DOCTRINA CONSTITUCIONAL Y ADMINISTRATIVA

LA PROTECCIÓN DEL DERECHO A LA INTIMIDAD EN EL TRATAMIENTO DE DATOS PERSONALES

Por:
Libardo Orlando Riascos Gómez
Doctor en Derecho
Lriascos@udenar.edu.co
2008

LA PROTECCIÓN DEL DERECHO A LA INTIMIDAD EN EL TRATAMIENTO DE DATOS PERSONALES: EL CASO DE ESPAÑA Y LA NUEVA LEGISLACIÓN LATINOAMERICANA

Alejandra Castro Bonilla(*)
acastro@activelex.com
Doctora en Derecho Constitucional de la Universidad Complutense de Madrid.

Contenido:

I. INTRODUCCION

El derecho fundamental a la intimidad ha adquirido nuevas dimensiones en la sociedad de la información. Muchos autores sostienen que es el mismo derecho y otros le han dado nuevas denominaciones en virtud de las características que lo hacen diferir de lo que tradicionalmente entendíamos como intimidad en la era analógica (1). La tecnología ha sido capaz de generar cambios tan dramáticos en la vida económica, laboral y en la vida cotidiana actual, que es preciso redimensionar la protección a favor de ciertos derechos de los ciudadanos, con el fin de que no se vean menoscabados ante la vulnerabilidad en la que se encuentran a raíz de la revolución tecnológica.

El derecho a la intimidad como pilar fundamental de la protección a la individualidad de la persona se ha visto vulnerado por el trasiego indiscriminado de datos que sobrepasa las fronteras y la soberanía de cada región, con una rapidez y facilidad sorprendentes.

Internet introdujo una modalidad de tratamiento invisible de los datos (2) que se ha acentuado a través del comercio electrónico. Todos los días miles de ciudadanos proporcionan sus datos personales (identificatorios de la personalidad y hasta crediticios) de forma expresa o tácita a empresas públicas y privadas a través de Internet. Eso provoca que las empresas realicen ciertos tratamientos de datos que no son perceptibles al usuario, ya sea porque se presentan en principio como intrascendentes o bien porque se obtienen sin el consentimiento del usuario o a expensas de omisiones ilegítimas de información que afectan su autodeterminación informativa.

“Por todo ello las limitaciones a los tratamientos invisibles y la recogida de datos por los titulares desde las páginas Web debe encontrarse en un sistema de protección de datos personales adaptado a las características de los tratamientos y a la peculiar fisonomía de Internet. Esta adaptación se encuentra en el reconocimiento de deberes específicos en la fase de recogida de datos, en particular el derecho a realizar opciones informadas, el derecho al anonimato y la seguridad en la red.” (3) Ante esta situación, si bien desde la década de los setenta distintos Estados han optado por establecer ciertas regulaciones genéricas en el seno de sus legislaciones, lo cierto es que dichas iniciativas autónomas han resultado insuficientes ante el evidente dominio

universal de la tecnología. Lejos de que se estén generando acuerdos universales coincidentes a nivel jurídico, la tendencia ha sido establecer pautas de un derecho mínimo regional para que cada Estado estipule regulaciones internas que coincidan con esa voluntad común de una zona geográfica a la que esté políticamente adscrito.

Por lo pronto, debemos evaluar los avances individuales en la regularización del fenómeno de la nueva sociedad de la información con respecto a la protección de la intimidad en el tratamiento automatizado de datos, por ser la tendencia que hoy en día impera ante el fracaso de establecer políticas universales coincidentes.

Específicamente abordaremos la normativa imperante al respecto en Europa, como región pionera de la protección de la intimidad en el tratamiento de datos personales y la inclusión del Recurso de *Habeas Data*, haciendo especial mención al caso español, cuyo desarrollo legislativo evidencia un interés creciente en actualizar la ley ante las exigencias del mundo tecnológico. Finalmente veremos la adopción particular del Recurso de *Habeas Data* en la experiencia latinoamericana, por aportar esta región una nueva perspectiva en la protección de la intimidad por el trasiego de los datos personales en el mundo informático. Valga adelantar ahora que si bien en Latinoamérica la tendencia ha sido regular el recurso de *Habeas Data*, prescindiendo de la aprobación de normativa específica sobre el tratamiento de datos personales en ficheros manuales o automatizados, las regulaciones tienden a basarse en el Convenio 108 Europeo, sobre el cual haremos un análisis crítico preciso, por poseer tal importancia de norma base (aunque genérica y con contenidos mínimos).

II. ANTECEDENTES

El derecho a la intimidad es un derecho reciente cuyo origen se remonta al conocido artículo *The Right to Privacy* de S. Warren y L. Brandeis (4) , en donde exponían la inquietud sobre la necesidad de que el derecho a la intimidad o los acontecimientos de la vida privada de un individuo recibiesen una protección adecuada frente a la injerencia de los medios de comunicación. En ese momento, los juristas se refirieron a un derecho de exclusión (*the right to be let alone*) como una reafirmación de la intimidad y la individualidad.

Con la era de la información, efectivamente esa privacidad se ve debilitada, tal como lo afirma Emilio Suñé Llinás en su obra *Tratado de Derecho Informático*:

“Al entrar en la era de la informática, cosa que sucederá inmediatamente después de la Segunda Guerra Mundial, el ser humano se vuelve más y más de cristal, a partir del tratamiento masivo de los más diversos datos de las múltiples acciones de su vida cotidiana, que son susceptibles de quedar, y de hecho quedan, registrados en un ordenador.” (5)

La sociedad de la información ha puesto de manifiesto la vulnerabilidad de la vida privada del individuo de manera que en la actualidad la tecnología ha producido dos nuevas mercancías: los perfiles individuales y los colectivos de los usuarios, situación a la que alude María Luisa Fernández Esteban en su obra *Nuevas Tecnologías, Internet y Derechos Fundamentales*. Dice Fernández lo siguiente:

“Los medios de comunicación interactivos modifican también la capacidad de recogida de datos, instituyendo una comunicación electrónica continua y directa entre los gestores de los servicios y los usuarios. Por tanto, no solo es posible un control más directo de los comportamientos de los usuarios, sino también un conocimiento más estrecho de sus costumbres, inclinaciones, intereses y gustos.“ (6)

Ese control virtual que se ejerce sobre la vida íntima de los usuarios debe tener una regulación que ha iniciado ya en diversas geografías desde la segunda mitad del siglo pasado, basado en un derecho de la tercera generación que muchos denominan ya como libertad informática, sin que –como anotamos al inicio- exista una intersubjetividad entre los juristas con respecto a la naturaleza jurídica autónoma de este derecho, como un derecho novedoso o como concreción histórica de un derecho antiguo.

En el Consejo de Europa en 1967 se conformó una Comisión Consultiva de expertos para analizar el impacto de las nuevas tecnologías de la información sobre los derechos de los ciudadanos. Un año después se emitiría la Resolución 509 de 1968 en la Asamblea “sobre los derechos humanos y los nuevos logros científicos y técnicos” que si bien no hace alusión explícita a la protección de datos como tal, sí revela la necesidad de establecer mecanismos de protección tanto sobre la vida privada de las personas como sobre otros derechos fundamentales que podrían afectarse con la aparición de las nuevas tecnologías.

“El mérito inicial correspondió a un Estado integrado en la antigua República Federal de Alemania, el Land alemán de Hesse, que tuvo su ley en 1970 (7). El primer Estado propiamente soberano que dispuso de las que abreviadamente se denominan Leyes de Protección de Datos fue Suecia, que promulgo la suya en 1973 (...)” (8).

Otro antecedente podría ser el *Fair Credit Reporting Act* del 26 de Octubre de 1970 en el que -si bien no se hace mención a archivos automatizados- sí se intenta una primera regularización del tratamiento genérico de los datos

personales del individuo como norma de origen del *Privacy Act* del 31 de diciembre de 1974; ambos en Estados Unidos de Norteamérica. A partir de entonces múltiples países de la Comunidad Europea dieron sus iniciativas para la legalización y control del manejo privado y público de los datos personales de sus ciudadanos a través de Internet y otros medios de comunicación; considerando la evidente desventaja de poder que tiene el usuario en relación con el proveedor de servicios. Los países americanos y demás naciones en vías de desarrollo, sin embargo, se han quedado rezagados en esa carrera del derecho comparado y aún del derecho internacional, pues con algunas salvedades existe una desregularización total en la protección de los datos personales para el resguardo del derecho a la intimidad. La gran influencia de Estados Unidos quien incluso a principios de los noventa intenta detener la aprobación de una ley al respecto en Argentina, se ha hecho sentir en la región, por la amenaza anunciada de un menoscabo en las inversiones. La gran nación del norte considera que regular el avance de las autopistas de la información deviene en un menoscabo al desarrollo industrial y económico, lo que coincide con su legislación y política economicista (9) .

Europa ha entendido la necesidad de prevalecer el derecho a la intimidad sobre la libertad de comercio y constitucionalmente ya se ha consagrado tal protección en diversas naciones. Tal es el caso de la pionera Constitución Portuguesa de 1976 (10) , la austríaca de 1978 y especialmente la Española cuyo artículo 18.4 dice:

"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." (11)

Junto a esa norma, también la Constitución Española posee otra referencia legal muy relacionada a este tema, y consagrada en el artículo 105.b CE que dice:

"El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas."

Sobre estos artículos constitucionales, asegura el Dr. Riascos lo siguiente:

"Las fuentes normativas constitucionales de la relación-tensión; informática e intimidad, se hallan previstas en el art. 18.4 y el art. 105-b, pues mientras en el primero se impide el uti nom abusi de la informática frente a los derechos fundamentales y se asegura el uso pluralista de las nuevas tecnologías de la información y la comunicación (TIC), el art. 105-b, permite el acceso de los ciudadanos a archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas. Vale decir, el ejercicio de uno de las más emblemáticas facultades estructurales del derecho de habeas data: el acceso a la información a los bancos de datos o ficheros (manuales o informatizados). " (12)

Diversos Estados soberanos han emitido sus leyes para la protección de datos personales, previas al Convenio 108. Tal es el caso de la Ley Sueca del 11 de mayo de 1973 sobre archivos automatizados (13) , la ley alemana del 27 de enero de 1977 (14) , la ley francesa del 6 de enero de 1978, la ley noruega del 9 de junio de 1978, la ley danesa del 8 de junio de 1978, la ley austríaca del 18 de octubre de 1978 y la de Luxemburgo del 31 de marzo de 1979.

Dentro del Consejo de Europa las acciones para fijar una legislación universal en la materia iniciaron incluso antes de la Ley de Hesse de 1970. Precisamente en 1964 se instauró el Comité de Cooperación Jurídica del Comité de Ministros que dos años después incluyen la inquietud sobre la protección de la intimidad frente a las nuevas tecnologías, en la Recomendación 509 conocida por la Asamblea.

A partir de esas observaciones se acuerda nombrar un Comité de Expertos en el seno del Comité Europeo de Protección Jurídica que luego de varias discusiones decidieron iniciar un proyecto de Convenio Internacional, ante la evidente promulgación aislada de leyes que intentaban la protección de la intimidad. En 1973 se aprueba en el Consejo de Ministros la Recomendación No. 22 sobre protección de la intimidad de los datos en el sector privado, y en 1974 la recomendación No. 29 referida al sector público. Esas recomendaciones son los antecedentes para que en 1976 el Consejo de Europa encomendara al Comité de Expertos (a través del Consejo de Ministros) la elaboración de un proyecto de Convenio de la región para la protección de datos, que fue abierto a la firma de los Estados en Estrasburgo, el 28 de enero de 1981.

Es importante indicar que las discusiones en algún momento generaron la duda de si era o no conveniente realizar un convenio individual que pretendiera la protección de datos o si por el contrario hubiese sido mejor enmendar los alcances del articulo 8 del Convenio Europeo para la Protección de los Derechos y de las Libertades Fundamentales (Convenio de Roma del 4 de noviembre de 1950) (15) a través de una reforma de la norma, un protocolo adicional u otro instrumento legal que dependiese del Convenio de Roma. De tal forma, rescato el antecedente del articulo 8 de ese cuerpo legal como un punto de referencia del Convenio 108, que finalmente fue aprobado como texto independiente, dada la importancia de la materia.

El *Convenio para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal*, conocido como el CONVENIO 108, fue firmado por Alemania, Francia, Noruega, Suecia y España, que al conformar las 5 adhesiones mínimas, permitieron la vigencia del texto. España ratifica el Convenio en 1984 y es ley publicada por el Boletín Oficial del Estado (BOE) del 15 de noviembre de 1985. Antes de proceder al análisis del convenio es importante hacer notar que durante su proceso de aprobación y ratificación, el Tribunal Constitucional alemán emitió su famosa sentencia del 15 de diciembre de 1983 sobre la Ley del Censo (16), cuya traducción fue publicada en España en el Boletín de Jurisprudencia Constitucional No. 33, 1984, páginas 126 y siguientes. En dicha resolución, el Tribunal Alemán utiliza el término del derecho a la autodeterminación informativa, haciendo alusión al derecho de la protección de la intimidad frente a las nuevas tecnologías de la información, o lo que se ha conocido en doctrina como libertad informativa o derecho informático que le permite al individuo tener potestades e injerencia en el manejo que entidades públicas y privadas hagan sobre sus datos personales. Este precedente jurisprudencial señala que el interesado posee la autodeterminación informativa como una facultad para el resguardo del derecho a la intimidad, haciendo especial hincapié en la necesidad de evitar la elaboración de un perfil de la persona a partir de la interacción de archivos que resguardan distintos datos personales del individuo.

