Autodeterminación Informativa y Leyes sobre Protección de Datos

Alberto Cerda Silva
Magíster en Derecho Público, Universidad de Chile
Investigador del Centro de Estudios en Derecho Informático

Resumen

El texto considera la evolución conceptual producida en torno al bien jurídico protegido por la normativa que regula el tratamiento de datos personales, desde su inicial construcción sobre la base del derecho a la intimidad para arribar a la autodeterminación informativa, ampliando horizontes explicativos respecto de este cúmulo de facultades que se confieren a la persona concernida por los datos para anteponerse a los riesgos inherentes al procesamiento de información a su respecto y, a su vez, velar por el cumplimiento de la legislación, para enseguida describir sucintamente los rasgos fundamentales de la legislación extranjera –incluye la normativa comunitaria de la Unión Europea, la legislación interna de Alemania, Suecia, España, Francia e Italia, así como la normativa de Argentina, y los acuerdos suscritos entre Estados Unidos y la Unión Europea para asegurar el flujo tranfronterizo de datos personales, conocidos como Acuerdos de Puerto Seguro (Safe Harbor Agreement)–, a efectos de apreciar la evolución experimentada por las leyes sobre protección de las personas frente al tratamiento de datos personales y, particularmente, la progresiva diversificación de los medios de que éstas se han prevalido para efectos de asegurarse del debido cumplimiento de sus previsiones.

1. El derecho a la Intimidad

Aun cuando desde antiguo el hombre ha buscado un lugar de sosiego y refugio para el desarrollo de su ser interior, a buen recaudo del tumulto y frenesí de la vida en sociedad, la

intimidad no se constituyó en una preocupación central sino con el desarrollo del liberalismo; serán Thomas HOBBES, John LOCKE y John STUART MILL quienes apuntarán, con matices, la necesidad de conciliar el accionar del Estado con los intereses del individuo, quien dispondrá de un margen de vida privada exento de la intervención estatal.[1] Y es que sólo la mutación desde una sociedad feudal a otra burguesa ofrecía las condiciones para que la disponibilidad de un ámbito de acción reservado se constituyera en una sentida necesidad de los individuos.[2]

Este repliegue del individuo en su vida privada no dejó de causar reparos; así se percibe en la obra de Alexis de TOCQUEVILLE, quien repudia el abandono del poder en los expertos por el riesgo que representa para las minorías, e igualmente en Benjamín CONSTANT, quien, tras constatar que mientras la libertad de los antiguos se concretaba en la participación en la vida pública, para los modernos se traduce en mayores espacios de recogimiento y exclusión de aquella, exhorta a conjugar equilibradamente vida privada y pública.[3]

Sólo en las postrimerías del siglo XIX tiene inicio el proceso de elaboración jurídica del derecho a la intimidad. En efecto, en 1890 Louis BRANDEIS y Samuel WARREN publican en la Harvard Law Review el artículo titulado "The Rigth to Privacy", en el cual, con base en el derecho de propiedad y denotando la versatilidad evolutiva del common law, esbozan el derecho a la intimidad, sirviéndose de la formulación del juez COOLEY, como "the right to be left alone".[4] El propósito era cimentar un derecho para hacer frente al hostigamiento por los medios de comunicación social de la época, para guardar reserva respecto de aquel aspecto de la vida personal que legítimamente podía ser excluido de la injerencia de la prensa.

A mediados del siglo recién pasado, el derecho a la intimidad viene a merecer reconocimiento en un instrumento internacional, cual es la Declaración Universal de Derechos Humanos de 1948, que prevé que nadie será objeto de injerencias arbitrarias en su vida privada y, a su vez, asegura a toda persona el derecho a la protección de la ley contra tales injerencias o ataques.[5] De entonces a esta parte, con un mayor o menor desarrollo normativo, el derecho a la intimidad está previsto sistemáticamente en los tratados internacionales sobre derechos humanos y en términos más o menos explícitos en la Carta Fundamental de los diversos Estados.[6]

1 En este sentido BÉJAR, Helena, "El ámbito íntimo. Privacidad, individualismo y modernidad", Alianza Editorial. Madrid, 1990. passim. LUCAS MURILLO DE LA CUEVA, Pablo. "El Derecho a la Autodeterminación Informativa. La Protección de los Datos Personales frente a la Informática". Editorial Tecnos. Madrid, 1990, pp. 45 y ss.

2 MARTÍNEZ MARTÍNEZ, Ricard, "Tecnologías de la información, policía y Constitución", Tirant lo blanch, Valencia, 2001, pp. 59 - 60. Yendo aún más allá, para develar la ideología subyacente en la protección de la intimidad y su evolución desde un privilegio a un valor constitucional, Cf. PÉREZ-LUÑO, Antonio Enrique, "Derechos humanos, Estado de derecho y constitución", 5ª edic., Editorial Tecnos, Madrid, 1995, pp. 317 – 344.

3 CONSTANT, Benjamín, "De la libertad de los antiguos comparada con la de los modernos", cit. por BÉJAR, Helena, op. cit., pp. 41 – 49.

4 BRANDEIS y WARREN, "The Rigth to Privacy", en Harvard Law Review, vol. IV, núm. 5, 1890, passim. Trad., "El derecho a la intimidad", Editorial Civitas, Madrid, 1995.

5 Artículo 12 de la Declaración Universal de Derechos Humanos, adoptada y proclamada por la Asamblea General de las Naciones Unidas en su resolución 217 A (III), de 10 de diciembre de 1948.

6 Cf. entre otros instrumentos internacionales, además de la Declaración Universal, el artículo 5 de la Declaración Americana de los Derechos y Deberes del Hombre, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966, el artículo 11 de la Convención Americana de Derechos Humanos de 1969, y el artículo 16 de la Convención de Derechos del Niño de 1989.

Ahora bien, las mayores dificultades de la doctrina giran en torno a establecer los márgenes a los cuales se extiende la protección que brinda el derecho a la intimidad. En este sentido, entre los intentos por verificar una delimitación, PÉREZ-LUÑO destaca la elaboración por la doctrina alemana de la que se ha venido en llamar teoría de las esferas, en la cual, a grandes rasgos, se distinguen ámbitos de acción del individuo de extensión radial, cuyo centro más cercano corresponde a lo secreto, su periferia a aquello que atañe a la individualidad de la persona, y una franja intermedia correspondiente a la intimidad, en que se sitúa aquello que se desea mantener al margen de la injerencia de terceros.[7]

Sin embargo, prescindiendo del valor pedagógico que la doctrina de las esferas evidencia, muestra asimismo dificultades para establecer qué ha de calificarse como íntimo, lo que le fuerza a recurrir a criterios auxiliares, que no hacen sino reafirmar su escasa eficacia.[8] Precisamente, GARCÍA SAN MIGUEL estima que se han esbozado cuando menos tres concepciones al respecto: una espacial, una subjetiva, y una tercera, objetiva.[9]

Para la concepción espacial o geográfica, la extensión de la intimidad está asociada con el control que se tiene sobre determinadas áreas u objetos. De tal suerte, aquello que acontece al interior de los hogares queda al amparo de intromisión alguna; por extensión, se brinda similar protección a la correspondencia y a las comunicaciones telefónicas. Sin embargo, fuera de que el criterio resulta ambiguo en determinados contextos –tal como la calificación de aquello que acontece en un restaurante–, la concepción espacial resulta excesivamente restringida, desde que circunscribe el alcance del derecho a factores externos y minusvalora la trascendencia social de las conductas desplegadas por las personas en el medio, junto con resultar insuficiente para brindar respuesta a las agresiones al derecho cometidas "a distancia", en las cuales no se verifica una invasión al medio espacial en que se desenvuelve la persona, por ejemplo mediante el empleo de cámaras con lentes de largo alcance.

De otro lado, la concepción subjetiva de la intimidad descansa en el distingo entre personaje público y funcionario público, de un lado, y persona privada, de otro. Mientras las actuaciones de aquellos, por la naturaleza de sus funciones o por la influencia que detentan, deben estimarse excluidas del abrigo del derecho a la intimidad, las de los últimos, precisamente por carecer de tales circunstancias, deben estimarse cubiertas por él. No obstante, la concepción subjetiva resulta insuficiente para precisar la extensión de la intimidad, desde que descansa en condiciones esencialmente relativas, pero fundamentalmente porque repugna a criterios de igualdad jurídica, ya que admite la privación del derecho a los funcionarios y personajes públicos con independencia de la relevancia de su comportamiento, salvo que recurra a nuevos criterios correctivos, que no hacen sino confirmar que carece de suficiencia para brindar una respuesta apropiada.

7 PÉREZ-LUÑO, Antonio Enrique, "Derechos humanos...", op. cit., pp. 327 – 331, donde considera las elaboraciones de H. Hubmann, así como de Vittorio Frosini, entre otras. También acude a la teoría de las esferas, con cita a Leo Reisinger, ÁLVAREZ-CIENFUEGOS SUÁREZ, José María, "El derecho a la intimidad personal, la libre difusión de la información y el control del Estado sobre los bancos de datos", en Encuentros sobre Informática y Derecho, Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 1990 – 1991, p. 185.

8 En similar sentido, MARTÍNEZ MARTÍNEZ, Ricard, op. cit., pp. 62 – 64.

9 Vid. GARCÍA SAN MIGUEL, Luis "Reflexiones sobre la intimidad como límite de la libertad de expresión", en Estudios sobre el Derecho a la Intimidad, Editorial Tecnos, 1992, pp. 15 – 35, quien las sintetiza como sigue en el texto.

En cambio, la concepción objetiva prescinde de consideraciones materiales o fundadas en la calidad de las personas y más bien atiende al distingo entre conductas públicas y privadas. Serán conductas privadas, y por tanto quedan al alero del derecho a la intimidad, aquellas desplegadas con el propósito de satisfacer necesidades propias; en cambio, las conductas públicas, aquellas que han tenido por finalidad satisfacer necesidades ajenas, quedarán privadas de tal cobertura y será lícita la intromisión a su respecto. Para mitigar la rigidez de esta concepción, se recurre a un factor de corrección, de tal suerte una conducta que en principio merece el calificativo de privada, por su "trascendencia", puede dejar de ser tal y devenir en pública.[10]

Con todo, la mayor parte de la doctrina apunta al carácter esencialmente casuístico que reviste la extensión que se atribuye al derecho a la intimidad.[11] Sin embargo, cualquiera fuere este, así como ella surgió históricamente como una reacción frente a las ilegítimas intromisiones de la prensa en la vida de las personas, el boyante desarrollo de los medios de comunicación de masas evidenció la insuficiencia del derecho a la intimidad como simple expresión de ámbitos de exclusión a la injerencia de terceros, e hizo patente la necesidad de ampliar la protección que brindaba a su titular, para permitir que éste pudiese disponer de control sobre la información personal que le compete.

Precisamente, las sucesivas aportaciones formuladas por la doctrina americana en la materia, en especial por WESTIN y FRIED a fines de la década de los sesenta, contribuyeron a extender la privacidad desde una noción pasiva, centrada en la simple retención de información –esto es, la ausencia de información sobre nosotros en las mentes de otros, o, si se prefiere, reivindicación de un espacio exclusivo y excluyente–, a una activa, que releva el control y disposición sobre cuándo, quién y para qué puede acceder a la información que nos concierne, "the right to control information about oneself".[12]

Si los medios de comunicación de masas importaban un serio riesgo para la intimidad, las nuevas tecnologías lo son aún más, desde que han generado una insospechada capacidad para recoger, procesar y transmitir información; en efecto, el progresivo incremento en el empleo de la informática por servicios públicos y particulares, ha permitido a estos disponer de más y mejor información, conforme a la cual adoptar las decisiones atinentes a sus ámbitos de competencia: así, por ejemplo, en unos casos se tratará de la concesión de subsidios o beneficios, en otros el propósito será prever el comportamiento del mercado ante la introducción de un nuevo bien o servicio.

