuación admite que la autoridad fiscal que reciba los datos, frente a su capacidad, requiera otras informaciones complementarias[916].

Pero en la doctrina y jurisprudencia está bastante controvertida la constitucionalidad del acceso directo a los datos por parte del Fisco. Existe en la

---

913 "§ 3º A Secretaria da Receita Federal resguardará, na forma da legislação aplicável à matéria, o sigilo das informações prestadas, facultada sua utilização para instaurar procedimento administrativo tendente a verificar a existência de crédito tributário relativo a impostos e contribuições e para lançamento, no âmbito do procedimento fiscal, do crédito tributário porventura existente, observado o disposto no art. 42 da Lei no 9.430, de 27 de dezembro de 1996, e alterações posteriores. (Redação dada pela Lei nº 10.174, de 2001)"

914 "as autoridades e os agentes fiscais tributários da União, dos Estados, do Distrito Federal e dos Municípios somente poderão examinar documentos, livros e registros de instituições financeiras, inclusive os referentes a contas de depósitos e aplicações financeiras, quando houver processo administrativo instaurado ou procedimento fiscal em curso e tais exames sejam considerados indispensáveis pela autoridade administrativa competente". El concepto de lo que puede ser considerado *indispensable* fue reglamentado en el artículo 3º del Decreto 3.724/2001.

915 Actualmente estos criterios se encuentran en el Decreto presidencial n º 4.489/2002.

916 "§ 4o Recebidas as informações de que trata este artigo, se detectados indícios de falhas, incorreções ou omissões, ou de cometimento de ilícito fiscal, a autoridade interessada poderá requisitar as informações e os documentos de que necessitar, bem como realizar fiscalização ou auditoria para a adequada apuração dos fatos."

aceptación de que los movimientos bancarios y financieros constituyen el *aspecto económico*[917] de la esfera particular del ciudadano que merece protección constitucional una consecuencia con otro postulado un tanto más controvertido: la que la flexibilización del secreto bancario depende *siempre* del orden judicial, estando sometida a una "reserva de jurisdicción", aunque no expresamente determinada en el texto constitucional.

El Ministro JOSÉ AUGUSTO DELGADO, del Tribunal Superior de Justicia, en conferencia posteriormente transformada en artículo, resumió los presupuestos y consecuencias antevistas por los que concentran el quiebre del secreto bancario solamente en el Poder Judicial:

> "A administração tributária, por melhor que seja a sua estrutura e os seus propósitos, não está emocionalmente preparada para conceber e aplicar os princípios que sustentam a cidadania fiscal. Isso ocorre, primeiramente, pelo fisco ter como missão exclusiva exercer a função de arrecadar tributos. É a sua meta essencial, por ser atribuição na organização administrativa estatal está obrigado a desempenhar. Não lha cabe administrar o tributo arrecadado, limitando-se, unicamente, a envidar esforços para o cumprimento das metas impostas para imprimir aumentar a arrecadação tributária. O sucesso da administração tributária é medido pelo maior volume de recursos fiscais atraídos para os cofres do Governo, nunca pelo respeito que exerça para com os direitos fundamentais do contribuinte. É questão de cultura administrativa, de distribuição de funções no sistema estatal, difícil de ser mudado só com sugestões doutrinárias. Necessita de vontade política.
> Por outro lado, a fiscalização tributária não consegue afastar as pressões exercidas sobre ela determinados segmentos da organização estatal que defendem uma atuação mais agressiva para a cobrança tributos, tudo em decorrência dos efeitos produzidos pela conduta ilícita marcante da sonegação fiscal.
> Esses fatores contribuem para que a fiscalização tributária atue parcialmente para avaliar a necessidade objetiva da quebra do sigilo bancário do cidadão. Por melhor que seja o seu desempenho, nunca ganhará a confiança do contribuinte.
> A atribuição da quebra do sigilo bancário, em um regime democrático onde predomina o respeito maior aos direitos fundamentais da cidadania, deve ser exercido pelo Poder Judiciário, não só porque seus membros estão revestidos da garantia da vitaliciedade, inamovibilidade e irredutibilidade de vencimentos, bem como, porque exercem suas funções com independência absoluta em relação ao Poder interessado na cobrança do tributos e consequentemente, no resultado a ser obtido pela ação fiscal.
> Esse sistema misto, onde o fisco faz a solicitação motivada para a quebra do sigilo bancário ao Judiciário e este, após analisá-la com objetividade e cautela, defere ou indefere, impõe segurança e confiabilidade da atuação fiscal e sublima o respeito à dignidade do contribuinte, em outras palavras, da cidadania fiscal, isto é, de ´cidadania de liberdade, que o estado fiscal pressupõe,

[917] WALD, Arnoldo. "O sigilo bancário no projeto de Lei Complementar de reforma do sistema financeiro e na lei complementar nº 70." *Revista de información legislativa*, 1992, p. 234.

> para não ser postergada impõe um sistema fiscal balizado estritos limites jurídico-constitucionais. Limites esses que integram a chamada constituição fiscal e que podem reconduzir, para não nos alongarmos nesse aspecto, a duas idéias: uma idéia de segurança, que tem o tradicional e principal suporte no princípio da legalidade fiscal, e uma idéia de justiça ou equidade, que tem a ver com a medida dos impostos e assenta no princípio da capacidade contributiva´
> Em conclusão, a adoção de um sistema, para a quebra do sigilo bancário, em que o Poder Judiciário é árbitro dos pedidos da Administração Pública, não é somente mais justo, mas, consegue impor maior credibilidade atuação fiscal e presta homenagem, com intensa potencialidade, aos princípios democráticos consistentes na garantia da segurança jurídica, do respeito aos direitos fundamentais do cidadão, nesse rol incluídos os à privacidade e intimidade. Além disso, torna mais respeitável a relação entre fisco e contribuinte, valorizando, portanto, a opção do Estado pelo regime democrático."[918]

Además de los excesos de exacción de la fiscalización sobre la esfera privada, crea también en la doctrina la preocupación de que el Estado use estas informaciones bancarias como medio de conocer otros detalles de la vida del contribuyente. Saber donde son realizados gastos puede incluir detalles relevantes de la personalidad, como permitir conocer preferencias político partidarias o religiosas[919].

Esas fuertes reticencias explican que en cuanto a la constitucionalidad de la posibilidad de autoridades fiscales acceder a informaciones bancarias sin previa autorización judicial y de la ley complementaria Nº 105 hay 5 Acciones Directas de Inconstitucionalidad (ADINS 2386, 2397, 2390, 2406 y 2389), también pendientes de juicio en el Supremo Tribunal Federal.

Sin embargo existe hoy en el derecho brasileño un instrumento procesal civil que permite a Tribunales Superiores, STJ y STF, reunir recursos de su capacidad de la misma especie que traten del mismo tema para uniformizar de una única vez determinada duda jurídica. El Tribunal Superior de Justicia, responsable por la interpretación de la legislación federal, decidió sobre el tema a fines de noviembre de

[918] DELGADO, José Augusto. "Os sigilos bancário e fiscal no ordenamento jurídico brasileiro". *Interesse Público*, setembro 2002.
[919] Assim CARRAZZA , Roque Antonio. *Curso de Direito Constitucional Tributário*. São Paulo: Malheiros, 2000, p. 403.

2009.

En el recurso especial Nº 1.134.665, el STJ entendió que la controversia en cuanto a la posibilidad de que el Fisco verifique sin previa autorización judicial datos bancarios debe resolverse en favor de la legalidad de la acción del agente fiscal. Esta extensión de los poderes de la Administración Tributaria, según el voto del relator en el STJ, Min. Luiz Fux[920], se justificaría por el artículo 145, § 1º de la Constitución de 1988[921], que busca garantizar al Estado los medios correspondientes para la medición de los tributos debidos por cada uno de los ciudadanos.

En el Supremo Tribunal Federal esta cuestión del suministro de informaciones bancarias directamente al Fisco para fines de cálculo tributario aún se encuentra esperando dictamen, por medio de la denominada "repercusión general" admitida en el Recurso Extraordinario Nº 601.314. Sin embargo, otro Recurso Extraordinario, Nº 389.808, fue juzgado sobre el mismo tema en diciembre de 2010. Y en este caso, se mostró la inseguridad que aún domina el tema, pues hubo una preliminar dada monográficamente por el relator, Min. Marco Aurélio, que el 24 de noviembre de 2010 fue revocada por el voto de 6 ministros (con 4 votos en contra) en el sentido de estar de acuerdo con la constitucionalidad del quiebre directo del secreto bancario por Ingreso Federal.

Pues bien, la cuestión aún no estaba decidida. Porque en el dictamen del mérito, el 15 de diciembre siguiente, fue estimado a ese mismo Recurso Extraordinario, con el

[920] Y que es, desde marzo de 2011, ministro del Supremo Tribunal Federal.

[921] "§ 1º - Sempre que possível, os impostos terão caráter pessoal e serão graduados segundo a capacidade econômica do contribuinte, facultado à administração tributária, especialmente para conferir efetividade a esses objetivos, identificar, respeitados os direitos individuais e nos termos da lei, o patrimônio, os rendimentos e as atividades econômicas do contribuinte."

fundamento de que la orden judicial sería imprescindible para el acceso a las informaciones bancarias por parte del Fisco, la actuación "moderadora" del Judicial, para establecer el adecuado balance del respeto al deber de abstención estatal en la vida privada de las personas y del interés público existente en la fiscalización tributaria[922]. Durante los debates se verifica que solamente el Min. Gilmar Mendes cambia su voto con relación al de la decisión sobre la preliminar (y por eso hay nuevamente una decisión por 6 votos contra 4) y la surgida minoría concentra sus fundamentos en la preocupación de que la necesidad de decisión judicial solape la eficacia fiscalizadora del Estado.

4.4.1.2.2 Límites al secreto fiscal

La LC Nº 104, a su vez, incluyó diversas excepciones al secreto fiscal por medio de la inclusión de los §§ 1º y 3º en el artículo 198 del CTN. Por eso debe la Hacienda de la Unión, de los estados miembro y de los municipios informar los datos que poseen en sus bases de datos en cuanto a sus contribuyentes cuando sea requerido por autoridad judicial (§ 1º, I) o cuando sea solicitado por otra autoridad administrativa para una investigación de infracción administrativa de responsabilidad de la solicitante (§ 1º, II). La identificación personal del receptor, la exigencia de que sea persona idéntica al solicitante y la obligación de mantenimiento del secreto, previstas en el párrafo 2º del artículo 198[923] sin duda facilitan la responsabilidad posterior por el "vacío" de informaciones a terceros. También el presupuesto de proceso administrativo ya

[922] Conforme expresa el voto que hace con la mayoría de este juzgamiento el decano del STF, Min. Celso de Mello.

[923] "§ 2º O intercâmbio de informação sigilosa, no âmbito da Administração Pública, será realizado mediante processo regularmente instaurado, e a entrega será feita pessoalmente à autoridade solicitante, mediante recibo, que formalize a transferência e assegure a preservação do sigilo."

instaurado impide que ocurran investigaciones sin objeto definido y cuya ausencia de formalización impida el control posterior. Algunos autores agregan también que la existencia de un proceso administrativo significa que ya se debe haber formado un acuerdo, o sea, ya debe haber investigado ejerciendo el contradictorio y la amplia defensa junto a la Administración[924].

La fiscalización también debe remitir "Representación Fiscal para fines penales" (RFFP) al Ministerio Público cuando concluya el procedimiento fiscal que verifique la incidencia de la falta contra el orden tributario (art. 83 de la ley 9.430/96).

Para finalizar, está generalmente autorizada a divulgar datos de esas RFFP (§ 3º, inciso I del art. 198 del CTN), de las inscripciones en la deuda activa de la Hacienda Pública (§ 3 º, inciso II) y los relativos a cuotas y moratorias de tributos (inciso III siguiente)[925]. Este párrafo es objeto de fuerte crítica doctrinaria, pues se trata de informaciones capaces de provocar limitaciones a los deudores tributarios, especialmente en la divulgación de la lista de deudores inscriptos en la deuda activa[926]. Pero es una práctica que viene explayándose en las Administraciones brasileñas, sin rechazos por el Poder Judicial[927], que acepta un carácter *público* de ese registro[928]. Para favorecer la evaluación de riesgos crediticios de entidades públicas y privadas y como requisito a la concesión de recursos públicos federales existe también la previsión legal

924 PEIXOTO, Marcelo Magalhães e LACOMBE, Rodrigo Lourenço Masset (orgs.). *Comentários ao código tributário nacional*. São Paulo: MP, 2005, p. 1397.

925 Ello proporcionó que el tributarista afirmara que " Na prática, pode-se dizer que já não existe o sigilo fiscal, pelo menos para impedir o que as autoridades da administração tributária mais gostam de fazer, que é utilizar a publicidade sensacionalista como forma de constranger o contribuinte." (BRITO MACHADO, Hugo de. *Curso de direito tributário*. São Paulo: Malheiros, 2004, p. 239).

926 En ese sentido CALMON NAVARRO COÊLHO, Sacha. *Curso de direito tributário brasileiro*. Rio de Janeiro: Forense, 2004, p. 901, que lo califica como "constrición política" y SILVEIRA DIFINI, Luiz Felipe. *Manual de Direito Tributário*. São Paulo: Saraiva, 2005, p. 351.

927 Vide, por ejemplo, la des-provisión por unanimidad de la apelación civil nº 200338000277800 por el 8ª grupo del Tribunal Regional Federal de la 1ª Región (juzgamiento el 10 de septiembre de 2010).

928 Ello estaba expresado también en el artículo 11 del decreto ley 1.893.

del acceso por estas instituciones a un "Registro Informativo de créditos no abonados del sector público federal" (Cadin – *Cadastro Informativo de créditos não quitados do setor público federal*) por la ley 10.522/2002.