Por tanto, desde la obra de Warren y Brandeis, el concepto de derecho a la intimidad ha sufrido una importante variante, pues evoluciona de ser un simple derecho de exclusión en el que el individuo reafirmaba su derecho a la privacidad o "derecho a estar solo" para adquirir una nueva dimensión como derecho facultativo que le permite ejercer acciones en defensa de su vida privada. Precisamente, en la obra de Warren y Brandeis, se exalta la posibilidad que ostenta el individuo en el *common law* de ejercer acciones indemnizatorias a favor de su derecho a la intimidad o la vida privada. La propuesta de ambos juristas era resaltar la posibilidad del individuo de ejercer acciones legales para la defensa de un derecho personal en razón de un derecho de "reparación" sobre las violaciones que sufriera un sujeto sobre su intimidad.

En España se ha venido asumiendo esa misma dimensión del derecho a la intimidad. Por ejemplo -y aún bajo la influencia de la terminología alemana- el Dr. Pablo Lucas Murillo de la Cueva publica en 1990 su libro *El Derecho a la Autodeterminación Informativa* en el que, entre otras cosas y citando a la *Privacy Protection Study Commission* creada en Estados Unidos en 1974, señala los cambios surgidos en torno a la reciente noción del derecho a la intimidad ante el uso de las nuevas tecnologías. Como resumen del ámbito de protección que exige el nuevo bien jurídico que implica tal derecho, Lucas Murillo alega que todo Estado democrático debe prever:

"1. El reconocimiento a cada individuo del derecho de acceder a la información personal que le afecte, especialmente a la existente en los bancos de datos informatizados.
2. El reconocimiento a cada individuo del derecho a controlar, de forma razonable, la transmisión de la información personal que le afecte.
3. Para garantizar el derecho a la intimidad individual, las leyes deben regular: a) la limitación del periodo de tiempo durante el que se pueden conservar los datos personales; b) la definición de los objetivos para los que puede usarse dicha información, que, además, han de declararse al momento de iniciar la recogida de datos; c) garantías para hacer efectiva la calidad de los datos personales, es decir, su veracidad, integridad y actualidad; d)la prohibición de la revelación de datos personales." (17) Lucas Murillo advertía entonces del predominio doctrinal de una noción preinformática del derecho a la intimidad, en virtud de la cual eran pocas las definiciones que reivindicaban como contenido del derecho a la intimidad el de acceder y controlar, además de las informaciones personales o que afecten al interesado, también aquellas que sean extrañas a su esfera individual o incluso anónimas, pues en determinados contextos o ante cruce de datos de otra índole pueden generar perfiles que sí los conviertan en datos especialmente protegidos.(18) Quizás como adelanto de lo que hoy día conocemos como derecho a poseer la intimidad como un poder y una facultad, valga citar la sentencia 134/1999 emitida por el Tribunal Constitucional de España que dice:

"El derecho a la intimidad garantiza al individuo un poder jurídico sobre la información relativa a una persona o a su familia, pudiendo imponer a terceros, sean estos simples particulares o poderes públicos, su voluntad de no dar a conocer dicha información, o prohibiendo su difusión no consentida." (19) Más reciente aún podemos citar la sentencia 292/2000 del 30 de noviembre de 2000 del Tribunal Constitucional español que pretende diferenciar la intimidad de la libertad informática como un intento jurisprudencial de empezar a construir los conceptos que definirán la protección de los datos personales a nivel constitucional. Esta sentencia, sin embargo, en lugar de reconocer aquella nueva dimensión de la intimidad como un poder por parte del individuo de ejercer control sobre sus datos, escinde (a mi juicio de forma precipitada) el derecho fundamental de la intimidad del derecho fundamental a la protección de datos, indicando que ambos derechos poseen distintas funciones. La sentencia cita:

"La función del derecho fundamental a la intimidad del art.18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (...) En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos

personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado."(20)

Existen, sin embargo, muchas otras sentencias en las que los Tribunales han acogido la interpretación del artículo 18.4 de la Constitución Política Española que define al derecho a la intimidad tanto como una defensa de la individualidad (según la teoría del derecho a estar solo) como en su componente de derecho facultativo en virtud del cual el individuo está en el pleno ejercicio de defensa de su intimidad, pudiendo exigir acciones a entes públicos y privados para el control de la vida privada (poder de disposición y control sobre los datos personales).

A esta nueva tendencia de concebir un derecho activo, se le denomina *Habeas Data* aunque la correcta acepción sería la *autodeterminación informativa*. Precisamente, el *Habeas Data* es un recurso procesal para defender el derecho a la intimidad como un instrumento del individuo de control y disposición de sus datos personales. El *Habeas Data* consistente en el instrumento de garantía que poseen los ciudadanos para el acceso a todos los bancos de datos que contengan información que afecte su vida privada siendo la finalidad de tal derecho, la protección contra cualquier ataque a la esfera de la intimidad.

El *Habeas Data* ampara el derecho del ciudadano a exigir la exhibición o eliminación pública de sus datos, de conformidad con los ajustes normativos regionales, mediante un instrumento procesal que emula al *Habeas Corpus* como defensa de un derecho fundamental (ya no la libertad o la vida sino la intimidad personal).

Esta noción la recoge el Tribunal Constitucional de España en la sentencia 11/1981 en la que sostuvo lo siguiente:

"La libertad informática reconocida por el artículo 18.4 de la Constitución, ya no es la libertad de negar información sobre los propios hechos privados o datos personales, sino la libertad de controlar el uso de esos mismos datos insertos en un programa informático: lo que se conoce con el nombre de *Habeas Data*." La reciente doctrina también ha hecho grandes aportes para entender la naturaleza del derecho que se pretende proteger en estas nuevas directrices legales que emergen con la tecnología. Por ejemplo, debemos aclarar que el *Habeas Data* es en sí un recurso judicial y no una mera definición doctrinal, como pudiera serlo la facultad de la autodeterminación informativa (21). En el mismo sentido, el *Habeas Data* (que significa en su literalidad "tener los datos") no protege en sí los datos de los individuos, sino que protege el derecho a ejercer la defensa de la intimidad ante la manipulación indebida de tales datos. Miguel Angel Davara formula la siguiente aclaración:

"La doctrina utiliza la expresión protección de datos para referirse a la protección jurídica de las personas en lo que concierne al tratamiento automatizado de sus datos personales. [...] En este mismo sentido, nosotros entendemos por protección de datos 'el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los limites de su intimidad'." (22) Efectivamente, el objeto no es proteger las bases de datos ni los ficheros, sino que se pretende la protección de la intimidad de la persona en el manejo que se hace de sus datos personales, a través de esos ficheros automatizados o no. Si bien se habla de "protección de datos", debe interpretarse no en el sentido literal, sino en el valor intrínseco de la expresión, cuya intención es la protección de la intimidad que el uso de esos datos implica. Aclarado lo anterior, procedamos entonces a estudiar los diferentes instrumentos internacionales que amparan la protección de datos personales y la nueva concepción del derecho a la intimidad, retomando el *Habeas Data* como la garantía procesal para la protección de la intimidad.

III. ANALISIS DEL CONVENIO 108 DEL CONSEJO DE EUROPA DE 1981

El Convenio 108 del Consejo de Europa está compuesto de 27 artículos, cuya redacción denota en el legislador una intención de establecer un marco jurídico amplio y permisivo para los Estados Parte en cuanto a la protección de la intimidad.

El objeto del Convenio según se indica en su artículo primero es garantizar en el territorio de cada Estado Parte, el respeto a todas las personas de sus derechos y libertades fundamentales, concretamente del derecho a la vida privada con respecto al tratamiento automatizado de datos personales.

Es importante hacer notar que el Convenio en su traducción oficial utiliza el término "vida privada" como anglicismo derivado de la obra de Warren y Brandeis, a partir de la cual se empieza a hablar en doctrina de "privacy", e intenta establecer la protección genérica de lo que denominan "vida privada" cuyo contenido es el derecho a la intimidad. No obstante, ante la doctrina imperante, la Directiva 95/96 de la Unión Europea retoma el término que mejor se ajusta a nuestra lengua: el de *intimidad*.

Una segunda observación derivada de esa norma inicial, estriba en el hecho de que el objeto del Convenio pareciera ser exclusivamente los archivos automatizados de datos, quedando excluidos los archivos manuales.

Pese a lo anterior, sin mucho éxito en la redacción de este cuerpo normativo, en el artículo 3.2.c, se obliga a los Estados Parte a declarar si aplicarán el Convenio a ficheros no objeto de tratamiento automatizado. Esta tendencia de apertura del Convenio, resulta lógica como una propuesta de regulación inicial en la materia, pero insuficiente para la protección efectiva de la intimidad del individuo en el manejo genérico de todo tipo de ficheros sean automatizados o manuales.

El Convenio también despliega una serie de definiciones amplias, que en lo que interesan definen al dato de carácter personal de forma tan abierta que resulta incluido como dato de esta índole cualquier información sensible o no, que tenga que ver con la persona. Toda información o referencia a la vida privada y eventualmente hasta la vida pública del individuo, será entonces susceptible de ser protegida por dicho convenio. Esta circunstancia vista de forma aislada pareciera excesiva, pero sin embargo resulta razonable si evaluamos la vulnerabilidad del individuo ante la posibilidad de que se elabore un perfil de su personalidad con diversos datos de distintas fuentes que detallen aspectos de su vida. Ante esta situación facilitada por la informática, efectivamente todo dato de la vida cotidiana resultaría un dato susceptible de protección. El artículo 2.b deja a discreción de cada Estado Parte fijar como autoridad controladora de los ficheros que administran datos personales, ya sea a autoridades publicas o privadas. El problema de esta norma es que no impone mecanismos estatales de control sobre los entes privados, ni en el ámbito legal ni deontológico, dejando al individuo en clara inseguridad ante el administrador de los ficheros; punto que veremos, será corregido en la respectiva Directiva.

Con respecto a la aplicación del Convenio, el artículo 3 señala que rige para ficheros del sector público y del sector privado. Como una concesión peculiar, el Convenio concede que cada Estado parte pueda en el momento de su adhesión o ratificación e incluso durante una vigencia ulterior, proporcionar una lista de los ficheros a los que no aplicará el Convenio, siempre que sobre esos ficheros no recayese una legislación interna distinta de protección de datos.

Esta potestad evidentemente le otorga a los Estados en su condición de entes públicos, ciertas prerrogativas de manejo y control de sus ficheros, con respecto a los ficheros del sector privado. Además deja un margen abierto para que la aplicación del Convenio en cada Estado Parte sea heterogénea, alejándose de la intención inicial del Consejo de Europa de establecer pautas genéricas para la homologación de un régimen jurídico regional y efectivo.

El Convenio también dedica un capítulo a lo que denominan *principios*, pero que en realidad se refiere a los deberes a los que se obligan las partes (Capitulo II). Dentro de estos deberes se incluyen los siguientes:
1.) El Compromiso que deben asumir los Estados parte de adoptar las medidas necesarias para que la protección de datos sea efectiva (art. 4)
2.) Mantener la calidad de los datos (art. 5). Esa calidad se refiere específicamente a que los datos de carácter personal sean archivados bajo las siguientes condiciones:
a. Que se obtengan y traten por los medios legales idóneos
b. Que se registren para fines determinados y legítimos
c. Que sean adecuados, pertinentes y precisos, procurando evitar que sean excesivos
d. Que sean exactos y actualizados
e. Que se conserven por un tiempo prudencial de conformidad con el fin para el que fueron recabados.
3.) Se prohiben las categorías particulares de datos (conocidos como sensibles) que puedan determinar la raza, la afinidad política, la preferencia sexual, las condiciones de salud, la religión, las condenas penales u opiniones particulares de los individuos en general. (art. 6) Este artículo, precisamente, coincide con la preocupación externada por el Tribunal Constitucional alemán en su famosa resolución sobre la Ley de Censo de Población (*Volkszählungsgesetz*), en lo que respecta a evitar la elaboración de un perfil personal, cuando señalaba:

"(...) es ilícito, en efecto, incluso en el anonimato de las encuestas estadísticas, todo registro y catalogación omnicomprensiva de la personalidad, mediante reunión de datos singulares sobre el modo de vida y la persona, para componer así un perfil de la personalidad del ciudadano."(23)

4.) El Convenio también dentro de sus principios/deberes exige a los Estados Parte la adopción de medidas de seguridad contra la destrucción accidental o no autorizada, perdida, acceso, modificación o difusión ilegítima de los datos contenidos en los ficheros. (Art. 7)

5.) Señala también un deber de protección o principio de garantía real a los ciudadanos sobre los siguientes aspectos (art. 8):
a. Que los ciudadanos sean capaces de conocer la existencia de un fichero, sus fines, ubicación y autoridad que lo controla.
b. Que el interesado directo pueda tener la información suficiente sobre la totalidad y características de los ficheros que guardan sus datos personales.
c. Que puedan rectificar e incluso ordenar borrar los datos cuya custodia implique una violación al derecho interno o a los principios señalados por el Convenio.
d. Que puedan recurrir a la autoridad que no atienda sus peticiones.

6.) Finalmente, el Convenio exige a los Estados Parte el imponer sanciones y recursos contra cualquier incumplimiento (art. 10). Sin embargo, nos encontramos nuevamente ante una norma genérica que exige la adopción de legislación interna en cada Estado Parte, que permita ejecutar tales sanciones y delimitar los recursos con el fin de no hacer ilusoria la pretensión de efectividad de los alcances del Convenio.