10 Entre nosotros, adopta un parecer similar, Noguera, quien, al examinar los límites de la libertad de opinión y expresión y el conflicto de éstas con la privacidad, y en especial, el derecho a la intimidad, desestima el criterio de veracidad y acude a la trascendencia pública de la información para su resolución. En abono e ilustración de su posición, colaciona amplia jurisprudencia nacional como extranjera. NOGUERA ALCALÁ, Humberto, "El derecho a la libertad de opinión e información y sus límites". Lexis-Nexis, Chile, 2002, pp.190 – 194.

11 Entre estos, José Antonio Martín Pallín, quien estima que no es posible construir un concepto de intimidad, siquiera aproximado, desde que se trataría de un bien jurídico indeterminado, con la plasticidad suficiente para adecuarse a toda subjetividad. Cf. ROMEO CASABONA, Carlos María, "Poder informático y seguridad jurídica". FUNDESCO. Madrid, 1988, p. 12 (prólogo).

12 WESTIN, Alan, "Privacy and freedom", Atheneum, New York, 1967, y FRIED, Charles, "Privacy", en Yale Law Journal, vol. 77, 1968, cit. por PÉREZ-LUÑO, Antonio Enrique, "Derechos humanos...", op. cit., pp. 327 – 331. En el mismo sentido MANNY, Carter, "European and American privacy: commerce, right and justice – part 1" en Computer Law and Security Report, vol. 19 num. 1, 2003, pp. 4 – 10.

Como quiera que sea, disponer de información apropiada y oportuna deviene en una necesidad revestida de juridicidad, al amparo del derecho a ser informado. Sin embargo, el excesivo celo que puede mediar en la recogida de información y los abusos a que puede conducir su empleo, particularmente cuando ella se refiere a circunstancias íntimas de la persona, ha merecido el reparo del legislador.

En efecto, si el derecho es la respuesta normativa de la sociedad a la fenomenología que tiene lugar en su seno, este entramado normativo no ha podido permanecer impermeable a los cambios que se producen en ella, sino más bien debe nutrirse de las siempre cambiantes condiciones de la sociedad a la cual está llamado a reglar.[13] En ese orden, las estructuras normativas surgidas en la modernidad y en la etapa de la codificación no han podido sustraerse a los efectos de la creciente aplicación de las nuevas tecnologías que caracteriza a la "sociedad de la información".

2. EL DERECHO A LA AUTODETERMINACIÓN INFORMÁTICA

El caudal de información nominativa susceptible de ser tratada por medios informáticos y aun transmitida a distancia gracias al desarrollo de las telecomunicaciones, ha despertado la precaución de quienes creen ver en ello un serio riesgo para los derechos fundamentales, desde que permite a quien dispone de la información acceder a parcelas de nuestra vida que legítimamente debían tenerse a su resguardo, y aun servirse de ella para condicionar el ejercicio de nuestras libertades.[14]

Si bien la recolección de información constituye una necesidad imprescindible de ser satisfecha por el Estado a la hora de adoptar decisiones que conciernen a la sociedad, debe establecerse un límite que determine la legitimidad del acopio, procesamiento y transmisión de tal información, de forma que tales operaciones compatibilicen los derechos fundamentales de las personas con el fin último del Estado, cual es propender hacia la mayor realización espiritual y material posibles de los integrantes de la comunidad, con pleno respeto de los derechos que a estos correspondan.

La protección que un ordenamiento jurídico confiere a las personas frente al tratamiento de los datos personales que les conciernen constituye, al decir de PÉREZ-LUÑO, un criterio para dimensionar la legitimación política de los sistemas democráticos en los países tecnológicamente desarrollados. En efecto, desde que la información personal denota valores personales, la prevención frente a su tratamiento no suscita tan solo problemas individuales, sino conflictos que importan a la sociedad en su conjunto, ya que el uso de la información permite coartar y controlar el comportamiento ciudadano.[15] Más aún, DAVARA llega

13 PÉREZ-LUÑO, Antonio Enrique. "Manual de Informática y Derecho", Editorial Ariel S.A., Barcelona, 1996, p. 35.

14 Sobre el particular, con especial énfasis en el valor político-social y económico de la información en relación con las nuevas tecnologías, Cf. ROMEO CASABONA, Carlos María, op. cit., pp. 19 - 23.

15 PÉREZ-LUÑO, Antonio Enrique. "Los Derechos Humanos en la Sociedad Tecnológica", en Cuadernos y Debates, Centro de Estudios Constitucionales, Madrid, 1989, núm. 21, p. 138. En el mismo sentido, PÉREZ-LUÑO, Antonio Enrique, "Del Habeas Hábeas al Habeas Data", en Encuentros sobre Informática y Derecho, Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 1990 – 1991, pp. 171 – 179; y, en Informática y Derecho, Cuadernos elaborados por la UNED, Centro Regional de Extremadura, Editorial Aranzadi, número 1, 1995, pp. 153 – 161.

a afirmar que un marco normativo apropiado debe prevenir la constitución de verdaderas "dictaduras tecnológicas".[16]

En consecuencia, los ciudadanos han de consentir en hacer entrega al Estado de una serie de datos personales, en tanto éste se obliga a no usar y disponer de ellos sino con las debidas garantías.[17] En caso contrario, la labor del Estado se reduce a mero agente de control social y las libertades ciudadanas quedan restringidas a un comportamiento condicionado, pues, gracias a la información de que dispone, puede anticipar la conducta de las personas, promoverlas o restringirlas de conformidad con los intereses del gobierno de turno.

Con todo, no debe subestimarse el potencial que las concentraciones privadas de poder tienen sobre nuestras libertades –tales como empresas transnacionales, consorcios empresariales, asociaciones gremiales y otras–, las que, como en el caso del Estado, demandan igualmente la adopción de resguardos para contrarrestar el empleo que hacen de datos personales.

En estas condiciones, la intromisión de la informática y las telecomunicaciones en el quehacer cotidiano ha obligado a una reformulación conceptual del derecho a la intimidad, en términos de ser concebido como el derecho de toda persona a decidir cuánto de sí –de sus pensamientos y sentimientos, así como los hechos de su vida personal– está dispuesto a compartir con otros.

De tal forma, el concepto tradicional que manifestaba una faz negativa del derecho, en cuanto imponía límites a la injerencia de terceros respecto de su titular, por motivo y obra de la informática ha develado una faceta positiva, en cuanto confiere a su titular un haz de facultades para controlar la información que respecto de los datos personales que le conciernen puedan ser albergados, procesados o suministrados informáticamente.

Cabe precisar si la protección frente al tratamiento de los datos personales constituye la expresión de un derecho ya existente, cual es el derecho a la intimidad,[18] o bien representa una nueva categoría de derecho, que garantiza a las personas facultades de información, acceso y

16 DAVARA, Miguel Angel, "Manual de Derecho Informático", Aranzadi Editorial. Pamplona, 1997, pp. 83 y ss. El autor profundiza su concepto de "dictadura tecnológica", en "De las Autopistas de la Información a la Sociedad Virtual", Edit. Aranzadi, Pamplona, 1996, pp. 115 a 141.

17 Con cierto dejo de romanticismo se ha hablado de la configuración de un verdadero "pacto social informático", cf. PÉREZ-LUÑO, Antonio Enrique, "Manual de Informática...", op. cit., p. 67.

18 Es el parecer de Orti Vallejo, quien afirma que el desarrollo tecnológico permite transformar, mediante su empleo, toda información en un atentado a la intimidad; de tal suerte resulta satisfactoria una simple reformulación del concepto de derecho a la intimidad, ya se lo considere de la personalidad o fundamental, aunque acepta alguna conveniencia social en la categoría de fundamental. ORTI VALLEJO, Antonio, "Derecho a la intimidad e informática", Editorial Comares, España, 1994, passim.

control de los datos que le conciernen, prescindiendo de si por su propia naturaleza el tratamiento de tales datos constituye una lesión a la intimidad de las personas a quienes se refieren.[19]

Estiman algunos autores que resulta innecesario esbozar un nuevo derecho fundamental para explicar las leyes protectoras de datos, juicio que, en general, proviene de aquellos que creen ver en él un exceso positivista y un menoscabo a la valía de los derechos fundamentales, visualizando el conjunto de facultades que confiere a su titular como la mera readecuación del derecho a la intimidad a los desafíos de las nuevas tecnologías: una "intimidad informatizada".[20]

Entre quienes desestiman la posición precedente, se sostiene que ella obvia el carácter histórico de los derechos fundamentales, minimiza la insuficiencia de las construcciones jurídicas tradicionales para dar cabal respuesta a los problemas que suscitan las nuevas tecnologías y, en el caso en examen, desconocen la extensión que se atribuye al control sobre la información que concierne al titular de la misma.[21]

En efecto, como sostiene PÉREZ-LUÑO, el catálogo de derechos fundamentales no reviste un carácter estático y, así como a los derechos de primera generación –con un marcado sello liberal que imputaba un rol pasivo al Estado– se adicionó una segunda generación –que demandaba un quehacer de impronta del Welfare State–, a estos se ha sumado una tercera generación que responde a

19 La extensión que se confiere a la privacy en Estados Unidos rebasa –gracias a su desarrollo jurisprudencial– con creces el marco que se le atribuye en la experiencia continental, aun cuando los problemas en que se aprecia su concurrencia suelen vincularse a cuestiones sobre procreación, matrimonio, vida familiar y sexual. Cf. ORTI VALLEJO, op. cit., pp. 35 y ss. La amplitud conferida a la privacy entre los norteamericanos explica por qué la protección de los datos queda circunscrita en ella. En cambio, para la doctrina continental es discutible si las prerrogativas que se confieren al titular de datos personales por las leyes protectoras de datos son expresión del derecho a la intimidad, o bien es necesario construir un nuevo derecho que brinde tal amparo, que se ha dado en llamar "autodeterminación informativa" en la jurisprudencia alemana y "libertad informativa" en el desarrollo de la doctrina italiana y española. Cf. FROSSINI, Vittorio. "Los derechos humanos en la sociedad tecnológica", Anuario de Derechos Humanos, número 2, 1983, pp. 101-115; PÉREZ-LUÑO, Antonio Enrique. "Los Derechos Humanos...", op. cit.; LUCAS MURILLO DE LA CUEVA, Pablo. "El Derecho a...", op. cit.., passim. Por su parte, entre nosotros, es de la opinión que el enfoque de la autodeterminación informativa es complementario a la configuración del derecho al respeto de la vida privada, NOGUERA ALCALÁ, Humberto, "El derecho...", op. cit., pp.152-153.

20 Entre estos, Emilio Suñé, para quien el derecho a la intimidad ha sido siempre, en el fondo, autodeterminación informativa. SUÑÉ LLINÁS, Emilio, "Tratado de Derecho Informático. Volumen I: Introducción y Protección de Datos Personales", Universidad Complutense Madrid, España. 2000. pp. 29-31. Que el bien jurídico salvaguardado sea la intimidad es compartido por ORTI VALLEJO, op. cit., passim; ESTADELLA YUSTE, Olga, "La protección de la Intimidad frente a la Transmisión Internacional de Datos Personales", Editorial Tecnos, Madrid, 1995, pp. 24-33; EKMEKDJIAN, Miguel Angel y PIZZOLO, Calogero. "Habeas Data. El derecho a la intimidad frente a la revolución informática", Ediciones Depalma, Buenos Aires. 2ª Edición, 1998, passim. GRIMALT SERVERA, Pedro, "El derecho a controlar los datos personales: algunas consideraciones jurídico-constitucionales", en Encuentros sobre Informática y Derecho, Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 1996-1997, pp. 151-157; GRIMALT SERVERA, Pedro, "La responsabilidad civil en el tratamiento automatizado de datos personales", Editorial Comares. Granada, 1999, pp. 22-25.