También está permitida la "permuta de informaciones" entre las Administraciones Tributarias de los entes federativos internos, por medio de ley o convenio (art. 199, "caput" del CTN) y también con estados extranjeros, por medio de tratados, acuerdos o convenios (art. 199, párrafo único). La importancia del intercambio de informaciones entre las administraciones tributarias, un tema que tiene gran importancia, sin duda, por las presiones presupuestarias de los entes federativos, alcanzó *status* constitucional en Brasil con la Enmienda Constitucional Nº 42 de 2003, que agregó el inciso XXII al artículo 37 de la Constitución[929]. Este texto constitucional, aunque esencialmente parecido a la disposición del Código, reforzó como una *obligación* el diálogo entre los Fiscos de la Unión, Estados miembro y municipios[930].

4.4.1.2.3 Límites al sigilo de datos en los registros de las empresas concesionarias de telecomunicaciones

En materia de los datos en poder de empresas de telefonía, la LGTel no establece ninguna limitación, lo que llevó al propio órgano regulador a preservarse restringiendo por sí mismo la protección constitucional a fronteras que no abalen el ejercicio de sus

[929] "XXII - as administrações tributárias da União, dos Estados, do Distrito Federal e dos Municípios, atividades essenciais ao funcionamento do Estado, exercidas por servidores de carreiras específicas, terão recursos prioritários para a realização de suas atividades e atuarão de forma integrada, inclusive com o compartilhamento de cadastros e de informações fiscais, na forma da lei ou convênio."

[930] ALEXANDRINO, Marcelo e PAULO, Vicente. *Direito tributário na Constituição e no STF: teoria e jurisprudência*. Niteroi, RJ: Impetus, 2004, p. 11.

finalidades. Esa laguna legal motivó que ANATEL reglamentase su esfera propia, para evitar óbices en sus actividades de fiscalización. En el artículo 29 del anexo de su Reglamento Nº 441/06 afirmó que cualquier suministro de datos para su fiscalización no configuraría violación de la privacidad de nadie[931]. Al mismo tiempo, en el artículo 43 del mismo anexo impuso *sigilo* a los fiscales sobre las informaciones que reciban, salvo por motivo de determinación legal o autorización de superior jerárquico (§ 2º de este artículo).

La única limitación legal que expresa la privacidad del registro telefónico en Brasil se encuentra en el artículo 3º de la ley 10.703/2003, que determina a las empresas de telefonía que habiliten la lista de aparatos de teléfonos celulares robados conteniendo nombre de usuario, número de serie del aparato y código de acceso del teléfono, cuando así lo requiera el juez, Ministerio Público o la policía, norma estimulada por el uso de organizaciones delictivas de esa práctica delictiva como medio para cometer delitos más graves, como extorsiones y secuestros.

4.4.1.2.4 Limitación al secreto de datos según el órgano solicitante: investigaciones realizadas por las Comisiones Parlamentarias de Investigación y por el Ministerio Público

[931] Ese artículo es, sin embargo, implícitamente negado por el artículo 39 de la propia LGTel, que admite la consulta pública en la Biblioteca de toda la documentación de la Agencia, salvo aquella que que "violar a segurança do País, segredo protegido ou a intimidade de alguém". La Procuraduría de ANATEL desarrolla ese entendimiento en otro parecer, afirmando que no se viola la intimidad porque el dato conocido del usuario no servirá para inhibirle la libertad individual, como ocurre en el conocimiento con fines policiales (ítem 30 del Parecer nº 1314/2009/LBC/PGF/PFE-ANATEL). Ello, sin embargo, es una enorme restricción del ámbito normativo del concepto constitucional de "intimidad", no obstante, se reconoce que la interpretación busca el interés público de garantizar los medios necesarios a la efectiva fiscalización que debe ser hecha por la agencia en los términos del párrafo único del artículo 1º de la LGTel.

Cualquier imposición de secreto de datos no alcanza la posibilidad de "quiebre" (o sea determinación de limitación del derecho individual) por Comisión Parlamentaria de Investigación (CPI). El STF, en el Mandado de Segurança Nº 23.452[932], relator Min. Celso de Mello, del 16 de septiembre de 1999, que al interpretar el artículo 58, párrafo 3º de la CF, que concede a las CPIs "poderes de investigaciones propios de autoridades judiciales", afirmó que eso implica en su poder de retirar el manto de secreto sobre esos datos de protección especial en Brasil, informaciones *bancarias, fiscales* y *datos de registro/registros telefónicos,* siempre que lo hiciese tal cual un juez, o sea, motivadamente y bajo el control final de legalidad por el propio Supremo Tribunal Federal. Eso porque, al contrario del secreto de las comunicaciones telefónicas en que la Constitución Brasileña exige expresamente, al final del inciso XII del art 5º, que su alejamiento se dé por medio de orden judicial, no hay cláusula de *reserva de jurisdicción* equivalente en la protección de datos o en la intimidad. Las bases del entendimiento del STF quedan muy claras en este trecho del voto del relator:

> "Também admito a possibilidade jurídico-constitucional de as comissões parlamentares de inquérito, agindo *ex propria autoritate*, determinarem, sempre mediante resolução fundamentada, a ruptura do sigilo fiscal e do sigilo concernente aos registros/dados telefônicos (hipótese esta absolutamente inconfundível com a da interceptação das comunicações telefônicas, que constitui matéria sujeita ao princípio da reserva de jurisdição, nos termos do art. 5º, XII, *in fine*, da Carta Política).
> [...]
> A interceptação das comunicações telefônicas, além de submetida ao postulado da reserva constitucional de jurisdição – que somente deixa de incidir nas hipóteses de estado de defesa (CF, art. 136, § 1º, c) e de estado de sítio (CF, 139, III) -, possui finalidade específica, pois a utilização desse meio probatório apenas se justifica, havendo ordem judicial, "para fins de investigação criminal ou de instrução processual penal" (CF, art. 5º, XII, in fine), circunstância esta que exclui, por completo, a possibilidade constitucional de uma CPI determinar, por autoridade própria, a escuta de conversações telefônicas.
> Diversa é, porém, a situação concernente ao acesso da CPI aos registros telefônicos, pois, consoante enfatiza o magistério da doutrina (LUIZ CARLOS DOS SANTOS GONÇALVES, "Direito Civil Constitucional – Cadernos I", p. 249, 1999, Max Limonad; TÉRCIO SAMPAIO FERRAZ JÚNIOR, "Cadernos de Direito Constitucional e Ciência Política", vol. 1/85), o inciso XII do art. 5º da Carta Política "impede o acesso à própria ação comunicativa, mas não aos dados comunicados", mesmo porque estes – os dados comunicados – protegidos pela cláusula tutelar da intimidade, inscrita no inciso X do art. 5º da Constituição, "não constituem um limite absoluto" à ação do Poder Público.

[932] Mandado de Segurança n.º 23452 – RJ, Pleno del Supremo Tribunal Federal, Relator Ministro Celso de Mello, j. el 16/09/1999, DJ 12/05/2000.

> [...]
> Impõe-se analisar, agora, um postulado, que, destinado a proteger valores essenciais resguardados pela própria Constituição, representa um relevante fator de limitação jurídica aos poderes de investigação da Comissão Parlamentar de Inquérito.
> Nesse contexto, assume indiscutível importância político-jurídica o postulado da reserva constitucional de jurisdição.
> É por tal razão – e não obstante a amplitude da competência investigatória da CPI – que entendo não se revelar lícito a qualquer órgão parlamentar de investigação a prática de atos sujeitos ao princípio constitucional da reserva de jurisdição, vale dizer, a prática de atos cuja efetivação a Constituição Federal atribuiu, com absoluta exclusividade, aos membros do Poder Judiciário.
> [...]
> Isso significa – considerada a cláusula de primazia judiciária que encontra fundamento no próprio texto da Constituição – que esta exige, para a legítima efetivação de determinados atos, notadamente daqueles que implicam restrição a direitos, que sejam eles ordenados apenas por magistrados."

Declaró también el Tribunal en ese dictamen que las Comisiones Parlamentarias de Investigación y sus integrantes no pueden publicar los datos referentes al secreto que tuvieran conocimiento. O sea, los datos revelados a ellos no se convierten en datos públicos.

De forma similar de los argumentos que buscan impedir el acceso a datos bancarios por el Fisco, se encuentra una fuerte resistencia en la *requisición* de este y de cualquier otro dato secreto por parte del Ministerio Público, o sea, cuando esta institución se coloca en la posición activa de pedir las informaciones. El argumento central se concentra nuevamente en la parcialidad del órgano, que no tendría la distancia necesaria para ponderar los bienes jurídicos en cada caso en concreto de acceso sin el consentimiento del afectado. Esto podría causar que siempre debieran previamente obtener mandato judicial, permitiendo así al Poder Judicial el control previo de sus acciones. Para el Ministerio Público, por lo tanto, la tendencia es en el sentido directamente contrario, o sea, la jurisprudencia crecientemente exige autorización judicial en el acceso a datos secretos o confidenciales.

El STF decidió en este sentido en el Recurso Extraordinario Nº 215.301, del 13 de abril de 1999. En este caso, teniendo como relator al Min. Carlos Veloso, se afirmó

que solamente excepción con expresa mención al Ministerio Público permitiría que el órgano, sin el deber de la imparcialidad, realizase en el caso concreto la ponderación de intereses necesaria a la flexibilización de derechos fundamentales. Así, de forma pacífica para la Corte Suprema brasileña, el secreto bancario es un específico campo inmune al "poder de requisición" genérico del "Parquet", previsto en el inciso VI del artículo 129 de la CF y en los incisos II y IV y párrafo 2º del artículo 8º de la ley complementaria Nº 75. Más aún, indica la no recepción por la actual orden constitucional del artículo 29 de la ley 7.492 (ley de crímenes contra el sistema financiero nacional), del 16 de junio de 1986[933].

En la Acción Cautelar Nº 1928, en que se encontraba este Tribunal con la cuestión de si era posible el acceso del Ministerio Público y la policía a datos de registros telefónicos en cualquier investigación delictiva, la preliminar es concedida por el Min. Gilmar Mendes, en el ejercicio de la presidencia, para impedir ese acceso solamente la siguiente fundamentación:

> "De fato, a questão não parece ser da inviolabilidade das comunicações de dados (inciso XII), mas, sim, de proteção ao sigilo dos dados, tido como projeção do direito à privacidade (inciso X).
> É bem verdade que, no entendimento desta Corte, esse não é um direito absoluto, mas 'que deve ceder diante do interesse público, do interesse social e do interesse da Justiça' (…)
> (…) o acesso a dados constitucionalmente protegidos somente [deve] ocorrer no exercício de um caso concreto e com motivação substancial." (Subrayado en el original)[934]

Por fin, también hay decisiones de tribunales superiores que niegan el acceso directo del MP a datos bajo el secreto fiscal[935].

---

933 "Art. 29. O órgão do Ministério Público Federal, sempre que julgar necessário, poderá requisitar, a qualquer autoridade, informação, documento ou diligência, relativa à prova dos crimes previstos nesta lei.
Parágrafo único O sigilo dos serviços e operações financeiras não pode ser invocado como óbice ao atendimento da requisição prevista no caput deste artigo."

934 Decisión del 7 de enero de 2008. Esa decisión no llega a tener su análisis de mérito por el pleno, en razón de la pérdida del objeto, pues se impugnaba decisión interlocutoria en proceso que ya llegara a la sentencia final en 1ª instancia.

935 RHC 20329 / PR, 5ª Grupo del STJ, relatora Ministra Convocada Jane Silva, decisión del 4 de octubre de 2007.

Se nota, por lo tanto, un vacío en la jurisprudencia más actual de ese *poder de requisición* directa del Ministerio Público, que exactamente serviría para ese acaparamiento de documentos de fuentes públicas y privadas en la instrucción probatoria destinada a formar su convencimiento en el ejercicio de sus atribuciones[936]. Eso ocurre, aunque haya sido originalmente concebido para resistir especialmente a estas informaciones cubiertas bajo el sigilo, como certifican los párrafos 1º y 2º del artículo 8º de la LC 75/93[937] y la jurisprudencia más cercana a la promulgación de la Constitución de 1988[938].

4.4.2 La legislación del *Habeas Data* en Brasil

La regulación principal del *habeas data* en Brasil es la ley 9.507/97. Constitucionalmente el objeto del habeas data es el *conocimiento* y la *rectificación* de informaciones relativas a la persona del impetrante[939], el cual es agregado por el inciso III del artículo 7 º de la ley 9.507/97 de la posibilidad de *anotación* de contestación o explicación sobre hecho controversial. Hay una concentración de las facultades concedidas al individuo, por tanto, en preservar la *verdad* en sus registros

936 NIGRO MAZZILLI, Hugo. *A Defesa dos interesses difusos em juízo meio ambiente, consumidor e patrimônio cultural*. São Paulo: Revista dos Tribunais, 2007, p. 408.

937 „LXXII - conceder-se-á "habeas-data":
a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;“

938 Vide el MS 5370 de la 1ª Sección del STJ, juzgado el 12 de noviembre de 1997.

939 „LXXII – se concederá "habeas-data":
a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante, constantes de registros o bases de datos de entidades gubernamentales o de carácter público;
b) para la rectificación de datos, cuando no se prefiera hacerlo por proceso sigiloso, judicial o administrativo;“

particulares[940]. Aisladamente, CELSO RIBEIRO BASTOS defiende que, aun no expresado, no es lógico no incluir como posible pedido también la *supresión* de datos cuando no adecuadas con "las finalidades legalmente definidas del órgano recolector"[941].

Esta acción judicial puede tener en el polo pasivo al titular de bases de datos públicas, cualquier que sea el uso o finalidad del archivo gubernamental, o privado, pues la ley conceptuó que tiene el *carácter público* constitucional todo registro que no sea para uso privativo del depositario, o sea, en que se posibilite la transferencia (art. 1º , § único de la ley 9507). No hay, por tanto, exigencia que la información esté en un ordenador o automatizada[942].