El Convenio 108 también señala las excepciones y restricciones de aplicación de dicho cuerpo normativo. Básicamente indica las dos siguientes:
1.) Se prohiben restricciones a los deberes o principios citados, salvo que sea por la aplicación de una medida necesaria en un Estado Democrático, específicamente para la protección de la seguridad del Estado o la represión de infracciones penales (art. 9.2)
2.) Es flexible en lo que respecta a la amplitud que pueden tener los ficheros estadísticos o de investigación científica, siempre que no atenten contra la vida privada de las personas. Sin embargo, el Convenio omite la redacción de un limite a esos ficheros, como podría ser implementar la anonimidad.

En lo que respecta a flujos transfronterizos de datos, previendo un uso abusivo de la prerrogativa de un Estado de negarse a la transmisión de datos fuera de su jurisdicción, el Convenio 108 en su artículo 12 señala que un Estado no puede, bajo el pretexto de proteger la vida privada, prohibir o someter a una autorización especial el flujo de datos con destino a otro Estado Parte, salvo en los siguientes dos casos:

1.) Si su derecho interno prevé reglamentación especifica para determinadas categorías de datos, salvo si el otro Estado establece una protección equivalente.
2.) Si los datos se destinan a un Estado no parte por medio del Estado parte.

El problema que surge ante esta redacción es quién determina la existencia de normativa equivalente o de protección suficiente acorde con el Estado que expide la base de datos correspondiente, lo cual podría generar conflictos de competencia y jurisdicción. Tal competencia recaería en la entidad (agencia de protección de datos) del país que expide la información, pero el fondo de su intervención consiste en evaluar las normas de un tercer Estado, situación que bien podría generar ciertos roces de competencia.

El Convenio igualmente dedica un apartado a lo que denominan *Ayuda Mutua*, que es en sí el principio de reciprocidad (art. 13). Para hacer cumplir tal máxima de relación entre los Estados, se les exigen las siguientes acciones:
1.) Cooperación en la designación de una autoridad cuya función será comunicar al Secretario General del Consejo de Europa lo atinente a la ejecución del Convenio.
2.) Asistencia recíproca que se traduce en dos obligaciones:
a. Que cada Estado proteja a personas con residencia en el extranjero para que se les aplique el derecho interno de su país en materia de protección de datos de carácter personal.
b. Si el interesado reside en otro Estado Parte, éste le facilitara las acciones ante la autoridad del otro Estado en defensa de sus derechos.
La asistencia a otro Estado parte solo podrá negarse bajo tres circunstancias:
a. Que la petición sea incompatible con las competencias en materia de protección de datos.
b. Que la petición no coincida con las disposiciones del Convenio.
c. Que atender a la petición implique violentar la soberanía o el orden publico del Estado a quien se le solicita la actuación o esté en contra de los derechos y libertades fundamentales de las personas bajo la jurisdicción de dicho Estado.

El texto legal en cuestión también procura evitar que se lucre con la tramitación de la defensa del individuo a su derecho a la vida privada en materia de protección de archivos que resguardan datos de carácter personal, indicando que los costos serán únicamente por los trámites y traducciones que se requieran; situación que coincide con el principio de gratuidad de las gestiones ante la Administración Pública.

Se constituye mediante el Convenio (art. 20) un nuevo órgano denominado Comité Consultivo que tendrá un representante y un suplente por cada Estado Parte y los observadores que se recomienden de cada Estado no parte del mismo.

Las funciones del Comité Consultivo, básicamente se resumen en las siguientes:
• Emitir propuestas de mejora o enmienda del Convenio.
• Emitir criterio sobre la aplicación o las reformas del convenio.
• Reunirse cada dos años o cuando 1/3 de sus miembros lo solicite.
• Someter sus memorias al Comité de Ministros del Consejo de Europa.

Las enmiendas al Convenio son propuestas tanto por el Comité Consultivo como por el Comité de Ministros del Consejo de Europa. Este último debe aprobar esas enmiendas antes de someterlas a los Estados Parte para su aceptación.

Prosiguiendo con la apertura de dicho texto, se avala la participación de Estados no miembros del Consejo de Europa, posiblemente bajo la conciencia de que el manejo de datos personales a través de los nuevos medios de comunicación de la sociedad de la información, son incontrolables y se trasiegan en el ámbito universal. No obstante, esa adhesión de Estados no miembros debe venir precedida de una invitación expresa del Comité de Ministros del Consejo de Europa (art. 23), por lo que la norma lleva implícito un procedimiento que no se indica, pero que se presume que deberá mediar solicitud del Estado interesado en la adhesión ante el Comité de Ministros. En efecto, el Convenio 108 no se aprobé con el carácter de "Convenio Europeo", por lo que cualquier otro país ajeno a Europa podrá solicitar la adhesión. Si bien el ánimo del texto fue incorporar a todos los países fuera de la Unión Europea que estuviesen interesados en acogerse a las políticas de protección de datos, el texto no concede una serie de prerrogativas a esos Estados externos que les permitiesen participar en igualdad de condiciones. Por ejemplo, teniendo en consideración el amplio poder que posee el Consejo de Ministros (incluso para el aval de reformas o enmiendas del texto), debió preverse una participación real y equitativa de los Estados externos a la Unión que no estuviese sujeta a las decisiones del órgano continental. Sin embargo, para ello, considero que una iniciativa tan loable como la que propone el Convenio 108 debería ser discutida en el seno de un organismo internacional de mayor representación, tal como la ONU, en el entendido de que también la estructura de poder de dicho órgano debe ser revisada para que permita una democracia participativa de todos los Estados, incluso aquellos en vías de desarrollo. No obstante lo anterior, no me detendré en este análisis, por ser objeto de otro estudio particular, pero basta con indicar que como iniciativa regional el Convenio tiene logros importantes que deben ser retomados para un tratado internacional universal que haga efectiva su aplicación en la nueva sociedad de la información.

Considerando que el Convenio pretende otorgar pautas mínimas para que sean acatadas por todos los Estados parte obligados a la emisión de normativa específica de ejecución, no se permiten las reservas al Convenio. Sin embargo es de recordar que en estricto sentido legal la tolerancia de que cada Estado pueda emitir una lista de los ficheros a los que no les aplica el Convenio, es un sí misma una reserva legal cuya pertinencia debe considerarse para una ulterior revisión del texto jurídico.

El Convenio 108 fue aplicado en una resolución del Tribunal Constitucional Español, en la que se definió el contenido mínimo del derecho que este cuerpo normativo pretende proteger. En esa oportunidad dijo el Tribunal lo siguiente:

"Un primer elemento, el más elemental de ese contenido, es, sin duda, negativo, respondiendo al enunciado literal del derecho: El uso de la informática encuentra un limite en el respeto al honor y la intimidad de las personas y en el pleno ejercicio de sus derechos. Ahora bien, la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria, y es aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España, pues, como señala el Ministerio Fiscal, la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (Habeas Data)." (24)

Esta sentencia constituye un antecedente jurisprudencial de vital importancia para la ulterior aplicación e interpretación del convenio, cuyo espíritu efectivamente pretende proteger el derecho a la intimidad como un nuevo derecho fundamental tanto de defensa de la individualidad como en su contenido de facultad de acción que posee el individuo para la salvaguarda de su vida privada. La sentencia le otorga al derecho a la intimidad un contenido de corte positivo pues otorga al ciudadano una facultad de acción y control de sus datos personales. El convenio, además, es una fuente jurídica que incluso fue retomada en la década de los noventa por algunos estados latinoamericanos para la redacción de su normativa sobre protección de la intimidad en el trasiego de datos y merece por tanto el trato de fuente jurídica internacional y pionera en la materia.

Esta tendencia fue reiterada en la sentencia del Tribunal Constitucional del 30 de noviembre del 2000, en virtud de la cual igualmente se insiste en la autodeterminación informativa como un Derecho Fundamental autónomo.

IV. LA DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO

Antes de la adopción de la Directiva 95/46, en 1992 España emite la Ley Orgánica para el tratamiento automatizado de los datos personales, conocida como LORTAD. Sin embargo, nos interesa en este estudio el análisis específico de los contenidos de aquella Directiva que vino a complementar una legislación que había iniciado el Convenio 108, sobre todo porque una vez derogada la LORTAD, la actual Ley Orgánica de Protección de Datos de Carácter Personal del 13 de diciembre de 1999 (LOPD) incorpora tanto lo indicado por la Directiva 95/46/CE del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, como la Directiva 97/66/CE del Parlamento Europeo y del Consejo sobre al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones.

Esta Directiva 95/46/CE está compuesta de 72 considerandos iniciales y consta de 34 artículos. Se denomina *Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, publicada en el Diario Oficial de España número L281 del 23 de noviembre de 1995.

Dentro de la exposición de motivos de los considerandos se resume básicamente el contenido de la Directiva, pero es importante destacar ciertos aspectos que incluye en esta etapa preparatoria del articulado, pues para todo intérprete de normas, la etapa introductoria que suponen los considerandos devela la intención real del legislador en la elaboración de la dirección jurídica que se pretende, independientemente de si considere o no acertado la inclusión de considerandos con tales extensiones, que incluso llegan a superar el contenido de la Directiva.

CONSIDERANDOS

En primer término, se indica que los sistemas de tratamiento de datos están al servicio del ser humano por lo que la Directiva viene a aclarar la intención que tiene el legislador en la materia, en lo que respecta a concebir la informática como una ventaja y no un obstáculo en el desarrollo de la humanidad, y por tanto la regulación lo que pretende es un ordenamiento del desarrollo de los avances tecnológicos para proteger derechos fundamentales de los usuarios y de los prestamistas de servicios de tal índole. Ante la idea de que los avances tecnológicos facilitan el tratamiento e intercambio de datos, la Directiva pretende dar un marco jurídico al que deben adscribirse los Estados con el fin de fortalecer la cooperación científica y tecnológica y coordinar las redes de telecomunicaciones sin que el nuevo derecho sea un óbice en tales transformaciones.

Reconocen además que el mercado interior de la comunidad facilita el trasiego de datos por agentes públicos y privados y que por tanto el Derecho Comunitario exige una colaboración estricta entre los Estados. Esa protección equivalente o reciprocidad que se pretende, sostiene el legislador, impide a los Estados obstaculizar la libre y legítima circulación de datos alegando la protección al derecho a la intimidad. En este sentido es loable que una regulación jurídica de las relaciones científicas y técnicas procure al mismo tiempo una liberalización de la circulación de datos. Podríamos decir entonces que se trata de una normativa de control y no de prohibición, como lo han querido ver quienes defienden la libertad de comercio sobre la protección de la intimidad.

El considerando 15 es importante en el sentido que expresamente señala que la Directiva será aplicable a datos automatizados o contenidos en un archivo estructurado según criterios específicos relativos a las personas, lo que incluye datos no automatizados. A diferencia de lo regulado en el Convenio, ya en la Directiva el legislador fue capaz de comprender la trascendencia del contenido de los ficheros manuales y el peligro de su manipulación indebida, por lo que se regulan en los mismos términos que los ficheros automatizados.

La Directiva es más enfática en la solicitud de medidas internas que ejecuten el Convenio y conmina a los Estados a emitir las leyes que precisen los alcances de la Directiva. Los Estados al trasponer la Directiva asumen tal compromiso como un deber de parte, haciendo con ello efectiva la protección del derecho a la intimidad de los ciudadanos europeos.

Sostiene el documento que las personas físicas, jurídicas y autoridades públicas deben procurar la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control de las circunstancias que afecten el tratamiento; todo lo cual constituye los principios a los que el Convenio 108 hacía alusión. También los considerandos recuerdan la necesidad de informar al ciudadano de los archivos que contengan sus datos, darle facilidades de acceso expedito a los mismos, solicitar la rectificación y oponerse a los tratamientos en ciertas circunstancias.

El considerando sétimo señala nuevamente que el tratamiento automatizado y manual quedará regido por la Directiva pero solo cuando se trata de un conjunto estructurado de datos que contengan información sobre la persona, de manera que no cualquier fichero deberá estar sometido a estas regulaciones. Sobre este punto ni los considerandos ni el articulado de la Directiva llegan a definir lo que se entiende por un “conjunto estructurado de datos”, definición cuya ambigüedad podría resultar peligrosa en una interpretación maliciosa que definiera un amplio número de archivos como “no estructurados” que – aunque manipulen información que afecte la vida privada del individuo- quedarían excluidos de la aplicación de la Directiva.

El considerando 24 señala que la Directiva no protege a las personas jurídicas del tratamiento de datos, por lo que esta figura queda excluida de forma expresa. No obstante, si consideramos la importancia que eventualmente puedan tener la recaudación de datos sobre tendencias ideológicas, políticas o religiosas de personas físicas en las que eventualmente se puede extraer un perfil social de sus asociados o bien utilizar tal información en sistemas represivos no democráticos, es claro que el legislador no previó tal circunstancia y que ahora es el momento de evaluar su inclusión en el régimen legal de la protección de datos. No es ilusorio prever

esta situación, pues aunque el Convenio está dirigido a un ámbito de democracias, no debe perderse de vista que el poder de *autoritas* también requiere de ciertos controles legales.

En cuanto a las personas jurídicas, es claro que lo que debe regularse es el tratamiento de ficheros con datos personales que puedan estar manipulando, pero en ninguna medida podría fundarse una ley de protección de la intimidad de la persona jurídica para desviar un fin hacia el ocultamiento de la actividad comercial (que siempre debe ser transparente) o bien ocultar información económica o empresarial que afecte otros derechos y máximas como el de la libre competencia, la lealtad comercial, el derecho del consumidor o la buena fe en los negocios.