21 Cf. LUCAS MURILLO DE LA CUEVA, Pablo. "El Derecho a...", op. cit., passim. PÉREZ-LUÑO, Antonio Enrique, "Intimidad y Protección de Datos Personales: del Habeas Corpus al Habeas Data", en Estudios sobre el Derecho a la Intimidad, Editorial Tecnos, 1992, pp. 36-45. También discurre sobre las limitaciones del amparo cifrado en la intimidad, Cf. ROMEO CASABONA, Carlos María, op. cit., p. 30-31.

la "liberties' pollution" por las nuevas tecnologías, entre los cuales menciona los originados para la protección de los consumidores, del medio ambiente y de los propios datos personales.[22]

Por otro lado, coincidimos con LUCAS MURILLO DE LA CUEVA, en que el derecho a la autodeterminación informativa se construye a partir del derecho a la intimidad, tanto como éste lo hizo sobre la base del derecho de propiedad; y, en que, a diferencia de cuanto ocurre con el derecho a la intimidad, la autodeterminación informativa no se circunscribe a amparar a la persona frente al tratamiento de datos personales que le conciernan y que revelen circunstancias personales que merezcan permanecer en la esfera privada, sino que, en general, se extiende a todo dato que se predica de determinada persona.[23]

Excusando que la doctrina haya recurrido al derecho a la intimidad para explicarse las leyes sobre protección de datos, HEREDERO HIGUERAS estima que su invocación estaba inicialmente justificada por la ausencia de un concepto más idóneo, a lo cual agrega que las primeras reflexiones en torno a ellas se originaron en el medio angloamericano, sobre la base de la privacy, impronta que no ha logrado eludir cabalmente la doctrina continental.[24]

Fue el Tribunal Constitucional Alemán, al anular la Ley de Censo de Población de 1982, quien primero brindó reconocimiento jurisprudencial a esta nueva categoría jurídica para explicar la protección brindada a las personas ante el tratamiento automatizado de sus datos, en lo que dio en llamar el "derecho a la autodeterminación informativa".[25]

En efecto, cuestionada la legalidad de la Ley de Censo, por estimarse que la entidad y el número de preguntas que él contenía importaba una lesión a la libertad personal, el Tribunal Constitucional Alemán estimó que:

> *"...el derecho general de la personalidad... abarca... la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida...: la libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona"* y que...

22 Sobre la polución o contaminación de las libertades, en relación con la protección de los datos personales, cf. PÉREZ-LUÑO, Antonio Enrique, "Derechos humanos...", op. cit., pp. 345-349; "Intimidad y Protección...", op. cit., pp. 36-45. Ahora, hay doctrina que va aun más allá, esbozando derechos humanos de cuarta generación, cf. RODRÍGUEZ, Ma. Eugenia, "La Nueva Generación de Derechos Humanos. Origen y Justificación", Universidad Carlos III de Madrid, Editorial Dykinson, 2002.

23 LUCAS MURILLO DE LA CUEVA, Pablo. "El Derecho a...", op. cit., passim. También, apuntando que el contenido de la autodeterminación informativa excede el del derecho a la intimidad, DEL REY GUANTER, Salvador. "Tratamiento automatizado de datos de carácter personal y contrato de trabajo", en RL, t. II/1993, p. 141, y FERNÁNDEZ VILLAZÓN, Luis Antonio, "Tratamiento automatizado de datos personales en los procesos de selección de trabajadores" en RL, t. I/1994, pp. 535-536.

24 HEREDERO HIGUERAS, Manuel, "Informática: Leyes de Protección de Datos" (nota preliminar), Madrid, Presidencia del Gobierno y MAP, 1988, pp. 19-21.

25 Tribunal Constitucional Alemán, sentencia de 15 de diciembre de 1983, publicada en BJC Boletín de Jurisprudencia Constitucional, número 33, Enero 1984, Publicaciones de las Cortes Generales, Madrid. Trad. Manuel Daranas. pp. 126-170.

> *"... este derecho a la autodeterminación informativa no está, sin embargo, garantizado sin límites... el individuo tiene pues que aceptar en principio determinadas limitaciones de su derecho a la autodeterminación informativa en aras del interés preponderante de la comunidad".*

Con posterioridad, en sucesivos pronunciamientos los tribunales hispanos han acogido el derecho a la autodeterminación informativa o libertad informativa. Así en 1993, el Tribunal Constitucional, al pronunciarse sobre la solicitud formulada por un ciudadano a una repartición pública para ser informado y acceder a los datos referidos a su persona que ésta albergaba, aplicando el Convenio de Estrasburgo de 1981 como elemento interpretativo,[26] reconoció el derecho a controlar los datos insertos en un programa informático que a su titular compete, al cual denominó "libertad informática", aun cuando asoció tal derecho a la intimidad del actor.[27] En cambio, en sucesivas sentencias emitidas durante 1998, el mismo Tribunal Constitucional, ante el empleo desviado de datos personales correspondientes a afiliación sindical, reconoció...

> *"... un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática... un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona..., pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos".*[28]

Como puede apreciarse, para el Tribunal Constitucional de España la facultad de controlar la información que concierne a determinada persona no sólo resguarda el derecho a la intimidad, sino que constituye un derecho fundamental autónomo y, a su vez, una garantía adjetiva, mediante la cual se preservan los derechos fundamentales frente a los ataques de que puedan ser objeto mediante la tecnología informática; lo cual conduce a sostener que este nuevo derecho permite realizar una lectura en "clave informática" de los derechos fundamentales.[29]

Constitucionalmente, el derecho a la autodeterminación informativa ha merecido reconocimiento, con mayor o menor precisión y extensión, en diversas cartas fundamentales; así lo es en los artículos 35 de la Carta Fundamental de Portugal de 1976, 18 de la Constitución de España de 1978, 10 de la Constitución de los Países Bajos de 1983, 5 de la Constitución de la República Federativa de Brasil de 1988, 59 de la Constitución de Hungría de 1989, 3 de la Carta Fundamental de Suecia de 1990, 5 de la Constitución Política de Colombia de 1991, 2 de la Constitución Política del Perú de 1993, 43 de la Constitución de la Nación Argentina de 1994, 10 de la Carta Fundamental de Finlandia de 1999, entre otras.

En cambio, la autodeterminación informativa o libertad informativa carece de reconocimiento en tratados internacionales sobre derechos humanos, pues la mayor parte de ellos

26 Se refiere al Convenio de 28 de enero de 1981, del Consejo de Europa para la protección de las personas en lo referente al tratamiento automatizado de los datos personales.

27 Tribunal Constitucional de España, sentencia 254/1993, de 20 de julio de 1993.

28 Tribunal Constitucional de España, sentencia 124/1998, de 15 de junio de 1998. Este pronunciamiento, con matices, se encuentra en las sentencias 11/1998, de 13 de enero de 1998; 105/1998, de 18 de mayo de 1998. En iguales términos, LUCAS MURILLO DE LA CUEVA, Pablo, "Informática y Protección de Datos Personales", Cuadernos y Debates Nº43, Centro de Estudios Constitucionales. Madrid, 1993, p. 33.

29 ÁLVAREZ-CIENFUEGOS SUÁREZ, José María, "La Defensa de la Intimidad de los Ciudadanos y la Tecnología Informática", Editorial Aranzadi. Pamplona, 1999, pp. 15 a 22.

fueron aprobados con anterioridad a que se suscitaran problemas jurídicos en relación con el tratamiento automatizado de datos personales; de hecho, su debate internacional tiene inicio recién en 1968, durante la celebración de la Conferencia Internacional de Derechos Humanos de Teherán, organizada por Naciones Unidas, en la cual se consideraron los límites que una sociedad democrática debía imponer para proteger los derechos humanos frente al creciente uso de la tecnología.

No obstante, las Naciones Unidas han emitido directrices aplicables al tratamiento de datos personales; se trata de los "Principios rectores para la reglamentación de los ficheros computarizados de datos personales", adoptados por la Asamblea General de la Naciones Unidas en su resolución 45/95, de 14 de diciembre de 1990. Más aun, recientemente la Unión Europea, al aprobar la "Carta de Derechos Fundamentales", ha contemplado, aunque sin referencia explícita a la categoría doctrinal y jurisprudencial, la libertad informativa entre aquellos.[30] En efecto, después de asegurar en su artículo 7 el derecho a la vida privada, consagra, como categoría autónoma, la libertad informativa en los siguientes términos:

> *"... la Unión reconoce los derechos, libertades y principios enunciados a continuación.*
> *Artículo 8. Protección de los bienes 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".*

Por su parte, la Organización de Estados Americanos se encuentra actualmente abocada a la elaboración de un anteproyecto de convención americana sobre autodeterminación informativa.[31]

Puede pues apreciarse que la construcción del derecho a la autodeterminación informativa, o libertad informativa si se prefiere, sigue los derroteros propios de los derechos fundamentales de nueva generación: surgen a raíz de la "liberties' pollution" de las categorías precedentes, se abren paso tímidamente entre la doctrina y jurisprudencia nacionales, para finalmente cristalizar su reconocimiento en disposiciones legales, llegando a constitucionalizar su contenido y aun inclusive a recibir acogida en instrumentos internacionales.

3. Las Leyes de Protección de Datos

Las primeras leyes sobre protección de las personas frente al tratamiento automatizado de sus datos se remontan a la primera mitad de la década de los setenta; hoy, todos los Estados

[30] Carta de Derechos Fundamentales de la Unión Europea, proclamada por el Parlamento Europeo, el Consejo y la Comisión, en Niza el 7 de diciembre de 2000.

[31] Anteproyecto de Convención Americana sobre Autodeterminación Informativa, Organización de Estados Americanos, [en línea] [consulta e impresión: 16 noviembre 2002] <http://www.oas.org/en/prog/dil/areportic/castellano/pdfs/pagi23.pdf>.

miembros de la Unión Europea disponen de ellas; son varios los Estados americanos que también las han adoptado, o bien se encuentran en proceso de hacerlo; existen asimismo países en Asia y Oceanía que cuentan con ellas. En fin, se trata de un fenómeno normativo que progresivamente abraza las diversas latitudes del globo, y cuyo desarrollo está irremediablemente asociado a la creciente capacidad de almacenamiento y recuperación de la información contenida en el equipamiento informático, así como al extensivo uso de la informática y las telecomunicaciones.

Antes de examinar los diversos mecanismos de control previstos en el derecho comparado y las modalidades que asumen en los diversos países, parece necesario describir siquiera someramente los rasgos fundamentales de la legislación en que se inserta cada uno de ellos, oportunidad en que podremos apreciar la evolución experimentada por las leyes sobre protección de las personas frente al tratamiento de datos personales y, particularmente, la progresiva diversificación de los medios de que éstas se han prevalido para efectos de asegurarse del debido cumplimiento de sus previsiones.

En un primer período, cuando el número y costos asociados al funcionamiento de equipamiento computacional suponían su empleo sólo por grandes reparticiones públicas, tiene lugar la promulgación de la primera legislación en la materia. Así, en 1970 se promulga la Datenschutz, ley sobre tratamiento de datos personales del Land de Hesse, en la República Federal de Alemania, mediante la cual se pretendía brindar protección a las personas naturales ante la amenaza que representaba el tratamiento informatizado de datos nominativos por las autoridades y administraciones públicas del Estado, los municipios y entidades locales rurales, así como las demás personas jurídicas de derecho público y agrupaciones sujetas a la tutela estatal. A efectos de asegurar el cumplimiento de sus previsiones, la ley creaba el Comisario de Protección de Datos, al cual garantizaba independencia para el desempeño de sus funciones, cuales eran velar por la observancia de los preceptos de la propia ley y cuantos otros hicieren referencia al trato de los datos de los ciudadanos.

Posteriormente, cuando ya se contaba con una serie de disposiciones federales y territoriales que regulaban el tema, con pretensiones de generalidad o cierta especificidad, se dicta la Bundesdatenschutzgesetz, Ley Federal de Protección de Datos de la República Federal Alemana de 1977, en la cual se establece una normativa general de principios susceptibles de ser aplicados subsidiariamente a otros ámbitos o contextos, lo cual explica que acuda con frecuencia al empleo de conceptos jurídicos indeterminados y se cuide de no entrometerse en competencias que excedan las del gobierno federal.