Ya en el polo activo deberá siempre estar el individuo a que se refiere la información, siendo diverso del derecho general de los ciudadanos de conocimiento de los archivos públicos (CF, art. 5º, inciso XXXIII), que es un reflejo de la *publicidad* que es impuesta la Administración Pública en Brasil por el "caput" del artículo 37 de la Constitución[943]. Aunque, en caso de un fallecido o afectado, pueden sus herederos requerir en favor del muerto, como forma de no dejar desguarnecida su memoria[944]. No hay tampoco ninguna indicación de que su uso esté vedado a personas jurídicas[945]. A propósito, ROSCOE BESSA defiende la importancia en el campo de la protección de datos la de verificar un derecho de rectificación a las personas jurídicas como forma de

---

940 GONÇALVES FERREIRA FILHO, Manoel. *Curso de Direito Constitucional*. São Paulo: Saraiva, 2005, p. 331.
941 RIBEIRO BASTOS, Celso. *Curso de direito constitucional. cit.*, p. 195.
942 SORICE BARACHO THIBAU, Tereza Cristina. *O Habeas data*. Belo Horizonte: Del Rey, 1997, p. 140.
943 SORICE BARACHO THIBAU, Tereza Cristina. *O Habeas data... cit.*, p. 119.
944 SILVA, José Afonso da. *Curso de direito constitucional positivo... cit.*, p. 454 y Tribunal Federal de Recurso, HD 001-DF, DJU, 2 de mayo de 1989.
945 MORAES, Alexandre de. *Direito constitucional*. São Paulo: Atlas, 2003, p. 156.

preservar su *honra* (objetiva) de informaciones falsas[946], conforme autoriza la conjugación de los artículos 20 y 52 del Código Civil brasileño.

En el campo de la inter-vinculación entre el derecho de acceso constitucional y el habeas data, la ley 9507 no fija ningún límite al acceso a las informaciones. Dejó así de posicionarse en una gran controversia relativa al *Habeas Data*, que es la aplicación también a él de la parte final del inciso XXXIII del artículo 5º de la Constitución[947], o sea, el mantenimiento del secreto también con relación al afectado de informaciones con el potencial de perjudicar la "seguridad de la sociedad y del Estado". Hay quien defienda la imposibilidad de la analogía para restringir el alcance del *habeas data*[948], incluso porque el contenido de la información ya sería de conocimiento de aquel que pueda amenazar el orden público estatal. Por otro lado, cuando enfrentó el tema, el Tribunal Federal de Recursos entendió que "frente a la cláusula del secreto (art. 5, XXXIII, CF), por indeclinable sumisión al interés público (seguridad de la sociedad y del estado), no es absoluto el derecho de acceso a las informaciones. Le compete al Judicial examinar el alegato del secreto, evaluando su procedencia o no, compatibilizando la seguridad del Estado con el derecho a la revelación de las informaciones pretendidas"[949].

---

946 ROSCOE BESSA, Leonardo. *O consumidor e os limites dos bancos de dados... cit.*, p. 103.

947 "XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;"

948 En este sentido MORAES, Alexandre de. *Direito constitucional.... cit.,* p. 162 , NOBRE MATTA, José Eduardo. *Habeas data*. Rio de Janeiro: Lumen Juris, 2005, p. 145 y Min. Ilmar Galvão, entonces en el TFR, tras ministro del STF, en su voto con la minoría en el HD 4, del 16 de junio de 1989.

949 HD 1 del Tribunal Federal de Recursos, decisión el 2 de febrero de 1989, relator para sentencia Min. Milton Pereira. Esa posición era la defendida por el entonces Consultor General de la República Saulo Ramos en su Parecer SR-71, del 6 de octubre de 1988, DOU v. 126, n. 194, sección 1, 11 de oct de 1988, p. 19.811 y es adoptada por JOSÉ CRETELLA JÚNIOR (*Os "Writs" na Constituição... cit.*, p. 122). THEREZA THIBAU, de manera más cuidadosa, admite el secreto solamente para preservar la efectividad de investigaciones (*O Habeas data*. Belo Horizonte: Del Rey, 1997, p. 118).

Es un proceso gratuito[950] y de rito sumario, con prioridad sobre todos los demás actos judiciales, salvo habeas corpus y mandatos de seguridad[951]. Su procedimiento es bifásico: primero está la notificación del reo para suministro de los datos que posea sobre el autor; tras la ciencia de este, se abre plazo para pedir eventual rectificación o anotación en sus registros (artículos 2º y 3º de la ley de *Habeas Data*).

El artículo 8º de la ley 9507 de 1997, siguiendo la jurisprudencia de casi una década del STJ, solidificada en el resumen nº 2[952], impuso como requisito de admisibilidad del HD la prueba de que el sujeto pasivo recusó el acceso, rectificación o anotación o estaba sin pronunciarse sobre ese pedido hace más de diez días en el primer caso y hace más de quince días en los dos últimos. ALEXANDRE MORAES critica esa orientación pacífica de los tribunales por imponer una limitación al ejercicio de derecho que no está prevista en la Constitución. Se termina de esa forma, para él, limitando el acceso al Judicial de forma arbitraria[953].

Hay aun reglas especiales[954] para regular esas facultades en las bases de datos referentes a relaciones de consumo, permitiendo que se diga que hay un "*habeas data* del consumo"[955]. La aplicación del Código de Defensa del Consumidor (ley 8.078/90) sin duda permite la obtención de mayor conformidad con la directiva europea. Su

---

950 CF, art. 5 º , inciso LXXVII. Y de la misma forma es gratuito el procedimiento administrativo de acceso, rectificación y anotación en bases de datos públicos (artículo 21 de la ley 9507).

951 Art. 19 de la ley 9507.

952 "Não cabe o habeas data (CF, art. 5.°, LXXII, a) se não houve recusa de informações por parte da autoridade administrativa"

953 MORAES, Alexandre de. *Direito constitucional... cit.*,p. 155.

954 ROSCOE BESSA, Leonardo. *O consumidor e os limites dos bancos de dados... cit.,* p. 277.

955 HERMAN DE VASCONCELLOS E BENJAMIN, Antônio. "Arts. 29 a 45". In *Código do Consumidor comentados pelos autores do anteprojeto*. Rio de Janeiro: Forense Universitária, 2007, p. 336. También la colocación del género "bancos de dados de consumidores" y de una de sus especies serviços de proteção ao crédito" expresamente, por el §4º. del artículo 43 del CDC, como "entidades de caráter público"" demuestra que el legislador pretendió conectarse con la garantía del *habeas data*, al repetir el concepto del párrafo "a" del inciso LXXII del art. 5º. de la CF.

artículo 43, aplicable a bases de datos públicas y privadas, automatizadas o no, impone una *transparencia*[956] a los archivos, al exigir que los datos sean registrados con objetividad, clareza, verdad[957] y en lenguaje de fácil comprensión (§1º.); que haya comunicación por escrito del registro al afectado cuando realizado sin intervención directa de él[958] (§2º.); y que el acceso y la posible "inmediata" rectificación, a ser comunicada en 5 días por el funcionario de archivos a eventuales cesionarios, es independiente del manejo de acción judicial ("caput" y §3º.). Además, establece una bienvenida *temporalidad* en el mantenimiento de la información, que es definida con plazo estipulado (5 años de plazo para la prescripción de cobranza de débitos) y relativamente a informaciones despreciativas del consumidor (§1º, parte final y §5º.).

Además, refuerza en general el cumplimiento de esos deberes la fiscalización y posibilidad de sanciones administrativas aplicadas por los órganos de defensa del consumidor[959]. Adicionalmente, para garantizar el respeto del derecho de acceso y de

---

956 BATISTA DE ALMEIDA, João. *Manual de Direito do Consumidor*. São Paulo: Saraiva, 2003, p. 98.

957 Lo que exige la actualización de la información "en breve espacio de tiempo" de su conocimiento (REsp 994638 / AM, 4ª. Grupo del STJ, Relator Min. Aldir Passarinho Júnior).

958 Aunque la ley no establezca plazos, la doctrina menciona 5 días, por analogía al plazo del párrafo siguiente, y de todo modo previamente a cualquier colocación a disposición de terceros (HERMAN DE VASCONCELLOS E BENJAMIN, Antônio. "Arts. 29 a 45"... *cit.*, p. 332). En cuanto a este último punto es pacífica la jurisprudencia del STJ, conforme admitido en el Recurso Especial Nº 1.061.134 – RS de la 2ª. Sección del STJ, Relatora Min. Nancy Andrighi, juzgamiento el 10 de diciembre de 2008.

959 "Art. 56. As infrações das normas de defesa do consumidor ficam sujeitas, conforme o caso, às seguintes sanções administrativas, sem prejuízo das de natureza civil, penal e das definidas em normas específicas:

I - multa;
II - apreensão do produto;
III - inutilização do produto;
IV - cassação do registro do produto junto ao órgão competente;
V - proibição de fabricação do produto;
VI - suspensão de fornecimento de produtos ou serviço;
VII - suspensão temporária de atividade;
VIII - revogação de concessão ou permissão de uso;
IX - cassação de licença do estabelecimento ou de atividade;
X - interdição, total ou parcial, de estabelecimento, de obra ou de atividade;
XI - intervenção administrativa;
XII - imposição de contrapropaganda.

Parágrafo único. As sanções previstas neste artigo serão aplicadas pela autoridade administrativa, no âmbito de sua atribuição, podendo ser aplicadas cumulativamente, inclusive por medida cautelar,

rectificación existen tipos penales específicos relativos al estorbo o impedimento del primero y al no cumplimiento inmediato del segundo (artículos 72 y 73 de la ley 8.078).

Nuevamente, no obstante, así como en las limitaciones que afectan el uso en la práctica del *habeas data* en general, son las presuposiciones que inspiran el CDC y su artículo 43 en particular que son reflejos a su influencia sobre el ejercicio de funciones administrativas. Primeramente, las relaciones de consumo sólo tienen incidencia en los denominados "servicios públicos impropios", o sea, que son prestados solamente mediante directa remuneración[960], no afectando las demás actividades estatales y servicios públicos, como salud, educación, policía, fiscalización, etc., que son costeados por los ingresos tributarios en general[961].

Además, el reglamento, no obstante su posible aplicación general a bases de datos de consumidores, fue pensado primordialmente como instrumento para alcanzar los registros relativos a crédito. Ello es unánime en la doctrina, desde uno de los autores de proyecto, al justificar el artículo 43 por las mismas razones de la exposición de motivos del *Fair Credit Reporting Act* estadounidense[962], a la descripción del espíritu de los debates legislativos[963], y se refleja en la realidad jurisprudencial, donde casi la totalidad de las causas involucra infracciones cometidas por registros de crédito o de incumplidores de pagos[964].

---

antecedente ou incidente de procedimento administrativo."

960 Los cuales, en Brasil, son hoy prácticamente todos realizados por empresas privadas que recibieron concesiones.

961 En ese sentido claro el STJ, Resp 1187456/RJ, rel. Min. Castro Meira, 2ª. Grupo, juzgado el 16/11/2010 y Resp 493.181/SP, rel. Ministra Denise Arruda, 1ª. Grupo, juzgado el 15/12/2005).

962 HERMAN DE VASCONCELLOS E BENJAMIN, Antônio. "Arts. 29 a 45"... *cit.*, p. 328.

963 Dice JOÃO BATISTA DE ALMEIDA: "Atento à verdadeira avalanche de abusos cometidos nessa área – que iam da utilização irregular de informações para forçar o pagamento de débito até a inabilitação creditícia do interessado na via extra-oficial -, procurou [o legislador] inibir tais condutas abusivas e regulamentar a matéria (...)" (*Manual de Direito do Consumidor... cit.*, p. 98).

964 La jurisprudencia existente en el STJ sobre ese artículo 43 es constante en la incidencia de esas

Esa concentración en el tema se explica en la práctica porque la veda de acceso a crédito por anotaciones pasadas es la forma de conocimiento por el individuo de la existencia de bases de datos con sus informaciones. Existe la carencia de un registro general que torne posible la *consulta* previa de los locales donde podrían constar sus datos. Sin embargo, ese control anterior no es de ninguna forma esperado de los órganos públicos en que, exclusivamente o no, se propongan a la defensa del consumidor. Al contrario, el artículo 44 del CDC sólo impone que ellos formen registros para divulgación de los reclamos de las violaciones de los derechos que el consumidor ya sabe violados, con el fin de auxiliar a los consumidores en sus elecciones en el "mercado de consumo"[965].

Por último, cabe destacar el surgimiento de la ley n. 12.414/11, del 9 de junio de 2011, que otorga todavía más facultades al particular, pero incide bajo un tipo de base de datos aun más restricto. Esta norma pretende estimular la creación de "registros positivos", en que la catalogación del historial de puntual pagamento serviría para estimular al mercado para que conceda menores intereses en el préstamo de dinero a los voluntariamente relacionados. En esa ley, que se agrega a la protección del CDC (art. 17 de la norma), se consagra la *información* previa al almacenamiento de identidad y objetivos del responsable por la base de datos (art. 5º. V), siendo el *consentimiento*, revocable (art. 5º., I), requisito para la creación (art. 4º.) y transferencia (art. 9º.) de sus registros; se impide la utilización de información *excesiva* (art. 3º., §3º., I), fuera de las

situaciones, como se ve en el Edcl en la Rcl 6132, AgRg en el Aresp 6098, AgRg en el Resp 1077808, AgRg en el Ag 1250156, AgRg en el Resp 1186062, AgRg en el Resp 1194277, AgRg en la MC 18038, AgRg en los Edcl en el Ag 881401, AgRg en el Ag 1377273, Rcl 4598, AgRg en el Resp 679845, Resp 1117319, AgRg en el Resp 1136802, AgRg en el Resp 1182290, sólo para quedar en los juzgamientos ocurridos en el año 2011 por ese tribunal.