Dentro de los principios que esgrimen los considerandos, se dice que el tratamiento es lícito si se basa en el consentimiento del interesado, si se recaban los datos para un contrato que obligue al afectado, si constan para cumplir una ley o algún asunto de interés público o para ejercer una autoridad pública; y se pueden utilizar y comunicar con terceros para actividades legítimas de empresas con miras a la protección comercial. En este último punto queda evidenciada la influencia de las teorías que abogan por jerarquizar la protección comercial sobre la vida íntima, situación que va en detrimento de las libertades del individuo.

En esta etapa se resalta también que los datos que afectan las libertades fundamentales y el derecho a la intimidad (abandonando la terminología anglosajona de *privacidad*) no deben ser objeto de tratamiento alguno salvo para cuestiones relativas a la salud y la protección social, y están sometidos al secreto profesional de quien manipula el archivo respectivo. No obstante, deja a juicio de los Estados determinar otras excepciones distintas a la salud en las que sí pueden tratarse dichos derechos, situación que deviene en otra nueva potestad que se le otorga al Estado, sin ninguna limitación sensible que proteja al ciudadano de arbitrariedades y abusos de poder.

Se valora también la necesidad de ponderar ciertos intereses sociales por lo que se puede permitir el tratamiento de datos para fines periodísticos, artísticos, literarios, históricos, estadísticos o científicos. Surge aquí un problema de vital interés que retomaré en el análisis del articulado y que consiste en que la amplitud que otorga esta consideración en la asignación de un poder de acceso privilegiado para artistas, científicos, historiadores, profesionales de la información, estadísticos y para quien alegue poseer un interés que coincida en tales excepciones resulta a todas luces excesivo. Ese poder, a mi juicio, pudo haber contenido una limitación de vital trascendencia para la protección de la vida privada que consiste en guardar la identidad del agente cuyos datos se estén manipulando para tales fines, de manera que no se vean menoscabadas esas áreas de interés público y que a la vez se resguarde con la anonimidad la identidad del individuo mientras que sus datos (que no lo vinculan en lo personal) sirven para fines colectivos. La doctrina más reciente ha dado a conocer esa desvinculación de la identidad del sujeto con sus datos como *disociación de datos*. Igualmente, si el derecho a la intimidad consiste también en una facultad de acción del individuo, debe preverse que en estos casos de excepción el afectado tenga oportunidad de decidir si presta o no sus datos personales para los fines indicados, pues se trata al fin y al cabo de una manipulación de los aspectos que conforman su vida personal.

La Directiva pretende otorgarle a los Estados un amplio margen de acción para que en aras del interés público establezcan sus propias restricciones que en ninguna medida pueden ser inferiores a los mínimos que dicta la Directiva, lo que coincide con lo comentado al inicio de esta reflexión en cuanto a la tendencia por la autorregulación (legislaciones regionales y no universales).

Como un nuevo principio señala que el uso del correo electrónico responsabiliza al dueño de la cuenta que transmite datos pero no al que ofrece el servicio de transmisión. En países como Estados Unidos ya existen sendos pronunciamientos judiciales sobre el uso del correo electrónico y los alcances que tiene la injerencia del administrador sobre la vida privada del usuario, sobre lo cual la Directiva es omisa pues no precisa regulaciones sobre la vida privada en correos administrados por entes públicos o privados, o por los grandes proveedores de servicios de navegación (25).

Los considerandos también resaltan la importancia que reviste la notificación a una autoridad de control para asegurar la publicidad de todo lo relativo a los archivos automatizados o manuales que tratan datos de carácter personal de los ciudadanos.

La Directiva refuerza también la idea de implementar recursos judiciales para defender el tratamiento de datos sobre la vida privada, así como la inclusión de indemnizaciones e individualización de responsabilidades por violaciones a normas relativas a la Directiva o el derecho interno en esta materia. Se indica que los flujos transfronterizos de datos son necesarios para el desarrollo del comercio internacional y que la protección de las personas no es un obstáculo para garantizar esa transferencia salvo que un tercer país no ofrezca niveles de protección adecuados, situación que coincide con la intención del legislador de que la normativa no limite o impida el desarrollo comercial de la región.

La Directiva otorga un plazo de 12 años para que todos los ficheros manuales se ajusten a las exigencias de la Directiva, como un plazo obligatorio para poder hacer efectiva la protección de la vida privada en todos los ámbitos.

ARTICULADO

El artículo primero señala que el objeto de la Directiva es la protección de las libertades y derechos fundamentales de las personas físicas y en particular el derecho a la intimidad en el tratamiento de datos personales, con lo que el término jurídico de "vida privada" se homologa a la reciente doctrina que se refiere al "derecho a la intimidad".

El artículo 2 indica ciertas definiciones que amplían las contenidas en el Convenio 108. Básicamente señala que el tratamiento de datos se refiere a datos automatizados o no, dando con ello protección a los ficheros manuales. También es importante resaltar que distingue entre el *responsable del tratamiento de datos* y el *encargado del tratamiento*, siendo este último el que administra por cuenta del primero un archivo. Con la intención de declarar los alcances de la Directiva, el artículo 3 es explícito al señalar que la misma se aplica al tratamiento automatizado o no y se excluyen los datos cuyo objeto sea la seguridad pública, la defensa del Estado, la seguridad del Estado y lo relativo a materia penal. Esta es una prerrogativa del Estado, en cuya inconveniencia insisto por no haberse previsto ningún tipo de límite al ente público. Pensemos en un quebrantamiento del estado social de derecho interno en el que se disponga como parte de una nueva política de seguridad estatal el crear bases de datos que constituyan perfiles de los ciudadanos que contengan datos políticos o sensibles en general, que en alguna medida pudiesen ser utilizados en perjuicio de las personas por un régimen dictatorial. Ante esta España, han dejado entrever la no reprochabilidad del acceso que tiene la empresa a las cuentas de correo de sus funcionarios, aunque aún no existe un pronunciamiento expreso al respecto.

(sic) situación, valga indicar que dichas actuaciones podrían encontrarse dentro del marco legal preceptuado por la Directiva ante la infeliz redacción de la norma.

El artículo 4 indica que los Estados deben aplicar su normativa interna cuando el responsable del tratamiento resida en otro territorio, por lo que se produce una atracción del fuero jurisdiccional (*forum actoris*), tal como sucedió en la famosa sentencia del caso Shevill del Tribunal de Justicia de la Comunidad Europea del 7 de marzo de 1995 (26), de la que parte ahora toda la interpretación sobre jurisdicción en estos asuntos.

El artículo 5 deja a criterio de los Estados decidir cuándo son lícitos los tratamientos de datos personales, situación que refuerza el poder del Estado ante el ciudadano, que aunado al artículo tercero constituyen facultades propias de un poder de *autoritas* que supera al del ciudadano.

Al igual que lo hizo el Convenio, el artículo 6 señala los siguientes aspectos que deben garantizar los Estados para hacer efectivo el principio de la calidad de los datos:
a. Que sean tratados leal y lícitamente.
b. Que sean recogidos con fines determinados, explícitos y legítimos.
c. Que sean exactos y actualizados.
d. Que se conserven en forma responsable.
Para garantizar el principio sobre la legitimación del tratamiento de los datos, el artículo 7 exige lo siguiente:
a. Que el interesado haya consentido en el tratamiento de sus datos.
b. Que se recaben para un contrato u obligación jurídica.
c. Que sea necesario el tratamiento para proteger al interesado.
d. Que sea necesario el tratamiento para el interés público.
e. Que sea necesario para el interés legitimo del responsable del tratamiento siempre que no prevalezcan los derechos y libertades fundamentales.

Como una máxima que también defendía el Convenio 108, el artículo 8 indica que están prohibidos los datos que revelen el origen étnico, la opinión política, la convicción religiosa o filosófica, la pertenencia sindical, la salud o sexualidad salvo que el interesado lo consienta expresamente, o si resulta necesario para respetar garantías laborales o del interés del afectado, que sea adecuado para una entidad afín o sean datos públicos (27), necesarios para la salud. Esa posibilidad de permitir el archivo y custodia de estos datos sensibles hace que sean legítimos los archivos que por ejemplo mantienen los partidos políticos y los sindicatos en el ejercicio normal de sus funciones, mismos que en una lectura con interpretación literal del Convenio 108 resultaban ilegítimos, pues no se otorgaba esa excepción necesaria que incluye la Directiva en esta norma. Así, debe quedar claro que las excepciones que se señalan no son taxativas pues como ya se ha dicho a lo largo de este estudio, el espíritu del legislador ha sido siempre beneficiar a los ciudadanos
y no obstaculizar sus relaciones sociales, económicas, laborales y administrativas. Una norma que llama a la reflexión es el artículo 9 que señala que deben establecerse excepciones en el tratamiento de archivos que determinen un perfil como el que pretende evitar el artículo 8 (coincidiendo con la sentencia alemana de la Ley de Censo), cuando se trate de fines periodísticos, previendo conciliar el derecho a la intimidad con la libertad de expresión. Esta norma debe valorarse a la luz también del artículo 13.2 que permite establecer el tratamiento de datos personales y permitir el acceso a archivos restringidos cuando se trate de fines científicos o estadísticos;

pues como ya adelanté en el apartado anterior, resulta injustificado otorgar tales privilegios a ciertos profesionales (28).

Por ejemplo, en el caso del fin periodístico, esta norma permitiría al profesional de la información un acceso ilimitado a archivos con datos de carácter personal para que realice labores "periodísticas". Si la labor del periodismo es informar, cabe preguntarse si estamos aquí ante la posibilidad legal de divulgar o informar a la comunidad sobre el contenido de archivos y por ende de datos íntimos, basados en un derecho de comunicar o el correlativo de estar informados. Piénsese por ejemplo en un archivo que contenga detalles de enfermedades infectocontagiosas de ciertos sujetos: el periodista, en aras de informar a la comunidad, no solo tiene acceso a esos datos sino que -ejerciendo su profesión- los difunde en perjuicio de los afectados, alegando un interés periodístico de informar a la comunidad. No hay límites éticos a los que aluda la Directiva ni parámetros axiológicos o deontológicos que impliquen una utilización dañosa de los datos por parte de estos grupos que privilegia el Convenio. Tal concentración de poder resulta aún más desmedida si tomamos en consideración que los profesionales de la información ya tienen un régimen o fuero de protección especial incluso amparado a la Constitución Política, en virtud del cual gozan de la cláusula de conciencia, de la libertad de información y del secreto profesional (art. 20 inciso 1.d. de la Constitución Española y normas conexas o semejantes de otras Cartas Magnas). Igual interpretación se aplica para el caso de los científicos, estadísticos, artistas o historiadores que aleguen poseer ese interés legítimo que cobija la excepción indicada para acceder a archivos que custodian datos de carácter privado. Debo indicar que si bien los Estados Parte pueden hacer restricciones o delimitar esta excepción de forma más precisa, la Directiva resulta muy permisiva y por ende peligrosa en este aspecto, con la salvedad de que deja a discreción de los Estados buscar la conciliación entre el derecho a la intimidad y la libertad de expresión.

Sobre esta salvedad de la norma llamaba también la atención Emilio Suñé en su *Tratado de Derecho Informático* cuando decía:

"No cabe sino estar de acuerdo con los criterios de la Directiva, puesto que hacer excepción, sin más, de los datos para fines periodísticos, podría abrir un fácil procedimiento para burlar las disposiciones de la legislación protectora de datos personales, precisamente en beneficio de los poderosos, puesto que bastaría con ser dueño de una empresa de comunicación social, para poder disponer, con bastante libertad, de datos personales. La finalidad del Derecho, como recordaba muy bien el antiguo Comisario de Protección de Datos del Land de Hesse, Spiros Simitis, no debe ser reforzar los privilegios de los poderosos, sino controlar y equilibrar el poder."(29)

Con ello no quiero decir que la norma contenga una mala intención. Simplemente no es feliz su redacción o resulta incompleta para la satisfacción del interés general que es la protección de la vida privada (tal como lo señala el artículo primero). Por ello, es necesario pensar en los siguientes límites que propongo para esta excepción:

1. Que quien alegue poseer un interés que se ajuste a la excepción, demuestre ser un profesional en historia, periodismo, arte, ciencia o estadística, y que demuestre la necesidad de tener el acceso a los archivos solicitados para un fin específico, cierto y proporcional.
2. Que se permita el acceso a los datos de las personas pero resguardando la identidad de los sujetos con la anonimidad, con el fin de proteger efectivamente el derecho a la intimidad, aplicando la disociación del dato de la persona.
3. Que se requiera de tales profesionales unos códigos de conducta suficientes para que con su secreto profesional resguarden la vida íntima de las personas.
4. Que el individuo sea informado de los accesos que este tipo de sujetos tengan sobre sus datos y tenga la potestad de autorizar o no tales accesos o incluso permitir la revelación de su identidad cuando el estudio así lo requiera.
5. Que se prevean sanciones contra el profesional que exceda sus competencias en este ámbito o bien se prevalezca de su condición para causar daño a la vida privada de las personas.

Las Secciones IV y V se refieren al derecho del interesado a recibir información y del encargado del tratamiento a ofrecerla según los parámetros de la Directiva, e indica que en el derecho de acceso debe garantizársele al individuo lo siguiente:

a. Que sea libre, periódico, oportuno, sin costos excesivos y sin restricciones. A este derecho se le adicionan las condiciones que debe reunir la respuesta a la petitoria del interesado la cual debe ser pronta confirmando la existencia o inexistencia del tratamiento de datos, los fines, las categorías, los destinatarios, etc; y esa comunicación debe ser inteligible, total y evidenciar la lógica utilizada para el tratamiento.

b. Que tenga derecho a la rectificación, supresión o bloqueo de datos incompletos o inexactos y
c. Que se proceda a la notificación a terceros sobre las enmiendas respectivas.

