

**UNIVERSIDAD DE GRANADA**

**FACULTAD DE DERECHO**

**DEPARTAMENTO DE DERECHO CIVIL**

**Tesis Doctoral**

**ESTUDIO COMPARADO DEL RÉGIMEN  
JURÍDICO DE LOS FICHEROS DE  
SOLVENCIA PATRIMONIAL Y CRÉDITO  
EN ESPAÑA, ITALIA Y BRASIL**

**Doctoranda**

**Ludmila Albuquerque Douettes Araújo**

**1531**

**Granada 2010**

Editor: Editorial de la Universidad de Granada  
Autor: Ludmila Albuquerque Douettes Araújo  
D.L.: GR 762-2012  
ISBN: 978-84-693-6008-8

**ESTUDIO COMPARADO DEL RÉGIMEN JURÍDICO DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO EN ESPAÑA, ITALIA Y BRASIL**

**Ludmila Albuquerque Douettes Araújo**

**ESTUDIO COMPARADO DEL RÉGIMEN JURÍDICO DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO EN ESPAÑA, ITALIA Y BRASIL**

Tesis doctoral presentada por la licenciada en Derecho Ludmila Albuquerque Douettes Araujo, bajo la dirección de los Profesores Dr. D. Guillermo Orozco Pardo, Catedrático de Derecho Civil y Dr. D. Jose Luis Pérez Serrabona Catedrático de Derecho Mercantil en la Universidad de Granada, para la obtención del grado de doctor.

**ESTUDIO COMPARADO DEL RÉGIMEN JURÍDICO DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO EN ESPAÑA, ITALIA Y BRASIL**

**Ludmila Albuquerque Douettes Araújo**

**ESTUDIO COMPARADO DEL RÉGIMEN JURÍDICO DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO EN ESPAÑA, ITALIA Y BRASIL**

**DOCTORANDA:**

**LUDMILA ALBUQUERQUE DOUETTES ARAÚJO**

**DIRECTORES:**

**DR. GUILLERMO OROZCO PARDO**

CATEDRÁTICO DE DERECHO CIVIL

**DR. JOSE LUIS PEREZ-SERRABONA**

CATEDRÁTICO DE DERECHO MERCANTIL

## DEDICATORIA

A mis padres, **Ângela** y **Felix**, que me han enseñado a través de sus ejemplos de vida, día tras día, la importancia de la dedicación al estudio y el esfuerzo del trabajo, valores sembrados en la tierra de su cariño y su comprensión. A vosotros, dedico el fruto materializado de un sueño, que habeis apoyado y confiado tan de cerca que aún en la distancia os he podido sentir y fortalecerme en vuestro amor.

A los que un día despiertos han sembrado un sueño, y en algún lugar, durmiendo, lo ven brotar sus flores: **Felix** de Sousa Araujo y **Heleno** Soares.

## AGRADECIMIENTOS

A **Dios**, por haberme iluminado y me dado la fuerza necesaria para vencer los desafíos.

A **toda mi familia**. A mis padres, **Ângela** Cristine Albuquerque Araújo y **Félix Araújo** Filho; a mis hermanos, **Laise** y **Fernando** Araújo;

A mi hermano **Felix** y mi cuñada **Juliana**: jamás habría conseguido dar mis primeros pasos aquí, en el Viejo Mundo, si no fuese por vuestra acogida, vuestro apoyo y vuestro cariño. Me habéis abierto todas las puertas, y yo, a vosotros, os mantendré siempre abierto mi corazón lleno de gratitud.

A **Maria de Felix** y **Elizete**; a **Felizinho** y **Nicole** Araújo; a **Tamar**, **Isabella** y **Edivanete**. También, a **Ana** Regina y **Alexandre** Albuquerque; **Celino** Neto y **Rodrigo** Celino; **Ricardo** y **Pedro**; Les agradezco su preocupación, incentivo y participación.

De modo muy, muy especial a mi tío **Adalberto** Albuquerque, por todas y cada una de las veces que me ha apartado del camino aquellas piedras que siquiera me ha dejado verlas;

A **Juan**, **Lola**, **Magdalena** y **Paco**, mi familia española. Habeis creado en mi las raíces más profundas del amor de aquella que considero mi segunda patria, España. A vosotros, la expresión de mi más sincero afecto y gratitud.

A mi novio, **Juan Manuel**, que ha sido siempre la brisa afable que me ha traído la alegría y la esperanza para seguir navegando en las aguas de un sueño que lo ha hecho también suyo. He buscado en esta misteriosa

ciudad la realización de un proyecto académico y he encontrado el tesoro más sublime de su amor. A ti, mi puerto seguro en el Mar Mediterráneo, que tienes anclado en tus aguas a este barco esperando zarpar contigo hacia otros mares de sueños, mi gratitud y mi amor..

A los **Departamentos de Derecho Civil y Mercantil** de la Universidad de Granada (UGR): A todos los *profesores, doctorandos, becarios y funcionarios*, en especial a mi querido maestro y amigo Dr. **Guillermo Orozco Pardo** y al Dr. **José Luis Pérez-Serrabona**.

Al prof. Dr. Jose Antonio **Navarro** y prof. Dr. **Klaus Jochen Albiez Dohrmann**.

E igualmente a Dña. **Beatriz** Arquelladas y Dña. **Soledad** Lozano.

A la Università de Roma Trè, en especial a profesora **Liliana Rossi Carleo**. También, a **Elisabetta** Quagliado por todo su apoyo en mi estancia en Roma.

Al *Garante per la protezione dei dati personali*, en especial a **Riccardo Sanchini**.

A mis amigas doctorandas **Thamara, Fabiana y Eveline**, por las horas echadas compartiendo las mismas preocupaciones, miedos, *saudades*, pero sobre todo celebrando cada una de las victorias conseguidas.

A los amigos queridos que nos hacen olvidar y soportar la distancia: **María** Lafuente, **Marta Vélez**, **Verónica** Martin Cabrera y **Francesco** Lugliese; **Conchi** Martinez y J. **David** Peinado. A las familias **Torres Cardona** y **Ruiz Vílchez**.

A la embrujada **Granada**. A mi tierra, **Campina Grande** (Paraíba, Brasil).

## **ÍNDICE**

<b>ABREVIATURAS .....</b>	<b>- 13 -</b>
<b>RESUMEN (CASTELLANO) .....</b>	<b>- 16 -</b>
<b>RESUMO (PORTUGUÉS) .....</b>	<b>- 24 -</b>
<b>CAPITULO PRIMERO: EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA .....</b>	<b>- 32 -</b>
<b>I. Planteamiento General. ....</b>	<b>- 33 -</b>
<b>II. El derecho a la autodeterminación informativa y la sentencia alemana sobre la ley del censo de 1983. ....</b>	<b>- 39 -</b>
<b>III. El derecho a la autodeterminación informativa en España.....</b>	<b>- 45 -</b>
<b>1. La polémica entre el derecho a la intimidad y el derecho a la autodeterminación informativa. ....</b>	<b>- 48 -</b>
<b>2. El derecho fundamental autónomo a la autodeterminación informativa. La posición doctrinal y jurisprudencial. ....</b>	<b>- 53 -</b>
<b>IV. El derecho a la protección de datos personales y la evolución normativa y jurisprudencial en Italia.....</b>	<b>- 62 -</b>
<b>V. El derecho a la autodeterminación informativa en el derecho brasileño. ....</b>	<b>- 83 -</b>
<b>1. El derecho brasileño y la tutela de los datos personales. ....</b>	<b>- 86 -</b>
<b>2. El fundamento jurídico-constitucional del derecho a la autodeterminación informativa en el sistema jurídico brasileño. ....</b>	<b>- 90 -</b>
<b>3. El “Habeas Data”.....</b>	<b>- 95 -</b>



VI. Toma de Posición.....	110 -
<b>CAPITULO SEGUNDO: LEYES DE PROTECCIÓN DE DATOS. PERSPECTIVA HISTÓRICA Y CONCEPTOS ACTUALES.....</b>	<b>125 -</b>
<b>I. La evolución legislativa de la protección de los datos personales en Europa.....</b>	<b>126 -</b>
1. El Consejo de Europa: el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. ....	133 -
2. La Directiva del Consejo 95/46, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos. ..	136 -
<b>II. La ley de protección de datos de carácter personal en España.....</b>	<b>140 -</b>
1. Evolución legislativa.....	140 -
2. La Ley Orgánica de protección de datos personales nº 15/1999. ....	149 -
2.1 Objeto de la ley y su ámbito de aplicación. ....	149 -
2.2. Los principios de la protección de datos en la LOPD. ....	152 -
2.2.1 <i>La Calidad de los datos.</i> ....	153 -
2.2.2. <i>Principio del consentimiento.</i> ....	155 -
2.2.3. <i>Información en la recogida de datos.</i> .....	171 -
2.2.4. <i>Seguridad de los datos.</i> ....	174 -
2.2.5. <i>Deber de secreto.</i> ....	177 -
<b>III. La ley de protección de datos de carácter personal en Italia.....</b>	<b>179 -</b>
1. Evolución legislativa.....	179 -
2. El Texto Único en materia de protección de datos personales italiano .....	186 -
3. La finalidad de la ley. ....	189 -
4. El Código en Materia de protección de datos personales italiano y los Códigos de Buena Conducta.....	192 -
<b>VI. Las definiciones generales en las leyes de protección de datos española e italiana.....</b>	<b>194 -</b>
1. Datos de carácter personal.....	196 -
1.1. Concepto y características en la LOPD. ....	196 -
1.2. Concepto y características de dato personal en el <i>Codice in materia di protezione dei dati personali</i> .....	202 -

# ESTUDIO COMPARADO DEL RÉGIMEN JURÍDICO DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO EN ESPAÑA, ITALIA Y BRASIL

Ludmila Albuquerque Douettes Araújo

<b>2. Tratamiento de datos personales.....</b>	<b>210 -</b>
2.1. La noción de tratamiento de datos personales en la LOPD.....	210 -
2.2. La noción de tratamiento de datos personales en el <i>Codice in materia di protezione dei dati personali</i> .....	211 -
<b>3. Fichero.....</b>	<b>215 -</b>
3.1. El concepto de fichero en la LOPD.....	215 -
3.2. El concepto de fichero en el <i>Codice in materia di protezione dei dati personali</i> .....	217 -
<b>4. Cesión o comunicación de datos.....</b>	<b>219 -</b>
<b>5. Los responsables del fichero o tratamiento y los encargados del tratamiento.....</b>	<b>220 -</b>
5.1. Los conceptos en la LOPD.....	220 -
5.2. Los conceptos en el <i>Codice in materia di protezione dei dati personali</i> .....	224 -
<b>6. Afectado o interesado.....</b>	<b>226 -</b>
6.1. España.....	226 -
6.2. Italia.....	227 -
<b>7. Fuentes accesibles al público.....</b>	<b>228 -</b>
7.1. España.....	228 -
7.2. Italia.....	233 -