965 HERMAN DE VASCONCELLOS E BENJAMIN, Antônio. "Arts. 29 a 45"... *cit.*, p. 338-339.

finalidades de recolección (art. 5º., inciso VII) o *sensible* (que viene definida en el art. 3º., §3º., II como aquella referente "al origen social y étnico, a la salud, a la información genética, a la orientación sexual y a las convicciones políticas, religiosas y filosóficas") y se vedan tratamiento exclusivamente automatizados, al mismo tiempo que se garantiza el acceso a los criterios del análisis de riesgo (incisos IV y VI del artículo 5º.). Aunque el párrafo único del artículo 1º deje claro que la ley es inaplicable a las bases de datos de derecho público, al menos queda la remisión al advenimiento de legislación específica (futura) sobre el tema[966].

4.5 Conclusiones

1. El estudio de las legislaciones nacionales de protección de datos de Alemania, España y Brasil pretende conocer el derecho en lo que respecta a las pretensiones jurídicas que están admitidas, sus límites y garantías.
2. La configuración legislativa del contenido, a su vez, será tanto mayor cuanto sea la abstracción con relación a la realidad fáctica o histórica de los contornos de un derecho, que, en el caso de la protección de datos, brinda una especial libertad de conformación al legislador, sin que ello supere los parámetros antes definidos en la Jurisdicción Constitucional.
3. Estos derechos configurados son naturalmente limitados en pro de otros bienes constitucionales, en una operación de ponderación en que interactúan el legislador y los tribunales constitucionales para, al fin, proveer el contenido esencial de cada derecho fundamental.
4. Por último, las legislaciones ofrecen las garantías individuales e

[966] "Art. 1º. , Párrafo único. Las bases de datos instituídos o mantenidos por personas jurídicas de derecho público interno serán regidos por legislación específica."

institucionales que protegen la efectividad del derecho a la protección de datos y se suman a las garantías constitucionales generales de los derechos constitucionales.

5. La ley actual de protección de datos en Alemania es de 2001, en concordancia con la Directiva 95/46, aunque fue alterada en 2009 para mantenerla actualizada de las nuevas amenazas surgidas a lo largo de la década para el individuo. La denominada BDSG tiene aplicación general, aunque subsidiaria a legislaciones específicas, y pretende proteger a la persona en cuanto a sus datos que puedan ser recogidos o tratados en bases de datos públicos y privados, inclusive en un medio móvil, automatizados o no, exceptuándose las de ámbito personal o familiar. Nótese que la BDSG sólo se aplica a órganos públicos federales, quedando los órganos de los estados federados bajo la regulación de cada *Land*.
6. El concepto de dato personal en Alemania involucra escritos, y también imágenes y grabaciones, que sean archivadas y estén relacionadas a un ser humano identificado. Al contrario, datos bajo pseudónimo o anónimos no involucran afectación al derecho individual.
7. La no extensión del derecho a la protección de datos a las personas jurídicas puede ser considerada una continuación de la no aplicación del concepto de dignidad constitucional a ellas. Sin embargo, datos de empresas pueden ser protegidos caso se refieran a sus socios o se trate de una firma individual.
8. En la protección de datos, la recolección debe incidir sobre el mínimo indispensable (principio de la *necesidad*) y se somete al *consentimiento*, en general por escrito, personalísimo y revocable "ex nunc" del afectado, lo cual debe ser de forma transparente informando los destinatarios y usos. Aun

así, hay *preguntas*, como, las pertinentes acerca de datos sensibles en las entrevistas de empleo, y *finalidades*, o como el uso meramente comercial, que son en general consideradas prohibidas.

9. Las reglas de consentimiento son reveladas en la hipótesis de investigaciones científicas y son reforzadas en el caso de los "datos sensibles" (origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, historial sindical, de salud y sexual). Se admite en general la excepción al consentimiento en pro de otros intereses prioritarios.
10. La recolección debe darse directamente sobre el afectado (*lealtad*), salvo si una ley específica prevé en sentido contrario o si no es compatible con la finalidad o si exige esfuerzo desproporcional, ponderados los intereses involucrados. Cuando sea la Administración la encargada de no recoger directamente, deberá justificar por medio de un acto administrativo.
11. Hay *inmunidades* para los afectados en el uso de sus informaciones recogidas. En consecuencia, los empleados de las bases de datos deben trabajar con las informaciones de los individuos de manera que preserve su *confidencialidad*; ellas están *vedadas para* servir como *decisiones* (negativas) *exclusivamente automatizadas*, sin intervención activa humana; deben ser manejadas en una estructura y maquinaria con *seguridad*. La preocupación con la seguridad de los datos aun se refleja en una regulación propia de su transferencia automatizada y del *outsourcing*.
12. Cuanto a los derechos, tiene el afectado, en primer lugar, un *derecho de acceso* al contenido de las informaciones archivadas que le refieran, por medio de nombre o sobrenombre conocido e inclusive en conjunto con otros medios, como muestras de ADN de ascendentes. El derecho de acceso

incluye también saber la finalidad del registro, la fuente que suministró la información, los eventuales destinatarios siguientes de la información y hasta, en pro de la transparencia, la lógica de construcción de la base de datos. El que peticiona y el que responde deben ser plenamente identificados.

13. Hay un requisito adicional en el acceso que involucra como fuente o destinatario órgano de protección de la Constitución o defensa del Estado, que es la anuencia de este. Además, en bases públicas o privadas puede haber veda del derecho de acceso cuando ello inviabilice el objetivo de la base de datos, afecte gravemente el orden público o perjudique el interés de terceros. El agente público (y privado) *deberá* en estos casos, si es posible, justificar su recusación y cabe pedido de revisión del acto a la Autoridad de Control.
14. El derecho de acceso a la base de datos privados se expandió con la reforma de la BDSG de 2009, para asegurar la máxima transparencia al individuo. Aun así, el titular privado de base de datos *puede* dejar de informar cuando afecte su secreto comercial o el dato proceda de fuentes accesibles al público y el esfuerzo de divulgación sea desproporcional, siempre de manera motivada.
15. La *notificación* al afectado cuando no haya recolección directa u ocurra una transferencia está también inspirada por el "principio de la transparencia", en este caso por exigencia del artículo 11 de la Directiva europea. La dispensa de la notificación ocurre cuando no hay el derecho de acceso, cuando existe otro modo para el conocimiento del afectado, cuando ocurre en razón de la ley y por la desproporcionalidad (limitada a ciertos casos en bases de datos

privados y amplios en los públicos). De todos modos, hay en general una justificación obligatoria de las condiciones que llevaron a la dispensa *por escrito*.

16. La existencia de los *derechos de rectificación, supresión y bloqueo* son el resultado lógico de un derecho de acceso que pretende la protección del individuo. Por ello, es que son legalmente de rara denegación y no impiden la defensa por medio de las medidas civiles de garantía a los derechos de la personalidad. La *rectificación* envuelve la corrección de cualquier dato que no corresponda a la realidad factual ocurrida; la *supresión* se refiere al deber de eliminar datos de almacenamiento o tratamiento contrarios a la ley, inclusive al superar las finalidades de la recolección; mientras que el *bloqueo* funciona cuando desea el ordenamiento que no se haga más el uso por aquel poseedor del dato, pero, al mismo tiempo, no se recomienda la supresión, con la finalidad de mantener la posibilidad de uso por otros en el futuro.
17. El *derecho de oposición* es nuevamente una creación originaria de la Directiva europea (artículo 14) y permite el intento por el afectado de impedir la recolección, uso o tratamiento por la invocación de una ponderación de los intereses involucrados, en situaciones sin otra exigencia legal.
18. El *derecho de indemnización* de los afectados por el manejo vedado o irregular de sus datos en el derecho alemán es pasible de críticas, pues sujeta a fuertes restricciones, no existiendo el daño inmaterial en las bases de datos privados y sujeto a un techo en el quantum en las bases de órganos públicos.
19. Existe también en la BDSG alemana la presencia de reglas que exclusivamente limitan el derecho en pro de la actuación de la

Administración Pública Federal, en todas las etapas de manejo de los datos: recolección, tratamiento conforme la finalidad y transferencias.

20. La recolección sin consentimiento puede ser justificado por el desempeño de las funciones legales, pero solamente en la medida de lo esencial e indispensable para alguna tarea específica. Hay una constante preocupación en la doctrina y jurisprudencia con esos criterios para la verificación de la legitimidad de la conducta administrativa y de la proporcionalidad en esas normas de limitación de derecho fundamental.
21. En especial, en cuanto a la recolección de los "datos sensibles" la BDSG, al principio, autoriza la falta de consentimiento del afectado cuando se da por la previsión en otra ley, por la protección del bien común o de un importante interés público, en lo que se destaca la seguridad pública, la prevención y tratamiento de enfermedades, la investigación científica, obligaciones nacionales e internacionales y objetivos humanitarios, o cuando se proteja el interés del afectado que no esté en condiciones de consentir o ya haya tornado los datos públicos. La mayoría de estas hipótesis sirve también para legitimar igualmente el cambio de la finalidad del tratamiento de "datos sensibles" por parte de la Administración, así como, transferencias entre los entes públicos y privados. Además, cambio de finalidad y transferencia de datos "no sensibles" exigen, sin el consentimiento del afectado, que se busque la protección de sus intereses, intereses superiores de terceros o la defensa del bien común.
22. La principal instancia de control de la protección de datos en Alemania es el Comisario Federal para la protección de datos, autoridad indicada por el gobierno y aprobada por mayoría de votos en el Parlamento para un mandato

de 5 años renovables por un igual período. Sus funciones involucran la prevención y la represión de violaciones por órganos públicos a la legislación de protección de datos y, adicionalmente, la emisión de recomendaciones y pareceres a la Administración Federal y al Parlamento relativos a la condición general de protección de datos en Alemania, o sea, incluyendo también el análisis de los entes privados. Por otro lado, la fiscalización de los entes privados queda a cargo de las "Autoridades de Supervisión", indicadas por los Estados miembro.

23. El Comisario Federal de Protección de Datos y las "Autoridades de Supervisión" de los estados federados también archivarán los registros de casi todos los procesos de tratamiento automatizado de datos de sus entes fiscalizados para el archivamiento y esclarecerán dudas en las situaciones en que se exige un *pre control* por parte de los "encargados internos de protección de datos", los cuales son los encargados de garantizar el *autocontrol* en las instituciones que posean bases de datos.
24. La ley general de protección de datos en España es la LO 15/99. A pesar, de la aplicación subsidiaria con relación a leyes que traten sobre protección de datos en materias específicas, tal cual la ley alemana, hay algunas relevantes bases de datos que salen completamente de su regulación, como cuando se refieren a "materias clasificadas", terrorismo y delincuencias de mayor gravedad y aquellas formadas con las imágenes captadas por las cámaras de vídeo de órganos de seguridad del Estado.
25. El derecho a la protección de datos en España es otorgado a personas naturales con relación a cualquier información suya, inclusive profesionales. Se aplica a toda situación que esas sean identificables, o sea, combinables

con el ser humano sin grandes esfuerzos y que se destinen a la colocación en una base de datos. Las disposiciones de la LOPD afectan tanto titulares de esas bases de datos como los responsables por el tratamiento.

26. El consentimiento en la protección de datos, como regla general del derecho en España, debe ser dado por el afectado que esté *informado*, de forma *específica y* con carácter *inequívoco*. Sin embargo, no se exige cuando la información es recogida de "fuentes accesibles al público".
27. Hay, siguiendo el modelo legislativo del Convenio de 1981 y de la Directiva 95/46, una serie de *principios* a ser seguidos, empezando por la c*alidad* en el registro, lo que significa que debe haber *exactitud* en su contenido y *pertinencia, adecuación y no exceso* con su correspondiente *finalidad*. Sin embargo, hay aceptación de que el requisito de la finalidad no impide el uso de los datos para proteger el bien de los ciudadanos o la confianza de clientes. Por la desvinculación directa con el individuo, se acepta también el uso para fines históricos, estadísticos o científicos.
28. Otro principio es el de una *información* previa a la recolección directa y posterior a la indirecta, así como, en las cesiones de datos a terceros, garantizando completa *transparencia* para ser legal la operación. El destinatario de los datos debe comunicar de manera *expresa*, *precisa* e *inequívoca* el modo de uso e identidad de quien usará los datos, los derechos de los afectados y las consecuencias de su recusación. Ese deber de información sólo se ve alejado en la cesión por ley especial, para fines históricos, estadísticos y científicos o cuando exige esfuerzo desproporcionado, a ser evaluado en procedimiento por la Agencia Española de Protección de Datos, y es reducido en la recolección para fines

comerciales en fuentes accesibles al público.

29. El principio de un *consentimiento* que sea *inequívoco* no impone forma en la manifestación de voluntad, pero exige que ella se infiera claramente de actos del afectado, salvo una hipótesis en que la legislación española da significado al silencio del individuo. El consentimiento otorgado es a cualquier tiempo revocable. Sólo se dispensa el consentimiento si es necesario al cumplimiento de otras relaciones jurídicas del afectado, para proteger su "interés vital", cuando hay interés legítimo de quien recoge y si usan "fuentes accesibles al público" y para el ejercicio de funciones propias de la Administración, a ser verificadas conforme las finalidades del fichero de datos.
30. La finalidad de la base de datos receptora y el consentimiento del afectado funcionan de forma similar como requisitos en la cesión de datos. Hay una dispensa de esto, en caso haya una ley autorizante (como con relación a la CNVM y su poder de requisición), si provienen de "fuentes accesibles al público", si inherente a otra relación jurídica, si ocurrieron en dirección al Defensor del Pueblo, Ministerio Público, Poder Judicial o entre órganos análogos o que tengan por objeto mismas materias, entre Administraciones para fines históricos, estadísticos y científicos o cuando una produzca a la otra y para necesidades de salud o estudios impuestos por las normas sanitarias.
31. La mayor protección a los "datos sensibles" encuentra diferentes grados en la LOPD, conforme la especie. En las elecciones de religión, ideología, creencias y de la afiliación sindical se incrementa el consentimiento exigido para "expresado y por escrito", salvo si están dirigidos a personas jurídicas

cuyos propios fines tengan ese contenido. Ya para los datos de origen racial, salud y vida sexual es suficiente el consentimiento expresado, incluso si no es por escrito. Son vedadas las bases de datos que sólo retengan esas especies de datos, sin que ello perjudique archivos para tratamientos médicos. Datos relativos a condenas administrativas y penales también son más protegidos, al sólo poder tener fichero creado por ley.