La Ley Federal de Protección de Datos de 1977 contempla las disposiciones generales, cuyo objeto es evitar el detrimento de intereses dignos de protección de las personas naturales afectadas por el tratamiento automatizado de datos que le conciernen efectuados por el sector público y privado; entre sus disposiciones se observan diversas innovaciones, posteriormente acogidas por otras legislaciones, tales como el "comisario de protección de datos", la concesión a los titulares de datos del "derecho de bloqueo", y la tipificación de ilícitos penales e infraccionales asociados al tratamiento de datos. Además, impone a los entes que procesen datos la adopción de medidas técnicas y de organización necesarias para garantizar la observancia de la ley, las que precisa en anexo a la misma.

La ley, que establece regímenes jurídicos paralelos para el tratamiento de datos por el sector público y privado, fija también un sistema de control que atiende a tal distingo: respecto de los organismos públicos, impone a las diversas entidades de la administración federal la obligación de velar por el cumplimiento de la legislación y dictar disposiciones administrativas que regulen la aplicación de la ley en su respectivo ámbito de competencias y, a su vez, contempla una autoridad de control llamada a velar por la observancia de la misma y otras disposiciones aplicables a la protección de datos: el Comisario Federal de Protección de Datos.

En cambio, en cuanto al tratamiento de datos por entes no públicos, la ley acude al denominado comisario de protección de datos y las autoridades de tutela estatal. El primero debe ser nombrado por cada entidad que elabora datos personales y depende de ella, aun cuando no queda sujeto a sus instrucciones en el desempeño de su cometido, cual es velar por la observancia de la legislación relativa a la protección de datos; en tanto que la autoridad de tutela es fijada por los gobiernos de los Estados y le compete velar por la observancia de la Ley de Datos y demás disposiciones sobre protección de datos previstas dentro del ámbito de aplicación a los privados, aunque sólo a requerimiento del afectado.

También responde a este período la Data Lag 1973/289, por la cual Suecia imponía un sistema de registro abierto para publicitar los bancos de datos personales relativos a personas físicas realizados por medios automatizados, los que debían ser previamente autorizados para funcionar, asociado a una autoridad de control –la Datainspektionen, expresión del Ombudsman proyectado al tratamiento de datos– que vela por el respeto de la ley, con facultades inspectoras, normativas y procesales para requerir la aplicación judicial de sanciones.[32]

Como su homónima alemana, la Data Lag 1973/289 contemplaba un extenso catálogo de ilícitos sancionados penalmente con penas alternativas de multa y privativas de libertad; mientras que, tratándose del titular de los datos registrados, brindaba un escaso reconocimiento de derechos.

El férreo control previsto en la normativa sueca, por lo demás posteriormente asumido por la mayor parte de las experiencias del derecho comparado, le ha valido a Suecia el calificativo de modelo de heterocontrol. Con todo, algunas de sus trabas, tal como aquellas concernientes a la autorización previa al funcionamiento de bases de datos han debido ser mitigadas, mediante la adopción de un sistema de notificación e inscripción registral, siempre de responsabilidad de la autoridad de control nacional.

Esta primera legislación se caracterizó por centrar la protección en una reglamentación de las bases de datos, imponiendo ciertas restricciones a su constitución, tales como sistemas de autorización, previa inspección, etc. Además, en ella se contemplan entidades de naturaleza administrativa encargadas de velar por el cumplimiento de la normativa, con facultades de fiscalización tanto a la época de constitución de la base, como durante su operación.

[32] La Inspección de Datos junto con controlar el cumplimiento de la Ley de Datos, supervisa a las autoridades, compañías, organizaciones e individuos respecto de la Ley de Recuperación de Deudas de 1974, que reglamenta el tratamiento de datos con motivo de las acciones destinadas a obtener el cumplimiento de obligaciones de dinero, y la Ley de Informaciones Crediticias de 1973, que regula el tratamiento de datos por agencias de calificación de crédito.

Los progresos habidos en la informática y la creciente capacidad de almacenamiento de información, dieron lugar a una segunda generación de leyes, que fijaron menos trabas para la constitución de bases de datos, pero, en contrapartida, confirieron un abanico de facultades al titular de los datos a fin de velar por aquellos que le conciernen: información, acceso, rectificación y cancelación. Además, en ellas existe una preocupación adicional por brindar garantía ante el tratamiento de los denominados "datos sensibles", aquellos que por su naturaleza suponen un riesgo en su tratamiento, ya porque lesionan la intimidad de la persona, o bien porque le exponen a prácticas discriminatorias. Es el caso de la Privacy Act de Estados Unidos y la Ley relativa a la Informática y Libertades de Francia.

La exposición de motivos de la Privacy Act de 1974 manifiesta que su objetivo es proteger la privacidad de los individuos identificados en sistemas de información llevados por entes y órganos federales –por excepción alcanza al sector privado, cuando se encuentra vinculado contractualmente al público para el tratamiento de datos por su encargo–, mediante la regulación de la captación, conservación, uso y difusión de información por éstos, prescindiendo del soporte en que se contiene, de modo que la ley resulta aplicable sea que las operaciones de tratamiento se realicen por medios informáticos o manuales.

La ley asegura que la revelación de los datos –la Privacy Act habla de registros en este caso– por el órgano de la administración federal podrá tener lugar sólo mediando petición o consentimiento del individuo a quien conciernen, salvo excepciones fundadas en necesidad de orden público. Se reconoce al titular derecho de acceso, que incluye el detalle de las revelaciones del registro. Asimismo, el órgano debe asegurar el acceso del individuo a los registros que le conciernen, así como una copia de ellos y permitirle solicitar la modificación de ellos, en su caso. Igualmente, ha de franquear al individuo concernido en el registro la revisión administrativa de la negativa de rectificación e instruirle de las disposiciones aplicables a la revisión judicial de tal decisión.

Por su parte, la Loi n.º 78–17 du janvier, relative à l'informatique, aux fichiers et aux libertés, adoptada en Francia en 1978, como su nombre ya lo anticipa, ha procurado garantizar el empleo de la informática al servicio de los ciudadanos, de manera que ella no importe un atentado a la identidad humana ni a los derechos humanos, ni a la vida privada ni a las libertades individuales o públicas, para tales fines el texto originario reglamentaba el tratamiento automatizado de datos personales referidos a personas naturales realizado por personas naturales o jurídicas de derecho público y privado, si bien admite la aplicación parcial de sus disposiciones al tratamiento mecanográfico de datos nominativos.

La Ley 78–17 contempla una extensa regulación de los derechos que se confieren a la persona concernida por los datos: el ejercicio del derecho de acceso queda condicionado al abono de una tasa fijada reglamentariamente, cuyo importe es devuelto en caso de modificación del registro, además se concreta en el suministro de información inteligible para el afectado; en su caso, el titular podrá ejercer los derechos de rectificación y cancelación y, de negarse el organismo tratante, recaerá la carga de la prueba en éste. Con todo, la ley impone al organismo la corrección de los registros de oficio, así como la notificación a terceros a quienes se hubieren transmitido los datos modificados. La ley impone el ejercicio del derecho de acceso por medios indirectos en dos hipótesis: la primera, tratándose de datos médicos, deberá

procederse por mediación de un profesional de la medicina y, en el caso de datos que afectaren la seguridad del Estado, defensa o seguridad públicas, se procede a través de la Comisión. Además, la ley innova al prohibir la adopción de decisiones judiciales, administrativas o privadas respecto de las personas fundadas en un tratamiento automatizado de los datos que le conciernen y, más aun, confiere derecho a toda persona para conocer e impugnar las informaciones y lógicas de tratamiento de datos cuyos resultados se invocaren en su contra.

La ley establece un verdadero catálogo con infracciones y sanciones de naturaleza penal, figuras que son sancionadas con penas privativas de libertad y multas, acumulativa o alternativamente según los casos; además, se faculta al tribunal para imponer la publicación del fallo.

A diferencia de la legislación estadounidense, y tal cual sucede con la legislación sueca y alemana, la ley francesa prevé un órgano de control, si bien representativo e interpoderes, la Commission Nationale de l'Informatique et des Libertés, encargado de velar por su aplicación, recibir las reclamaciones de los afectados y dotado de potestad reglamentaria, cuyo ejercicio ha garantizado la perdurabilidad normativa.[33]

En cierta forma estas legislaciones representaron un giro en la protección, desde que pasaron a centrar la misma de la reglamentación de las bases de datos a los datos en sí, diseñando regímenes jurídicos diferenciados según su naturaleza, amén de conferir mayores derechos a los titulares de datos para velar por sí respecto de la legalidad en el tratamiento de aquellos que les conciernen.

Ya ante el uso generalizado de equipos computacionales y la insuficiencia de una garantía limitada a los datos sensibles, desde que la telemática –esto es, la transmisión de información automatizada mediante el empleo de medios de telecomunicación– incorpora prácticas de recuperación y cruce de información sin precedentes, con el consiguiente riesgo de menoscabo para los derechos fundamentales, la protección de los datos personales se extiende a la dinámica de uso o funcionalidades asociadas a ellos, con especial énfasis en precaver los riesgos involucrados en la transmisión internacional de datos personales.

Responde a esta orientación el Convenio 108 adoptado por la Comunidad Económica Europea en 1981, primer instrumento internacional que procura reglar el fenómeno del tratamiento automatizado de datos correspondientes a personas naturales desde una perspectiva que trasciende a la legislación interna y cuyo contenido informará diversas legislaciones europeas originadas durante la década de los ochenta, con miras a disponer de una normativa

[33] Para una brevísima reseña comparativa de la legislación francesa, cf. BIBENT, Michel, "Informática, Personas y Libertades. El proyecto de ley español y la experiencia francesa", en Encuentros sobre Informática y Derecho, Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 1992 – 1993, pp. 53 – 62.

El texto de la ley permaneció inalterable por más de una década, siendo modificado posteriormente en diversas ocasiones a fin de trasponer a las disposiciones de derecho interno la normativa comunitaria, esto es, el Convenio 108 y la Directiva 96/45/CE. Para efectos de esta revisión hemos cotejado el texto original de la ley con el actualmente vigente consolidado por la Commission Nationale de l'Informatique et des Libertés de fecha 16 de mayo de 2002.

comunitaria para hacer frente a una previsible proliferación de leyes nacionales que en su día hicieran difícil su armonización.[34]

El ámbito de aplicación del Convenio era comprensivo del procesamiento de datos –desde su almacenamiento hasta borrado inclusive– verificado en el sector público y privado, con tal que él se refiriese a personas naturales y fuese realizado por medios informáticos; sin embargo, el Convenio admitía que los Estados miembros facultativamente extendiesen sus disposiciones a agrupaciones de personas con o sin personalidad jurídica, así como a los datos personales que fueren objeto de tratamiento no automatizado.

El Convenio 108 también se ocupa del flujo internacional de datos de carácter personal, abogando por disponer de una "protección equivalente" en la legislación aplicable a quienes participaban de la transmisión, a efectos de evitar que ellas dieran lugar a soslayar la aplicación de la normativa de los Estados partes.

Especial atención presta el Convenio 108 al auxilio mutuo que impone a los Estados partes, para cuyos efectos supone la existencia de una o varias autoridades en el derecho interno de cada uno de ellos, las que encauzan la cooperación institucional entre las partes, así como la asistencia a los interesados residentes en el extranjero en el ejercicio de sus derechos.

Los Estados partes del Convenio se obligaban a adoptar en su derecho interno las medidas necesarias para dar efecto a los principios fundamentales de protección de datos a que adscribía el instrumento. Así sucedió con Reino Unido y España, según apreciaremos más adelante.

[34] La necesidad de disponer de una normativa comunitaria en la materia venía siendo sostenida por el Parlamento Europeo desde 1973, cuando se instó al Consejo a explicar si contaba con alguna política al respecto y en 1974 el mismo Parlamento elaboró un estudio que proponía el diseño de una Directiva en la materia.