## CAPITULO TERCERO: ASPECTOS GENERALES DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL Y CREDITO .....- 234 -

### I. Cuestiones preliminares.....- 235 -

### II. Marco normativo de los ficheros de solvencia patrimonial y crédito...- 236 -

1. Marco normativo español.....	237 -
2. Marco normativo italiano.....	238 -
3. Marco normativo brasileño.....	240 -

### III. La finalidad de los ficheros.....- 242 -

1. La finalidad de los ficheros de solvencia patrimonial y crédito.....	247 -
1.1. Los ficheros de solvencia patrimonial y crédito y la crisis económica mundial de 2008.....	254 -
1.2. La vinculación de la consulta a las informaciones de los ficheros de solvencia patrimonial y crédito y el reparto del riesgo de la operación de concesión del crédito..	260 -

### IV. Objeto de los ficheros de solvencia patrimonial y crédito.....- 265 -

1. Legislación Española.....	265 -
2. Legislación Italiana.....	281 -

3. Legislación Brasileña.....- 287 -

V. Los destinatarios de la información de los ficheros de solvencia patrimonial y crédito.....- 295 -

CAPITULO CUARTO: .....- 314 -

PARTE I: EL TRATAMIENTO DE LOS DATOS SOBRE LA SOLVENCIA PATRIMONIAL Y CRÉDITO DE LOS INDIVIDUOS EN ESPAÑA E ITALIA. ....- 314 -

I. Introducción.....- 315 -

II. Los requisitos para la inclusión de los datos.....- 317 -

1. La Legislación Española. ....- 317 -

1.1. Datos sobre solvencia patrimonial y crédito.....- 318 -

1.2. Datos sobre el cumplimiento e incumplimiento de obligaciones dinerarias. ....- 322 -

1.2.1. Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada.....- 324 -

1.2.2. Inexistencia de reclamación sobre la deuda. ....- 325 -

1.2.3. Existencia de un principio de prueba que contradiga los requisitos de inclusión...- 328 -

1.2.4. Límite temporal de tratamiento de los datos.....- 332 -

1.2.5. Requerimiento de pago. ....- 334 -

1.2.6. Conservación de documentación. ....- 339 -

1.2.7. Información previa a la inclusión de datos. ....- 343 -

1.2.8. Consecuencias de la no observancia de los requisitos de inclusión de los datos. ....- 348 -

2. La Legislación Italiana.....- 351 -

2.1. Cuestiones preliminares.....- 351 -

2.2 Requisitos y categorías de datos.....- 353 -

2.2.1. Tratamiento de datos provenientes de fuentes públicas. ....- 356 -

III. Modalidad de recogida y registro de los datos.....- 357 -

1. Legislación Española. ....- 358 -

1.1. Notificación de inclusión.....- 359 -

1.1.1. Datos sobre solvencia patrimonial y crédito.....- 359 -

# ESTUDIO COMPARADO DEL RÉGIMEN JURÍDICO DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO EN ESPAÑA, ITALIA Y BRASIL

Ludmila Albuquerque Douettes Araújo

1.1.2. Datos sobre el cumplimiento e incumplimiento de obligaciones dinerarias. ...	367 -
1.2. Información en el recabo de los datos. ....	372 -
<b>2. La Legislación Italiana</b> .....	373 -
2.1. La información en la recogida de los datos. ....	377 -
<b>IV. Acceso a la información contenida en el fichero</b> .....	<b>381 -</b>
1. Legislación Española. ....	381 -
2. Legislación Italiana.....	384 -
<b>V. Conservación y actualización de los datos</b> .....	<b>386 -</b>
1. Legislación Española. ....	386 -
2. Legislación Italiana.....	391 -
<b>VI. Ejercicio de los derechos de acceso, rectificación, cancelación y oposición</b> . ....	<b>395 -</b>
1. Legislación Española .....	395 -
2. Legislación Italiana.....	399 -
<b>VII. Particularidades de la legislación italiana</b> . ....	<b>403 -</b>
1. Uso de técnicas o sistema automatizado de credit scoring.....	403 -
2. Medidas de seguridad de los datos .....	405 -
3. Sanciones .....	406 -
<b>PARTE II: EL TRATAMIENTO DE LOS DATOS SOBRE LA SOLVENCIA PATRIMONIAL Y CRÉDITO DE LOS INDIVIDUOS Y LA LEGISLACIÓN BRASILEÑA</b> . ....	<b>408 -</b>
<b>I. Introducción</b> .....	<b>409 -</b>
<b>II. Requisitos y categorías de datos</b> . ....	<b>413 -</b>
<b>III. Modalidad de recogida y registro de los datos</b> .....	<b>426 -</b>
<b>IV. Acceso a la información</b> .....	<b>432 -</b>

# ESTUDIO COMPARADO DEL RÉGIMEN JURÍDICO DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO EN ESPAÑA, ITALIA Y BRASIL

Ludmila Albuquerque Douettes Araújo

V. Conservación y actualización de los datos.....	436 -
VI. Los derechos del afectado .....	444 -
1. El derecho al acceso .....	444 -
2. El derecho de rectificación.....	448 -
3. El derecho de información.....	452 -
3.1. Forma, contenido y acreditación de la notificación.....	457 -
3.2. La comunicación y los datos recabados de fuentes accesibles al público.....	462 -
4. El <i>Habeas Data</i> y los derechos del afectado.....	470 -
4.1. El ejercicio de los derechos del interesado.....	472 -
5. Sanciones .....	478 -
CONCLUSIONES (ESPAÑOL) .....	482 -
CONCLUSÕES (PORTUGUÊS).....	493 -
ÍNDICE BIBLIOGRÁFICO .....	504 -
A. Fuentes legislativa, jurisprudencial y documentos de las agencias de protección de datos.....	504 -
A.1. Legislación.....	504 -
A.1.1. <i>Internacional y Comunitaria</i> .....	504 -
A.1.2. <i>España</i> .....	505 -
A.1.3. <i>Italia</i> .....	506 -
A.1.4. <i>Brasil</i> .....	506 -
A.2. Jurisprudencia.....	507 -
A.2.1. <i>España</i> .....	507 -
A.2.2. <i>Italia</i> .....	511 -
A.2.3. <i>Brasil</i> .....	512 -
A.2.4. <i>Otras Sentencias</i> .....	515 -
A.3. Documentos de las Agencias de Protección de Datos.....	516 -
A.3.1. <i>España</i> .....	516 -
A.3.2. <i>Italia</i> .....	518 -
B. Bibliografía .....	519 -
C. Bibliografía digital .....	546 -
C.1. Artículos.....	546 -

**ESTUDIO COMPARADO DEL RÉGIMEN JURÍDICO DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO EN ESPAÑA, ITALIA Y BRASIL**

**Ludmila Albuquerque Douettes Araújo**

C.2. Periódicos y documentos electrónicos.....	- 550 -
C.3. Fuentes digitales consultadas.....	- 552 -

## ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
AN	Audiencia Nacional (España)
Amp.	Ampliada
Art. /Arts.	Artículo/Artículos
BOE	Boletín Oficial del Estado
CAI	Centrale d'Allarme Interbancaria
Cap./cap.	Capítulo
CCAA	Comunidades Autónomas
CCB	Código Civil de Brasil
CCE	Código Civil de España
CDC	Código de Defensa del Consumidor de Brasil
CE	Constitución Española
CF	Constitución Federal de Brasil
Cfr.	Confróntese
CICR	Comitato Interministeriale del Crédito e del Risparmio
Coord.	Coordinador
DEJF	Diário Eletrônico da Justiça Federal (Brasil)

# ESTUDIO COMPARADO DEL RÉGIMEN JURÍDICO DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO EN ESPAÑA, ITALIA Y BRASIL

Ludmila Albuquerque Douettes Araújo

DJU	Diario da Justiça
DOUE	Diario Oficial de la Unión Europea
Ed.	Edición
IVAP	Instituto Vasco de Administración Pública
LO	Ley Orgánica
LOPD	Ley Orgánica 5/1999, de 13 de diciembre, de protección de datos de carácter personal Ley Orgánica 5/1992, de 29 de octubre, de regulación del
LOTARD	tratamiento automatizado de los datos de carácter personal
OCDE	Organización para la Cooperación y el Desarrollo Económico
ONU	Organización de las Naciones Unidas
Op. Cit.	Obra Citada
Pág./p.	Página
Págs./pp.	Paginas
PL	Proyecto de ley
RD	Real Decreto
REP	Revista de Estudios Políticos
Rev.	Revisada
RPD	Reglamento 1720/2007, de 21 de diciembre, de desarrollo de la Ley Orgánica 15/1999
RT	Revista dos Tribunais (Brasil)
s./ss.	Siguiente/Siguientes



# ESTUDIO COMPARADO DEL RÉGIMEN JURÍDICO DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO EN ESPAÑA, ITALIA Y BRASIL

Ludmila Albuquerque Douettes Araújo

SIA	Società Interbancaria per l'Automazione
SIS	Sistema Informativo Schegen
SPC	Fichero brasileño denominado Serviço de Proteção ao Crédito
STC	Sentencia del Tribunal Constitucional de España
STF	Supremo Tribunal Federal de Brasil
STJ	Superior Tribunal de Justicia de Brasil
STS	Sentencia del Tribunal Supremo de España
TC	Tribunal Constitucional de España
TJ	Tribunal de Justicia
TJDF	Tribunal de Justicia del Distrito Federal de Brasil
TJRO	Tribunal de Justicia de Rondonia - Brasil
Trad.	Traducción
TS	Tribunal Supremo de España
TUB	Testo Único Bancario de Italia
UE	Unión Europea
V. Gr.	Verbigracia
Vol.	Volumen
Web/WWW	World Wide Web

## RESUMEN (CASTELLANO)

Son indudables los beneficios y ventajas que han traído el uso y el desarrollo de las nuevas tecnologías. Iniciamos este trabajo con esta primera consideración para que, fundamentalmente, quede transparente nuestra postura ante un fenómeno que por generalizado, ha provocado conceptualizar a nuestra sociedad como “sociedad de la información”.

Hoy por hoy, las tecnologías de información y comunicación (TIC) influyen de modo significativo en el desarrollo social, ocupando un papel decisivo, pues patrocinan el progreso en los más diversos aspectos de la vida colectiva o individual.

Sin embargo, es incontestable que estamos ante un fenómeno ambivalente, una vez que, tampoco se puede negar los peligros para los derechos fundamentales de los ciudadanos de las consecuencias de la utilización desenfrenada de todo el aparato tecnológico que se puede tener acceso en los días de hoy, además de los profundos cambios introducidos por esta nueva revolución de las tecnologías. No es por otra razón que respetados juristas como Pérez Luño<sup>1</sup> llega a afirmar que, “el horizonte actual de la ciudadanía que orienta y circunscribe las pautas de su ejercicio, se halla determinado por el desarrollo de las nuevas tecnologías de la información y la comunicación”.