32. Hay también una extensa regulación infra-legal y legal del "principio de la seguridad" para la prevención de los riesgos provenientes del manejo de los datos. Hay niveles de gravedades, conforme el objeto de la base de datos, que conforman series de medidas a ser tomadas y un deber de secreto amplio a los involucrados.
33. Las facultades previstas en la ley española para el ejercicio del derecho a la protección de datos tiene carácter personalísimo, quedando la protección de fallecidos garantizada solamente por la tutela de la intimidad.
34. La primera facultad que se establece en la ley general española es la de *oposición* por razones personales legítimas a tratamientos que, de otra forma, son permitidos sin su consentimiento. En la secuencia hay una v*eda de tratamientos automatizados,* en verdad constituyendo una inmunidad a que ocurran decisiones meramente computarizadas sin que el afectado pueda exponer y haber evaluado sus razones por otro ser humano.
35. El denominado *derecho de consulta* permite que todos conozcan gratuitamente los registros de tratamientos de datos que hayan sido realizados en la Agencia Española de Protección de Datos, hoy a través de Internet. Esta facultad auxilia la factibilidad de las demás, que son el *acceso* a todo lo que consta en su "carpeta" personal en cualquier base de datos, y la

consecuente *rectificación* o *cancelación*, cuando los datos, respectivamente, sean inexactos o no haya permisión para su archivamiento/tratamiento. La cancelación puede ser precedida del *bloqueo* de la utilización provisoria mientras son investigadas las responsabilidades.

36. La Administración Pública española, como regla general, es obligada en todos sus ramos a respetar la protección de datos individual en su actuación. Bases de datos de "naturaleza pública" deben ser creadas por acto publicado en periódico oficial correspondiente, sin que ello dispense el registro en la Agencia española.
37. En la cesión de datos entre administraciones se dispensa el consentimiento del afectado cuando está prevista esta posibilidad en otra ley española o comunitaria, entre órganos que posean mismas competencias o materias, con fines históricos, estadísticos y científicos o cuando la información conseguida en la realidad se destine a otra. Excepcionalmente la Administración Tributaria posee un rol cerrado de entes que le deben prestar informaciones.
38. Los archivos para fines policiales dependen de una investigación concreta y aun en abierto para que, motivadamente y cuando sea necesario, sea admitida la recolección y tratamiento de datos sin consentimiento del afectado.
39. Tras la labor del Tribunal Constitucional español en la STC 292/2000 solamente se admiten limitaciones por la Administración de las facultades de acceso, rectificación y cancelación del derecho fundamental a la protección de datos en las restricciones no excesivas que fueron adecuadamente vehiculadas por ley emitida por el parlamento y que protejan bienes

constitucionales. Así que esta STCconcluye por la constitucionalidad de la LOPD cuando *en pro de la defensa del Estado, preservación de la seguridad pública e investigación penal y en la actuación administrativa con relación a tributos*.

40. El principal órgano de protección de datos en España es la Agencia Española de Protección de Datos. Ella es independiente dentro del marco legal, al elaborar su propuesta presupuestaria y poseer un Director con mandato fijo. En su objetivo de hacer cumplir la ley de protección de datos, tiene poder normativo de expedir instrucciones, verificar y eventualmente sancionar las conductas de las bases de datos, recibir el registro de los ficheros existentes y producir una memoria de la situación general cada año. Además, cuando los derechos del individuo fueran incumplidos tras la petición al responsable de la base de datos, admiten reclamo ante la Agencia de Protección de Datos española y, frente a esta, recurso judicial.
41. En Brasil, hace cerca de 20 años, empezó una doctrina de mayor atención a la afectación del ser humano por las nuevas tecnologías. Sin embargo, al contrario de una ley general de protección de datos, lo que se ve son destaques de áreas humanas donde hay *secreto* y así se excluyen de las miradas y usos de los demás. En estas protecciones diferenciadas de la *intimidad*, a su vez, está el lado de la casi mera veda de divulgación, como en el secreto médico, de abogados y procesales, otros más pormenorizados, como el secreto bancario, fiscal y, en menor grado, de los datos/registros telefónicos. Siempre, sin embargo, es admitida la limitación del derecho por la evaluación del poder judicial de que hay otro interés superior.
42. Siendo el secreto de datos protegido por la intimidad, podemos inferir

inicialmente que, conforme afirma el STJ, no afectan los “datos de registro”, pues suministrables usualmente, sin el carácter de privado y que, conforme la doctrina y jurisprudencia del STF, involucra primordialmente a personas físicas, siendo las jurídicas protegidas en razón de los efectos que la divulgación pueda traer a sus socios y empleados.

43. El secreto bancario ya existe en Brasil desde el siglo XIX, aunque la conformación actual data de 2001, por la LC n. 105. La obligación de no divulgar los datos que tenga conocimiento de las instituciones financieras, sin embargo, legislativamente, admite el alejamiento en pro de la preservación del sistema crediticio, de la realización del poder de policía de los órganos de fiscalización y en la comunicación de indicios de ilícitos administrativos y penales. No obstante estas hipótesis no tengan grandes resistencias judiciales, los artículos 5º y 6º de la LC 105 sufren bastante impugnación de constitucionalidad en la doctrina y en la jurisprudencia, frente a una cierta parcialidad del Fisco caso acceda directamente a extractos bancarios que sólo sería remediada por la necesidad siempre de autorización judicial. El STJ “uniformizó” en el final de 2009 el entendimiento que la norma era constitucional a simplemente garantizar al Estado medios para recaudar los tributos, pero el STF, en 2010, optó, en caso individual, por la obligatoriedad de una intervención del Judicial en estos casos.

44. El secreto fiscal, que tiene la peculiaridad de formarse a través de poderes administrativos que usualmente limitan otros secretos para constituir el *quantum* tributario, encuentra límites legales en el pedido de autoridades judiciales y administrativas que tengan procesos a resolver que necesiten estos datos, en la comunicación de “crímenes contra el orden tributario” para

el Ministerio Público y en la divulgación de listas de deudores tributarios. Existe también la posibilidad de intercambio de datos entre Administraciones Tributarias internas e internacionales.

45. La protección de datos por la intimidad en general combinada con poca densidad normativa encuentra una buena ejemplificación de su funcionamiento en la cuestión de los datos en pose de concesionarias de servicios de telefonía. Por un lado, hay expresa afirmación de que los datos calificativos y direcciones de los servicios de telefonía *fija* son públicos, siendo la manifestación de voluntad necesaria para no divulgarlos. Aunque en la telefonía *móvil* la ley no tenga disposición parecida, la agencia reguladora brasileña, por analogía a la ley de registros públicos, termina aplicando también la ausencia de secreto en esas informaciones, reservando la privacidad solamente a los registros telefónicos, aunque el artículo 3º, IX y artículo 72 de la LGTel no hagan precisamente esa distinción. Existe también, coherentemente, la autorización del uso estadístico con anonimato. Sin embargo, la laguna a cualquier límite del objeto protegido impuso a la agencia que produjera un *reglamento* para preservar sus poderes de fiscalización.

46. La posición del STF en cuanto a la fuerza de normas constitucionales que otorgaban un límite general al secreto de datos a las Comisiones Parlamentarias de Averiguación y para el Ministerio Público es absolutamente inversa de un caso al otro. Mientras los "poderes propios de autoridades judiciales" otorgados a los primeros no cobran autorización judicial en ningún caso de secreto de datos el "poder de requerimiento" constitucional de la Fiscalía sólo envuelve informaciones no protegidas por

secreto, siendo en estas esencial el orden judicial, en función de la parcialidad del órgano en su decisión de recolección.

47. Las facultades positivas para la protección de datos en Brasil de bases de datos públicas se encuentran primordialmente en la Ley 9507, que regula el *habeas data*. En esta se agrega al a*cceso* y *rectificación* constitucionales la posibilidad de *anotación* esclarecedora, pero no de *supresión* de datos. La ley es aplicable a registros automatizados o no y permite que sea titular persona física o jurídica. Jurisprudencialmente se entiende que el acceso puede ser restringido en pro de la seguridad del Estado. La acción judicial del *habeas data* debe ser obligatoriamente precedida de pedido junto al responsable por la base de datos.

48. Hay una presencia creciente de más características propias de la regulación europea, como la idea de *transparencia* y *temporalidad* de los registros y de sumisión de la recolección a la *información* y al *consentimiento*, en legislaciones más recientes, como la Ley 8.078 y la Ley 12.414. Pero ellas no afectan la actuación administrativa, teniendo un carácter eminentemente de regulación de los ficheros vinculados al sistema crediticio en el país, tanto por la intención del legislador, como por la ausencia de una obligación de registro de las bases de datos para *consulta* general, lo que termina en la práctica alertando al individuo acerca de la existencia de su registro solamente cuando se ve impedido de adquirir un bien del mercado por la no fruición de crédito.

CONCLUSIÓN

Hay cambios tecnológicos, en informática y telecomunicaciones que proponen desafíos comunes a los Estados nacionales en el sentido de utilizarlos en pro del bienestar de sus sociedades sin que ello signifique el debilitamiento de la dignidad de sus ciudadanos, en especial a través de su *catalogación* comprensiva por medio de sus informaciones conocidas y archivadas en ordenadores. En ese sentido, los Tribunales Constitucionales de Alemania y España, en diferentes momentos, reconocieron la existencia de una nueva posición *jus- fundamental* que justificaría derechos individuales que irían más allá del momento de la recolección de las informaciones de cada persona, incluyendo un control continuo en cuanto al contenido y uso finalísimo de lo archivado.

Por otro lado, el Supremo Tribunal Federal brasileño tiene jurisprudencia fundada básicamente en la idea de veda de acceso a determinados datos personales, en función de su carácter *íntimo*. La posibilidad de control de la *corrección de la* información, posible por la existencia del *habeas data* constitucional se ve en la práctica limitada a un uso que fue concentrado en el momento de la redemocratización brasileña a fines de la década del 80.

Hay, sin embargo, iniciativas internacionales, generadas a partir del continente europeo, que sirven para la consolidación de un marco aceptado como necesario para la protección del individuo. En esas proposiciones que facilitan la formación de una

uniformización, se destaca, en la directiva 95/46/CE, la veda de la transferencia de datos de los países componentes de la Unión Europea a otros que no provean al menos una "protección adecuada" a los datos personales en sus ordenamientos internos. El concepto de "protección adecuada" tiene la calidad de proveer los parámetros de principios y derechos apremiantes, sin que ello desprecie las peculiaridades de cada sociedad. En ese sentido, las legislaciones de Alemania y España señalan que incluso países de protección *equivalente* pueden, dentro de los mismos principios, mantener límites que preservan distintos intereses más relevantes en casos concretos.

La legislación brasileña, al contrario, termina valorando, tal cual la jurisprudencia constitucional en las normas que afectan la Administración Pública, una mera existencia evidenciada de *sigilo* en algunas especies de datos, como los bancarios, fiscales y registros telefónicos, e inherentes a algunas actividades profesionales, como la medicina y la abogacía, dejando una amplia zona legislativamente sin defensa. No hay, por tanto, una presencia exacta de una categoría de "datos sensibles" como en la legislación europea e internacional.

Aunque en esas categorías especialmente protegidas de datos se aplique, por consecuencia, la regla del uso *consentido* y de la *confidencialidad*, no se destacan expresamente ni siquiera otros principios necesarios a la protección adecuada, como la *información* previa, la *veda del tratamiento automatizado* y la imposición clara de *no exceso* en la recolección y uso. Añádase, que la jurisprudencia no estimula la labor legislativa en la fijación de límites en la protección de datos personales, pues pocos existentes para la Administración tienden a ser alejados en favor de la concentración de análisis previo judicial en los casos concretos.

La legislación del *habeas data,* aunque no prevea la *oposición* y *cancelación* al registro, repite la Constitución en el *acceso* y eventual *rectificación* del dato erróneo, y añade la *anotación* entre las facultades personales. Además, la legislación de consumo, marcadamente en el mercado relativo al crédito, viene adoptando parámetros progresivamente más parecidos con los que constan en la directiva europea. Esas normas, con características más enfocadas en el control de los datos y no a su mera utilización, indican el camino de producción legislativa que debe ser recorrido en Brasil para alcanzar una "protección adecuada de los datos", pero también que la efectividad de los derechos pasa, en la realidad de la sociedad brasileña, por la existencia de un órgano regulador de la protección de datos y, principalmente, por la presencia de un registro general que permita la *consulta* por cada uno, sin lo cual, los derechos terminan sólo ejercidos en cuanto a sus violaciones más gravosas y evidentes.

BIBLIOGRAFIA

AHUMADA RUIZ, Marían. *La jurisdicción constitucional en Europa: bases teóricas y políticas*. Cizur Menor (Navarra): Thomson-Aranzadi, 2005.

AKANDJI-KOMBE, Jean-François. *Positive obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention on Human Rights*. Human rights handbooks No. 7. Strasbourg: Council of Europe, 2007.

ALEXANDRINO, Marcelo e PAULO, Vicente. *Direito tributário na Constituição e no STF: teoria e jurisprudência*. Niteroi, RJ: Impetus, 2004.

ALEXY, Robert. *Constitucionalismo discursivo*. Traducido por Luís Afonso Heck. Porto Alegre: Livr. do Advogado, 2008.