Diversas comunicaciones dirigió el Parlamento Europeo a la Comisión, sin resultados satisfactorios, hasta que en 1979 el Parlamento adopta una Resolución sobre la materia y una serie de Recomendaciones dirigidas ambas a los restantes órganos comunitarios, en las cuales llamaba la atención sobre una serie de circunstancias que hacían patente la necesidad de que la Comisión elaborase "una propuesta de Directiva tendente a armonizar las legislaciones en materia de protección de datos a un nivel que ofrezca el máximo de garantías a los ciudadanos de la Comunidad" y delineaba los rasgos fundamentales que debían contemplarse en tal normativa, su aplicación a ficheros manuales y automatizados, referentes a datos de personas naturales o jurídicas, e inclusive de simples agrupaciones de personas, con un control previo al funcionamiento de las bases de datos. Más aun define y perfila el estatuto de una autoridad de control de protección de datos, y anticipa algunos criterios para las transferencias internacionales de datos. Una buena parte de las propuestas cristalizarán años más tarde en la Directiva 95/46/CE. Cf. Resolución de 8 de mayo de 1979, del Parlamento Europeo, sobre la protección de los derechos de las personas ante el desarrollo de los progresos técnicos en el ámbito de la informática (DOC número 140, de 5 de junio) y Recomendaciones del Parlamento a la Comisión y al Consejo, de conformidad con el parágrafo 10 de la propuesta de Resolución referente a los principios en los que deberán inspirarse las normas comunitarias en materia de protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática.

Por su parte, la Comisión no sostuvo la idea de una Directiva, por estimar que la evolución legislativa aún no estaba madura para emprender tal desafío, a lo cual se agregaban ciertas dudas y reservas en cuanto a la competencia de la Comunidad para intervenir en este ámbito. Cf. HEREDERO HIGUERAS, Manuel. "La Directiva Comunitaria de Protección de Datos de Carácter Personal", Editorial Aranzadi, Pamplona, 1997, p. 21 – 23.

Antes bien, la Comisión recomendó la suscripción por los Estados miembros del Convenio 108, el cual estimaba suficiente para introducir un nivel de protección uniforme en cuanto a la protección de los datos. Cf. Recomendación de la Comisión 81/679/CEE, de 29 de julio de 1981 relativa al Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Por su parte, la "Recomendación relativa a las directrices aplicables a la protección de la vida privada y a los flujos transfronteras de datos personales", adoptada por el Consejo de Ministros de la Organización de Cooperación y Desarrollo Económicos (OCDE) el 23 de septiembre de 1980, también formula proposiciones que en lo sustancial establecen principios a que debe sujetarse el tratamiento de datos susceptibles de ser adoptados en el derecho interno, siendo una buena parte de ellas coincidentes con las contempladas en el Convenio 108, puesto que fueron unos mismos los especialistas que concurrieron a la redacción de uno y otro documento. E, igualmente, es el caso de los "Principios rectores para la reglamentación de los ficheros computarizados de datos personales", adoptados tardíamente por la Asamblea General de la Naciones Unidas en su resolución 45/95, de 14 de diciembre de 1990, que con el propósito de facilitar su incorporación en la normativa interna de cada Estado, constituyen directrices generales y flexibles, para cuya elaboración se han tenido presentes las fijadas por la OCDE.[35]

La impronta del Convenio 108 recae en la Data Protection Act de 1984 adoptada por el Reino Unido tras una extensa reflexión legislativa, que se remonta a las postrimerías de la década del sesenta; sucesivas comisiones estudiaron la proyección de la privacy y el tratamiento de los datos personales incorporados en sistemas informáticos, así como las diversas medidas aplicables a efectos de controlar el cumplimiento de la legislación que se adoptara en la materia, el resultado de algunos de tales informes fue posteriormente acogido por la normativa con que la Comunidad Europea ha emprendido la regulación del tema, así por ejemplo el Lindop Report anticipó buena parte de las medidas promovidas por la Directiva 95/45/CE. [36]

La Data Protection Act 1984 constituye una legislación compleja, en la cual se conjugan disposiciones generales, con normas relativas a la inscripción y vigilancia de los "usuarios de datos y de las oficinas de servicios informáticos" –denominación con que se califica a los responsables de base o registro de datos–, derechos de las personas concernidas, un atiborrado sistema de excepciones y régimen de recursos; a lo anterior se adicionan diversos anexos: sobre los principios aplicables al tratamiento y su interpretación; sobre el procedimiento de recursos; y sobre la entrada y registro de lugares cerrados.

En síntesis, la demorada legislación inglesa de 1984 sobre tratamiento de datos personales, extiende sus previsiones al sector público y privado, aun cuando se limita a los datos objeto de un procesamiento automatizado. Ahora bien, en cuanto a los mecanismos de control, si bien contempla la adopción de códigos de conducta y el recurso a reglamentación

35 Para una sucinta reseña de ambos documentos, cf. igualmente EKMEKDJIAN, Miguel Angel y PIZZOLO, Calogero, op. cit., pp. 42 – 47, 59 – 62.

Los principios fueron adoptados por Naciones Unidas recién en 1990, no obstante haber reparado ya en la Conferencia de Teherán de 1968 en los riesgos que los medios informáticos estaban representando para la democracia. Sin embargo, tal alerta no concitó respaldo durante las décadas de los setenta y ochenta por parte de los Estados correspondientes al tercer mundo, al bloque de países socialistas y las dictaduras latinoamericanas; sólo los países desarrollados alentaron los procesos normativos y, a partir de la década de los noventa, se han sumado a ellos otros países, de ahí el retraso de Naciones Unidas en la adopción de recomendaciones al respecto.

36 Para una revisión del proceso que decantó con la Data Protection Act de 1984, vid. LOSANO, Mario, "Los orígenes del 'Data Protection Act' inglesa de 1984", en Cuadernos y Debates, Centro de Estudios Constitucionales, Madrid, 1989, núm. 21, pp. 9 – 60. Puede consultarse igualmente EKMEKDJIAN, Miguel Angel y PIZZOLO, Calogero, op. cit., pp. 12 – 21, 35 – 37.

especial, ellos se engarzan con las funciones de una autoridad de control, el Registrer, a quien confía el registro de los bancos de datos, el control sobre el cumplimiento de la normativa, la recepción de afectados, la asistencia a los interesados y la aplicación de medidas cautelares, a lo cual adiciona un Data Protection Tribunal, que obra como tribunal de reclamación respecto de las decisiones tomadas por el primero, sin perjuicio de los recursos ante los tribunales ordinarios. Para efectos de aplicación del Convenio 108, el Registrer hace las veces de la entidad que cursa la cooperación internacional.

Es también la situación de la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de carácter personal (LORTAD), adoptada por España en 1992, que constituiría la piedra angular sobre la cual se diseñó nuestra Ley 19.628.[37]

Si bien la Constitución Española de 1978 asegura en su artículo 18 inciso cuarto 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", esta temprana declaración constitucional no se concretó en la adopción de una pronta legislación sobre protección de datos personales, pese a que diversos proyectos se sucedieron a partir de 1984 para reglar la materia.[38]

No será sino hasta 1992 que España se dotará de un cuerpo normativo que regle el tratamiento de datos personales, la antes mencionada LORTAD.[39] Ya antes, había ratificado el Convenio 108, pese a lo cual había retardado ostensiblemente la transposición de sus principios en el derecho interno, proceso acelerado por los Acuerdos de Schengen de 1985 sobre supresión gradual de controles en las fronteras comunes, que contempla el funcionamiento del llamado Sistema de Información Schengen, complejo y eficaz sistema de tratamiento de datos personales de que se sirve Europa, especialmente para fines policiales y de seguridad, y que supone que todos los Estados partícipes cuenten con una normativa interna que brinde un nivel de protección cuando menos igual al previsto en el Convenio 108.[40]

37 Para una revisión sobre el proceso histórico de la legislación sobre protección de datos personales en España, vid. SUÑÉ LLINÁS, Emilio, "Tratado...".

38 Sobre las primeras iniciativas parlamentarias en la materia, cf. SUÑÉ LLINÁS, Emilio, "Tratado...", pp. 73 y ss.

39 Del 29 de octubre de 1992, publicada en el BOE de 31de octubre de 1992, núm. 262. Para una revisión colectiva de la LORTAD, Cf. "Informática y Derecho", Director Valentín Carrascosa. Cuadernos elaborados por la UNED, Centro Regional de Extremadura. Ed. Aranzadi., número 6 – 7, 1994. Entre nosotros, para una revisión de la primera legislación española en la materia, cf. FERNÁNDEZ SEGADO, Francisco, "El régimen jurídico del tratamiento automatizado de los datos de carácter personal en España", en Ius et Praxis, Universidad de Talca, Facultad de Ciencias Jurídicas y Sociales, Año 6 N°2, 2000, pp. 33-69.

40 SUÑÉ LLINÁS, Emilio, "Tratado...", pp. 84 y ss. En el mismo sentido, GARCÍA AGUILAR, Nicolás, "Origen y significado del Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal", en Revista Internauta de Práctica Jurídica, Núm. 2 (mayo-agosto, 1999). Para una revisión del marco jurídico del tratamiento de datos para fines policiales a nivel interno y comunitario, con especial énfasis en el Sistema de Información Schengen y el Convenio Europol, Cf. MARTÍNEZ MARTÍNEZ, Ricard, op. cit., en especial pp. 277–319.

Con todo, ante la ausencia de legislación interna, el Tribunal Constitucional, si bien se resistía la aplicación directa del Convenio 108, apuntaba a admitir su empleo para efectos de integración normativa, ante los vacíos que manifestaba la legislación interna. Tribunal Constitucional de España, sentencia 254/1993, de 20 de julio de 1993.

Pues bien, atendida la demora con que el país peninsular emprendió la adopción de una ley en la materia, ha podido beneficiarse de la experiencia legislativa extranjera, a la par de servirse de las propuestas preparativas de la Directiva 95/46/CE, si bien es el Convenio 108 el que informa una buena parte de las opciones adoptadas por el legislador, quien emprende la transposición del mismo al derecho interno.[41]

La LORTAD extendió su ámbito de aplicación a los ficheros automatizados, tanto de sectores público y privado, con una serie de excepciones que se encarga de precisar, y circunscribía su protección a los datos relativos a personas físicas. Se encargaba de enunciar los principios que informan la protección de los datos y los derechos que se conferían a los afectados, aspectos en los cuales no difería sustancialmente del Convenio.

A efectos de velar por el cumplimiento de la normativa, la LORTAD encomienda el control de su aplicación a un ente de derecho público independiente, al que denomina Agencia de Protección de Datos, a cuyo frente sitúa un Director, asesorado por un Consejo consultivo, órgano colegiado y compuesto por representantes institucionales de diversos poderes del Estado, el sector privado, las organizaciones de usuarios y consumidores, entre otros miembros; con todo, se admite la existencia de entidades de control creadas o gestionadas por las comunidades autónomas.[42]

La LORTAD contenía previsiones relativas a la transmisión internacional de los datos, punto en el cual trasponía el Convenio 108, optando por exigir que el país de destino proporcione un nivel de protección equivalente al español, aunque admitiendo la autorización de la Agencia de Protección de Datos cuando tal sistema no exista pero se ofrezcan garantías suficientes, junto con otras fundadas excepciones. Es también la mencionada Agencia la entidad encargada de gestionar la asistencia mutua exigible en virtud de la ratificación del Convenio 108 por España.

También se aprecia la impronta del Convenio 108 en la Ley de Datos de la República Federal Alemana de 1990, que cuenta con un largo trabajo preparatorio que trae por causa la declaración de inconstitucionalidad de la Ley de Censo de Población de 1982, lo que le ha conducido a relevar el rol del consentimiento del afectado en la materia.[43] Con todo, la ley no ha instaurado un sistema nuevo, antes bien responde a la misma sistemática de la Ley de Datos de 1977, la cual perfecciona o desenvuelve.[44]

41 Cf. HEREDERO HIGUERAS, Manuel, "La transposición de la Directiva 95/46/CE en el Derecho positivo español. Una segunda oportunidad", en Encuentros sobre Informática y Derecho, Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 1996–1997, p. 133, quien resalta también la influencia que tuvieron en las disposiciones de la LORTAD las leyes de datos personales de Alemania de 1990 y Francia de 1978.

42 A la fecha, sólo la Comunidad Autónoma de Madrid dispone de una autoridad de control propia, la Agencia de Protección de Datos de la Comunidad de Madrid.