Efectivamente, no es difícil aceptar la idea de que actualmente estamos en presencia de una convivencia entre un mundo físico y otro virtual y es

---

<sup>1</sup> PÉREZ LUÑO, Antonio Enrique. *Cibercidadani@ o ciudadaní@.com?*, Barcelona, Gedisa, 2004, p. 11.

inevitable que ello haya interferido en nuestro entorno social<sup>2</sup>. Esto ha ocurrido porque mucho de lo que antes solamente se vislumbraba en este mundo analógico, fue literalmente sustituido por el digital<sup>3</sup>. Hace apenas algunas décadas no se podía prever que estos dos espacios de convivencia humana en plataformas distintas pudiesen cohabitar de una manera tan próxima.

El hecho de que se utilice el término “virtual” puede que connote la idea de que dichos espacios se encuentren lejos, desplazados y apartados de nuestro entorno físico, lo que no es verdad. Ellos están habitados como cualquier otro y como ha resaltado J. Mitchell<sup>4</sup>, “usados y controlados por grupos determinados de gente, tienen sus costumbres locales y su cultura, y su carácter va de lo íntimo y privado a lo globalmente público”.

En realidad, el modelo social que hoy vivimos está absolutamente integrado e interconectado a través de redes tecnológicas que sin ninguna duda han roto las barreras de tiempo y de espacio<sup>5</sup>. Todo esto está

---

<sup>2</sup> Para Paul Saffo, existen dos universos paralelos: el cotidiano universo analógico que habitamos y un nuevo universo digital creado por humanos, pero habitados por las máquinas digitales. «Sensors: The Next Wave of Infotech Innovation», <http://www.saffo.com/essays/sensors.php>, acceso en 1 de abril de 2008.

<sup>3</sup> Por poner un ejemplo, los ficheros manuales son cada vez más escasos. Es decir, las nuevas tecnologías permitieran que muchas actividades fuesen reemplazadas de su forma material para una digital, como es el caso del almacenamiento de datos.

<sup>4</sup> J. MITCHELL, William. *E-topía*. Valderrama, Fernando (trad.). Barcelona: Gustavo Gili, 2001.

<sup>5</sup> La diferencia esencial de los dos espacios estaría más en la forma de acceder a ellos que propiamente en su fondo. El espacio digital también es un mundo y, resáltese, más interconectado que el físico. La telecomunicación indudablemente ha revolucionado el modo de conectar a las personas. Las barreras físicas son casi inexistentes dentro de este ciberespacio. Antiguamente, cuando eran las líneas telefónicas las protagonistas del mayor acercamiento entre las distancias físicas, era fácil notar que lo que nos unía era el conjunto de maquinaria e hilos conductores. Hoy las redes inalámbricas siquiera

justificado por la diseminación y penetración del uso de la informática y telemática desde el instante en que extrapola el ámbito de las empresas públicas y privadas y alcanza también el doméstico, estimulado de modo vertiginoso por la Internet<sup>6</sup>.

Actualmente, las informaciones llegan cotidianamente a gran velocidad a las personas y, con independencia de que estas consigan o no captarlas en su totalidad, este hecho, traza una línea divisoria entre el presente y pocas décadas atrás, sin que se pueda precisar con exactitud a partir de cuándo ese torrencial de informaciones pasó a dominar el ambiente público y privado. Esa velocidad no se refleja solamente en una sensación social, sino que efectivamente es la principal característica de los medios tecnológicos puestos a disposición de esta colectividad. En definitiva, el

---

permiten que nuestros ojos perciban a través de qué estamos conectados, tampoco donde nos llevan y cuanto a los aparatos, estos a cada día se reducen.

<sup>6</sup> En 1997, Paul Staffo previa que la próxima grande sorpresa se verificaría en la World Wide Web. Eso porque en aquella época la Web estaba definida para persona que accedían a informaciones. Para él, en los años subsiguientes el foco de la Web cambiaría para un nuevo modelo de personas que se conectarían a otras personas en un ambiente rico en informaciones. En otras palabras, la Web dejaría de ser un ambiente de información para transformarse en un entorno interpersonal en el cual las informaciones serían una importante pieza para el desarrollo de las interacciones humanas. «Sensors: The Next Wave of Infotech Innovation», *op. cit.*, acceso en 1 de abril de 2008. En 18 de marzo de 2008, la comScore, Inc, compañía dedicada a proover a empresas informaciones globales sobre el comportamiento de los consumidores en Internet, publicó un estudio que pone de relieve los cambios en el mundo sobre el uso de la red mundial de ordenadores entre el período de enero de 2007 a enero de 2008. Concluye que los mercados emergentes – América Latina, Asia, Oriente Medio y África – en un año, han experimentado un significativo crecimiento por encima de la media en el número de usuarios de Internet, mientras que América del Norte y Europa han crecido a tasas más modestas. Según este estudio, la región de Asia se pone en la cumbre con más de 300 millones de accesos, seguida por Europa. En <http://www.comscore.com/press/release.asp?press=2115>, acceso en 20 de abril de 2008.

desarrollo informático posibilita suplir la demanda exigida por la nueva sociedad, y que implica una de sus mayores riquezas: la información<sup>7</sup>.

Este nuevo parámetro de *modus vivendi*, basado principalmente en la relación directa de proporcionalidad información-poder, ha exigido una nueva respuesta jurídica de reglamentación en la utilización de los medios tecnológicos, buscando el equilibrio de éste y la riqueza que guarda la concentración de informaciones, paralelamente a la protección de derechos fundamentales que confrontan directamente con estos dos principales vectores de la nueva sociedad: la tecnología y la información.

Es en esta perspectiva donde surge el problema de la privacidad y de los datos personales. Dicho aspecto orbita en las más diversas esferas de la vida humana, muy distintas hoy de las que se planteaban Warren y Brandeis<sup>8</sup>. Una de ellas, es la vertiente del hombre-consumidor.

Actualmente, el ciudadano se enfrenta a numerosos y diversos problemas que una sociedad consumista informatizada provoca al requerir cada vez más la necesidad de obtener informaciones diversificadas sobre la faceta individual. Algunas veces las empresas procuran conocer mejor a su público, no solamente al colectivo, sino también al individual. No obstante, esto no es una característica propia o inventada en la actualidad. El acopio de información, ya se sabe que desde épocas anteriores se hacía, pero manualmente. Sin embargo, indudablemente hoy es un producto de gran valor para cualquier

---

<sup>7</sup> En la opinión de Castells, “Debido a la convergencia de la evaluación histórica y del cambio tecnológico, hemos entrado en un modelo puramente cultural de interacción y organización sociales. Por ello, la información es el ingrediente clave de nuestra organización social, y los flujos de mensajes constituyen la fibra básica de nuestra estructura social”. CASTELLS, Manuel. *La era de la información*, Vol. 1, Madrid: Alianza, 2001.

<sup>8</sup> Cfr. WARREN, Samuel, BRANDEIS, Louis. “The Right to Privacy”, *Harvard Law Review*, Vol. IV, No. 5, 1890

institución o empresa, sea pública o privada, además de ser responsable por determinar los rumbos de sus políticas empresariales. En verdad, lo que siempre hay que tener en cuenta, como resaltan Marx y Smith<sup>9</sup> con mucha propiedad, es que ninguna tecnología ha iniciado nunca una acción que no hubiera sido programada previamente por el ser humano. En definitiva, esta búsqueda por informar y por informaciones, actualmente, se ve extremadamente facilitada por las nuevas tecnologías. Y son la forma de conseguir las mismas y la manera de darlas a conocer que nos preocupa, para que no implique una vulneración de dos de los derechos fundamentales del ser humano: su privacidad y su autodeterminación informativa.

Concretamente, dentro de tales derechos una de las preocupaciones suscitadas es justamente la solvencia patrimonial y crédito. Nada más atractivo para las empresas que poseer datos sobre la real capacidad adquisitiva de sus potenciales clientes. Entender la protección de datos desde esta vertiente es de fundamental importancia para que se pueda plantear la orientación interpretativa de las leyes sobre ésta materia.

Este es, esencialmente, el objeto de esta investigación, analizar la “legitimidad” de los ficheros de solvencia patrimonial y crédito vistos desde la perspectiva del derecho a la protección de datos, en el ámbito del derecho comparado. Para ello se hace una palingenesia entre tres países: España, Brasil e Italia.

---

<sup>9</sup> MARX, Leo., SMITH, Merritt Roe. Historia y Determinismo Tecnológico. Madrid: Alianza, 1996, p. 15. Además, lo cierto es que las empresas se utilizan tanto de las nuevas tecnologías como también son responsables por la supervivencia de las “viejas tecnologías”, cuando conviene a su política empresarial. Como observó con mucha lucidez Richard S. Tedlow, profesor especialista en historia de la empresa en la Harvard Business School, “el auge y caída de las tecnologías se debe principalmente a una cuestión empresarial, y no al determinismo tecnológico”. En “Tecnologías que evolucionan y perduran”, El País, documento disponible en la pagina web: [http://www.elpais.com/artículo/espana/Tecnologias/evolucionan/perduran/elpeputec/20080412elpepunac\\_10/Tes](http://www.elpais.com/artículo/espana/Tecnologias/evolucionan/perduran/elpeputec/20080412elpepunac_10/Tes), acceso en 12/04/2008.

La idea de investigar este tema y haber elegido específicamente estos países ha surgido tras la observación de algunos factores principales: primero, la de constatar la necesidad de plantear los límites de la actuación de los ficheros de solvencia patrimonial y crédito en Brasil ante la continua evolución tecnológica pues la misma puede afectar a los derechos fundamentales de las personas; y segundo, la evolución del derecho a la protección de datos en Europa en las últimas décadas ha sido tan extremadamente relevante que ha llevado a este continente a un elevado grado de tutela del mencionado derecho. En este sentido, España e Italia poseen una matriz normativa común que es la Directiva 95/46, no obstante dentro de esa directriz, han elegido maneras distintas de legislar sobre la materia, sea por la forma, o por el contenido, dentro de los límites posibles.

Aparte de ello, resulta oportuno resaltar que en Brasil, la disciplina de los ficheros de solvencia patrimonial está ubicada en el Código de Defensa del Consumidor. En efecto, la cultura social y jurídica de este país en materia de protección de datos es aún muy incipiente, y desde nuestro punto de vista, los principios del derecho del consumidor no son suficientes, actualmente, para enfrentar todos los problemas derivados del uso abusivo de las nuevas tecnologías.

La relevancia y el aporte de este estudio también radica en ofrecer una nueva perspectiva para el derecho brasileño, en lo que concierne a los servicios de información crediticia, insertándole dentro del ámbito del derecho a la protección de datos, a través de la investigación comparada de países que notablemente han avanzado en éste tema como España e Italia.

La metodología utilizada fundamentalmente en este trabajo de investigación ha sido la documental y la bibliográfica. La principal dificultad que hemos encontrado para su realización, se ha centrado en la escasa historiografía específica sobre los ficheros de solvencia patrimonial

y crédito en España e Italia, al igual que los poquísimos estudios científicos generales en Brasil sobre la protección de datos, asimismo la laguna historiográfica especial de los sistemas de protección al crédito, vistos desde una perspectiva del derecho a la autodeterminación informativa.