____ *Teoría de los derechos fundamentales*. Madrid: Centro de Estudios Constitucionales, 1993.

ALVAREZ CONDE, Enrique, y TUR AUSINA, Rosario. “Los derechos en el constitucionalismo: tipología y tutela "multilevel".” *Teoría y realidad constitucional*, 2007.

ÁLVAREZ-CIENFUEGOS SUÁREZ, José María. *La defensa de la intimidad de los ciudadanos y la tecnología informática* . Pamplona: Aranzadi, 1999.

ÁLVAREZ-OSSORIO MICHEO, Fernando. “Los Derechos Fundamentales”. In *Hacia la europeización de la Constitución española : la adaptación de la Constitución española al marco constitucional de la Unión Europea*. Bilbao: Fundación BBVA, 2006

APARICIO SALOM, Javier . *Estudios sobre la ley orgánica de protección de datos de carácter personal*. Cizur Menor (Navarra) : Aranzadi, D.L., 2002

ARENAS RAMIRO, Mónica. *El derecho fundamental a la protección de datos personales en Europa*. Valencia: Agencia Española de Protección de Datos, 2006

ARENDT, Hannah. *A condição humana*. Rio de Janeiro: Forense Universitária, 2007

ARIÈS, Philippe. *História social da criança e da família*. Traducido por Dora Flaksman. Rio de Janeiro: Zahar, 1981

BALKIN, Jack. “The First Amendment is an Information Policy.” In *The 20th Annual Hugo L. Black Lecture on Freedom of Expression*. Wesleyan University, 2011.

BARNES, Javier. “Sobre el derecho administrativo de la información”. *Revista catalana de derecho público*, 2007.

BARNES VÁZQUEZ, Javier. “Sobre el procedimiento administrativo: evolución y perspectivas.” In *Innovación y reforma en el derecho administrativo.* Sevilla: Derecho Global, 2006.

____. “Una reflexión introductoria sobre el Derecho Administrativo y la Administración Pública de la Sociedad de la Información y del Conocimiento.” *Administración de Andalucía: revista andaluza de administración pública*, 2000.

BARROS, Marcos Antonio de. “Sigilo professional. Reflexos da violação no âmbito das provas ilícitas.” Justitia, Septiembre 1996.

BARROSO, Luís Roberto. “A Viagem Redonda: habeas data, direitos constitucionais e as provas ilícitas.” In *Habeas Data*. São Paulo: RT, 1998.

BATISTA DE ALMEIDA, João. *Manual de Derecho do Consumidor*. São Paulo: Saraiva, 2003

BECKHUSEN, Michael. “Das Scoring-Verfahren der SCHUFA im Wirkungsbereich des Datenschutzrechts”. *BKR*, 2005

BELLEIL, Arnaud . *@-privacidade: o mercado de dados pessoais: protecção da vida privada na idade da internet*.Lisboa: Instituto Piaget, 2001.

BENDA, Ernst. “Dignidad Humana y Derechos de la Personalidad”. In *Manual de derecho constitucional*. Madrid [etc.]: Marcial Pons, 2001.

____. “Privatsphäre und ‘Persönlichkeitsprofil’”. In *Menschenwürde und freiheitliche Rechtsordnung : Festschrift fur Willi Geiger zum. 65. Geburtstag*, organizado por Gerhard Leibholz et al. Tübingen: Mohr, 1974

BERCIC, Bostjan, y GEORGE, Carlisle. “Identifying Personal Data Using Relational Database Design Principles.” *International Journal of Law and Information Technology*, 2009,

BERGMANN, Lutz, MÖHRLE, Roland, y HERB, Armin. *Datenschutzrecht: Handkommentar zum Bundesdatenschutzgesetz, Datenschutzgesetze der Länder und Kirchen, Bereichsspezifischer Datenschutz.* Stuttgart: Boorberg, 2007.

BERNAL PULIDO, Carlos. “La metafísica de los derechos humanos.” *Revista Derecho del Estado*, diciembre de 2010.

____. *El principio de proporcionalidad y los derechos fundamentales: el principio de proporcionalidad como criterio para determinar el contenido de los derechos fundamentales vinculante para el legislador*. Madrid: Centro de Estudios Políticos y Constitucionales, 2003.

BETHGE, Herbert, WEBER-DÜRLER, Béatrice, SCHOCH, Friedrich K., y TRUTE, Hans-Heinrich. *Der Grundrechtseingriff*. Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 57. Berlin ; New York: de Gruyter, 1998.

BLANKE, Jordan M.. “‘Safe Harbor’ and the European Union’s Directive on Data Protection”. *Albany Law Journal of Science & Technology*, 2000

BLASI CASAGRAN, Cristina. “La protección de los derechos Fundamentales en el Tratado de Lisboa”. *Quaderns de treball*, outubro 2010.

BOBBIO, Norberto. *O futuro da democracia*. São Paulo: Paz e Terra, 2004.

BÖCKENFÖRDE, Ernst-Wolfgang. "Teoría e interpretación de los derechos fundamentales." In *Escritos sobre derechos fundamentales*, traducido por Ignacio Villaverde Menéndez y Juan Luis Requejo Pagés. Baden-Baden: Nomos-Verlagsgesellschaft, 1993.

BOGDANDY, Armin von. *Hacia un nuevo derecho público. Estudios de Derecho Público Comparado, Supranacional e Internacional.* México, D. F.: Universidad Nacional Autónoma de México, 2011.

BOROWSKI, Martin. *La estructura de los derechos fundamentales*. Bogotá: Univ. Externado de Colombia, 2003.

BRAGE CAMAZANO, Joaquín. *Los límites a los derechos fundamentales*. Madrid: Dykinson, 2004

BREMS, Eva. "The Margin of Appreciation Doctrine in the Case-Law of the European Court of Human Rights." *Heidelberg Journal of International Law (HJIL)*, 1996

BRITO MACHADO, Hugo de. *Curso de direito tributário*. São Paulo: Malheiros, 2004

BRUGGER, Winfried. "Menschenrechte im modernen Staat." AöR, 1989

BUISÁN GARCÍA, Nieves et al. *La Ley de protección de datos : análisis y comentario de su jurisprudencia*. Organizado por Carlos Lesmes Serrano. Valladolid: Lex Nova, 2008.

CALMON NAVARRO COÊLHO, Sacha. *Curso de direito tributário brasileiro*. Rio de Janeiro: Forense, 2004.

CANÇADO TRINDADE, Antônio A.. *El Derecho Internacional de los Derechos Humanos en el siglo XXI*. Organizado por Máximo Pacheco Gómez. Santiago de Chile: Editorial Jurídica de Chile, 2001.

CARRAZZA , Roque Antonio. *Curso de Direito Constitucional Tributário*. São Paulo: Malheiros, 2000.

CASTELLS ARTECHE, José Manuel. La limitación informática. In: *Estudios sobre la Constitución Española (Homenaje al Profesor Eduardo Garcia de Enterria): Tomo II ("De los derechos y deberes fundamentales").* Editora Civitas: Madrid, 1991.

CASTELLS, Manuel. *A Sociedade Em Rede :* a era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 2007.

____. *La era de la información: economía, sociedad y cultura*. Vol. II. Barcelona: Aliança Editorial, 1997.

CERVANTES SAAVEDRA Miguel de. *O engenhoso cavaleiro D. Quixote da Mancha : segundo libro*. Traducido por Viscondes de Castilho e de Azevedo. Vol. 2. Rio de Janeiro: R.B.A. Editores, 1994

COHEN, Julie E.. "Examined Lives: Informational Privacy and the Subject as Object." Stan. L. Rev., 1999

CONDE ORTIZ, Concepción. *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*. Madrid: Dykinson, 2005.

CRETELLA JÚNIOR, José. *Os "Writs" en la Constitución de 1988 : Mandato de Segurança, mandato de segurança colectivo, mandato de injunção, habeas data, habeas corpus, ação popular*. Rio de Janeiro: Forense Universitária, 1996,

CRUZ VILLALÓN, Pedro. "Derechos Fundamentales y Legislación." In *La curiosidad del jurista persa, y otros estudios sobre la Constitución*. Madrid: Centro de Estudios Políticos y Constitucionales, 2006.

____. "El Ordenamiento Constitucional: una indagación empírica". In *La curiosidad del jurista persa, y otros estudios sobre la Constitución*. Madrid: Centro de Estudios Políticos y Constitucionales, 2006.

____. "Formación y evolución de los derechos fundamentales." *Revista española de derecho constitucional*, 1989.

____. *La constitución inédita*. Madrid: Editorial Trotta, D. l., 2004.

DÄUBLER, Wolfgang et al. *Bundesdatenschutzgesetz*. Frankfurt am Main: Bund-Verl., 2007.

DÄUBLER, Wolfgang. *Gläserne Belegschaften? : Datenschutz für Arbeiter, Angestellte und Beamte*. Köln: Bund-Verl., 1987.

DELGADO, José Augusto. "Os sigilos bancário e fiscal no ordenamento jurídico brasileiro". *Interesse Público*, setembro 2002.

DENNINGER, Erhard. "El derecho a la autodeterminación informativa." In *Problemas actuales de la documentación y la informática jurídica : actas del Coloquio*

Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986. Madrid: Tecnos, 1987.

____. "Staaliche Hilfe zur Grundrechtausübung." In Handbuch des Staatsrecht der Bundesrepublik - Bd.V : Allgemeine Grundrechtslehren, organizado por Josef Isensee e Paul Kirchhof. Heidelberg: Müller Juristischer Verlag, 1992.

DERZI, Misabel de Abreu Machado. "O sigilo bancário, a Lei 9.613/98 e a intributabilidade do ilícito." *Repertório IOB de jurisprudência: civil processual penal e comercial*, Julho 1998,

DI FABIO, Udo. "Rn 173. Das Recht auf informationelle Selbstbestimmung als Ausprägung des Selbstdarstellungsschutzes, insbesondere gegenüber modernen Gefährdungsformen." In *Maunz/Dürig, Grundgesetz*. München: Beck, 2010

____. "Rn 174. Verselbstständigung gegenüber dem Privatsphärenschutz." In *Maunz/Dürig, Grundgesetz*. München: Beck, 2010.

FERRAZ JUNIOR, Tercio Sampaio. "Sigilo de dados: o direito à privacidade e os limites à función fiscalizadora do Estado." In *Sigilo Fiscal e Bancário [Reinaldo Pizolio, Jayr Viégas Gavaldão Jr., coordenadores]*. São Paulo: Quartier Latin, 2005

FERREIRA MENDES, Gilmar, MARTIRES COELHO, Inocêncio, y GONET BRANCO, Paulo Gustavo. *Curso de direito constitucional*. São Paulo, Brasília: Saraiva, 2008.

FIORAVANTI, Maurizio. *Los derechos fundamentales: Apuntes de historia de las constituciones*. Trotta, 2009.

FOUCAULT, Michel. *Vigiar e Punir : Historia Da Violência Nas Prisões.* Petrópolis: Vozes, 2004.

FRANKENBERG, Günter. "Constitutional transfer: The IKEA theory revisited". *Int J Constitutional Law*, 2011.

FROOMKIN, A. Michael. "The Death of Privacy?." *Stan. L. Rev.*, 1999.

FROSINI, Vittorio. "Bancos de datos y tutela de la persona". *Revista de Estúdios Políticos,* noviembre 1982.

____. "Problemas Jurídicos de la información y la documentación." In *Problemas actuales de la documentación y la informática jurídica: actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986*. Madrid: Tecnos, 1987.

GARCÍA-BERRIO HERNÁNDEZ, Teresa. *Informática y libertades : la protección de datos personales y su regulación en Francia y España*. Murcia: Servicio de Publicaciones de la Universidad de Murcia, 2003.

GAVARA DE CARA, Juan Carlos. *Derechos fundamentales y desarrollo legislativo: la garantía del contenido esencial de los derechos fundamentales en la Ley fundamental de Bonn*. Madrid: Centro de Estudios Constitucionales, 1994.

GOLA, Peter. "Die Entwicklung des Datenschutzrechts in den Jahren 2008/2009". *NJW*, 2009.

GOLA, Peter, y SCHOMERUS, Rudolf. *Bundesdatenschutzgesetz*. München: Beck, 2005.

GOMES CANOTILHO, José Joaquim. *Derecho Constitucional e Teoria Da Constituiçao*. Coimbra: Almedina, 1993.

GONÇALVES FERREIRA FILHO, Manoel. *Curso de Direito Constitucional*. São Paulo: Saraiva, 2005.

GREENLEAF, Graham. "Global data privacy laws: Forty years of acceleration". *Privacy Laws and Business Special Report*, September 2011.

GRIMMELMANN, James. "Saving Facebook". *Iowa Law Review*, 2009.

GROSS, Gerhard. "Das Recht auf informationelle Selbstbestimmung - mit Blick auf die Volkszählung 1987, das neue Bundesstatistikgesetz und die Amtshilfe." *AöR*, 1988

GUASTINI, Riccardo. "Problemas de Interpretación." *Isonomía. REVISTA de Teoría y Filosofía del Derecho*, Octubre 1997

____. *Estudios sobre la interpretación jurídica*. México, D.F.: Universid Nacional Autónoma de México, 1999.

HÄBERLE, Peter. "El Tratado de Reforma de Lisboa de 2007." *Revista de Derecho Constitucional Europeo 9*, Junio 2008.

____. "Grundrechte und parlamentarische Gesetzgebung im Verfassungsstaat " *AöR*, 1989.

____. *El Estado Constitucional*. México, D. F.: Universidad Nacional Autónoma de México, 2003.

____. *Estado constitucional cooperativo.* Rio de Janeiro: Renovar, 2007.

HABERMAS, Jürgen . *Verdade e justificação : ensaios filosóficos*. São Paulo: Loyola, 2004.