43 En este sentido, HEREDERO HIGUERAS, Manuel, "Panorama General de la Legislación Mundial sobre Protección de Datos", en Encuentros sobre Informática y Derecho, Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 1992–1993, p. 20.

44 Un breve comentario, que precede a una traducción parcial del texto de la ley del mismo autor, Cf. HEREDERO HIGUERAS, Manuel, "La nueva ley alemana federal de protección de datos", en Boletín de Información, número 1630, año XLVI, 25 de marzo de 1992, Ministerio de Justicia, editado por Secretaría General Técnica, Centro de Publicaciones, Madrid, pp. 125–146.

La Ley de Datos de 1990 amplía el ámbito objetivo de tutela, al aplicarse tanto frente al tratamiento informatizado de los datos como al manual; confiere carácter irrenunciable a los derechos del afectado, para cuyo resguardo impone obligaciones a las entidades tratantes en relación con el Comisario Federal de Protección de Datos; establece responsabilidad objetiva, sin culpa, solidaria y con un límite indemnizatorio, frente a los perjuicios ocasionados por la elaboración automatizada de datos por organismos públicos; en cambio, cuando tal daño proviene de la elaboración efectuada por organismos no públicos, altera la carga de la prueba ante la controversia respecto del nexo causal de los perjuicios.

En cuanto a los medios de control, la ley conserva el Comisario Federal de Protección de Datos, como autoridad llamada a velar por la observancia de la misma y otras disposiciones aplicables a la protección de datos procesados por organismos públicos, regulación que en lo sustancial se ajusta a la precedente, con alguna precisión respecto de su ámbito de competencia y ejercicio de la misma. En cambio, tratándose del tratamiento de datos por los organismos no públicos, la ley introduce importantes enmiendas respecto de la autoridad de tutela, a la cual se permite ejercer sus facultades de oficio y adoptar medidas correctivas ante las irregularidades técnicas u organizativas descubiertas, las que pueden llegar inclusive a exigir el despido del comisario de protección de datos designado.

Sin embargo, con el transcurso del tiempo la eficacia del Convenio 108 se fue agotando, pues hasta entrada la década de los noventa no hubo nuevas ratificaciones y sólo se adoptaron tres nuevas leyes nacionales en la materia.[45] Por otro lado, la sola ratificación no mostraba eficacia alguna, tal como sucedía con España que pese a haber ratificado en 1984 no procuró trasponer las normas del Convenio a su legislación interna sino hasta 1992. Estimando pues la Comisión que el Convenio resultaba poco coactivo, habiéndose dilucidado las dudas por lo concerniente a la competencia de la Comunidad en la materia y visualizándose la concreción de un mercado interior con el consiguiente incremento en la circulación de los datos personales en su seno, la Comisión asumió la elaboración de una Directiva Comunitaria al respecto.[46]

4. LA DIRECTIVA COMUNITARIA 95/46/CE

La necesidad de brindar protección a las personas tanto frente al tratamiento automatizado como manual de sus datos, pues la exclusión de este daba lugar a riesgos graves de elusión en el cumplimiento de las normas, así como la imperiosidad de potenciar las autorida-

45 La carencia de un nivel equivalente de protección de los datos personales entre los países europeos venía generando inconvenientes para la aplicación de proyectos que supusieran la trasferencia internacional de tales datos, así para SOSENET (Social Security Network Programme) que pretendía la coordinación de los servicios de seguridad social europeos, cf. ALONSO BLAS, Diana, "El futuro de la protección de datos a nivel europeo", en Encuentros sobre Informática y Derecho, Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 1995–1996, pp. 163–176.

46 HEREDERO HIGUERAS, Manuel. "La Directiva Comunitaria...", op. cit., pp. 23–30, quien destaca que la propuesta de Directiva inicialmente no se concebía tanto como un texto destinado a brindar protección a las personas frente al tratamiento de sus datos, como uno llamado a aproximar las legislaciones de los países integrantes de la comunidad con miras a obtener un nivel de protección "equivalente" que asegurase el desarrollo de un creciente intercambio de información entre los Estados miembros previsible para el funcionamiento del mercado interior.

des previstas en la legislación interna de los Estados, y, frente al incremento del flujo transfronterizo de datos personales, asegurar un nivel de protección adecuado entre los diversos Estados, la Unión Europea, considerando las insuficiencia y falencia que progresivamente mostró el Convenio 108 para hacer frente a la creciente circulación de datos nominativos en el mercado interno comunitario, adopta en 1995 la Directiva 95/46/CE.[47]

La Directiva 95/46/CE establece condiciones generales de licitud en el tratamiento de los datos, en que amplía y detalla en diversos aspectos las previsiones del Convenio 108, dejando a los Estados miembros un margen de maniobra del que podrán servirse para precisar en el derecho interno tales condiciones. Al efecto, la Directiva impone plazo a los Estados miembros para la transposición de sus previsiones en el derecho interno.[48]

La Directiva 95/46/CE se circunscribe al tratamiento de datos personales correspondientes a personas naturales, excluyendo explícitamente de sus previsiones a las personas jurídicas, extiende sus prescripciones al tratamiento verificado por el sector público y privado, tanto por medios automáticos como manuales. A diferencia del Convenio 108, la Directiva amplía su protección a cualquier operación o conjunto de operaciones aplicadas a datos personales, desde el instante mismo de su recogida. Asimismo, la Directiva innova introduciendo normas para dirimir los conflictos de legislación originados en la materia, haciendo prevalecer la ley del Estado en que se sitúa el establecimiento del responsable de tratamiento y, en su defecto, aquél en que se ubiquen los medios empleados.

Respecto de las condiciones generales de tratamiento, la Directiva insiste en la aplicación de principios relativos a la calidad de los datos, esta vez, a diferencia de cuanto acontecía con el Convenio 108, imponiendo a los responsables del tratamiento la obligación de cumplir con ellos; persiste en que la legitimidad del tratamiento de datos descansa en el consentimiento del interesado, aun cuando admite una extensa gama de excepciones a tal regla; tal cual el Convenio 108, contempla categorías especiales de tratamiento (datos sensibles), respecto de los cuales en principio aboga por su prohibición, si bien establece un sistema reglado de excepciones. En general, la Directiva, sin desconocer el principio del consentimiento, a juzgar por el número de sus excepciones, parece hacer descansar la rigurosidad del tratamiento en el respeto al principio de la finalidad, al cual acude con miras a circunscribir la legitimidad de las operaciones que recaen sobre los datos.

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

Para una excelente síntesis sobre el proceso comunitario que condujo finalmente a la elaboración de la Directiva 95/46/CE y un minucioso análisis de ésta, vid. HEREDERO HIGUERAS, Manuel. "La Directiva Comunitaria...", op. cit, passim.

48 Sobre los efectos de la ausencia de transposición de la Directiva al derecho interno de los Estados miembros, Cf. DUMORTIER, Jos, "Aplicación de la Directiva de Protección de Datos en Bélgica", en Encuentros sobre Informática y Derecho, Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 1996 – 1997, pp. 51 – 74.

Sobre la eficacia de la Directiva en relación con el derecho interno de los Estados partes, el Tribunal de Justicia de las Comunidades Europeas, en sentencia de fecha 20 de mayo del 2003, recaída en los casos C-465-00, C-138/01 y C-139/01 ha resuelto, en particular, que "Los artículos 6, apartado 1, letra c), y 7, letras c) y e), de la Directiva 95/46 son directamente aplicables, en el sentido de que un particular puede invocarlos ante los órganos jurisdiccionales nacionales para evitar la aplicación de normas de Derecho interno contrarias a dichas disposiciones".

En cuanto a los derechos del interesado, la Directiva regla el derecho a información, sea que los datos se recaben de él o de terceros, fijando el contenido mínimo de tal comunicación; reconoce el derecho de acceso al interesado, el que proyecta inclusive al conocimiento de la lógica que subyace al tratamiento automatizado de los datos que conciernen, resguardando el menoscabo al secreto de los negocios, la propiedad intelectual y los derechos de autor; de igual forma, reconoce los derechos de rectificación y cancelación, e incorpora los derechos de bloqueo y notificación a terceros a quienes se haya comunicado los datos ante la rectificación, supresión o bloqueo de los mismos; con todo, admite ciertas excepciones y limitaciones a los derechos de acceso e información, así como a determinadas obligaciones del responsable del tratamiento, si bien estableciendo cortapisas para las mismas. Del mismo modo, reconoce el derecho del interesado a oponerse a ciertos tratamientos de datos que le conciernen y adiciona, al catálogo de derechos del interesado, la prohibición de que éste sea sometido a decisiones con efectos jurídicos fundadas únicamente en un tratamiento automatizado de sus datos, aun cuando con ciertos matices.

Con el propósito de asegurar la publicidad de los fines del tratamiento y de sus principales características, así como para efectos de fiscalización, la Directiva establece procedimientos de notificación a la autoridad de control por el responsable de tratamiento, sin perjuicio de ciertas exenciones y simplificaciones, a la par de ciertos casos que hacen necesario un examen previo de la autoridad de control o del encargado de protección de los datos en cooperación con aquélla. Tales antecedentes, al igual que los códigos de conducta que se adopten, deben ser publicitados por la autoridad de control mediante un registro público de los tratamientos.

La Directiva impone a los Estados miembros la obligación de velar por el respeto de las medidas técnicas y de organización apropiadas para garantizar un nivel de seguridad adecuado de tratamiento, fijando pautas para su determinación. Asimismo, exige la Directiva la adopción de un recurso judicial por las legislaciones nacionales, para hacer se respeten los derechos de los interesados conculcados por el responsable de tratamiento, sin perjuicio del recurso administrativo que pueda interponerse ante la autoridad de control.

Una de las preocupaciones centrales de la Directiva es hacer frente a los riesgos aparejados al flujo transfronterizo de datos personales, admitiendo que tal transferencia se verifique con terceros países que garanticen un nivel de "protección adecuado", para lo cual habrá de apreciarse todas las circunstancias relacionadas con la transmisión o la categoría de transmisiones. En caso contrario, esto es, tratándose de terceros países que no ofrezcan tal nivel de protección, prohíbe la transferencia, salvo excepciones, entre las que contempla el ofrecimiento de garantías adecuadas por el responsable del tratamiento, para lo cual obliga a la adopción de procedimientos de negociación entre la Comunidad y los terceros países de que se trate.

Respecto de la autoridad de control, a diferencia de cuanto preveía el Convenio 108, la Directiva califica su creación en cada uno de los Estados miembros como elemento esencial en la protección de las personas frente al tratamiento de los datos nominativos; exige que ella ejerza sus funciones con plena independencia; le atribuye facultades de investigación, intervención y capacidad procesal, cualquiera sean las disposiciones de derecho nacional aplicables. Con todo, admite el control judicial de sus actos y le impone la obligación de publicar sus informes periódicamente. Asimismo, la Directiva insiste en la necesidad de que las autoridades de control de los Estados miembros se brinden ayuda mutua en el ejercicio de sus funciones. Finalmente, la Di-

rectiva contempla la creación del Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, órgano comunitario de carácter consultivo e independiente, integrado por las autoridades de control nacionales, que asesorará a la Comisión y contribuirá a la aplicación uniforme de las normas nacionales adoptadas en aplicación de la Directiva.

Con posterioridad, salvo en el caso de Francia, la legislación interna de diversos Estados miembros de la Unión, ha sido adecuada a los principios y definiciones que adopta la Directiva, de suerte que sus legislaciones internas han alcanzado un notable grado de homogeneización, aun cuando guardan peculiaridades que la propia Directiva tolera, al admitir un margen de maniobra en la transposición de sus disposiciones al derecho interno; así, por ejemplo, ha sucedido con Suecia, Inglaterra y España.[49]

Suecia aprobó la nueva Ley 1998/204 sobre Protección de Datos de Carácter Personal, mediante la cual transpone las disposiciones de la Directiva comunitaria, si bien el nuevo texto importa más que una mera readecuación del primero, ya que adopta la terminología de la normativa comunitaria, así como buena parte de la institucionalidad y disposiciones contempladas en ella. Entre otras, las concernientes a sus ámbitos –objetivo y subjetivo– de aplicación y disposiciones de derecho internacional privado; las excepciones relativas al consentimiento de la persona para el procesamiento de los datos que le conciernen; y, las reglas referentes a transferencia transfronteriza de datos.