Por ello, el presente trabajo de investigación es innovador y pretende contribuir notadamente en Brasil a un nuevo panorama interpretativo de los aludidos bancos de datos, alterando su óptica del derecho del consumidor para la protección de los datos personales. En este entorno, el estudio comparado ha sido determinante para centrar y delimitar las fronteras de la investigación.

Así, para la consecución de tal fin, hemos vertebrado este estudio en cuatro partes. En el **primer** capítulo se trata dentro de un análisis general como el derecho a la autodeterminación informativa fue recibido por los sistemas jurídicos italiano y español. En relación al ordenamiento jurídico brasileño, investigar si tal derecho está previsto constitucionalmente, y de este modo, si puede ser considerado como un derecho fundamental en éste, a través sobre todo del examen del alcance del derecho al Habeas Data tal y como se encuentra hoy en el texto constitucional. Como es obvio, al final se manifiesta nuestra posición al respecto.

En el **segundo**, se hace un análisis histórico de la evolución normativa europea en materia de protección de datos, para después identificar los principales trazos de la legislación general del aludido derecho en España e Italia y los principales conceptos relativos al tema que consideramos importantes para el estudio del objeto de ésta investigación.

Estos dos capítulos componen la primera parte introductoria de este trabajo, imprescindibles para trazar los fundamentos que deberán conducir la interpretación específica.



En el **tercero**, se comienza a ubicar la materia objeto de nuestro estudio, centrando los aspectos esenciales concernientes a la reglamentación específica de los ficheros de solvencia patrimonial y crédito. Es decir, la finalidad, el objeto y los destinatarios de los datos registrados en los sistemas de protección al crédito, analizando como cada legislación de los países estudiados ha dirigido su disciplina, identificando los aspectos esenciales que diferencian España e Italia y a partir de este examen, hacer una comparación con el sistema brasileño, emitiendo nuestra opinión sobre las posibles soluciones que pudiesen mejorar la legislación brasileña en estos aspectos.

El **cuarto**, se estructura en dos partes: en la primera, se desarrolla el tratamiento legal específico de los ficheros de solvencia patrimonial en el ordenamiento jurídico de España e Italia, identificando y descomponiendo sus principales elementos, encontrando las soluciones dadas por los reglamentos de uno y otro país de las cuestiones que conllevan el equilibrio de los intereses implicados. En la segunda, se analiza pormenorizadamente los mismos aspectos en la legislación brasileña, identificando las diferencias y principalmente las omisiones legislativas, buscando en la disciplina española e italiana sus principales matices y soluciones presentadas, sopesándolas con el sistema jurídico de Brasil y aportando nuestra posición y conclusiones, en la esperanza que puedan ayudar a mejorar la interpretación de la actividad desarrollada por los sistemas de protección al crédito en este país.

## RESUMO (PORTUGUÉS)

São evidentes os benefícios e vantagens do uso e o desenvolvimento das novas tecnologias. Iniciamos este trabalho com esta primeira consideração para que fique transparente nossa postura diante de um fenômeno que pela sua extensão levou a conceituar a nossa sociedade como uma “sociedade da informação”.

Atualmente, as tecnologias da informação e comunicação (TIC) influem de modo significativo no desenvolvimento social, ocupando um papel decisivo, vez que patrocinam o progresso nos mais diversos aspectos da vida coletiva ou individual.

Não obstante, é incontestável que estamos diante de um fenômeno ambivalente. Não se pode negar os perigos para os direitos fundamentais dos cidadãos no tocante às conseqüências da utilização desenfreada de todo o aparato tecnológico a que se pode ter acesso nos dias de hoje. São profundas as mudanças introduzidas por esta nova revolução das tecnologias. Não é por outra razão que respeitadíssimos juristas como Pérez Luño<sup>10</sup> chega a afirmar que “o horizonte atual da cidadania que orienta e circunscreve as pautas do seu exercício, se encontra determinado pelo desenvolvimento das novas tecnologias da informação e comunicação”.

Com efeito, não é difícil aceitar a idéia de que atualmente estamos presenciando uma convivência entre um mundo físico e outro virtual. É

---

<sup>10</sup> Pérez Luño, Antonio Enrique. *Cibercidadani@ o ciudadaní@.com?*, Barcelona, Gedisa, 2004, p. 11.

inevitável que tal realidade interfira no nosso entorno social<sup>11</sup>. Isto tem ocorrido porque muito do que antes unicamente se vislumbrava no mundo analógico foi, literalmente, substituído pelo digital<sup>12</sup>.

Há poucas décadas, não se podia prever que estes dois espaços de convivência humana em plataformas distintas pudessem coabitar de uma maneira tão próxima. O fato de utilizar-se do termo “virtual” pode remeter à conotação equivocada de que ditos espaços se encontram afastados, separados e distantes do nosso entorno físico, o que não é verdade. Eles interagem, e operam, como ressaltou J. Mitchell<sup>13</sup>, “controlados por grupos determinados de gente, que tem seus costumes locais e sua cultura, e seu caráter vai do íntimo e privado ao globalmente público”.

Em verdade, o modelo social que vivemos hoje está absolutamente integrado e interconectado através de redes tecnológicas que, sem nenhuma dúvida, quebraram as barreiras do tempo e do espaço<sup>14</sup>. Tudo

---

<sup>11</sup> Para Paul Saffo, existem dois universos paralelos: o cotidiano universo analógico que habitamos e um novo universo digital criado pelos humanos, mas habitados pelas máquinas digitais. “Sensors: The Next Wave of Infotech Innovation”, <http://www.saffo.com/essays/sensors.php>, acesso em 1 de abril de 2008.

<sup>12</sup> Por exemplo, os arquivos manuais são cada vez mais escassos. Ou seja, as novas tecnologias permitiram que muitas atividades fossem substituídas de sua forma física para uma digital, como é o caso do armazenamento de dados.

<sup>13</sup> J. MITCHELL, William. *E-topía*. Valderrama, Fernando (trad.). Barcelona: Gustavo Gili, 2001, p. 37.

<sup>14</sup> A diferença fundamental dos espaços residiria mais na forma de acessá-los do que propriamente no seu fundo. O espaço digital também é um mundo e, ressalte-se, mais interconectado do que o físico. As telecomunicações sem nenhuma dúvida revolucionaram o mundo. As barreiras físicas são quase inexistentes dentro deste *cyber* espaço. Antigamente, quando as linhas telefônicas eram as protagonistas da maior aproximação entre as distâncias físicas, era fácil notar que o que nos unia era um conjunto de maquinaria e fios condutores. Hoje, as redes sem fio sequer permitem

isso se justifica pela disseminação e penetração do uso da informática e telemática desde o momento em que extrapola o âmbito das empresas públicas e privadas, para alcançar também o doméstico, estimulado de modo vertiginoso pela Internet<sup>15</sup>.

Na atualidade, as informações chegam cotidianamente com grande velocidade às pessoas, independentemente de que estas consigam ou não captá-las na sua totalidade. Este fato traça uma linha divisória entre o presente e poucas décadas atrás, sem que se possa fixar com exatidão a partir de quando este torrencial de informações passou a dominar o ambiente público e privado. Essa velocidade não se reflete somente numa sensação social, mas, a rigor, é a principal característica dos meios tecnológicos postos a disposição do indivíduo e da coletividade. Definitivamente, o desenvolvimento informático possibilita suprir a

---

que nossos olhos percebam através de que estamos conectados, assim como onde nos levam e relativamente aos aparatos, estes cada dia se reduzem.

<sup>15</sup> Em 1997, Paul Staffo previa que a próxima grande surpresa se verificaria no World Wide Web. Isso porque naquela época a Web estava definida para pessoas que acessavam a informações. Para ele, nos anos subseqüentes o foco da Web mudaria para um novo modelo de pessoas que se conectariam a outras num ambiente rico de informações. Em outras palavras, a Web deixaria de ser um ambiente de informação para se transformar em um entorno interpessoal no qual as informações seriam uma importante peça para o desenvolvimento das inter-relações humanas. Em: "Sensors: The Next Wave of Infotech Innovation", *op. cit.*, acesso em 1º de abril de 2008. Em 18 de março de 2008, a ComScore, Inc, companhia dedicada a fornecer a empresas informações globais sobre o comportamento dos consumidores na Internet, publicou um estudo que ressalta as mudanças no mundo sobre o uso da rede mundial de computadores no período de janeiro de 2007 a janeiro de 2008. Conclui que os mercados emergentes – América Latina, Ásia, Oriente Médio e África – em um ano experimentaram um significativo crescimento por cima da media no numero de usuários de Internet, enquanto que América do Norte e Europa cresceram a taxas modestas. Segundo este estudo, a região da Ásia se coloca na ponta com mais de 300 milhões de acessos, seguida por Europa. Disponível em <http://www.comscore.com/press/release.asp?press=2115>, acesso em 20 de abril de 2008.

demanda exigida pela nova sociedade, e que é, também, uma das suas maiores riquezas: a informação<sup>16</sup>.

Este novo parâmetro de *modus vivendi*, baseado principalmente na relação direta de proporcionalidade informação-poder, tem exigido uma nova resposta jurídica de regulamentação na utilização dos meios tecnológicos, buscando de um lado o equilíbrio deste e a riqueza que guarda a concentração de informações, e paralelamente a proteção de direitos fundamentais que confrontam de modo direto com estes dois principais vetores desta nova sociedade: a tecnologia e a informação.

Nesta perspectiva surge o problema da privacidade e dados pessoais. Este aspecto orbita nas mais diversas esferas da vida humana, hoje muito distintas das que enfocavam Warren y Brandeis<sup>17</sup>. Uma delas é a vertente homem-consumidor.

Atualmente o cidadão enfrenta a numerosos e diversos problemas que uma sociedade consumista informatizada provoca ao necessitar cada vez mais de obter informações diversificadas sobre a faceta individual. Algumas vezes as empresas procuram conhecer melhor seu público, não apenas o coletivo, mas também o individual. Sem embargo, esta não é uma característica própria ou inventada na atualidade. Como se sabe, o armazenamento de informações já se fazia desde há muito, entretanto de forma manual. Não obstante, sem nenhuma dúvida, hoje é um produto de grande valor para qualquer instituição ou empresa, seja ela de natureza

---

<sup>16</sup> Na opinião de Castells, “Debido a la convergencia de la evaluación histórica y del cambio tecnológico, hemos entrado en un modelo puramente cultural de interacción y organización sociales. Por ello, la información es el ingrediente clave de nuestra organización social, y los flujos de mensajes constituyen la fibra básica de nuestra estructura social”. CASTELLS, Manuel. *La era de la información*, Vol. 1, Madrid: Alianza, 2001.