____. *A inclusão do outro: estudos de teoria política.* São Paulo: Loyola, 2002.

____. *Direito e democrácia: entre facticidade e validade*. Rio de Janeiro: Tempo Brasileiro, 1997.

____. *The divided West*. Cambridge; Malden: Polity, 2006.

HEREDERO HIGUERAS, Manuel. "La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del censo de población." *Documentación administrativa*, 1983.

HERMAN DE VASCONCELLOS E BENJAMIN, Antônio. "Arts. 29 a 45". In *Código do Consumidor comentados pelos autores do anteprojeto*. Rio de Janeiro: Forense Universitária, 2007.

HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales en la sociedad de la información*. Bilbao : Universidad de Deusto, 2003

HERZOG, Roman. "Art. 5". In *Maunz/Dürig, GG*. München: Beck, 2010.

HESSE, Konrad, y BENDA, Ernst. Manual de derecho constitucional. Madrid [etc.]: Marcial Pons, 2001.

HESSE, Konrad, *Elementos de direito constitucional da República Federal da Alemanha*. Porto Alegre: S.A. Fabris, 1998.

____. “Significado de los Derechos Fundamentales.” In *Manual de derecho constitucional*. Madrid [etc.]: Marcial Pons, 2001.

____. *Escritos de Derecho constitucional (Selección)*. Madrid: Centro de Estudios Constitucionales, 1983.

HOFFMANN-RIEM, Wolfgang (ed.), *Verwaltungsrecht in der Informationsgesellschaft*. Baden-Baden: Nomos-Verl.-Ges., 2000.

____. “Der Staat muss Risiken eines Missbrauchs durch Infiltrierung vorbeugen”. Frankfurter Allgemeine Zeitung, 09.10.2011, [s.d.].

____. “Informationelle Selbstbestimmung in der Informationsgesellschaft - Auf dem Wege zu einem neuen Konzept des Datenschutzes”. *AöR*, 1998.

HOHFELD, Wesley Newcombe. *Fundamental legal conceptions as applied in judicial reasoning : and other legal essays*. New Haven: Yale University Press, 1920.

HUBMANN, Heinrich. *Das Persönlichkeitsrecht*. Köln: Böhlau, 1967.

HUFEN, Friedhelm. “Schutz der Persönlichkeit und Recht auf informationelle Selbstbestimmung.” In *Festschrift 50 Jahre Bundesverfassungsgericht*. Tübingen: Mohr Siebeck, 2001.

____. *Staatsrecht II - Grundrechte*. München: Beck, 2009.

____“Das Volkszählungsurteil des Bundesverfassungsgerichts und das Grundrecht auf informationelle Selbststimmung” *Juristenzeitung*, 1984.

KERR, Orin. “The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution”. *Michigan Law Review*, march 2004.

KLOEPFER, Michael, y SCHÄRDEL, Florian. “Grundrechte für die Informationsgesellschaft - Datenschutz und Informationszugangsfreiheit ins Grundgesetz?.” *Juristenzeitung*, 2009

LEITE SAMPAIO, Jose Adércio. *Direito à intimidade e a vida privada : uma visão jurídica da sexualidade, da família, da comunicação e informaciones pessoais, da vida e da morte*. Belo Horizonte: Del Rey, 1998.

LERCHE, Peter. “Schutzbereich, Grundrechtsprägung, Grundrechtseingriff.” In *Handbuch des Staatsrecht der Bundesrepublik - Bd.V : Allgemeine Grundrechtslehren*, organizado por Josef Isensee e Paul Kirchhof. Heidelberg: Müller Juristischer Verlag, 1992.

LEVY, Joshua S. “Towards a Brighter Fourth Amendment: Privacy and Technological Change”. *New York University Law and Economics*, paper 279.

LÓPEZ GARRIDO, Diego. “La sociedad informatizada y la crisis del Estado de bienestar.” *Revista de estudios políticos*, 1985.

MACHADO, Jónatas E. M. *Direito Internacional do Paradigma Clássico ao Pós-11 de Setembro*. Coimbra: Coimbra Editora, 2006.

MARCUSE, Herbert. *El hombre unidimensional: ensayo sobre la ideología de la sociedad industrial avanzada*. Barcelona: Ariel, 1994.

MARTÍNEZ MARTÍNEZ, Ricard. *Una aproximación crítica a la autodeterminación informativa*. Madrid: Civitas, 2004.

MARTINS, Ives Gandra da Silva, e REALE, Miguel. "Sigilo bancário. Inconstitucionalidade do Decreto n. 4.489 de 28/11/2002 por macular o processo legislativo plasmado na Lei Suprema e infringir direitos fundamentais do cidadão." In *Sigilo fiscal e bancário*. São Paulo: Quartier Latin, 2005.

MARTINS, Leonardo e DIMOULIS, Dimitri. *Teoria geral dos direitos fundamentais*. São Paulo: Revista dos Tribunais, 2008.

MARTINS, Leonardo. *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão / coletânea original: Jürgen Schwabe*. Traducido por Beatriz Henning ... [et al.]. Montevideo: Konrad Adenauer Stiftung, 2005.

MATUS, Jessica. "Transferencias Internacionales a Países con Niveles Adecuados y no Adecuados de Protección. Aspectos Prácticos." Montevideo, Uruguay, 2010.

MEDINA GUERRERO, Manuel. *La vinculación negativa del legislador a los derechos fundamentales*. McGraw-Hill Interamericana de España, 1996.

MEYER-LADEWIG, Jens. "Artikel 46". In *Europäische Menschenrechtskonvention : Handkommentar*. Baden-Baden: Nomos, 2010, Rn 28-37.

MICHELMAN, Frank I.. "Human Rights and the Limits of Constitutional Theory." *Ratio Juris*, 2000.

MIGUEL SÁNCHEZ, Noelia de. "Análisis de la sentencia del Tribunal Supremo de 9 de julio de 2007, relativa al fichero Sistema de Información sobre Nuevas Infecciones

(SINIVIH): una obligada reflexión en torno al principio de seguridad.” Revista jurídica de Castilla y León, n. 16, 2008.

MILLER, Jonathan M. “A Typology of Legal Transplants: Using Sociology, Legal History and Argentine Examples to Explain the Transplant Process.” *The American Journal of Comparative Law*, Fall 2003.

MORAES, Alexandre de. *Direito constitucional*. São Paulo: Atlas, 2003.

MURILLO DE LA CUEVA, Pablo Lucas. “La Constitución y el derecho a la autodeterminación informativa”. *Cuadernos de derecho público*, 2003.

____. “Perspectivas del derecho a la autodeterminación informativa.” *IDP: Revista de Internet, Derecho y Política, No. 5*, 2007.

____. *El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática*. Madrid: Tecnos, 1990.

____. Informática y protección de datos personales :estudio sobre la ley organica 5/1992, de regulacion del tratamiento automatizado de los datos de caracter personal. Madrid: Centro de Estudios Constitucionales, 1993.

NEVES, Marcelo. *Transconstitucionalismo*. São Paulo: Martins Fontes, 2009.

NICOLIELLO, Nelson. *Diccionario del Latín Jurídico*. Buenos Aires: Euros, 2004.

NIERHAUS, Michael. “Grundrechte aus der Hand des Gesetzgebers?.” *AöR 116*, 1991.

NIGRO MAZZILLI, Hugo. *A Defesa dos interesses difusos em juízo meio ambiente, consumidor e patrimônio cultural*. São Paulo: Revista dos Tribunais, 2007.

NOBRE MATTA, José Eduardo. *Habeas data*. Rio de Janeiro: Lumen Juris, 2005.

OLIVEIRA LIMA ROQUE, Maria José. *Sigilo bancário e direito à intimidade*. Curitiba: Juruá, 2001.

ORTI VALLEJO, Antonio. *Derecho a la intimidad e informática* . Granada: Comares, 1994.

OSSENBÜHL, Fritz. "§62 Vorrang und Vorbehalt des Gesetzes". In *Handbuch des Staatsrecht der Bundesrepublik - Bd.III*, organizado por Josef Isensee y organizado por Paul Kirchhof. Heidelberg: Müller Juristischer Verlag, 1987.

OTTO Y PARDO, Ignacio de. "La regulación del ejercício de los derechos y libertades. La garantía de su contenido esencial en el artículo 53.1 de la Constitución." In *Derechos fundamentales y Constitución*. Madrid: Civitas, 1988.

OVEY, Clare e WHITE, Robin. *The European Convention on Human Rights*. Oxford: Oxford Univ. Press, 2010.

PAPIER, Hans-Jürgen. "Das Volkszählungsurteil des Bundesverfassungsgerichts." In *25 Jahre Volkszählungsurteil / Datenschutz - Durchstarten in die Zukunft*, organizado por Peter Schaar. Berlin: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2008.

PECES-BARBA MARTÍNEZ, Gregorio. "Fundamental Rights: Between Morals and Politics." *Ratio Juris*, 2001.

____ "La universalidad de los derechos humanos." In *La Corte y el sistema interamericano de derechos humanos*. San José, Costa Rica: Corte IIDH, 1994.

____. *Curso de derechos fundamentales: teoría general*. Madrid: Universidad Carlos III de Madrid [etc.], 1995.

____. *La dignidad de la persona desde la filosofía del derecho*. Madrid: Dykinson, 2004.

PEIXOTO, Marcelo Magalhães e LACOMBE, Rodrigo Lourenço Masset (orgs.). *Comentários ao código tributário nacional*. São Paulo: MP, 2005.

PÉREZ LUÑO, Antonio E. "Informática y libertad. Comentario al artículo 18.4 de la Constitución." Revista de Estudios Políticos, Novembro 1981.

____. *Derechos humanos, estado de derecho y constitución*. Madrid: Tecnos, 2005.

____. *La tercera generación de derechos humanos*. Cizur Menor: Thomson-Aranzadi, 2006.

____. "La tutela de la libertad informática en la sociedad globalizada". *Isegoría*, 2000.

____. "Introducción a los sistemas informatizados de documentación jurídica." In Problemas actuales de la documentación y la informática jurídica : actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986. Madrid: Tecnos, 1987.

PÉREZ ROYO, Javier. *Curso de derecho constitucional*. Madrid: Marcial Pons, 2007.

PÉREZ TREMPS, Pablo. "La interpretación de los derechos fundamentales." In *Estudios de Derecho Constitucional: homenaje al profesor D. Joaquín García Morillo*, Valencia: Tirant lo Blanch, 2001.

PETERSEN, Stefanie. *Grenzen des Verrechtlichungsgebotes im Datenschutz*. Münster ; Hamburg [u.a.]: Lit, 2000.

PETTIT, Philip. *Republicanism: a theory of freedom and government*. Oxford: Oxford University Press, 1997.

PIEROTH, Bodo, e SCHLINK, Bernhard. *Grundrechte*. Heidelberg: C. F. Müller, 2009.

PIEROTH, Bodo, SCHLINK, Bernhard y KNIESEL, Michael. *Polizei- und Ordnungsrecht*. München: Beck, 2008.

PIÑAR MAÑAS, José Luis. "El derecho fundamental a la protección de datos personales ."In: CANALES GIL, Alvaro, BLANCO ANTÓN, María José, PIÑAR MAÑAS, José Luis (coords.). *Protección de datos de carácter personal en Iberoamérica : II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 de junio de 2003*. Valencia : Libreria Tirant lo Blanch, 2005.

PITSCHAS,Rainer y SCHOLZ, Rupert. *Informationelle Selbstbestimmung und staatliche Informationsverantwortung*. Berlin: Duncker & Humblot, 1984.

PRIMUS, Richard A.. *The American Language of Rights*. Cambridge, U.K. ; New York: Cambridge University Press, 1999.

PROSSER, William L.. "Privacy." *Cal. L. Rev.*, 1960.

PUENTE ESCOBAR, Agustín. "Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal." In: CANALES GIL, Alvaro, BLANCO ANTÓN, María José, PIÑAR MAÑAS, José Luis (coords.). *Protección de datos de carácter personal en*

Iberoamérica : II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 de junio de 2003. Valencia : Libreria Tirant lo Blanch, 2005.

QUADROS. Fausto de. *Direito da União Européia*. Coimbra: Almedina, 2004.

RAWLS, John. "The Law of Peoples." *Critical Inquiry*, Autumm 1993.

____. *Liberalismo Politico*. São Paulo: Ática, 2000.

REBOLLO DELGADO, Lucrecio. *Derechos fundamentales y protección de datos*. Madrid: Dykinson, D.L., 2004.

REIS NOVAIS, Jorge. *As restrições aos derechos fundamentales não expresamente autorizadas pela constituição*. Coimbra: Coimbra Editora, 2003.

RIBEIRO BASTOS, Celso . *Curso de direito constitucional*. São Paulo: Saraiva, 1999.

RODOTÀ, Stefano. "Democracia y protección de datos." *Cuadernos de derecho público*, 2003.

____. *A Vida na Sociedade da Vigilância* . Rio de Janeiro: Editora Renovar, 2008.

RODRÍGUEZ RUIZ, Blanca. "El caso "Valenzuela Contreras" y nuestro sistema de derechos fundamentales." In *Revista española de derecho constitucional*, 1999.

____. "The Right to Privacy: A Discourse-Theoretical Approach." *Ratio Juris*, 2002.

____. *El secreto de las comunicaciones: tecnología e intimidad*. Madrid: McGraw-Hill Interamericana de España, 1998.

____. *Privacy in telecommunications: a European and an American approach*. The Hague , Boston: Kluwer Law International, 1997.

ROSCOE BESSA, Leonardo. *O consumidor e os limites dos bancos de dados de proteção ao crédito*. São Paulo: Revista dos Tribunais, 2003.

ROßNAGEL, Alexander. "Die Novellen zum Datenschutzrecht". *Neue juristische Wochenschrift*, 2009.