A partir de aquí se deduce que la simple solicitud de supresión de un dato no basta, sino que ese dato debe ser "incompleto o inexacto", según la redacción indicada. Por ello, pareciera ser una potestad vacía de contenido, pues los supuestos en los que un individuo podrá solicitar que se eliminen sus datos, serán sumamente restringidos.

Como ya dijimos, hay supuestos en los que se pueden conservar archivos de datos personales sin las regulaciones ya citadas. Dentro de estas excepciones y limitaciones que incluso le otorgan facultades al Estado para organizar bases de datos para fines económicos (30), en la Sección VI se detallan las siguientes:

a. la seguridad del Estado
b. la defensa del Estado
c. la seguridad publica
d. la prevención o detección de infracciones legales
e. el interés económico del Estado
f. el control o inspección y
g. la protección de los derechos y libertades del interesado o de terceros.

Según lo que se indica en la Sección VII, el derecho de oposición del interesado exige que los Estados le garanticen su derecho a formular un reclamo que pretenda evitar el tratamiento de sus datos cuando éste no se ajuste a la normativa. El interesado puede oponerse de forma gratuita y anticipadamente al tratamiento de sus datos (principio de gratuidad de las gestiones y derecho de recibir información, extraídos del Derecho Administrativo) y debe ser informado cuando estos se comuniquen a terceros para ejercer su derecho a la oposición.

El artículo 15 rescata una nueva premisa introducida por esta Directiva que consiste en que los Estados miembros deben reconocer a las personas el derecho a no verse sometidas a decisiones judiciales basadas exclusivamente en el tratamiento automatizado de datos. No obstante, la redacción de la norma permite que eventualmente ese tratamiento de datos pueda ser utilizado como una prueba indiciaria o como soporte de otro marco probatorio más complejo, por lo que no se tasa su total discriminación. Además, esta premisa contiene dos excepciones dentro de la misma norma, a saber:

a. Que los datos se hayan recabado para un contrato y aún así se le permita la salvaguardia del interés legítimo del sujeto.
b. Que la ley lo autorice asegurando el interés legítimo del ciudadano.

La Sección VIII se refiere a la confidencialidad y seguridad que debe imperar en el tratamiento de datos y enfatiza en la necesidad de que los datos sean manipulados únicamente por el personal necesario quien tendrá restringido el acceso total o parcial a ficheros automatizados o manuales cuya manipulación no le compete (art. 16).

En lo que respecta a la seguridad que deben garantizar los Estados, se les exige las siguientes actuaciones (art. 17):

a. Deberán obligar al responsable del tratamiento para que aplique todas las medidas técnicas y de organización contra la destrucción accidental o ilícita, pérdida accidental o alteración, difusión o accesos no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

b. Deberán establecer que el responsable del tratamiento elija a un encargado del tratamiento capaz de garantizar las medidas de seguridad que resguarden el buen manejo del fichero.

c. Establecer que la realización de tratamientos por encargo se efectúe bajo la modalidad de un contrato formal que permita lo siguiente:
c.1. Vincular al responsable con el encargado
c.2. Que el encargado solo actúa siguiendo instrucciones del responsable
c.3. Que la legislación les es aplicable a ambos.

La Sección IX se refiere a la notificación obligatoria que debe realizarse a la autoridad de control que se constituye según el artículo 28 de la Directiva, y obliga a que cada Estado adopte medidas para que todo responsable o encargado de tratamiento de datos notifique sus actuaciones a la autoridad de control, de previo a iniciar el fichero respectivo. Los Estados pueden excluir de la obligación de notificar en los siguientes casos:

1. Si el tratamiento de datos no implica una afectación a los derechos y libertades de los interesados, habiendo el Estado definido los fines, alcances y categoría del fichero.

2. Cuando el encargado del tratamiento designado por el responsable tenga por cometido hacer aplicar las disposiciones de la Directiva, llevar un registro de los tratamientos con la información pertinente que garantice la protección de los derechos y libertades fundamentales.
3. Cuando el tratamiento esté destinado a llevar un registro que se abrirá al publico para consulta general o para consulta particular de quien demuestre un interés legítimo.
4. Cuando sea para fines legítimos de una asociación, fundación, sindicato u organismo similar.

La Directiva también indica algunos de los contenidos mínimos que debe llevar la notificación para que pueda determinarse la índole del tratamiento así como los responsables de su manipulación y determina la potestad estatal de impedir previamente el tratamiento de datos si existiese algún peligro para los derechos y libertades de los ciudadanos. (arts. 19 y 20)

Se incorpora en el artículo 21 el principio de publicidad del tratamiento de datos, en virtud del cual los Estados deben garantizar el acceso a los tratamientos existentes a través del registro que al efecto lleve la autoridad de control interno. (art. 21) En la actualidad, la comunidad europea cuenta con diversos centros de tratamiento de datos en cada país. En España, existe la Agencia Española de Protección de Datos como el órgano central y un único órgano descentralizado o autónomo con el que hasta la fecha solo cuenta la comunidad de Madrid.

Fernando Galindo define la importancia de esta entidad indicando lo siguiente:

"Como expresa la palabra inglesa con la que se denomina a la autoridad similar allí existente, *Register*, su función principal consiste en ocuparse del registro de ficheros públicos y privados, y de que, por medio del ejercicio de las funciones de inspección y sanción, en el funcionamiento y actividad se cumplan las leyes de protección de datos, satisfaciéndose el derecho de los ciudadanos a la autodeterminación informativa o al consentimiento. También se ocupa de aprobar los códigos de tipo de conducta que se presenten al Registro comprobando su ajuste a la legalidad. [...] La Agencia, por tanto, se ocupa especialmente de regular las actividades profesionales de los informáticos y de quienes utilizan sus productos: su observancia de las medidas de seguridad." (31)

La Directiva es más completa que el Convenio 108 en materia de impugnación, pues define la necesidad de establecer en cada legislación interna un recurso judicial para que cualquier afectado por un tratamiento de sus datos pueda recurrir ante la autoridad respectiva y sin perjuicio de los recursos administrativos que al efecto se dispongan al servicio del ciudadano (art. 22). Igualmente, la Directiva indica que el afectado podrá solicitar la reparación de todo daño que el responsable del tratamiento de datos le cause con su actuación, y advierte la necesidad de imponer sanciones en caso de incumplimientos. (arts. 23 y 24) He aquí la importancia de las figuras del *responsable del tratamiento* y *el encargado del tratamiento*, pues son el primer paso para individualizar responsabilidades que impliquen una efectiva reparación de daños causados a los sujetos cuyos datos sean manipulados de forma ilegítima.

La transferencia de datos a terceros países sólo se dará si ese país es capaz de garantizar el nivel de protección que exige la Directiva, misma que deberá ser evaluada por los Estados Miembros y la Comisión en caso que se considere que un tercer país no ha cumplido con tales requisitos. Si se comprobara la falta de ese tercer país, los Estados miembros quedan facultados para suspender cualquier transferencia e iniciar negociaciones para remediar la situación. Cabe aquí la interrogante sobre la prerrogativa, en materia de soberanía, que posee un Estado para decidir si otro cumple o no con tales requisitos de idoneidad.

El artículo 26 señala nuevas excepciones aplicables a la Directiva en virtud de las cuales procede la transferencia internacional de datos a un país que no garantice la protección si:

1. El interesado lo consiente.
2. Es necesario para suscribir un contrato entre el interesado y el responsable o, en interés del afectado, resulta necesario para suscribir un contrato entre el responsable y un tercero.
3. Es necesario para la salvaguarda de un interés público o el reconocimiento o ejercicio de un derecho o del interés del afectado.
4. La transferencia se hace desde un registro público que facilite tal información de forma legítima y esté abierto a consulta.
5. El responsable en ese tercer país ofrece garantías de protección constantes en un contrato.

Dichas excepciones deberán ser previamente conocidas por la Comisión, la cual tiene el derecho de oponerse fundadamente en los casos que lo considere pertinente. Lo idóneo es que esa prerrogativa de la Comisión no sea interpretada como una injerencia en la soberanía de ese tercer país pues lo que se pretende nuevamente de conformidad con los fines del articulado, es la protección de la vida privada de los ciudadanos como un derecho fundamental que exige medidas colectivas de esta índole. No obstante, es inevitable pensar en el roce que tal situación genera en la práctica.

La Directiva exige la implementación de códigos de conducta para los sectores que manejan datos de particulares según categorías, por ejemplo de asociaciones profesionales, sindicados, fundaciones, etc.; situación que debió también haberse contemplado para el artículo 9 de la Directiva, según lo comentado en estas líneas.

El artículo 28, como ya adelantamos antes, ordena la creación de al menos un órgano PÚBLICO como autoridad de control del manejo de datos que posea las siguientes potestades:

1. Servir de órgano consultivo para la creación de medidas reglamentarias o administrativas sobre protección de derechos y libertades personales en el tratamiento de datos de carácter personal.
2. Tener poder de investigación y acceso a datos objeto de algún tratamiento.
3. Tener poder de intervención como órgano dictaminador, antes de un tratamiento de datos.
4. Ordenar el bloqueo, supresión o destrucción de datos.
5. Prohibir un tratamiento de forma temporal o definitiva.
6. Someter sus inquietudes a las autoridades publicas que correspondan.
7. Atender solicitudes de particulares sobre la verificación de la licitud de un tratamiento.
8. Ejercer sus competencias en el territorio del Estado miembro que la designe o en otro Estado miembro cuando así sea instada.

Los miembros de dichos órganos estarán sujetos al deber del secreto profesional aún después de haber cesado en sus funciones, protección que podría interpretarse que se extiende por toda la vida, pues no existen limites temporales o cualitativos a ese deber de secreto.

Es importante ver que finalmente la Directiva define que el órgano debe tener una naturaleza pública, es decir, dependiente del Estado, pues recordemos que el Convenio 108 permitía en su artículo 2.b que el órgano encargado de controlar los ficheros existentes, fuese también de índole privada. Delegar tal responsabilidad en una entidad privada podría a mi juicio acarrear una desprotección al individuo ante el interés por lucrar en esa actividad que es lo que aquí se pretende evitar a través de un control en principio parcial y objetivo que usualmente ejercen los Estados democráticos; sin que por ello quiera decir que deban estar exentos de control.

La Directiva además crea un órgano adicional al que denomina “Grupo de protección de las personas en lo que respecta al tratamiento de datos personales”(art. 29 y 30), compuesto por un representante de la autoridad (es) de control de cada Estado miembro, por un representante de la autoridad (es) creada (s) por las instituciones y organismos comunitarios y por un representante de la Comisión. Sus funciones consisten en las siguientes:

a. Estudiar la aplicación de las normas nacionales para contribuir a su homogeneización en el ámbito comunitario.
b. Dictaminar el nivel de protección existente en la Comunidad y en los países terceros.
c. Asesorar a la Comisión sobre cualquier modificación de la Directiva o sobre cualquier mejora para el tratamiento de datos.
d. Dictaminar los códigos de conducta adoptados en el ámbito comunitario.

Los informes del Grupo serán conocidos en el Parlamento Europeo y el Consejo para su posterior publicación. Valga indicar la importancia que estos informes han tenido en la práctica, sobre todo en materia de protección de la intimidad a través de Internet. (32) Como un último órgano, el artículo 31 prevé la existencia de un Comité que asesore a la Comisión para adoptar las medidas de ejecución comunitaria que se necesiten. Dentro de la sección dedicada a las Disposiciones Finales, la Directiva exige que los Estados adopten las medidas legales, reglamentarias y administrativas para el cumplimiento de la Directiva, en un plazo de 3 años desde su adopción y da un plazo de 12 años para ajustar los ficheros manuales a lo que dictamina la Directiva para un óptimo tratamiento de sus contenidos. Como una previsión del ajuste que debe realizarse en el ámbito legal por los avances tecnológicos propios de la sociedad de la información en la que vivimos, el artículo 33 dispone que la Comisión deberá evaluar el tratamiento de datos a través de sonidos e imágenes para que en el plazo de tres años se presente una propuesta de protección a los derechos de los afectados.

En general, la Directiva es una iniciativa loable que pretende hacer efectiva la protección de la vida privada ante el tratamiento de datos de forma indiscriminada que sucede en el mundo. Pero es precisamente esa circunstancia del mundo “globalizado” lo que hace insuficiente una iniciativa regional, que nuevamente presenta pocos alicientes para que Estados de otras regiones se adscriban a la misma. En los aspectos señalados, la Directiva necesita un perfeccionamiento que debe partir de la buena voluntad de las partes y del compromiso real de cada Estado de ajustar su normativa interna a esa nueva regulación.

Como origen normativo, el Convenio 108 da pie para que en la Unión Europea se armonizara la regulación de la protección de la intimidad en el tratamiento de datos personales que se logra concretar a través de la Directiva 95/46/CE del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al

tratamiento de datos personales y a la libre circulación de esos datos –a la que aludimos en la primera parte de este estudio-, así como la Directiva 97/66/CE del Parlamento Europeo y del Consejo sobre al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones.

Nos corresponde por tanto analizar otras normas derivadas del Convenio 108 y hacer un repaso de las iniciativas legislativas en América Latina que pretenden regular el tratamiento de datos en la región.

Resulta necesario el análisis de ambas tendencias, pues como veremos, la naturaleza jurídica de recursos procesales como el *Habeas Data* y la consideración legal de la protección de la intimidad, varía de una región a otra, generándose una disimilitud terminológica y legislativa importante que debe ser considerada para una ulterior armonización del Derecho Internacional sobre la protección de la intimidad y el tratamiento transfronterizo de datos personales.