<sup>17</sup>Cfr. WARREN, Samuel, BRANDEIS, Louis. “The Right to Privacy”, *Harvard Law Review*, Vol. IV, No. 5, 1890

pública ou privada, além de ser responsável por determinar os rumos de suas políticas empresariais. Na verdade, o que sempre se deve levar em consideração, como ressaltam Marx y Smith<sup>18</sup> com muita propriedade, é que tecnologia nenhuma jamais iniciou uma ação que não tivesse sido programada previamente pelo ser humano. Definitivamente, esta procura por informar e por informações, nos dias atuais, é extremamente facilitada pelas novas tecnologias. E são as formas de conseguir estas ultimas e a maneira de divulgá-las que nos preocupa, para que não implique em uma vulneração de dois direitos fundamentais do ser humano: a privacidade e a autodeterminação informativa.

Concretamente, dentro de tais direitos, uma das preocupações suscitadas é justamente as informações relativas à solvência patrimonial e crédito. Nada mais atrativo para as empresas que possuir dados sobre a real capacidade aquisitiva dos seus potenciais clientes. Entender a proteção de dados a partir desta vertente é de fundamental importância para que se possa enfocar a orientação interpretativa das leis sobre esta matéria.

Este é, essencialmente, o objeto desta investigação: analisar a “legitimidade” dos bancos de dados de solvência patrimonial e crédito visto de uma ótica do direito a proteção de dados, no âmbito do direito comparado. Para tal fim, faz-se um confronto entre três países: Espanha, Brasil e Itália.

---

<sup>18</sup> MARX, Leo; SMITH, Merritt Roe. *Historia y Determinismo Tecnológico*. Madrid: Alianza, 1996, p. 15. Além disso, é verdade que as empresas se utilizam tanto das novas tecnologias como também são responsáveis pela sobrevivência das “velhas tecnologias”, quando convém a sua política empresarial. Como observou com muita lucidez Richard S. Tedlow, professor especialista em historia da empresa na Harvard Business School, “el auge y caída de las tecnologías se debe principalmente a una cuestión empresarial, y no al determinismo tecnológico”. Em “Tecnologías que evolucionan y perduran”, El País, texto disponible en [http://www.elpais.com/artículo/espana/Tecnologias/evolucionan/perduran/elpeputec/20080412elpepunac\\_10/Tes](http://www.elpais.com/artículo/espana/Tecnologias/evolucionan/perduran/elpeputec/20080412elpepunac_10/Tes), acceso en 12/04/2008.

A idéia de investigar esse tema e haver elegido especificamente estes países surgiu depois da observação de alguns fatores principais: primeiro, a constatação da necessidade de examinar os limites da atuação dos bancos de dados de solvência patrimonial e crédito no Brasil diante da continua evolução tecnológica, pois a mesma pode afetar aos direitos fundamentais das pessoas; e segundo, a evolução do direito a proteção de dados na Europa nas ultimas décadas tem sido muito relevante e por isso este continente goza atualmente de um alto grau de tutela deste direito. Neste sentido, Espanha e Itália possuem uma matriz normativa comum que é a Diretiva 95/46, não obstante dentro desta diretriz, cada um desses países elegeu modos distintos de legislar a matéria, seja pela forma, seja pelo conteúdo, dentro dos limites possíveis.

Ademais, deve-se ressaltar que no Brasil a disciplina dos bancos de dados de solvência patrimonial está localizada no Código de Defesa do Consumidor. De fato, a cultura social e jurídica deste país nesta matéria é ainda muito incipiente, e em nossa opinião, os princípios do direito do consumidor não são suficientes para enfrentar todos os problemas derivados das novas tecnologias.

A relevância e o aporte deste estudo também radica em oferecer uma nova perspectiva para o direito brasileiro, no que concerne aos serviços de informação creditícia, inserindo-lhes dentro do âmbito do direito a proteção de dados, através da investigação comparada entre países que notavelmente avançaram neste tema como Espanha e Itália.

A metodologia utilizada fundamentalmente neste trabalho de investigação é a documental e a bibliográfica. A principal dificuldade que encontramos para sua realização centrou-se na escassa bibliografia específica sobre os bancos de dados de solvência patrimonial e credito na Espanha e Itália, assim como os poucos estudos científicos empreendidos no Brasil sobre a proteção dos dados, da mesma forma que a lacuna

bibliográfica específica dos sistemas de proteção ao crédito, vistos de uma perspectiva do direito a autodeterminação informativa.

Por isso, o presente trabalho de investigação é inovador e pretende contribuir especialmente no Brasil a um novo panorama interpretativo dos aludidos bancos de dados, alterando sua ótica do direito do consumidor para a proteção de dados. Neste entorno, o estudo comparado foi determinante para centrar e delimitar as fronteiras desta investigação.

De forma que para a consecução de tal finalidade, estruturamos este estudo em quatro partes. No **primeiro** capítulo tratamos, dentro de uma análise geral, como o direito a autodeterminação informativa foi recebido pelos sistemas jurídicos italiano e espanhol. Em relação ao ordenamento jurídico brasileiro, investigamos se tal direito está previsto constitucionalmente e, deste modo, se pode ser considerado como um direito fundamental, através sobretudo do exame do alcance do direito ao *Habeas Data* tal e como se encontra hoje no texto constitucional. No final, manifestamos nossa opinião ao respeito.

No **segundo**, fazemos uma análise histórica da evolução normativa europeia em matéria de proteção de dados, para depois identificar os principais traços da legislação geral do mencionado direito na Espanha e na Itália e os principais conceitos relativos ao tema, que consideramos importantes para o estudo do objeto desta investigação.

Estes dois capítulos compõem a primeira parte introdutória deste trabalho, imprescindíveis para traçar os fundamentos que deverão conduzir a interpretação específica.

No **terceiro** capítulo, começamos a situar-nos na matéria objeto do nosso estudo, centrando os aspectos essenciais concernentes a regulamentação específica dos bancos de dados de solvência patrimonial e crédito. Ou seja, a finalidade, o objeto, e os destinatários dos dados



registrados nos sistemas de proteção ao crédito, analisando como cada legislação dos países estudados dirigiram sua disciplina, identificando os aspectos essenciais que diferenciam Espanha e Itália e a partir deste exame, fazer uma comparação com o sistema brasileiro, emitindo nossa opinião sobre possíveis soluções que pudessem melhorar a legislação brasileira nestes aspectos.

O **quarto** se estrutura em duas partes. Na primeira, discorreremos sobre o tratamento legal específico dos bancos de dados de solvência patrimonial no ordenamento jurídico espanhol e italiano, identificando e separando seus principais elementos, encontrando as soluções dadas pelas leis de um e outro país sobre as questões que equilibram os interesses implicados. Na segunda parte, analisamos pormenorizadamente os mesmos aspectos na legislação brasileira, identificando as diferenças e principalmente as omissões legislativas, buscando na disciplina da Espanha e Itália os principais matizes e soluções apresentadas, sopesando com o sistema jurídico brasileiro e aportando nossa posição e conclusões, na esperança de que possam ajudar a melhorar a interpretação da atividade desenvolvida pelos sistemas de proteção ao crédito neste país.

**CAPITULO PRIMERO: EL DERECHO A LA  
AUTODETERMINACIÓN INFORMATIVA**

## I. Planteamiento General.

La construcción del derecho a la autodeterminación informativa tal y como se encuentra configurada en la actualidad, extraído de la noción de intimidad (o *privacy*), se ha hecho a partir de reflexiones doctrinales y elaboraciones jurisprudenciales. Manifestaciones que aunque diferentes, tienen una relación muy estrecha. En ésta línea, en lo que concierne a la *privacy*, la doctrina atribuye su aparición por primera vez en la dialéctica jurídica en 1890, cuando lo suscitó Samuel Warren y Louis Brandeis<sup>19</sup>.

El perfil del llamado derecho a la autodeterminación informativa comienza a construirse, a partir de la década de los setenta<sup>20</sup>, cuando se da inicio a discusiones sobre la necesidad de buscar la respuesta jurídica a las nuevas exigencias sociales. Es decir, frente al peligro que podía suponer una informatización de datos, que pudiesen vulnerar algún derecho. Ante la gran ola tecnológica que se anunciaba, empezaba a percibirse el riesgo para muchos de los derechos fundamentales que podrían ser violados. Estaba surgiendo, sin ninguna duda, un nuevo espacio en el que hasta ese momento no había una tutela jurídica específica.

---

<sup>19</sup> WARREN, Samuel y BRANDEIS, Louis. "The Right to Privacy". *Harvard Law Review*. Vol. IV, nº. 5, Diciembre 1890.

<sup>20</sup> Para Frosini, "el momento crucial en la historia jurídica del "derecho a la privacidad", a la "libertad informática", ha sido marcado por las actas legislativas que se sucedieron después de 1970 y que abrieron un camino nuevo a lo largo del cual avanzaron decisivamente las legislaciones de los países de civilización industrial avanzada". FROSINI, Vittorio. "Banco de datos y tutela de la persona". *Revista de Estudios Políticos*, núm. 30 (Noviembre-Diciembre 1982), p. 25.

Como bien resalta Frosini<sup>21</sup>, la doctrina de la libertad informática tenía su matriz ideológica en la concepción de un nuevo liberalismo, dentro de la óptica social de aquella época, ubicado en un entorno de revolución tecnológica, y desarrollado desde una nueva perspectiva del derecho de libertad personal. En definitiva, para este autor, este derecho manifiesta un aspecto nuevo de la vieja idea de la libertad personal, “y constituye el avance de una frontera nueva de la libertad humana a través de la sociedad futura”.

El primer punto observado sobre esta temática, es su terminología. En Alemania, el ordenamiento jurídico utiliza la denominación “derecho a la autodeterminación informativa”. En Italia sin embargo, se puede apreciar que prácticamente no se usa la designación alemana, teniendo la doctrina italiana preferencia por los términos “*diritto alla riservatezza*”, “*privacy*”, o, la utilización de la expresión acogida por la legislación comunitaria, “*protezione dei dati personali*” para referirse a este nuevo derecho. Tal elección también refleja, como se verá, la intención de parte de la doctrina italiana en conferirle una autonomía respecto al derecho a la *riservatezza*. Con respecto a la doctrina española, podemos apreciar tanto la expresión germánica, como igualmente la denominada “libertad informática”.

Para encontrar el término preciso que exprese la tutela perseguida, tanto la jurisprudencia, doctrina, como las legislaciones, empiezan a enunciar lo que verdaderamente se pretende amparar<sup>22</sup>. Y esto ha sido así, porque con anterioridad era común su referencia de modo genérico, utilizando la expresión “protección de datos”, como por ejemplo en Alemania, con el uso del término *Datenschutz*, y el inglés *Data Protection*.

---

<sup>21</sup> FROSINI, Tommaso Edoardo. “Nuevas tecnologías y constitucionalismo”. *Revista de Estudios Políticos*, núm. 124, 2004, p. 131.

<sup>22</sup> Vid. PÉREZ LUÑO, Antonio Enrique. “El Derecho a la autodeterminación informativa”. En *Anuario de jornadas 1989-1990: (Servicio de Estudios del IVAP)*. Bilbao, 1991, p. 301 y ss.