____. "Das neue Recht elektronischer Signaturen." *Neue juristische Wochenschrift*, 2001.

ROTH, Wolfgang. *Faktische Eingriffe in Freiheit und Eigentum: Struktur und Dogmatik des Grundrechtstatbestandes und der Eingriffsrechtfertigung*. Berlin: Duncker & Humblot, Cop., 1994.

RUBIO LLORENTE, Francisco. "Derechos Fundamentales, Derechos Humanos y Estado de Derecho." *Fundamentos: Cuadernos monográficos de teoría del estado, derecho público e historia constitucional*, vol. 4.

SANTIAGO NIÑO, Carlos. *Fundamentos de derecho constitucional*. Buenos Aires: Astrea, 1992.

SCARANCE FERNANDES, Antonio. "O polêmico inciso XII do artículo 5º da Constitucional Federal." *Justitia*, Diciembre 2007.

SCHERZBERG, Arno. "Die öffentliche Verwaltung als informationelle Organisation ." In *Verwaltungsrecht in der Informationsgesellschaft*. Nomos, 2000.

SCHLAICH,Klaus y KORIOTH, Stefan. *Das Bundesverfassungsgericht*. München: Beck, 2004.

SCHLINK, Bernhard. "Das Recht der informationellen Selbstbestimmung." *Der Staat*, 1986.

SCHMIDT-ASSMANN, Eberhard. "Cuestiones fundamentales sobre la reforma de la Teoría General del Derecho Administration. Necesidad de innovación y presupuestos metodológicos." In *Innovación y reforma en el derecho administrativo*. Sevilla: Derecho Global, 2006.

____. "La ciencia del Derecho Administrativo ante el reto de la internacionalización de las relaciones administrativas." *Revista de administración pública*, 2006.

SCHNEIDER, Hans-Peter. "Peculiaridad y función de los derechos fundamentales en el Estado constitucional democrático". *Revista de estudios políticos*, 1979.

____. *Democracia y constitución*. Madrid: Centro de Estudios Constitucionales, 1991.

SCHNEIDER, Ludwig. *Der Schutz des Wesensgehalts von Grundrechten nach Art. 19 Abs. 2 GG*. Berlin: Duncker & Humblot, 1983.

SEOANE RODRÍGUEZ, José Antonio. "Ética, Derecho y datos personales." *Cuadernos de derecho público*, Nº 19-20 (Ejemplar dedicado a: Protección de datos), 2003.

SERRANO PÉREZ, María Mercedes. "El derecho fundamental a la Protección de Datos. Su contenido esencial." *Nuevas Politicas Públicas: Anuario multidisciplinar*

para la modernización de las Administraciones Públicas, Nº. 1 (Exemplar dedicado a: Los derechos fundamentales y las nuevas tecnologías), 2005.

SHAFFER, Gregory. "Transnational Mutual Recognition Regimes: Governance without Global Government". *Law and Contemporary Problems,* Summer/Autumn 2005.

SHANY, Yuval. "Toward a General Margin of Appreciation Doctrine in International Law?." *European Journal of International Law,* 2005.

SIEMEN, Birte. *Datenschutz als europäisches Grundrecht*. Berlin: Duncker & Humblot, 2006.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. São Paulo: Malheiros, 2006.

SILVA, Virgílio Afonso da. "Interpretación conforme la constitución: entre la trivialidad y la centralización judicial." *Revista Derecho GV 3*, 2006

SILVEIRA DIFINI, Luiz Felipe. *Manual de Direito Tributário*. São Paulo: Saraiva, 2005.

SIMITIS, Spiro. "Privacy–An Endless Debate?." *California Law Review*, 2010.

____. "Zur Datenschutzgesetzgebung: Vorgaben und Perspektiven." *Computer und Recht,* 1987.

____. *Kommentar zum Bundesdatenschutzgesetz*. Baden-Baden: Nomos-Verlagsgesellschaft, 2003.

____. “Der Transfer von Daten in Drittländer -ein Streit ohne Ende?” *Computer und Recht*, 2000.

____. “Privatisierung und Datenschutz.” *Datenschutz und Datensicherheit - DuD*, 1995.

SOLOVE, Daniel J. e ROTENBERG, Marc. *Information privacy law*. New York: Aspen Publishers, 2003.

SOLOVE, Daniel J.. “Privacy and Power: Computer Databases and Metaphors for Information Privacy”. *Stan. L. Rev.*, 2000.

____ “Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference”. *Fordham Law Review*, Winter 2005.

SOMMERMANN, Karl-Peter. “Völkerrechtlich garantierte Menschenrechte als Maßstab der Verfassungskonkretisierung.” AöR, 1989.

SORICE BARACHO THIBAU, Tereza Cristina. *O Habeas data*. Belo Horizonte: Del Rey, 1997.

STERN, Klaus. “Die Grundrechte und ihre Schranken”. In *Festschrift 50 Jahre Bundesverfassungsgericht II*, organizado por Peter Badura e Horst Dreier. Tübingen: Mohr Siebeck, 2001.

____. “Idee und Elemente eines Systems der Grundrechte.” In *Handbuch des Staatsrecht der Bundesrepublik - Bd.V : Allgemeine Grundrechtslehren*, organizado por Josef Isensee e Paul Kirchhof. Heidelberg: Müller Juristischer Verlag, 1992.

____. *Das Staatsrecht der Bundesrepublik Deutschland.* Vol. 3.1. München: Beck, 1988

____. *Das Staatsrecht der Bundesrepublik Deutschland*. Vol. 3.2 München: Beck, 1994.

____. *Derecho del Estado de la República Federal Alemana*. Traducido por Javier Pérez Royo y Pedro Cruz Villalón. Madrid: Centro de Estudios Constitucionales, 1987.

SWIRE, Peter. "Katz is Dead. Long Live Katz". *Michigan Law Review*, march 2004.

TÉLLEZ AGUILERA, Abel. *La protección de datos en la Unión Europea: divergencias normativas y anhelos unificadores*. Madrid: Edisofer, 2002.

____. *Nuevas tecnologías, intimidad y protección de datos: con estudio sistemático de la Ley Orgánica 15-1999*. Madrid: Edisofer, 2001.

TERRIGNO BARBEITAS, André. *O sigilo bancário: e a necessidade da ponderação dos intereses*. São Paulo: Malheiros, 2003.

TINNEFELD, Marie-Therese, EHMANN, Eugen, y GERLING, Rainer W. *Einführung in das Datenschutzrecht : Datenschutz und Informationsfreiheit in europäischer Sicht*. München ; Wien: Oldenbourg, 2005.

TRONCOSO REIGADA, Antonio. "La protección de datos personales: una reflexión crítica de la jurisprudencia constitucional." *Cuadernos de derecho público*, Nº 19-20, 2003.

TROPER, Michel. *A filosofía do direito*. São Paulo: Martins Editora, 2008.

TRUTE, Hans-Heinrich. "Der Schutz personenbezogener Informationen in der Informationsgesellschaft?." Juristenzeitung, 1998.

VIEIRA DE ANDRADE, José Carlos. *Os derechos fundamentales na constituição portuguesa de 1976*. Coimbra: Almedina, 2001.

VIZCAÍNO CALDERÓN, Miguel. *Comentarios a la ley orgánica de protección de datos de carácter personal*. Madrid: Civitas, 2001.

WALD, Arnoldo. "A legislação sobre "lavagem" de dinheiro." *Revista CEJ*, Dezembro 1998.

____. "O sigilo bancário no projeto de Lei Complementar de reforma do sistema financeiro e na lei complementar nº 70." *Revista de información legislativa*, 1992.

WALDRON. Jeremy. "Rights and Needs." In *Legal Rights: Historical and Philosophical Perspectives*. Ann Arbor: University of Michigan Press, 1995.

WARREN, Samuel D., e BRANDEIS, Louis D.. "The Right to Privacy." *Harvard Law Review*, 1890.

WEICHERT, Thilo. "Verbraucher-Scoring meets Datenschutz." *Datenschutz und Datensicherheit - DuD*, 2006.

WESTIN, Alan F., e BAKER, Michael A.. *Databanks in a free society*. New York: Quadrangle, 1972.

WESTIN, Alan F.. "Social and Political Dimensions of Privacy." *Journal of Social Issues*, v. 59, n. 2, 2003.

WÖLFL, Bernd. "Sphärentheorie und Vorbehalt des Gesetzes." NVwZ, 2002.

ZUCCA, Lorenzo. “The Limits of the Age of Rights.” In *Analisi e diritto 2005 ricerche di giurisprudenza analitica*. Torino: G. Giappichelli Editore, 2006.

LISTA DE ABREVIATURAS

ADIN	Ação Declaratória de Inconstitucionalidade (Brasil)
ADN	Ácido desoxirribonucleico
AEPD	Agencia Española de Protección de Datos
AG	Agravo (Brasil)
Ag Reg	Agravo Regimental (Brasil)
AI	Agravo de Instrumento (Brasil)
ANATEL	Agência Nacional de Telecomunicações (Brasil)
AO	Abgabenordnung (Ley fundamental de Derecho Tributario en Alemania)
AöR	*Archiv des öffentlichen Rechts*
AP	Ação Penal (Brasil)
Ap.	Application (en el TEDH)

Art.	Artículo
AuslG	Ausländergesetz (Ley de Extranjeria alemán)
BAG	Bundesarbeitsgericht (Tribunal Federal Laboral alemán)
BDSG	Bundesdatenschutzgesetz (Ley de Protección de Datos Federal alemán)
BetrVG	Betriebsverfassungsgesetz (Ley de derecho laboral en Alemania)
BGB	Bürgerliche Gesetzbuch (Código Civil de Alemania)
BGH	Bundesgerichtshof (Tribunal de Justicia Federal de Alemania)
BKAG	Gesetz über das Bundeskriminalamt (Ley Federal de la Policía Criminal alemán)
BKR	*Zeitschrift für Bank- und Kapitalmarktrecht*
BOC	Boletín Oficial de las Cortes
BVerfG	Bundesverfassungsgericht (Tribunal Constitucional Federal Alemán)
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (Sentencias del BVerfG)
BVerfSchG	Bundesverfassungsschutzgesetz (Ley Federal de Protección Constitucional alemán)
BVerwG	Bundesverwaltungsgericht (Tribunal Administrativo Federal de Alemania)
Cal. L. Rev.	*California Law Review*

CDC Código de Defesa do Consumidor (Brasil)

CE Constitución española de 1978

CEDH Convenio Europeo de Derechos Humanos

CF Constituição da República Federativa do Brasil de 1988

CPI Comissão Parlamentar de Inquérito (Brasil)

CR Computer und Recht

CTN Código Tributário Nacional (Brasil)

DJ Diário de Justiça (Brasil)

EDcl Embargo de Declaração (Brasil)

FJ Fundamento Jurídico

GG Grundgesetz für die Bundesrepublik Deutschland (Ley Fundamental para la República Federal de Alemania)

GPS Global Positioning System (sistema de posicionamiento global)

HC *Habeas Corpus* (Brasil)

HD *Habeas Data* (Brasil)

HIV Human immunodeficiency virus (virus de inmunodeficiencia humana)

Inq Inquérito (Brasil)

LAG Landesarbeitsgericht (Tribunal Superior Laboral del land alemán)

LC Lei Complementar (Brasil)

LGT Ley General Tributaria (España)

LGTel Lei Geral de Telecomunicações (Brasil)

LO Ley Orgánica (España)

LOPD Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

LOPJ Ley Orgánica del Poder Judicial (España)

LORTAD Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos Personales

LRJAP-PAC Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (España)

MC Medida Cautelar (Brasil)

Min Ministro (Magistrado del STF)

MS Mandado de Segurança (Brasil)

NJW *Neue Juristische Wochenschrift*

NJW-RR *NJW-Rechtsprechungs-Report* (Informe Judicial del NJW)

NVwZ *Neue Zeitschrift für Verwaltungsrecht*

OAB	Ordem dos Advogados do Brasil
OCDE	Organización para la Cooperación y el Desarrollo Económico
OLG	Oberlandesgericht (Tribunal Superior del land en Alemania)
Pet	Petição (Brasil)
QO	Questão de Ordem (Brasil)
RD	Real Decreto (España)
RE	Recurso Extraordinário (Brasil)
Rcl	Reclamação (Brasil)
Rec.	Recurso
REsp	Recurso Especial (Brasil)
RFFP	Representação Fiscal para fins penais (Brasil)
RHC	Recurso en Habeas Corpus (Brasil)
RJ	*Repertorio Aranzadi de Jurisprudencia*
RMS	Recurso em Mandado de Segurança (Brasil)
SAN	Sentencia de la Audiencia Nacional (España)
SGB X	Sozialgesetzbuch Zehntes Buch (Décimo libro del Código Social de Alemania

Stan. L. Rev. *Stanford Law Review*

STC Sentencia del Tribunal Constitucional (España)

STF Supremo Tribunal Federal de Brasil

STFC Serviço Fixo Telefônico Comutado (Brasil)

StGB Strafgesetzbuch (Código Penal alemán)

STJ Superior Tribunal de Justiça (Brasil)

StPO Strafprozessordnung (Código de Procedimiento Penal en Alemania)

STS Sentencia del Tribunal Supremo (España)

STSJ Sentencia del Tribunal Superior de Justicia de la Comunidade Autónoma (España)

SW LDSG Landesdatenschutzgesetz (Ley de Protección de Datos en el land de Schleswig-Holstein)

TDDSG Teledienstedatenschutzgesetz (Ley de Protección de Datos en los Teleservicios en Alemania)

TEDH Tribunal Europeo de Derechos Humanos

TJCE Tribunal de Justicia de las Comunidades Europeas (hoy Tribunal de Justicia de la Unión Europea)

TKG Telekommunikationsgesetz (Ley de Telecomunicaciones alemán)

U.S.	United States Reports
UCD	Unión de Centro Democrático
UE	Unión Europea
VwGO	Verwaltungsgerichtsordnung (Código de Procedimiento Administrativo alemán)
WP	Working Party