En cuanto interesa a esta tesis, los mecanismos de control en la materia, la legislación de Suecia evidencia diversos progresos imputables a la impronta de la Directiva, tales como la diversificación de sus mecanismos de control, al admitir junto a la autoridad de control el recurso al denominado "representante de tratamiento", esto es un agente de control interno independiente que se vincula en el desempeño de sus labores con la mencionada autoridad, y, tratándose del flujo transfronterizo de datos, la admisión de medios contractuales con terceros países para obtener el resguardo de los derechos de los interesados. Con todo, la legislación hace descansar la eficacia de su normativa en el rol desempeñado por la autoridad de control, la Inspección de Datos.

Por su parte, la transposición de la Directiva en el derecho interno fue acometida por el Reino Unido mediante la aprobación de un nuevo marco jurídico en la materia, la Data Protection Act de 1998, que en lo sustancial mantuvo el sistema de protección antes descrito, si bien introdujo ciertas modificaciones que informan decisiones tales como extender el ámbito de aplicación de la legislación al tratamiento manual de datos personales, brindar protección desde la recogida misma de tales datos, contemplar normas para dirimir conflictos de legislación aplicable, e inclusive adoptar la terminología comunitaria. Sin embargo, las modificaciones de mayor relevancia introducidas por la legislación británica dicen relación precisamente con el objeto de esta investigación, a saber, los medios de control en el tratamiento de

[49] La Directiva preveía un término de tres años para que los Estados miembros de la Unión verificarán la transposición de sus previsiones al derecho interno; sin embargo, dicho plazo fue satisfecho sólo por cuatro Estados. No obstante, a la fecha, la reciente adopción de una nueva ley por Irlanda, deja tan sólo a Francia, no obstante las modificaciones introducidas a su legislación, en la incómoda posición de poner al día las disposiciones, para lo cual ha anunciado su intención de aprobar una nueva ley que aún no se ha adoptado. Cf. Comisión de las Comunidades Europeas, "Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)", Bruselas, 15 de mayo de 2003.

datos personales, fundamentalmente por cuanto admite el control por un técnico independiente –el data protection supervisor– y potencia las facultades de la nueva autoridad de control, el Data Protection Commissioner.

En España, Ley de Protección de Datos de Carácter Personal de 1999, LOPD, mantuvo en lo medular el sistema de protección diseñado por la LORTAD, actualizando sus disposiciones al trasponer la Directiva 95/46/CE al derecho interno español, a la par de verificar algunas precisiones respecto de aquélla.[50]

La LOPD insiste en cuanto a que la protección tiene lugar sólo respecto de las personas físicas, pero extiende su ámbito de aplicación a todo tratamiento de datos, se verifique por medios automatizados o no. Por otro lado, la ley extiende la calificación de datos especialmente protegidos a aquellos que revelen la afiliación sindical y creencias del afectado; consagra el derecho a no verse sometido a decisiones con efectos jurídicos con base sólo en un tratamiento de datos; respecto de los ficheros de titularidad pública, perfecciona la creación de ficheros y restringe la comunicación de datos entre administraciones, entre otras. En cuanto al movimiento internacional de datos, la LOPD precisa las circunstancias que permiten evaluar el carácter adecuado del nivel de protección ofrecido por terceros países de destino y, en aplicación de la Directiva 95/46/CE, acoge diversas excepciones a las normas de restricción de tal flujo de datos. Finalmente, por lo que toca a los mecanismos de control, a efectos de resguardar el debido cumplimiento de la ley, la Agencia de Protección de Datos parece consolidarse a través del proceso legislativo; con todo, se ha mejorado el régimen de recursos administrativos, extendido la facultad para adoptar códigos tipo y enriquecido el haz de derechos de que dispone el propio interesado para velar por su autodeterminación informativa.

Recientemente, la Comisión ha evacuado un primer informe sobre la transposición de la Directiva, basado en una amplia consulta efectuada durante 2002, el cual arriba a la conclusión que la Directiva ha logrado asegurar una fuerte protección hacia los datos personales movidos en la Unión. Sin embargo, los retrasos en la transposición por ciertos Estados miembros y las diferencias observadas en la aplicación de ciertas previsiones –en particular aquellas relativas a derecho aplicable, suministro de información a los interesados, notificación a autoridades de control, entre otros– han evitado que la economía de Europa consiga las ventajas a que apunta la Directiva. Para hacer frente a ellas, el informe propone un plan de trabajo destinado a reducir esas diferencias, basadas en la cooperación entre Estados miembros y la propia Comisión.[51]

En cuanto a la proyección de la Directiva, nos parece del caso acusar que, ante la evolución tecnológica, la Unión Europea ha adoptado igualmente la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, que sirviéndose de los principios desarrollados por la Directiva 95/46/CE les ha especificado para el sector de

[50] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. Nº 298. Martes 14 de diciembre de 1999).

[51] Cf. Comisión de las Comunidades Europeas, "Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)", Bruselas, 15 de mayo de 2003; y, también, "Analysis and impact study on the implementation of Directive EC 95/46 in Member States", disponible en http://europa.eu.int/comm/internal_market/privacy/lawreport_en.htm. [en línea] [consulta e impresión: 16 julio 2003]

las telecomunicaciones; aquélla ha merecido una reciente actualización, mediante la Directiva 2002/58/CE, relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas, de 12 de julio de 2002, a fin de recoger la evolución de los mercados y tecnologías de servicios de comunicación electrónica, como Internet, con el fin de ofrecer el mismo nivel de protección de los datos personales y la intimidad para todas las tecnologías utilizadas.[52]

Por otro lado, nos parece oportuno consignar que las definiciones de la Directiva no han alcanzado sólo a los Estados miembros de la Unión Europea, sino también a los países candidatos a integrar la misma, los que, de conformidad con los criterios de Copenhague, están comprometidos a transponer la Directiva con antelación a su adhesión. Inclusive más, los efectos reflejos de la Directiva se proyectan a otras latitudes; ello se evidencia en la Ley 25.326 sobre Protección de los Datos Personales aprobada por Argentina.

En Argentina, la Constitución de 1994 asegura a las personas una acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos, sin perjuicio del secreto de las fuentes de información periodística.[53] Sin embargo, aun cuando diversas provincias contemplaban implícitamente la regulación de tal derecho e inclusive alguna ya contaba con legislación en la materia,[54] el desarrollo legislativo de tal garantía y de una normativa general relativa al tratamiento de datos de las personas sólo cristaliza a nivel federal con la aprobación el año 2000 de la Ley 25.326 sobre Protección de los Datos Personales.[55]

52 Por otro lado, siempre en cuanto a transposición de las previsiones generales de la Directiva 95/46/CE a contextos específicos en que se verifica tratamiento de datos, la Comisión ha estimado que, ante la intensificación de la recogida de datos personales de los trabajadores en relación con el empleo, pueda resultar oportuno tomar como base los principios generales ya existentes de la Directiva y aportando a dichos principios complementos y aclaraciones para adaptarlos al contexto laboral. Una decisión definitiva sobre el particular ha sido pospuesta por la Comisión para las postrimerías del 2003. Por su parte, a nivel del derecho interno, el tema ya ha sido objeto de una legislación específica en Finlandia, en tanto que Suecia se encuentra en procesos legislativos al efecto.

En el mismo sentido, la propuesta de Directiva del Parlamento Europeo y del Consejo, relativa a la armonización de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de crédito a los consumidores, la Comisión ha establecido disposiciones específicas sobre protección de datos en la materia, cuyo objetivo es reforzar aún más la protección de los consumidores. Cf. Comisión de las Comunidades Europeas, "Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)", Bruselas, 15 de mayo de 2003.

Con razón Ahti Saarenpää ha descrito el estado actual de la protección de los datos personales en Europa, como un estadio de fragmentación normativa, cuya proliferación deja en exposición los logros obtenidos por la Unión Europea hasta la fecha. Cf. SAARENPÄÄ, Ahti. "Europa y la Protección de los Datos Personales", trad. Alberto Cerda, en Revista Chilena de Derecho Informático, del Centro de Estudios en Derecho Informático de la Universidad de Chile, número 3, 2003 (en imprenta).

53 Artículo 43 inciso 3 de la Constitución de la Nación Argentina de 22 de agosto de 1994.

54 Se refiere a la Ley 4.444 de la Provincia de Jujuy, Cf. EKMEKDJIAN, Miguel Angel y PIZZOLO, Calogero. op. cit., pp. 95 y ss.

55 Ley 25.326 sobre Protección de los Datos Personales, sancionada el 4 de octubre de 2000 y promulgada parcialmente el 30 de octubre de 2000.

Sobre el desarrollo del habeas data hasta antes de ser dictada la Ley 25.326, cf. SAGÜÉS, Néstor, "El habeas data en Argentina (Orden Nacional)", en Ius et Praxis, Universidad de Talca, Facultad de Ciencias Jurídicas y Sociales, Año 6 N°2, 2000, pp. 137-150.

Es notable el sello de la normativa comunitaria en la ley argentina, que brinda protección a personas jurídicas y naturales ante el tratamiento automatizado o no de sus datos personales por entidades públicas o privadas; dicho sistema se ve reforzado por la atribución a los titulares de datos de un nutrido haz de facultades, a las cuales se asocia una acción judicial de tramitación sumaria para resguardo de sus derechos y una autoridad de control –la Dirección Nacional de Protección de Datos Personales–, de carácter administrativo y funcionalmente independiente, encargada de velar por el cumplimiento de la ley.

5. SAFE HARBOR PRIVACY PRINCIPLES

La normativa sobre tratamiento de datos personales en Estados Unidos presenta una característica que define su sistema: la opción por una legislación sectorial, esto importa un rechazo a las leyes de aplicación general promovidas por la Unión Europea y antes bien se opta por generar tantas regulaciones legales como contextos ameriten su existencia, con lo cual hace frente a la especificidad que sea requerida por la naturaleza de los datos, las finalidades de su tratamiento o de la entidad titular de la base. A modo meramente ejemplar pueden mencionarse: Cable Communications Policy Act de 1984, Driver's Privacy Protection Act, Electronic Communications Privacy Act de 1986, Electronic Funds Transfer Act, Telecommunications Act de 1996, Fair Credit Reporting de 1970 y Consumer Credit Reporting Reform Act de 1996, Right to Financial Privacy Act, Telephone Consumer Protection Act, Video Privacy Protection Act, y Aviation and Transportation Security Act de 2001, entre otras disposiciones federales y estatales.

La legislación estadounidense se caracteriza además por su adscripción a un laisez faire del viejo cuño, en que los propios interesados deben velar por el cumplimiento de la normativa relativa al tratamiento de los datos personales que les conciernen –ya sea a través del ejercicio de los derechos que se reconocen al titular de los datos, o bien mediante la formulación de códigos deontológicos y adopción de disposiciones reglamentarias por los órganos responsables de sistemas de registro–, y el Estado asegura su posición de gendarme mediante el establecimiento de excepciones fundadas en necesidades de orden público, prescindiendo de la consagración de una autoridad de control pública que vele por el cabal cumplimiento de la legislación.[56] Indudablemente un régimen jurídico tal, esto es, un modelo de autorregulación y autocontrol, unido al mosaico normativo, guardan franca oposición al favorecido por los Estados miembros de la Unión Europea, y había de resentir la pretensión de un nivel de protección adecuado en las transferencias transfronterizas de datos personales desde Europa a los Estados Unidos, lo cual dio lugar a extensas rondas de negociación que cristalizaron en los Acuerdos de Puerto Seguro (Safe Harbor Agreement), por los cuales se ha procurado conciliar ambas opciones legislativas y a los cuales nos pasamos a referir siquiera sucintamente.