De manera que la doctrina ha manifestado el carácter equívoco de tal designación, pues como opina Pérez Luño<sup>23</sup>, “parece evocar que el objeto de la protección jurídica son los datos, cuando, en realidad, lo son las personas concernidas en ellos”. En efecto, la pretensión de la tutela jurídica es proteger a las personas de una mala utilización de informaciones que les pueda concernir, y por lo tanto, para lograrla se impone un conjunto sistemático de derechos y deberes a todos los partícipes de los procesos que implica el tratamiento de información de carácter personal.

De esta manera, las leyes empezaron a especificar mejor su objeto como forma de evitar dilogía, así, el caso del Convenio del Consejo Europeo, para la **protección de las personas** con respecto al tratamiento de datos automatizados, y otras que han venido sucesivamente, como la Directiva 95/46, 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.

Sin embargo, la Ley Orgánica española, nº 15/1999, en nuestra opinión, no fue afortunada al titularse: Ley de protección de datos de carácter personal, al igual que, el *Codice in Materia di Protezione dei Dati Personali* italiano, contradiciendo de esta forma todos los esfuerzos de la legislación internacional y comunitaria por centralizar la finalidad de dichas normas en las personas.

La ausencia de uniformidad sea en el ámbito doctrinario, legislativo, o en el jurisprudencial, en el uso de las expresiones de este derecho retratan la dificultad actual de la ciencia jurídica en concebir en un único enunciado o de forma unívoca, el bien que se quiere proteger. Creemos que tanto el vocablo germánico como la “libertad informática” son términos que no se excluyen. Uno y otro pueden ser vistos como sinonimia jurídica, aunque exceptúa Pérez Luño<sup>24</sup>, que algunas

---

<sup>23</sup> *Ibid.*, p.303.

<sup>24</sup> *Ibid.*, p. 305.

formulaciones doctrinales conciben la expresión alemana como una categoría más restricta al entenderlo como una faceta de la intimidad o un aspecto del libre desarrollo, no obstante, el desarrollo jurisprudencial y teórico lo hacen coincidir con el alcance de la libertad informática.

A nuestro parecer, dichas expresiones reflejan un derecho subjetivo que asegura la protección del patrimonio informativo personal<sup>25</sup>. De ésta forma, la protección de datos sería el derecho objetivo que como tal, traza las normas de conducta que deben ser observadas, o por mejor decir, concretiza y disciplina el derecho subjetivo a la libertad informática. Sobre esa misma cuestión y recogiendo de nuevo la opinión del autor citado, él<sup>26</sup>, advierte que la protección de datos carecería de sentido si no se tradujera en un conjunto de garantías para las personas y la autodeterminación informativa o la libertad informática serían inconcebibles de no contar como presupuesto una opción axiológica *sobre* y un marco organizativo *de* la informática.

Por todo lo dicho, observase que si por un lado este derecho se inclina a proteger exclusivamente la privacidad, dejaría al margen todas las intromisiones ilegítimas a cualquier otro derecho que no estuviese con ella relacionado. De otra parte, habría que especificarse que objeto jurídico se pretende tutelar, siempre teniendo en cuenta que el derecho necesita paradójicamente de una tutela rigurosa, pero a la vez flexible, que pueda acompañar la principal característica del medio utilizado para afrontar lo que se pretende proteger: la velocidad de los cambios y del desarrollo tecnológico.

Además de todo ello, la discusión sobre el derecho a la protección de datos envuelve un debate sobre diversos derechos, fundamentales o no,

---

<sup>25</sup> Con esa expresión no se pretende conferir un contenido de derecho patrimonial a los datos personales, pero reforzar el conjunto de bienes subjetivos que posee el individuo tocante a las informaciones que les concierne.

<sup>26</sup> PÉREZ LUÑO, Antonio Enrique. *El Derecho a la... op. cit.*, p. 306.

que pueden verse afectados por la elaboración de informaciones, como resultado de un uso indebido de la tecnología.

Por tanto, los riesgos son innumerables. Las actuales sociedades que atingieran un nivel mínimo de desarrollo tecnológico, sea en el ámbito público o privado, necesitan del tratamiento automatizado de los datos para optimizar las funciones que les son inherentes. Dichas informaciones son recabadas para los más diversos propósitos y pueden ser almacenadas sin que actualmente existan límites físicos. En efecto, como bien observa Orozco Pardo<sup>27</sup>, que el tiempo y el espacio que antes se imponía, impedía que tuviesemos conocimiento de los hechos que protagonizados por los demás y operaban así, con salvaguardia de la “privacidad de la persona”. Sin embargo, a su sentir, estos límites han desaparecido hoy, de suerte que “tiempo y espacio no son obstáculo para la informática que puede recoger, almacenar, procesar, cruzar datos de muy distinta índole, sea cual sea su lugar y momento de procedencia, sin conocimiento ni consentimiento de la persona afectada”.

Todo ello conlleva a distintos problemas para los individuos: posibilidad de que se establezca un perfil de la personalidad de los ciudadanos; el confronto de informaciones con diversos y distintos bancos de datos; la posibilidad de manutención de estas informaciones por largo espacio de tiempo; utilización de estos registros como un instrumento decisorio, es decir, de resolución de aspectos de índole diversa de la vida social de un sujeto fundamentándose en el conjunto de informaciones puesto a disposición de quienes tengan acceso a la base de datos<sup>28</sup>, etc.,

---

<sup>27</sup> OROZCO PARDO, Guillermo. “Consideraciones sobre los derechos de acceso y rectificación en el proyecto de Ley Orgánica de Regulación del tratamiento automatizado de los datos de carácter personal”. *Informática y derecho: Revista iberoamericana de derecho informático*, nº 4, 1994, p. 221.

<sup>28</sup> Una de ellas, el problema que implica los datos personales en el ámbito laboral. De hecho, Pecorella y Di Ponti han advertido que “entre las múltiples perspectivas de la *privacy*, objeto de atención por las distintas autoridades nacionales, encargadas de la

son solamente algunas cuestiones más inmediatas que se deben tener en cuenta cuando se plantea la problemática de la protección de datos.

Dentro de este entorno, no es despropósito afirmar que quedaríamos todos como rehenes, en la cárcel de los sistemas informáticos responsables por el acopio de informaciones personales, subyugados por la imposición injusta, cobarde, tiránica y silenciosa de lo que un conjunto de informaciones que se posea tenga a decir sobre cada uno de los individuos.

Comprendiendo y valorando el fenómeno dentro de esta óptica, se puede llegar a la deducción de que sin sombra de duda, la Ciencia del Derecho se encuentra en un delicado momento, necesitando elaborar un replanteamiento de su propio sistema frente a las nuevas exigencias. Todo esto es imprescindible para que se pueda también asegurar la dignidad de la persona, criterio último de determinación del germen de los derechos que le son inherentes, donde se empieza y se termina una de las principales funciones confiada al Estado Democrático de Derecho, realizada a través de la plena protección de los derechos fundamentales y de las libertades constitucionales.

Sobre este último aspecto, la protección de datos tiene un papel esencial como instrumento para garantizar que el individuo pueda gozar de su libertad sin invasiones ilegítimas y silenciosas. Es incompatible hablar de garantías individuales, de libre desarrollo de la persona y de su dignidad humana si no se le proporciona instrumentos para que la goce con la libertad necesaria. Es interesante y todavía actual la observación de Stuart

---

tutela de los datos personales, han adquirido especial trascendencia en estos últimos años aquéllas relacionadas con la actividad laboral, como consecuencia de las cada vez más amplias posibilidades de intromisión en la esfera personal de los trabajadores, permitida a raíz del desarrollo tecnológico”. PECORELLA, Claudia; DI PONTI, Riccardo. “*Privacy y control del correo y de la navegación por la Red en el puesto de trabajo*”. En: BOIX REIG, Javier (Dir.). *La protección Jurídica de la Intimidad*, Madrid: Iustel, 2010, p. 583.



Mill<sup>29</sup>, cuando afirma que “el Estado, en tanto que respeta la libertad de cada uno en lo que especialmente le concierne, está obligado a mantener una vigilante intervención sobre el ejercicio de todo poder que se le haya sido conferido sobre los demás”. Este es uno de los retos del Estado en los días de hoy: asegurar la libertad individual a la vez que garantiza la seguridad pública y sobretodo sostener un sistema de derechos que se adelante a los cambios tecnológicos y no lo contrario.

## II. El derecho a la autodeterminación informativa y la sentencia alemana sobre la ley del censo de 1983.

Resultado de una construcción doctrinal y jurisprudencial, el derecho a la ‘autodeterminación informativa’ tuvo su origen en Alemania. No obstante, advierte Denninger<sup>30</sup>, que dicho derecho no es nuevo, ni en su formulación, ni en su denominación. Es decir, remite este autor a los años 1954 y 1958, afirmando que la jurisprudencia germánica trataba de perfilar la idea inicial de la autodeterminación informativa. En cuanto a la denominación, desde los años setenta<sup>31</sup>, ese término ya era utilizado por la doctrina alemán.

---

<sup>29</sup> STUART MILL, John. *Sobre la libertad*. Azcárate, Pablo de (trad.). Madrid: Alianza, 2004, p. 192.

<sup>30</sup> DENNINGER, Erhard. “El Derecho a la autodeterminación informativa”. En: PEREZ LUÑO, Antonio Enrique (Dir.). *Problemas actuales de la documentación y la informática jurídica*. Madrid: Tecnos, 1987, p. 271.

<sup>31</sup> Afirma el autor que en el año de 1971, en un informe encargado por el Ministerio Federal del Interior, Steinmüller y otros llegan a definir sus estructuras fundamentales,

Sin embargo, el rango de derecho fundamental se alcanzó por primera vez cuando el Tribunal Constitucional Alemán así lo interpretó, en el momento de la apreciación de la demanda de inconstitucionalidad contra la Ley del recuento de la población, de las profesiones, de las viviendas y de los centros de trabajo (Ley del Censo de 1983), de 25 de marzo de 1982.

Explica la Sentencia que, las razones para que la recogida de los datos ordenados por la Ley del Censo de 1983 despertara la inquietud de sectores de la sociedad, y con ella los recursos de inconstitucionalidad contra dicha ley, podrían haber surgido primero por la ignorancia respecto al ámbito y los objetivos de la utilización de la encuesta, segundo, la falta de advertencia sobre la necesidad e importancia de estas informaciones; en tercer lugar, el temor de los ciudadanos a una aprehensión incontrolada de su personalidad debido a las modernas técnicas de elaboración de datos. Ya que, aunque sea para simplemente recabarlos, son indispensables la exigencia de unos mínimos requisitos; y cuarto, por la alerta de personas expertas sobre la insuficiencia de requisitos de constitucionalidad de la ley en algunos de sus dispositivos.

Además del derecho a la autodeterminación informativa, fueron analizados en aquella oportunidad, también la posible lesión a los derechos fundamentales, la libertad de creencias, la inviolabilidad de domicilio y la libertad de expresión.