V. OTRAS DISPOSICIONES ORIGINADAS EN EL CONVENIO 108

Recientemente, en el seno del Consejo de Europa se han sometido propuestas de modificación al Convenio 108, en lo que respecta al flujo transfronterizo de datos, pues ha sido una de las normas más conflictivas del texto por implicar a países que no pertenecen a la Unión Europea y por la dificultad de homologar (en esas circunstancias) el derecho interno de cada Estado para cumplir con el principio de reciprocidad y el de protección mínima que se exige en la protección de datos. Así, el Proyecto de Protocolo Adicional elaborado el 10 de marzo de 2000 por la Comisión de Asuntos Jurídicos y Derechos Humanos (33), dejó constancia de su preocupación por la protección estadounidense a favor de las empresas privadas y el libre trasiego de datos en dichas instancias, y abogó por una defensa universal de la vida privada.

Uno de los considerandos que deja entrever el espíritu de la reforma que se pretende, sostiene que la protección de los datos de carácter personal y de la vida privada es una prioridad ante Internet y la nueva sociedad de la información proponiendo el
establecimiento de nuevas legislaciones que hagan efectiva la salvaguarda de derechos que pretende el Convenio. Hemos llegado entonces a una concientización de que si el derecho interno no regula la protección de datos, la Directiva y el Convenio resultan ineficaces. En este protocolo cuyos alcances se discuten aún en el Consejo de Ministros, se propone
concretamente un control público pero independiente, obligatorio y efectivo. Recomiendan además hacer un llamado de invitación para la adherencia del Convenio de otros Estados e incluso de los propios Estados de la Unión Europea que aún no lo han ratificado, con el fin de “reforzar la coherencia del orden constitucional europeo”. Pareciera por tanto que la sociedad de la información es la que podría implementar efectivamente ese orden universal al que Habermas y sus seguidores aspiran, sobre todo en momentos que se necesita la colaboración de todos los Estados para controlar el avance tecnológico de la mano del derecho. El Protocolo Adicional si bien hace referencia al orden constitucional europeo, reconoce la importancia de tres aspectos trascendentales:

1.) Que ese orden normativo regional, se conseguirá en esta materia con la adherencia de los Estados al Convenio 108 y a la Directiva.
2.) Que no basta la adhesión a los instrumentos legales de la región, sino que los Estados deben ajustar su normativa internapara hacer aplicables los mínimos de protección que se acuerdan en el seno de las organizaciones conjuntas.
3.) La participación activa de Estados que no son miembros de la Unión Europea resulta imprescindible, pues el flujo de datos supera los limites fronterizos, temporales y sociales que puedan imponerse, situación que exige un acuerdo más universal.

Pero existen otras disposiciones en la región que complementan tanto el Convenio 108 como la Directiva 95/46/CE. Se trata de la Directiva 97/66/CE del Parlamento Europeo y del Consejo del 15 de diciembre de 1997 relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones y publicada por el Diario Oficial del 30 de enero de 1998; así como la Recomendación R (95) 4 del Comité de Ministros del 7 de febrero de 1995 sobre la protección de datos personales en servicios de telecomunicación.

Sin que mi objetivo sea ahondar en el contenido de estos dos documentos, es importante dejar constando su existencia pues contienen una serie de normas que protegen al individuo en el nuevo mundo de las telecomunicaciones. Por ejemplo, como una novedad, esta segunda Directiva protege los derechos de las personas físicas, pero también lo que denominan “intereses legítimos” de las personas jurídicas, situación que adquiere trascendencia ante el manejo especial de datos en entidades sindicales o políticas. No debemos olvidar, sin embargo, que la protección de las datos de carácter personal no puede amparar por sí mismas la protección de los datos de una empresa, con el fin de favorecer el secretismo de sus actividades. Muy por el contrario, se deben buscar medidas para que se preserve la transparencia de las actuaciones de las personas jurídicas al amparo de los principios de libertad de empresa, libre competencia y la defensa de los derechos del consumidor.

La Directiva 97/66/CE regula la protección de datos en las guías telefónicas, ya sea en su versión impresa (que es la usual) o en versiones electrónicas incluso en infovías, indicando que deben ser accesibles a los usuarios con todos los servicios de información correlativos, que los datos de los abonados sean los necesarios para su identificación y consagra el derecho de exclusión para que el usuario pueda decidir si está o no en la guía telefónica respectiva. Los usuarios también adquieren con esta Directiva la potestad de pedir la omisión de datos que determinen su dirección o sexo en las guías respectivas.

Se prohibe el cruce de datos contenidos en guías telefónicas con los de otros ficheros, sin que se previeran excepciones en beneficio del principio de libertad de comercio, situación que implica en este campo una protección demasiado rigurosa a un aspecto de la intimidad.

Dentro del tema de facturación y tráfico, se le otorga el derecho al usuario de recibir facturas no desglosadas que impidan a terceros conocer el origen o destino de sus llamadas y se hace un llamado a proteger la seguridad y confidencialidad de los datos como principio máximo de la Directiva e incluso se le exige al proveedor del servicio informar al usuario sobre los riesgos de seguridad en la red.

La interceptación de las comunicaciones para escucha, grabación o almacenamiento está absolutamente prohibida salvo si el interesado lo consiente o por seguridad pública (art.14). La Directiva dedica también un amplio articulado a garantizar el secreto a las telecomunicaciones por parte de los operadores de redes y servicios.

Igualmente, esta Directiva regula aspectos de las nuevas tecnologías en materia de identificación y localización de llamadas, que puede ser suprimida con un proceso expedito, llamadas de servicios de telemarketing, desvío automático de llamadas, etc.. Sobre este punto, la Recomendación R (95) hace alusión a la seguridad de la telefonía móvil, cuyo desarrollo ha sido enorme en la última década.

La Directiva 97/66/CE fue incorporada parcialmente a la normativa española a través del Real Decreto 1736/1998 del 31 de julio que aprueba el Reglamento por el que se desarrolla el Título III de la Ley General de Telecomunicaciones. El Título V del Real Decreto se refiere específicamente a la Protección de los datos personales en la prestación de los servicios de telecomunicaciones.

En España, otras normas que regulan la protección de los datos personales en beneficio del derecho a la intimidad, son las siguientes:

1. Ley Orgánica 1/1982 del 5 de mayo, relativa a la Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la propia Imagen.

2. Código Penal en sus arts. 197, 205, 208, 210, 212 y 510.

3. Ley Orgánica 5/1992 del 29 de octubre sobre regulación del Tratamiento Automatizado de los Datos de Carácter Personal. (LORTAD) Esta, si bien se encuentra derogada, es un punto de referencia importante para el desarrollo legislativo sobre la materia en este país.

4. Ley Orgánica 15/1999 del 13 de diciembre sobre protección de datos de carácter personal publicada en el BOE del 14-12-99.

Toda esta normativa, por tanto, constituye el marco jurídico aplicable en España para la protección de datos personales, que siempre deberá evaluarse periódicamente a la luz del avance tecnológico universal y el desarrollo de las legislaciones en derecho comparado.

Además, en España existe el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal publicado por el BOE 151 del 25 de junio de 1999. Este cuerpo normativo fue aprobado en virtud del artículo 9 de la Ley Orgánica 5/1992 del 29 de octubre, que exigía la adopción de medidas reglamentarias específicas que garantizaran la seguridad en los ficheros. No obstante haber sido emitido en virtud de una normativa derogada, el texto sigue vigente pese a la omisión actual del legislador de emitir un reglamento en virtud de la nueva Ley de protección de datos.

Dentro de la exposición de motivos de este Reglamento, se evidencia la concientización del legislador en la necesidad de adoptar medidas de seguridad por vía legal con el fin de hacer cumplir la protección efectiva de la vida privada de los ciudadanos en lo que respecta al tratamiento de sus datos personales. Al efecto dice el legislador:

> "El presente Reglamento tiene por objeto el desarrollo de lo dispuesto en los artículos 9 y 43.3.h) de la Ley Orgánica 5/1992. El Reglamento determina las medidas de índole técnica y organizativa que

> garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado. (...) Las medidas de seguridad que se establecen se configuran como las básicas de seguridad que han de cumplir todos los ficheros que contengan datos de carácter personal, sin perjuicio de establecer medidas especiales para aquellos ficheros que por la especial naturaleza de los datos que contienen o por las propias características de los mismos exigen un grado de protección mayor."

En las últimas dos décadas esta práctica normativa se ha extendido tanto en Europa como en otros continentes, situación que evidencia una innegable necesidad de conminar a otros Estados a adoptar medidas de protección similares, con el fin de no hacer ilusoria una protección universal que ya resulta necesaria ante el poder de las infovías y las nuevas tecnologías de la información.

En su libro *La protección de datos en Europa* (*34)* Miguel Angel Davara reúne la lista de las diversas legislaciones adoptadas por los países de la Unión Europea en torno la protección de datos, indicando además cuáles son los órganos en cada Estado, encargados de ejercer el papel de Autoridad de Control del manejo de ficheros, figura adoptada originalmente en Alemania bajo el nombre de *Bundesbeauftragter fur den Datenshutz* o Comisario Federal para la Protección de Datos, cuyas competencias en algunos países han recaído como recargo en el Defensor del Pueblo u *Ombudsman* (*35)*.

Las agencias de protección de datos en cada país, son una fuente de experiencia importante que debe ser evaluada por los países que inician sus nuevas regulaciones en la materia. Las recomendaciones emitidas por estas entidades, si bien son orientativas no son vinculantes por no emanar de un órgano legislativo. Sin embargo, a nivel formal se deben los usuarios suscribir a sus instrucciones en la medida que el registro de ficheros y el tratamiento de datos de los diversos sectores públicos y privados, así como la definición práctica de los niveles de seguridad, necesita una ordenación específica que debe ser idéntica para situaciones de igualdad entre los usuarios, de manera que se instauren procesos justos de exigencia en el tratamiento de datos que otorguen una verdadera seguridad jurídica a las partes involucradas.

Se trata, por supuesto, de concienciar a los legisladores de la nueva sociedad de la información de la necesidad de establecer medidas jurídicas que garanticen una conciliación justa y apropiada del derecho de la información con el derecho de la intimidad; ambos derechos fundamentales que sin embargo persiguen la protección de bienes jurídicos disímiles.

VI. LA EXPERIENCIA LATINOAMERICANA EN LA REGULACIÓN DEL HABEAS DATA

Como ya adelantamos, en América Latina la adopción de medidas que protejan al ciudadano ante el auge de la tecnología ha sido más lenta que en el resto del mundo, precisamente porque el desarrollo tecnológico ha llegado a estas naciones de forma tardía. La prioridad en esta región es lograr el acceso equitativo de los ciudadanos a los bienes informáticos que ya forman parte de la cotidianeidad en el primer mundo.

La escasez de recursos es evidente. La prioridad del Estado es reconocer dentro de sus limitaciones económicas el derecho del conocimiento o educación en el área de la informática que consiste en el derecho a formarse en las nuevas tecnologías, de reconocer un acceso adecuado a la línea o punto de conexión (línea telefónica, satelital, cable, etc...), proporcionar un acceso a un hardware o equipo físico así como a un software en condiciones técnicas que permitan la conexión a las infovías. De tal forma, en los países en vías de desarrollo es evidente que la protección de los derechos fundamentales ha quedado rezagada para una segunda etapa de transición, que sin embargo ya empieza a dar sus frutos.

Cada vez hay más países en Latinoamérica que se suman a la promulgación universal de leyes internas que protejan los derechos de sus ciudadanos ante el uso de la informática y los cambios generados por la nueva sociedad de la información.

En lo que respecta a la protección de datos de carácter personal, en la región se ha optado generalmente por establecer legislaciones bajo la denominación de "Leyes sobre *Habeas Data*", recurriendo a tal recurso como la vía de defensa de la intimidad de los ciudadanos ante la manipulación indiscriminada de sus datos.

Argentina fue pionero en el establecimiento de una legislación adecuada sobre el tema. En su Constitución Nacional existen dos artículos que amparan la adopción de lo que es hoy en día su normativa en torno al *Habeas Data*, y se trata de los artículos 18 y 19 que a la letra dicen:

> "Artículo 18.- (...) El domicilio es inviolable como también la correspondencia epistolar y los papeles privados; y una ley determinará en que casos y con qué justificativos podrá procederse a su allanamiento y ocupación (...)"

> “Artículo 19.- Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral publica, ni perjudiquen a un tercero, están solo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ello no prohibe.”

Sin embargo, es el artículo 43, párrafo tercero, de la Constitución Nacional de 1994 el que recoge la protección de los datos personales de los ciudadanos al amparo del texto siguiente:

> “Artículo 43. (...) Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.“

Resulta importante el antecedente constitucional pues la inclusión de una protección expresa del tratamiento de datos en la constitución Política, otorga un rango de protección especial a este derecho que asegura la vinculación ulterior de los tribunales constitucionales en la elaboración jurisprudencial y doctrinal de este derecho.

Las leyes se han ido adoptando a esta nueva disposición, y en 1998 se promulga la Ley de Tarjetas de Crédito, No. 25.065, cuyo artículo 53 dice:

"Las entidades emisoras de Tarjetas de Crédito, bancarias o crediticias tienen prohibido informar a las bases de datos de antecedentes financieros personales sobre los Titulares y beneficiarios de extensiones de Tarjetas de Crédito u opciones cuando el Titular no haya cancelado sus obligaciones, se encuentre en mora o en etapa de refinanciación. Sin perjuicio de la obligación de informar lo que correspondiere al Banco Central de la República Argentina. Las entidades informantes serán solidaria e ilimitadamente responsables por los daños y perjuicios ocasionados a los beneficiarios de las extensiones u opciones de Tarjetas de Crédito por las consecuencias de la información provista". A la luz de esa ley, se han emitido directrices que regulan la seguridad de los datos crediticios y financieros de los deudores, tales como la Comunicación A 2729 del BCRA (36) y la Comunicación A 2950 del BCRA(37) .