56 El sistema de autocontrol promovido por Estados Unidos es objeto de serios cuestionamientos en su seno; así Andrew Shapiro, de la Universidad de Harvard, junto con rechazar el actual estado de desarrollo de la protección de la privacidad –especialmente de los datos personales– y repudiar un enfoque mercantilista como solución, ha abogado por la creación de un organismo federal que coordine la protección de la privacidad a nivel nacional como en el extranjero, o bien, en su defecto, cuando menos encargar a alguna entidad existente todas las políticas relacionadas con la materia. Cf. SHAPIRO, Andrew, "The control revolution" (1999). "El mundo en un clic", trad. Francisco Ramos, Grijalbo. Barcelona, 2001, pp. 259-268, 348-351.

A mediados del 2000, el Departamento de Comercio de los Estados Unidos publicó los denominados Safe Harbor Privacy Principles, traducidos como Principios de Puerto Seguro, texto que contempla los principios a que deben sujetarse las entidades estadounidenses para obtener el visto bueno de la Unión Europea, a fin de asegurar una política de protección de datos adecuada, que brinden privacidad y confidencialidad homologables a los estándares europeos, tras lo cual podrán recibir cesiones de datos personales provenientes de los Estados miembros de la Unión Europea sin problemas ni sanciones para cedente o cesionario.[57]

Por su adhesión a Safe Harbor los organismos y entidades asumen ciertos principios rectores del tratamiento de datos, a saber: notificación e información a las personas, previas a la recogida de datos que les conciernen; derecho de opción para divulgación a terceros o usos incompatibles con el objeto inicial de la recogida, ya sea en listas de exclusión o aceptación, según la naturaleza de los datos; se condiciona la transferencia ulterior de datos a terceros a la adopción de los principios de Safe Harbor; se impone a las entidades tratantes de datos la obligación de implementar medidas de seguridad y la obligación de velar por la calidad de los datos; reconocimiento de los derechos de acceso y rectificación a las personas concernidas; y, se establece la necesidad de que las entidades tratantes adopten mecanismos que brinden garantías para la aplicación de los principios, tales como recursos independientes, procedimientos de seguimiento y medios para subsanar infracciones y sancionarles, en su caso.

Sin embargo, Safe Harbor no es obligatorio per se para las empresas o entidades de Estados Unidos, ya que previamente deben aceptar voluntariamente la aplicación del Acuerdo, mediante autocertificación de su compromiso al respecto, la que debe ser notificada al Departamento de Comercio. Dicha notificación debe renovarse anualmente e incluye información básica relativa a la entidad u organización adherente, el tratamiento de datos personales provenientes de Europa que efectúa y una descripción de las políticas de protección a la vida privada a que somete el procesamiento de aquellos. La verificación de las prácticas de protección de la vida privada, así como su conformidad con los principios de Safe Harbor puede ser efectuada por terceros o por la propia entidad. Huelga decir que los compromisos asumidos por las entidades adscritas a Safe Harbor no son extensivos al tratamiento de toda la información personal, sino sólo a aquellos datos transmitidos desde la Unión Europea a partir del momento en que se adhiere al Acuerdo.

Adicionalmente, Safe Harbor contempla: hipótesis de tratamiento de datos personales a los cuales no le son aplicables sus principios, tales como aquel efectuado en el marco de actividades periodísticas; una aplicación parcial de sus disposiciones al tratamiento de datos obtenidos en el contexto de una relación laboral; y previsiones ante la fusión o absorción de las entidades adheridas por otras.

[57] Para una revisión de la materia pueden consultarse el texto definitivo y anexos de Safe Harbor, así como los trabajos preparatorios elaborados por el Departamento de Comercio de los Estados Unidos, todos ellos disponibles en http://www.export.gov/safeharbor/, en tanto que las observaciones, dictámenes e informes formulados por el Grupo de Trabajo previsto por la Directiva 95/46/CE a las diversas versiones de Safe Harbor está disponible en su página internet http://europa.eu.int/comm/internal_market/privacy/index_en.htm

A efectos de control, junto a los mecanismos adoptados por las propias entidades u organismos, el Departamento de Comercio de los Estados Unidos ha designado como autoridad de aplicación a la Federal Trade Commission (Comisión Federal de Comercio), la que goza de facultades ante actos o prácticas desleales o fraudulentos que constituyen un modelo de conducta continuado e inadecuado, en tanto ellos se relacionen con el comercio. Sin embargo, la FTC en principio carece de competencia cuando la información está destinada a otros fines, así como en actividades específicas, tales como las financieras, de telecomunicaciones, transporte, aéreas y otras, evento en el cual guarda, a lo sumo, competencia residual o concurrente con otras entidades, tales como las siguientes: Federal Reserve Board, Office of Thrift Supervision, National Credit Union Administration Board y los Departamentos de Transporte y Agricultura, por mencionar algunas.

Safe Harbor despertó inicialmente cierto optimismo en los especialistas, en especial porque había conjugado el régimen normativo europeo con la autorregulación estadounidense, aparentemente en términos satisfactorios; experiencia susceptible de proyectarse a otras experiencias en las cuales los sistemas de ambos bloques manifiestan distancia.[58]

Sin embargo, el tiempo permitió apreciar los reales efectos del acuerdo: la pluralidad de disposiciones legales aplicables, el mosaico de instituciones comparecientes como autoridades de aplicación, las restringidas facultades conferidas a éstas para velar por el cumplimiento, así como los márgenes de autorregulación, la fiabilidad de la autocertificación y el escaso número de entidades y organismos que han hecho propios los principios de Safe Harbor,[59] ha generado cierto grado de preocupación por la exigua eficacia del Acuerdo entre las autoridades competentes de los Estados miembros de la Unión Europea, quienes afrontan nuevas negociaciones con Estados Unidos con miras a obtener un adecuado nivel de protección para los datos personales transmitidos allende el Atlántico.

6. CONCLUSIONES

En cuanto al bien jurídico protegido, conviene dejar asentado que la normativa sobre protección de los datos personales más que pretender resguardar la intimidad de las personas, aquel ámbito de nuestro quehacer cotidiano respecto del cual excluimos a los demás, procura brindar amparo a un nuevo bien jurídico: la autodeterminación informativa o libertad informativa, bajo cuyo alero se confiere a los titulares de datos un nutrido haz de facultades para controlar la información que les concierne, con prescindencia de si la misma alude o no a circunstancias de su vida privada.

[58] MUÑOZ MACHADO, Santiago, "La regulación de la red. Poder y Derecho en Internet", Taurus. Madrid, 2000, pp. 181–189.

[59] Las proyecciones iniciales estimaban que a un año de haberse adoptado Safe Harbor cuando menos un millar de entidades y organismos estadounidenses se acogerían a los principios y obligaciones previstas en él; sin embargo, a la fecha, estando próximos a cumplir tres años desde su adopción, el número de adhesiones apenas si rebasa las trescientas. Información disponible en http://www.export.gov/safeharbor/

Como puede apreciarse de esta apretada reseña, la sucesiva adopción de leyes sobre protección de datos en diversos países evidencia cierto progreso en el contenido de las mismas, el avance desde un modelo de tutela estático a uno dinámico, un acusado proceso de aproximación y, en cuanto a los mecanismos de control, junto a su diversificación, la consolidación de las autoridades de control.

Mientras las primeras leyes sobre la materia circunscribían sus efectos al tratamiento automatizado de datos personales correspondientes a personas naturales verificado por organismos del sector público, actualmente, la casi generalidad de las legislaciones observadas extienden su ámbito al tratamiento de datos realizado por medios informáticos y manuales, realizado por entidades del sector público o privado, e inclusive son varios los países que han extendido sus previsiones al tratamiento de aquellos datos referentes a personas jurídicas. Así pues, la revisión nos muestra un incremento en el marco de los efectos de las leyes de datos.

Por otro lado, este tipo de legislación también exhibe un avance desde un modelo de tutela estático a uno dinámico. En efecto, la primera legislación prestaba atención a la base de datos o a la calidad de la información contenida en ella, de manera que de acuerdo a la naturaleza de los datos se establecía un tratamiento diferenciado para los mismos. Así por ejemplo, tratándose de los denominados datos sensibles se contemplaban mayores restricciones a su recogida, procesamiento y transmisión que respecto de otro tipo de datos personales. En cambio, un sistema de protección dinámico, sin renunciar a cierto distingo necesario fundado en la calificación de los datos, deja de considerar a los datos como neutros, ya que el potencial de la telemática puede tornarles nocivos o sensibles sin serlos per se, razón por la cual se centrará en el control de los programas y sus aplicaciones, así como en las medidas de seguridad y protección previstas al efecto, las condiciones de transmisión de los datos y la regulación del flujo transfronterizo de los mismos, entre otros.[60] Como ha puntualizado Heredero, la desconfianza en la informática fundada en unos pocos grandes sistemas de tratamiento cede paso a aquella originada en la dispersión de la información.[61] De tal suerte, aun cuando prevea una especial protección hacia datos sensibles, no desconocerá que el propósito previsto en la prohibición de su tratamiento puede verse burlado mediante la práctica del cruce de bases de datos, razón por la cual abogará por imponer limitaciones a esta y otras prácticas evasivas.[62]

60 Un modelo de protección estático tiene sentido hasta en tanto no sea factible verificar cruzamiento de bases de datos, esto es, mientras el desarrollo de la informática era incipiente y la telemática –o sea, la transmisión a través de la red de información de un lugar a otro del mundo– era precaria, pero una vez desarrolladas suficientemente sucede que es posible confrontar la base de datos de una gran multitienda, la base de datos de la administradora de tarjeta de crédito, y con ellas saber el tipo de lencería que compra determinada persona, la clase de locales que frecuenta por las noches, el tipo de publicaciones que adquiere y, a partir de ello disponer no de una fotografía, pero sí de un perfil relativamente claro de su opción sexual, sin siquiera haberle preguntado cuál es ella. Es lo que en doctrina se denomina la teoría del mosaico, que no importa renunciar a cierta categoría de datos sensibles, pero admitiendo que datos que inicialmente parecen inocuos pueden devenir en una fuente de riesgo similar según las funcionalidades o usos a que sean destinados. Alude a la teoría del mosaico, para evidenciar la relevancia que puede cobrar información inicialmente irrelevante, desde la perspectiva de la privacidad de las personas, NOGUERA ALCALÁ, Humberto, "El derecho ...", op. cit., pp.152–153. También con alusión a la teoría del mosaico, Cf. ROMEO CASABONA, Carlos María, op. cit., p. 26; VERA SANTOS, José Manuel, Derechos Fundamentales, Internet y Nuevas Tecnologías de la Información y de la Comunicación", en GARCÍA MEXÍA, Pablo (ed.), "Principios de Derecho en Internet". Tirant lo blanch. Valencia, 2002, pp. 19195.

61 HEREDERO HIGUERAS, Manuel, "Informática: ...", op. cit., pp. 18–19.

62 En este sentido, GALINDO, Fernando, "Derecho e Informática", Editorial La Ley-Actualidad, Madrid, 1998, p. 39.

Finalmente, un tercer proceso observado en la legislación sobre tratamiento de datos, dice relación con la creciente aproximación que abraza a los regímenes jurídicos adoptados en los diversos países. Ciertos signos de este proceso de proximidad normativa se venían produciendo ya antes de adoptarse el Convenio 108, que procuró alentar en sus Estados partes la adscripción a ciertos principios fundamentales. Otro tanto hicieron al respecto las Recomendaciones de la Organización de Cooperación y Desarrollo Económicos (OCDE) de 1980, al igual que los Principios adoptados por las Naciones Unidas en 1990. Sin embargo, ha sido la Directiva 95/46/CE la que más ha contribuido al efecto, al ser progresivamente traspuesta a la legislación interna de los Estados miembros de la Unión Europea, y, con miras a resolver las restricciones hacia el flujo transfronterizo de datos con terceros países, ser adoptada por tales terceros.

En efecto, a la consagración de ciertos principios fundamentales aplicables al procesamiento de la información, se agregan el reconocimiento de un núcleo de derechos a aquella persona a quien los datos conciernen, así como un contenido mínimo a las obligaciones a que quedan afectas las entidades responsables del tratamiento de datos nominativos. En cuanto al control, a la concurrencia de nuevos mecanismos de control se agrega la casi unánime consagración de una autoridad de control en la materia.