No obstante, por lo que interesa a este estudio, indudablemente es el análisis de la Sentencia sobre el artículo 9º de la Ley del Censo, de 25 de marzo de 1982<sup>32</sup>, que contenía disposiciones especiales sobre la utilización

---

introduciendo en esta ocasión denominaciones como la del “derecho a la autodeterminación informativa sobre la imagen de una persona o de un grupo de personas” y en 1976 como un título de un capítulo de Mallmann, “derecho a la autodeterminación informativa”. *Ibid.*, p. 271-272.

<sup>32</sup> Los apartados del artículo 9 que fueran declarados inconstitucionales disponían lo siguiente: “1. Los datos del censo previstos en el artículo 2º, apartados 1 y 2, podrán

y transmisión de los datos recogidos, como por ejemplo, el cotejo con el registro de empadronamiento.

El Tribunal comprendía que la Ley Fundamental del Estado alemán tenía como piedra angular de sus principios, el valor y la dignidad de la

---

ser cotejados con los padrones y utilizados para corregir éstos, si bien los conocimientos conseguidos merced a esos datos no podrán ser utilizados para medidas individuales contra las personas obligadas a suministrar esa información.

2. Los datos individuales sin nombre alguno referentes a los hechos abarcados por los artículos 2º al 4º podrán ser transmitidos, conforme al artículo 11, párrafo 3, de la Ley de Estadísticas Federales de 14 de marzo de 1980 (BGB1 1, pág. 289), por las Oficinas Estadísticas Federales y de las Regiones a las autoridades superiores técnicamente competentes de la Federación y de los Estados regionales, en tanto en cuanto fuera necesarios dichos datos para el lícito cumplimiento de las funciones de competencia de esas autoridades. Con excepción del Concepto de pertenencia legal o, en su caso, no pertenencia religiosa prevenido en el párrafo 1 del artículo 2º, así como de los hechos comprendidos en el artículo 4º, apartado 1, letra c), y en el artículo 4º, apartado 3, letra c), será válido también lo dispuesto en el inciso primero antecedente para la transmisión a las autoridades y demás entes públicos y no públicos que indiquen las autoridades supremas de carácter técnico en la Federación y en los Estados regionales, siempre que la transmisión sea necesaria para el cumplimiento de tareas transferidas por las autoridades supremas y técnicamente competentes de la Federación y de los Estados regionales. Será aplicable por analogía lo dispuesto en el segundo inciso del párrafo 1.

3. Para los fines de la planificación regional, de levantamientos topográficos, de planificación municipal y de protección del medio ambiente se podrán transmitir por las Oficinas Estadísticas Regionales a los municipios y consorcios de municipios los datos individuales necesarios, sin nombre alguno, sobre las circunstancias de los obligados a informar especificadas en los artículos 2º al 4º, con excepción de la pertenencia legal o, en su caso, la no pertenencia a una asociación religiosa a que se refiere el apartado 1 del artículo 2º, así como de los hechos comprendidos en el artículo 4º, apartado 1, letra c), y en el artículo 4º, apartado 3, letra c). Para sus propias elaboraciones estadísticas se podrán poner a disposición de los municipios y de los consorcios de municipios datos de índole individual por las Oficinas Estadísticas Regionales sobre los hechos comprendidos en los artículos 2º al 4º siendo aplicable por analogía lo preceptuado por el segundo inciso del párrafo 1”.

persona que se transpone al ciudadano a través de la libre autodeterminación, al estar inserto dentro de una sociedad libre<sup>33</sup>. Derivado de este principio, el eje del fallo se apoyaba en garantizar que el individuo pudiese decidir libremente sobre cuándo y dentro de qué límites entendiese conveniente revelar situaciones referentes a la propia vida. Aunque no dejó la sentencia de establecer algunos contornos a éste “derecho a la autodeterminación”.

Todo ello, porque, ya en aquella época era posible prever que a través de la elaboración automática de datos, las informaciones sobre circunstancias personales u objetivas de un individuo podrían ser almacenadas sin límites y rápidamente accesibles con independencia de la distancia. Además de la posibilidad de que tales informaciones, cuando refundidas con otras bases de datos, montasen un “perfil de personalidad parcial o ampliamente definida, sin que el interesado pueda controlar suficientemente su exactitud y su utilización”<sup>34</sup>, se tiene en este sentido, la percepción de la importancia, pero también de los peligros para las libertades del ciudadano ese tratamiento automatizado de datos. Referente a este aspecto se consignó en aquel *decisum* que “un dato carente en si mismo de interés puede cobrar un nuevo valor de referencia, y en esta medida ya no existe, bajo las condiciones de la elaboración automática de datos, ningún dato “sin interés”<sup>35</sup>.

El fallo, sustentaba la idea de que la ignorancia por un individuo sobre qué informaciones relativas a él son conocidas en determinados sectores de su vida social acotaba las oportunidades de desarrollo de la personalidad individual. Es decir, el ciudadano no podría libremente

---

<sup>33</sup> Tribunal Constitucional Alemán, sentencia de 15 de diciembre de 1983, publicada en Boletín de Jurisprudencia Constitucional (BCJ), DARANAS, Manuel (trad), núm. 33 (Enero 1984), Madrid: Publicaciones de las Cortes Generales, p. 152.

<sup>34</sup> *Ibid.*, p. 153.

<sup>35</sup> *Ibid.*, p. 154.

“planificar o decidir por autodeterminación” y justo por eso, un orden social y jurídico en el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo sabe algo sobre él era incompatible con el derecho a la autodeterminación informativa<sup>36</sup>.

Si, por un lado, la sentencia procuraba asegurar que el ciudadano pudiese decidir por libre autodeterminación sobre la difusión y utilización de sus datos personales, por otro, definía los límites a ese derecho. Así, la interpretación del alcance del derecho a la autodeterminación informativa era restrictiva, es decir, no se infería que los individuos tenían la “propiedad” absoluta de sus datos. Ello porque se deducía que, incluso en ese tema, algunos intereses colectivos se anteponían al individual. Efectivamente, el ciudadano, además de su recóndito íntimo, ineludiblemente posee una personalidad dentro del cuerpo social que con ella se relaciona<sup>37</sup>. No obstante, este punto de equilibrio entre la restricción del derecho a la autodeterminación informativa y la preponderancia del interés general debería ser encontrado a través del principio de la proporcionalidad.

Sobre todo, lo que se arguyó a este respecto, remata el juicio con rotunda firmeza, al añadir que “el grado de sensibilidad de las informaciones **ya no depende únicamente de que si afectan o no a procesos de la intimidad**. Hace falta más bien conocer la relación de utilización de un dato para poder determinar sus implicaciones para el derecho de la personalidad. Sólo cuando reine la claridad sobre la finalidad con la cual se reclamen los datos y qué posibilidades de interconexión y de utilización existen se podrá contestar la interrogante sobre la licitud de las restricciones del derecho a la autodeterminación

---

<sup>36</sup> *Ibid.*, p. 153.

<sup>37</sup> La información, dice la sentencia que se analiza, “incluso en la medida en que se refiera a la persona como tal, ofrece un retrato de la realidad social que no cabe asignar exclusivamente al interesado”. *Ibid.*, p. 153

informativa”<sup>38</sup>. Con esa consideración, ponía de manifiesto el Tribunal categóricamente que el Derecho que allí se analizaba iba más allá de una mera intromisión al derecho de intimidad y se llegaría a la importancia de la finalidad de utilización de los datos.

La comprensión respecto a esta importantísima cuestión por el Tribunal Constitucional Alemán era la siguiente: para que se pudiese obligar el suministro de datos de carácter personal **no anónimo**, debería exigirse un diligente trabajo del legislador en el sentido de que este apuntase con precisión la finalidad para lo cual son recabados, además de la atención para que dichos datos fuesen adecuados y necesarios para tal finalidad.

En el caso de datos destinados a la finalidad estadística, es decir anónimos, aunque sean para auxiliar una función pública, no se puede exigir del ciudadano cualesquiera datos. Así es función del legislador, para este Tribunal, comprobar desde el momento en que ordena el deber de facilitar información si esos datos comportan o no el peligro de calificar socialmente al interesado<sup>39</sup>.

De lo que se extraía de la norma en análisis, no podía determinar si la finalidad de los datos era únicamente estadística, o también administrativa. Aunque este hecho no conllevara en sí, **a primera vista**, una trasgresión al derecho de la personalidad, el artículo cuestionado lesionaba el derecho a la autodeterminación informativa en el entendimiento de aquellos juzgadores, puesto que no se deducía con claridad de la norma que esta previera comunicación alguna para fines administrativos, ni tampoco de qué finalidades concretas y nítidamente definidas se trataba, como era exigible en materia de datos no

---

<sup>38</sup> Subrayamos. *Ibid.*, p. 154

<sup>39</sup> *Ibid.*, p. 156.

anonimizados<sup>40</sup>. Por todo ello, el Tribunal entendió que dicho precepto involucraba “cosas que tienden a ser incompatibles e inapropiadas”<sup>41</sup>.

Dentro de esa perspectiva, se perfiló en la jurisprudencia alemana el derecho a la autodeterminación informativa, a través de una sentencia indudablemente innovadora que logró fincar las bases de este derecho.

Además, merece destacarse que, durante toda la argumentación de este fallo, lo que se pretende no es una protección de la disposición de los datos por los individuos, sino proteger esencialmente una parcela de la libertad individual; es decir, la lógica jurídica allí expuesta era la de que había que proteger al individuo en su autodeterminación informativa porque había que proteger su libertad de decisión en las relaciones sociales, su “poder tomar otra decisión”<sup>42</sup>.

### III. El derecho a la autodeterminación informativa en España.

“La consideración histórica enseña que los derechos fundamentales no son la expresión, ni el resultado de una elaboración sistemática, de carácter racional y abstracto, sino respuestas normativas histórico-concretas a aquellas experiencias

---

<sup>40</sup> *Ibid.*, p. 166.

<sup>41</sup> *Ibid.*, p. 165.

<sup>42</sup> DENNINGER, Erhard, *El derecho... op. cit.*, p 272.

más insostenibles de limitación y riesgo para la libertad” (Erhard Denninger<sup>43</sup>)

La historia de los derechos fundamentales ha sido marcada por una constante evolución resultado de las cambiantes necesidades humanas dentro de esa línea cronológica, cuyos valores ideológicos fueron variando con el pasar del tiempo. Tales derechos fueron incorporados paulatinamente a medida que la sociedad se encontraba, por su natural desarrollo, en momentos histórico-culturales distintos. Por esa razón, la doctrina suele dividir tal evolución de los derechos fundamentales en tres generaciones que demarcan el contexto social en lo cual fueron concebidos. No obstante esta división, estos derechos se complementan y actualmente los doctrinadores son unísonos en afirmar que no se trata de aislamiento u oposición de uno en relación a los otros<sup>44</sup>.