El 14 de septiembre del 2000 los diputados argentinos aprueban la Ley de protección de datos personales y *Habeas Data* (38) convirtiéndose en una de las pocas regulaciones estatales del continente que contemplan de forma detallada el *Habeas Data* como un recurso novedoso para la protección de la intimidad ante la informática.

La Ley de *Habeas Data* argentina recoge acertadamente, entre otros asuntos, los principios generales ya analizados en la Directiva de la comunidad europea, y se centra además en el derecho de los ciudadanos a recibir información. En virtud de esa última prerrogativa, los familiares de los desaparecidos en el régimen de la dictadura militar, poseen el derecho de acceso a archivos militares que pudiesen contener la información que antes les había sido vedada, con el fin de determinar el destino de sus familiares.

Hay que destacar que el proceso argentino se ajusta a las tendencias europeas que exigen una protección constitucional del derecho a la intimidad en el tratamiento de datos personales y la posterior regulación normativa a través de leyes que especifiquen tanto la regulación de la materia como el *Habeas Data* como un recurso procesal para exigir el respeto de lo dispuesto por las leyes especiales.

En la Constitución de Brasil de 1998, el artículo quinto, LXXII, consagra la existencia del *Habeas Data* como un recurso procesal para asegurar el conocimiento de la información registrada sobre la persona y como el medio para ejercer el derecho de rectificación de dichos datos. En este caso si bien aún no existe una ley sobre la protección de datos, sí existe un texto legal de naturaleza procesal denominado Ley nº 9.507, del 12.11.97, *Regula o direito de acesso a informações e disciplina o rito processual do Habeas data.*

El artículo 2 inciso 6 de la Constitución Peruana de 1993 prohibe el suministro de información que afecte la intimidad personal o familiar a través de archivos informatizados y consagra igualmente el recurso de *Habeas Data* en el artículo 200, como procedimiento para la defensa de una serie de derechos derivados de la nueva sociedad de la información: la libertad informática, la protección de la intimidad, el honor, la voz y la imagen. Además, en Perú ya se ha aprobado la Ley sobre *Habeas Data*, Ley No. 23.061 del 2 de Mayo de 1994 (39) ; siendo esta nación uno de los países con una regulación más completa sobre protección de datos.

La Constitución Política de 1987 de Nicaragua señala en su artículo 26 inciso 4 el derecho de todo ciudadano a conocer la información que sobre su persona han registrado las autoridades estatales, así como su derecho a saber porqué y con qué fin existe esa información. Una norma similar en contenido está recogida en la Constitución Política del Ecuador de 1998 cuyo artículo 94 dice:

Artículo 94.- Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional. (40)

Por su parte, en Paraguay también se ha optado por establecer la protección expresa de la intimidad en la manipulación de los datos personales, así como la garantía constitucionalmente reconocida del *Habeas Data* según lo revelan los siguientes artículos de la Constitución Política:

> "Artículo 28.- Se reconoce el derecho de las personas a recibir información veraz, responsable y ecuánime. Las fuentes públicas de información son libres para todos. La ley regulará las modalidades, plazos y sanciones correspondientes a las mismas, a fin de que este derecho sea efectivo. /Toda persona afectada por la difusión de una información falsa, distorsionada o ambigua tiene derecho a exigir su rectificación o su aclaración por el mismo medio y en las mismas condiciones que haya sido divulgada, sin perjuicio de los demás derechos compensatorios."
>
> *"Art.30.* - La emisión y la propagación de las señales de comunicación electromagnética son del dominio público del Estado, el cual, en ejercicio de la soberanía nacional, promoverá el pleno empleo de las mismas según los derechos propios de la República y conforme con los convenios internacionales ratificados sobre la materia. La ley asegurará, en igualdad de oportunidades, el libre acceso al aprovechamiento del espectro electromagnético, así como al de los instrumentos electrónicos de acumulación y procesamiento de información pública, sin más límites que los impuestos por las regulaciones internacionales y las normas técnicas. Las autoridades asegurarán que estos elementos no sean utilizados para vulnerar la intimidad personal o familiar y los demás derechos establecidos en esta Constitución."
>
> "Artículo 135. (...) Toda persona puede acceder a la información y a los datos que sobre sí misma o sobre sus bienes obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos si fuesen erróneos o afectaran ilegítimamente sus derechos."

La Constitución Política chilena, si bien contempla normas genéricas de protección a la intimidad, no expresa abiertamente una norma específica sobre el tratamiento de datos personal o el *Habeas Data*. Es la Ley de Protección de Datos Personales aprobada en 1999 la que define los alcances de la protección de la intimidad en el manejo, archivo y disposición de los datos de los ciudadanos. En el año 2000, el Ministerio de Justicia aprobó el Decreto 779-2000 que es el Reglamento del Registro de Bancos de Datos Personales a cargo de organismos públicos, separando con ello el tratamiento de datos de ficheros públicos de lo que respecta al tratamiento que otorgan los ficheros privados.

Valga citar también la inclusión de la protección de datos en la Constitución Política Colombiana cuyo artículo 15 en lo que interesa dice:

> Artículo 15.- Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
>
> De igual modo tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley. (41)

En Costa Rica, la Asamblea Legislativa tiene pendiente de aprobación bajo el expediente No. 12.827 el proyecto de ley conocido como *Habeas Data* (42) , que pretende adicionar un capítulo nuevo que regule el indicado recurso dentro de la Ley de Jurisdicción Constitucional (No. 7135 del 19-10-89). Dicho proyecto fue impulsado ante el evidente perjuicio a la intimidad que provocaban ficheros bancarios sobre morosos que en esa nación eran distribuidos entre bancos estatales y privados para limitar la capacidad crediticia de quienes constaban en tal lista. El texto legal que consta como proyecto de ley, pretende constituir una herramienta procesal para que personas físicas y jurídicas puedan proteger, de manera procedimental, el derecho de la persona a su intimidad, imagen, honor, autodeterminación informativa y libertad informática en el tratamiento de sus datos personales,

incorporando los principios y prerrogativas de protección legal que se incluyen en el Convenio 108 y en la Directiva Europea analizada supra.

Otra de las inquietudes del legislador costarricense fue la amplitud de lo que se denomina “Secreto de Estado”, denominación bajo la cual podría estarse ocultando información personal de los ciudadanos en detrimento de su intimidad y más específicamente, de su autodeterminación informativa.

En Costa Rica, no existe norma constitucional que prevea el recurso de *Habeas Data*, pese a la existencia del artículo 23 sobre la protección de la intimidad de los ciudadanos. El desarrollo del recurso de *Habeas Data*, sin embargo, se ha dado en la jurisprudencia desde hace algunos años, aplicando la defensa de la intimidad del individuo a través del Recurso de Amparo.

Efectivamente, la tendencia ha sido aprovechar la existencia de la figura procesal del Recurso de Amparo para ejercer la protección de la intimidad que le correspondería por especialidad al recurso de *Habeas Data*. No obstante, los Estados han comprendido la necesidad de conformar el *Habeas Data* como un recurso independiente que otorgue protección efectiva al afectado en la disponibilidad de la información que se recabe de su persona ya sea por sujetos de derecho público o privado, tutelando lo que se ha llegado a denominar la “autodeterminación informativa” como una facultad del individuo de ejercer acciones concretas ante el uso indiscriminado, falso, equívoco, excesivo, incorrecto, inexacto o ilegítimo de sus datos.

VII. BALANCE DE LA AUTODETERMINACIÓN INFORMATIVA EN AMÉRICA LATINA

La autodeterminación informativa, como ya adelanté en la primera parte de este estudio, es la transformación del derecho a la intimidad como un derecho de acción en defensa de los intereses personales, que otorga la facultad de ingresar a bases de datos y ejercer las acciones necesarias para conocer, acceder, corregir, actualizar, cambiar, incluir e incluso eliminar datos recabados con o sin consentimiento del sujeto. En general, el recurso pretende resguardar la identidad informática de la persona y evitar la constitución de perfiles subjetivos que pudiesen alterar el derecho a la intimidad, al honor, a la imagen y a la autodeterminación del individuo.

Finalmente, como iniciativa regional, a finales de la década pasada la Asamblea General de la Organización de Naciones Unidas adoptó al respecto la “Directriz para la Regularización de Ficheros Automáticos de Datos Personales” (43) que pretende conminar a los Estados miembros a adoptar la regularización interna para la defensa de la intimidad de los ciudadanos en la manipulación de sus datos de carácter personal.

Sin entrar en un exhaustivo análisis de estas legislaciones, basta indicar que en la carrera del derecho por ajustarse a los avances tecnológicos, se han cometido ciertos errores legislativos que deben ser evaluados a la luz de la experiencia de las naciones cuya normativa ya ha sido perfeccionada. Si se pretende incluir un recurso de *Habeas Data*, debe existir conciencia de la necesidad de adoptar una legislación previa, específica y pertinente que proteja la manipulación de datos a través de ficheros automatizados y manuales tanto en la empresa privada como en los órganos gubernamentales.

La mayoría de iniciativas americanas (incluyendo el proyecto de ley de la República de Costa Rica) carecen de la regulación inicial de los ficheros y de mecanismos que permitan a los encargados de tales ficheros adoptar las medidas básicas para garantizar al ciudadano tanto la protección de su intimidad como el acceso a los registros, situación que permitiría el control adecuado que se pretende. Esta situación deviene en una inseguridad jurídica con respeto al uso diario de estos ficheros o bases de datos e incluso, ante este vacío legal queda sin definir lo que debe entenderse como datos de carácter personal y los datos públicos. Por tanto, se ha optado por acudir directamente a un mecanismo o herramienta procesal que resulta debilitada ante aquella omisión, y se deja en manos de lo que será la jurisprudencia, la delimitación de la nueva figura legal que nos ocupa en este estudio. Esto ha provocado en Latinoamérica que la figura del *Habeas Data* adquiera distintas dimensiones con respecto a la figura europea, que muchas veces redundan en una mejora de la misma, y otras podrían implicar su estancamiento o inaplicabilidad.

Ante la falta de presupuesto para establecer órganos dedicados a la exclusiva vigilancia del cumplimiento de la protección de los datos en las empresas privadas y públicas o bien para el control de los ficheros; las legislaciones latinoamericanas optaron por redimensionar las funciones de órganos ya existentes (generalmente de índole judicial) evitando con ello menos burocracia. Esa ventaja, sin embargo, podría eventualmente crear un rezago en el desarrollo de esta figura (ya de por sí cambiante), debido a la inexistencia de órganos especializados y la imposibilidad de los juzgados de asumir eficientemente nuevas tareas o ejercer acciones cautelares inmediatas sin que se les dote de más recurso humano, logístico, técnico y económico.

Al *Habeas Data* latinoamericano se le han adicionado nuevas utilidades y áreas de protección que redundan en beneficio de una mejor defensa de los derechos de los ciudadanos. Por ejemplo, basta citar el caso de Argentina en donde tal recurso ha permitido el esclarecimiento de casos relacionados con el destino de los “desaparecidos”

en las dictaduras militares, al proporcionar acceso a los archivos donde tal información constaba desde hacía décadas.

Latinoamérica se ha separado esta vez de la tendencia legislativa impuesta por los Estados Unidos de Norteamérica en materia de Derecho Informático. Si la nación del norte aboga por no adoptar (por protección al sector privado) el *Habeas Data* sino dejar que se genere una autorregulación de las fuerzas comerciales basadas únicamente y de forma eventual en códigos de ética o en políticas de *puerto seguro*; Latinoamérica por su parte ha tomado conciencia de la necesidad de proteger al individuo ante la revolución tecnológica. Sin embargo, considero necesario que más que una herramienta judicial o procesal (como pretende hacerlo por ejemplo la República de Costa Rica), el Recurso de *Habeas Data* debe constituirse al amparo de una ley de protección de datos que adicionalmente sea respaldada por una norma de rango constitucional expresa para la materia.

No basta entonces con implementar un recurso procesal si existe un vacío legal importante que determine responsabilidades de los individuos y señale cuáles son las conductas anómalas que implicarían la violación de los derechos del afectado, así como las medidas de seguridad mínimas que se deben adoptar en cada caso de conformidad con el tipo de dato referido o el nivel de seguridad necesario para su resguardo. Dejar en manos de la jurisprudencia la construcción de este nuevo derecho, no es una alternativa que a mi juicio sea viable por la inseguridad jurídica que genera tanto para el usuario como para quienes deban manipular bancos de datos donde conste información personal de los ciudadanos.

Debemos enfrentar la necesidad de crear figuras jurídicas que se adapten a los nuevos requerimientos del mercado pero protegiendo como prioridad los derechos fundamentales de los usuarios. Se debe buscar un equilibrio entre los intereses de los ciudadanos y los intereses comerciales. La ley debe prever no establecer límites extremos que impidan el libre funcionamiento de las redes de información y del comercio electrónico (que es la inquietud planteada en Estados Unidos), pero tampoco desamparar a los ciudadanos en el libre ejercicio, goce y respeto de los derechos fundamentales que les corresponden. Dentro de esta idea, finalizo el presente estudio con una reflexión muy elocuente al respecto de Watson & Chervokas que dice:

"Solo porque la ley ignore la realidad, no quiere decir que la realidad va a cambiar y como resultado, los negocios y la industria continuarán bajo el asalto de las nuevas tecnologías hasta que desarrollemos mecanismos conscientes de principios básicos de dominio tecnológico que no impliquen la detención de su desarrollo."(44)

CITAS BIBLIOGRAFICAS

(1) Se habla por tanto indistintamente de derecho informático, de Habeas Data, de libertad informática, de derecho de la autodeterminación informativa y del derecho de la intimidad informática o informatizada. No obstante, no corresponde en este estudio ahondar en la naturaleza jurídica correcta de lo que *ab initio* considero efectivamente como un nuevo derecho fundamental. Para ello, aunque no comparta todas sus reflexiones, recomiendo la lectura del Dr. **RIASCOS GÓMEZ**, Libardo Orlando. *La visión iusinformática del derecho a la intimidad, no es un nuevo derecho fundamental.* En http://www.informatica-juridica.com/trabajos.asp?trabajo=ponencia.html

(2) Por ocultarse los mismos al usuario, como por ejemplo los datos de conexión, los que identifican el IP (dirección personal de la computadora o protocolo de Internet).

(3) CORRIPIO GIL-DELGADO, María de los Reyes. *Regulación Jurídica de los tratamientos de datos personales realizados por el sector privado en Internet.* Agencia de Protección de Datos, Madrid, 2001, p.175

(4) WARREN, Samuel y Louis Brandes. *El derecho a la intimidad*. Editorial CIVITAS, Madrid, 1995. Publicado originalmente en 1890 bajo el título *The Rigth to Privacy,* en la "Harvard Law Review" No. 5.

(5) SUÑÉ LLINAS, Emilio. *Tratado de Derecho Informático*. Volumen 1, Universidad Complutense de Madrid, Madrid, 2000, p. 36

(6) FERNANDEZ ESTEBAN, María Luisa. *Nuevas tecnologías, Internet y Derechos Fundamentales.* Mc Graw-Hill Interamericana de España, Madrid, 1998, p.139

(7) La fecha exacta de promulgación de la Ley de Hesse fue el 7 de octubre de 1970.

(8) SUÑÉ LLINAS, Emilio. *Tratado de Derecho Informático*. Volumen 1, Universidad Complutense de Madrid, Madrid, 2000, p. 37

(9) Recordemos por ejemplo la diferencia de la concepción comercialista del *Copyright* en comparación con la concepción humanista (o centrada en los derechos morales del autor) del *Droit d´auteur* de la doctrina francesa que han asumido la Unión Europea y los países de tradición latina.

(10) El artículo 35 regula la protección de datos personales en los registros informáticos, con miras a resguardar la intimidad de los ciudadanos.

(11) Constitución Política Española, art. 18.4

(12) **RIASCOS GÓMEZ**, Libardo Orlando. *La visión iusinformática del derecho a la intimidad, no es un nuevo derecho fundamental*. En http://www.informatica-juridica.com/trabajos.asp?trabajo=ponencia.html

(13) Esta ley es conocida como "Data Lag", que protege a los individuos del uso de la informática en la manipulación de sus datos.

(14) Recordemos sin embargo el antecedente de la "Datenshutz" del 7 de abril de 1970 del Estado alemán de Hesse que es el origen de la Datenshutz Federal.

(15) Igualmente, recordemos que el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, consagra también la protección de datos de carácter personal.

(16) Esta sentencia del Tribunal Constitucional Federal (Bundesverfassungsgericht) declara parcialmente con lugar el alegato de disconformidad de La Ley de Censo de Población del 4 de marzo de 1982
(Volkszählungsgesetz) con la Grundgesetz.
(17) LUCAS MURILLO, Pablo. *Derecho a la autodeterminación informativa.* Editorial Tecnos, Madrid, 1990,
p. 116.
(18) Ver en este sentido, LUCAS MURILLO, Pablo. *Derecho a la autodeterminación informativa.* Editorial
Tecnos, Madrid, 1990, p. 98.
(19) Sentencia del Tribunal Constitucional español, No. 134/1999 del 15 de julio de 1999.
(20) Sentencia del Tribunal Constitucional español, No. 292/2000 de 30 de noviembre de 2000.
(21) La libertad informática reconocida como un derecho fundamental perteneciente a los derechos de la tercera generación, es en esta materia la facultad del individuo de autodeterminación informativa, entendida como el derecho de ejercer acciones contra el ilegítimo procesamiento automatizado (o manual) de los datos de carácter personal e implica el correlativo deber de terceros de respetar su intimidad en la manipulación legítima de esos datos.
(22) DAVARA, Miguel Angel. *Manual de Derecho Informático*. Editorial Aranzadi, Madrid, 1997,p. 47.
(23) Boletín Judicial Constitucional No. 33, p.159
(24) Sentencia del Tribunal Constitucional No. 254/1993 del 20 de julio, publicada en el BOE 197 del 18 de
agosto de 1993.
(25) La sentencia del Tribunal Superior de Justicia de Cataluña, Sala de lo social del 14 de noviembre del 2000 sentencia 9382/2000 sobre Recurso de suplicación del DEUTSCHE BANK; la sentencia de la Audiencia Nacional, Sala de lo Social No. 17/2001 del 6 de noviembre del 2000 del Banco BBVA de España y en tercer lugar la sentencia del Juzgado de lo Social # 31, No. 3271 del 26 de marzo del 2001 de NCR de
(26) Fiona Shevill, Isora Trading Inc. Chequepoint SARL & Chequepoint International Ltd v. Press Alliance
S.A., C. 68/93, Rep. 1-0415
(27) La distinción entre datos públicos y privados ha generado fuertes discusiones doctrinales, pues un dato
público puede llegar a convertirse en un dato trascendente (propio de la esfera íntima o privada)
dependiendo del contexto en el que se le llegue a registrar, y por ende estar sujeto a regulaciones más
estrictas.
(28) Si bien aludo en este punto a "profesionales", téngase en consideración que la Directiva tampoco precisa que el interés científico, histórico, artístico, periodístico o estadístico sea alegado por un profesional en tales ramas, por lo que incluso podríamos interpretar que cualquier ciudadano que invoque tal interés puede tener acceso a datos personales de terceros y utilizarlos sin ningún obstáculo, por lo que la profesionalidad es algo que debió prever el texto legal para exigir, por ejemplo, responsabilidades derivadas del ejercicio legítimo de la profesión o bien tener una simple garantía del uso de los datos.
(29) SUÑÉ LLINÁS, Emilio. *Tratado de Derecho Informático*. Volumen 1, Universidad Complutense de Madrid, Madrid, 2000, p. 107.
(30) Nuevamente la inspiración personalista europea cede ante la orientación comercial propia de la nueva política de occidente, y de las tendencias actuales de la sociedad de la información.
(31) GALINDO, Fernando. *Derecho e informática*. La Ley-Actualidad, Madrid, 1998, p.87.
(32) Dichos informes se localizan en la página de Internet: www.coe.fr
(33) La versión oficial en francés de este documento se encuentra a disposición del público en la página de Internet: www.coe.fr
(34) DAVARA, Miguel Angel. *La protección de datos en Europa. Principios, derechos y procedimiento.* Grupo Asnef Equifax, Madrid, 1998 p. 204.
(35) En países latinoamericanos que, como veremos, no han instaurado la figura de una Agencia de Protección de Datos, es el Defensor de los Habitantes (o del Pueblo) quien, acorde con sus funciones y con el fin de seguir en la política de economía de recursos estatales, podría asumir algunas de las competencias ya citadas para velar por el cumplimiento de la protección de datos de los ciudadanos tanto dentro de la Administración Pública como en la empresa privada.
(36) Este texto se encuentra disponible en la página: www.bcra.gov.ar/pdfs/texord/clasdeud/pdf
(37) Este texto se encuentra disponible en la página: www.bcra.gov.ar/pdfs/texord/A2950/pdf
(38) Dicho texto se encuentra disponible en la página www.juschubut.gov.arg/ley4244.htm
(39) Texto disponible en la página: www.congreso.gob.pe
(40) Texto disponible en la página: http://www.cldonline.org/habeasdata.html
(41) Texto disponible en la página: www.georgetown.edu/LatAmerPolitical/Constitutions/Colombia/colombia.html
(42) Dicho proyecto fue declarado inconstitucional por haberse infringido en su proceso de aprobación ciertos requisitos formales que exige la Constitución Política de Costa Rica, por lo que el proceso de estudio y votación se ha retomado en el seno de la Asamblea Legislativa para enmendar el procedimiento. La Sala Constitucional, sin embargo, no emitió su pronunciamiento sobre el fondo del proyecto. (Voto No. 5958-98
de las 14:54 horas del 19 de agosto de 1998)
(43) Dicho texto se encuentra disponible en la página: www.onu.org
(44) Traducción libre del artículo "Open Source: Philosophy lies at the heart of media bussiness" de Watson & Chervokas." En Internet: www.newaydirect.com/watson&Chervokas/Philosophy .

VIII. BIBLIOGRAFIA

DOCTRINA:

CORRIPIO GIL-DELGADO, María de los Reyes. *Regulación jurídica de los tratamientos personales realizados por el sector privado en Internet.* Agencia de Protección de Datos, Madrid, 2000,.
DAVARA, Miguel Angel. *Manual de Derecho Informático*. Editorial Aranzadi, Pamplona, 1997.
DAVARA RODRÍGUEZ, Miguel Ángel. *Derecho informático*. Aranzadi, Pamplona, 1993.
DAVARA, Miguel Angel. *La protección de datos en Europa. Principios, derechos y procedimiento.* Grupo Asnef Equifax, Madrid, 1998.
FERNÁNDEZ ESTEBAN, María Luisa. *Nuevas tecnologías, Internet y Derechos Fundamentales*. Mc Graw-Hill Interamericana de España, Madrid, 1998.

GALINDO, Fernando. *Derecho e informática*. La Ley-Actualidad, Madrid, 1998.
HABERMAS, Jürgen. *La inclusión del otro*. Editorial Paidós, Barcelona, 1999.
LUCAS MARIN, Antonio. *La nueva sociedad de la información*. Editorial Trotta, Madrid, 2000.
LUCAS MURILLO, Pablo. *Derecho a la autodeterminación informativa*. Editorial Tecnos, Madrid, 1990.
MUÑOZ MACHADO, Santiago. *La regulación de la red. Poder y derecho en Internet*. Editorial Taurus, Madrid, 2000.
PEREZ LUÑO, Antonio Enrique. *Nuevas tecnologías, sociedad y derecho. El impacto socio-jurídico de las N.T. de la información.* FUNDESCO, Madrid, 1987.
RUIZ MIGUEL, Carlos. *La configuración constitucional del derecho a la intimidad*. Tecnos, Madrid, 1995.
SUÑÉ LLINÁS, Emilio. *Tratado de Derecho Informático*. Volumen 1, Universidad Complutense de Madrid, Madrid, 2000.
TEODORO I SADURNÍ, Jaume. *Intercambio electrónico de datos(EDI).* Ministerio de Obras públicas, Transportes y Medio Ambiente. Dirección General de Telecomunicaciones, Madrid, 1994..
VÁZQUEZ GALLO, Enrique y BERROCAL COLMENAREJO, Julio. *Comercio Electrónico, materiales para el análisis*. Ministerio de Fomento, Madrid, 2000.
VELAZQUEZ BAUTISTA, Rafael. *Protección Jurídica de datos personales automatizados*. Editorial COLEX, Madrid, 1993.
WARREN, Samuel y Louis Brandes. *El derecho a la intimidad*. Editorial CIVITAS, Madrid, 1995.

ARTÍCULOS DIGITALES:

BUSCHIAZZO (Sebastián). *Habeas Data: La solución latinoamericana al problema de protección de datos*. http://www.econolink.com.ar/derintern/derinter3.htm
CARRANZA TORRES (Luis). *Caracteres generales del Habeas Data*. http://www.informatica-juridica.com/trabajos.asp?trabajo=caracteres_generales_del_corpus_habeas.htm
GUADAMUZ (Andrés). *Habeas Data: The Latin-American response to Data Protection*. http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html#2.2
IRIARTE AHON (Erick). *Habeas Data*. http://publicaciones.derecho.org/redi/No.-03-octubre-de-1998/erick
NÚÑEZ PONCE (Julio). *La acción constitucional de Habeas Data y la comercialización judicial en Internet*. http://publicaciones.derecho.org/redi/No._13_agosto_de_1999/data
PALAZZI (Pablo). *El Habeas Data en el Derecho Argentino*. http://publicaciones.derecho.org/redi/No.-o4- noviembre-de-1998/palazzi
PUCCINELLI (Oscar Raúl). *El Habeas Data en el constitucionalismo indoiberoamericano*. http://www.enlsaperu.com/nleg/article/277DOC04.htm
RIASCOS GÓMEZ (Libardo Orlando). *La visión iusinformática del derecho a la intimidad, no es un nuevo derecho fundamental*. http://www.informatica-juridica.com/trabajos.asp?trabajo=ponencia.html
TORRES CARRANZA (Luis R.). *Caracteres generales del Habeas Data*. www.informatica-juridica.com/trabajos.asp?trabajo=caracteres--generales_del corpues-habeas.htm
WATSON & CHERVOKAS. *Open Source: Philosophy lies at the heart of media bussiness*. www.newaydirect.com/watson&Chervokas/Philosophy.

(*) La autora de este artículo es costarricense, socia y Directora del Area de Propiedad Intelectual de Active-Lex. Es Licenciada en Derecho, Notaria Pública y Máster en Literatura de la Universidad de Costa Rica. Especialista en Derechos de Autor (Ginebra, Suiza). Máster en Informática y Derecho y Doctoranda en Derecho Constitucional de la Universidad Complutense de Madrid. Asesora Legal de la UNED de Costa Rica. Email: acastro@activelex.com

---

Tomada de http://www.alfa-redi.org/upload/revista/120902--12-58-Microsoft%20Word%20-%20HABEAS%20DATA.pdf.