La primera generación sobre los derechos humanos, nace en el ambiente de la revolución burguesa del siglo XVIII, y refleja una de las características de aquella época: el individualismo. Impulsada por el ideal liberal y por lo tanto conocida por su lucha por alcanzar el derecho a la libertad plena (expresión, intimidad, ideología etc.) dicha generación pretendió que el Estado pasase de interventor a no ingerente, que respectase y preservase una esfera de autonomía del ciudadano, rompiendo de esa manera con los ideales del absolutismo. Es decir, aunque fuese el Estado soberano, habría una zona individual donde tal soberanía no pudiese interponerse. Por esa razón, se atribuye al Estado

---

<sup>43</sup> *Apud.* PÉREZ LUÑO, Antonio Enrique. “Concepto y Concepción de los Derechos Humanos (Acotaciones a la Ponencia de Francisco Laporta)”. *Doxa*, nº 4, 1987, p. 62.

<sup>44</sup> Vid. por todos, PÉREZ LUÑO, Antonio Enrique. “Las Generaciones de Derechos Humanos”. *Revista del Centro de Estudios Constitucionales*, núm. 10 (Septiembre-Diciembre 1991), p. 203-217.



obligaciones negativas y a los ciudadanos derechos de titularidad individual como por ejemplo, lo de aislamiento.

La crisis del Estado Liberal, y las injusticias sociales provocadas por la Revolución Industrial, fueron algunos de las razones históricas en las cuales surgieron los movimientos sociales del siglo XIX que fomentaron la ampliación del catálogo de derechos humanos, complementando el anterior, pues se reclamaba que el Estado intercediese para amenizar las desigualdades que surgieran en aquella época. Así, como bien define Pérez Luño<sup>45</sup>, estos son los correspondientes a los derechos económicos, sociales y culturales, que se traducen en derechos de participación “que requieren una política activa de los poderes públicos encaminada a garantizar su ejercicio, y se realizan a través de las técnicas jurídicas de las prestaciones y los servicios públicos”.

La tercera generación de los derechos humanos, tiene por valor de referencia la solidaridad. Es decir, ha habido una natural necesidad de protección de los intereses colectivos y difusos.

Uno de los planteamientos de la doctrina española sobre el derecho a la autodeterminación informativa es si éste se sostiene como un derecho fundamental autónomo, o bien, si estamos ante una protección de los ya existentes derechos fundamentales, sobre todo el derecho a la intimidad, frente a la informática.

Ese embate doctrinario encuentra partidarios de una y otra teoría, con partícipes del más alto grado científico. Y en éste sentido, nos parece conveniente hacer algunos comentarios sobre tan interesante tema, fruto de larga y intensa controversia científica.

---

<sup>45</sup> PÉREZ LUÑO, Antonio Enrique, *Las Generaciones... op. cit.*, p. 205.

## 1. La polémica entre el derecho a la intimidad y el derecho a la autodeterminación informativa.

Resulta importante subrayar que el somero repaso que pretendemos hacer sobre ésta cuestión se centrara en torno a la disputa doctrinal entre la concepción del derecho a la autodeterminación informativa y el derecho a la intimidad. Ya que entendemos que, la afinidad entre uno y otro derecho, es más evidente que en otros como honor, imagen, etc., y los razonamientos que fundamentan los seguidores de la tesis de la reformulación del concepto de intimidad, para justificar la inutilidad del aumento del catálogo de los derechos fundamentales, que podrían extenderse, *mutatis mutandi*, a los demás.

A éste tenor, los adeptos a esta teoría defienden que la creación de un nuevo derecho fundamental para la tutela de los datos de carácter personales resulta innecesaria. Entre los argumentos, aducen que el derecho a la intimidad podría perfectamente amoldarse a las más recientes exigencias sociales advenidas de los cambios introducidos por las nuevas tecnologías.

Ese razonamiento nos lleva a una antigua e interesante discusión del más elevado contenido científico respecto al surgimiento de nuevas generaciones de derechos humanos. Nos referimos al debate teórico sobre el planteamiento del prof. Francisco Laporta<sup>46</sup>, tocante al tema. Entendía él, que en la literatura especializada empezaba a detectarse “una cierta alarma ante la creciente abundancia y no infrecuente ligereza de las apelaciones a los derechos humanos. No sólo se han multiplicado y

---

<sup>46</sup> LAPORTA, Francisco. “Sobre el Concepto de Derecho Humanos”. *Doxa*, nº 4, 1987, p. 23. Subrayamos.

diversificado hasta grados de concreción sorprendentes a los venerables derechos del hombre y del ciudadano, sino que se dan por sentados derechos de contenido social y económico cada vez más minuciosos, que anuncia el nacimiento de una nueva “generación” de derechos relacionados con cosas tales como las nuevas tecnologías o la conservación del medio ambiente natural”.

También en el mismo sentido, sostenía Laporta, que le parecía razonable inferir que la multiplicación de los derechos humanos acarrearía proporcionalmente una disminución de la exigibilidad y, por otro lado, que “cuanto más fuerza moral o jurídica se les suponga más limitada ha de ser la lista de derechos que la justifiquen adecuadamente”<sup>47</sup>. Su argumento se centraba en que como son los derechos humanos universales, moralmente fuertes e inalienables, no se podía arriesgar a suponer que ellos crecieran rápidamente reproduciendo generaciones sin que se pudiese gravemente cuestionar que son derechos fuertes y para todos sin excepción<sup>48</sup>.

---

<sup>47</sup> *Ibid.*, p. 23.

<sup>48</sup> LAPORTA, Francisco. “Respuesta a Pérez Luño, Atienza y Ruiz Manero”. *Doxa*, nº 4, 1987, p. 74. El autor puntualizaba que “los derechos humanos, si son así, tienen que ser pocos para muchos y no muchos para pocos, y la teoría de las “generaciones” desemboca seguramente en esta segunda posibilidad. (...) Estoy seguro de que la preocupación de Pérez Luño por los problemas de los derechos humanos llamados de la “tercera generación” obedece a inquietantes realidades de nuestro tiempo que nadie con un mínimo de sensibilidad moral puede ignorar. De lo que no estoy tan seguro es de que se necesiten “nuevos” derechos humanos para hacer frente a esas realidades”. Y continúa “... creo que de las “viejas” premisas éticas se pueden seguir obteniendo conclusiones aptas para responder a los nuevos desafíos. **No se trataría, por tanto, de nuevos derechos o de nuevas generaciones de derechos, sino de respuestas de las exigencias morales básicas ante nuevos interrogantes**”. Subrayamos.

En una crítica moderada a este posicionamiento, Murillo de la Cueva<sup>49</sup>, manifiesta que tal argumento parece razonable si considerado *in abstracto*, y si el objetivo es cautelar la “fundamentalización” de pretensiones de relevancia escasa, ausentes de justificación o de imposible satisfacción práctica. No obstante, este autor no comparte de la idea de Laporta, si esto signifique entenderla como impedimento o resistencia categórica al ámbito de las situaciones jurídicas subjetivas cubiertas con el armazón de los derechos fundamentales.

Con otros matices, cree Pérez Luño<sup>50</sup>, entre otras consideraciones, que la precaución de la multiplicación de los derechos humanos y con ella la disminución de su fuerza de exigibilidad resulta infundada. Porque para este jurista, en el plano teórico el aumento de las necesidades humanas, que determina el progreso cultural, se traduce en sucesivas formas de ampliación de libertades. De otro lado, en el plano práctico, defiende que precisamente en el ámbito donde el catálogo de derechos humanos es más extenso, justamente en estos casos es donde más intenso se revela su mecanismo de protección — oponiéndose vehementemente a Laporta.

De vuelta a las razones de los defensores de la teoría, sobre que es excesivo hacer despuntar un nuevo derecho fundamental a la protección

---

<sup>49</sup> MURILLO DE LA CUEVA, Pablo Lucas. *El Derecho a la Autodeterminación Informativa*. Madrid: Tecnos, 1990, p. 41.

<sup>50</sup> PÉREZ LUÑO, Antonio Enrique. *Concepto y Concepción... op. cit.*, p. 61. No obstante ello, el citado autor llegó a expresar su preocupación con la los derechos de tercera generación cuando afirma que “la admisión apresurada y acrítica como derechos humanos de cuantas demandas se reivindican bajo el todavía impreciso rótulo de “derechos de la tercera generación”, equivaldría a condenar la teoría de los derechos humanos a zonas de tal penumbra y equivocidad que comprometería su status jurídico y científico. Pero negar a esas nuevas demandas toda posibilidad de llegar a ser derechos humanos, supondría desconocer el carácter histórico de éstos, así como privar de tutela jurídico-fundamental a algunas de las necesidades más radicalmente sentidas por los hombres y los pueblos de nuestro tiempo”. En *Las Generaciones... op.cit.*, p. 210.

de datos, argumentan sus seguidores, que el alcance del derecho a la intimidad protege la esfera personal del individuo respecto a su propia vida, y también entre ésta y la vida en sociedad. Es decir, en el ámbito doctrinario, la intimidad ha pasado de la concepción estática y cerrada a otra abierta y dinámica, como remarca Pérez Luño<sup>51</sup>. En este sentido, ese derecho tendría un contenido **negativo** frente a las invasiones indebidas o ilícitas en esa zona personal en la cual puede el individuo disponer y, en su caso, prohibir que otros la tengan acceso; y otro **positivo**, de control de los datos e informaciones concernientes al propio titular del derecho<sup>52</sup>; es decir, saber quién y de qué datos disponen sobre él, acceder a ellos, controlar su calidad y exactitud para que el afectado pueda, si es el caso, exigir la corrección o cancelación de aquellos que son incorrectos o indebidos.

En esta perspectiva, la informática sería solamente un nuevo instrumento a través del cual se puede atentar contra derecho de las personas, entre ellos, el de la intimidad, defendiendo esta vertiente doctrinal la reformulación, el replanteamiento y la profundización del alcance del citado derecho. En la opinión de Orti Vallejo<sup>53</sup>, no hay razones

---

<sup>51</sup> PÉREZ LUÑO, Antonio Enrique. *Derechos humanos, Estado de Derecho y Constitución*, Madrid: Tecnos, 2005, p. 356. Aún añade el autor que en la actualidad “la intimidad se contempla como la posibilidad de conocer, acceder y controlar las informaciones que conciernen a cada persona”. Pág. 357

<sup>52</sup> Sostiene Orti Vallejo que “Esta faceta positiva, en definitiva, presupone el derecho de manejar informaciones o datos de los demás, aunque siempre bajo el control del afectado. Este concepto de intimidad que nosotros propugnamos no lo es con exclusiva aplicación al ámbito informático, sino en general para toda realidad o medio técnico de transmisión de información con el que el derecho pueda entrar en conflicto”, en “El nuevo derecho fundamental (y de la personalidad) a la libertad informática (a propósito de la STC 254/1993, de 20 de julio)”, *Derecho privado y Constitución*, nº 2, 1994, pp. 327-328.

<sup>53</sup> ORTI VALLEJO, Antonio. “Cinco años de la Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal”, *La Ley*, Madrid, núm. 4438, 1997, p. 2.

para afirmar que la utilización informática de los datos personales requiera la introducción de un nuevo derecho de la personalidad o fundamental. Pese ello, este autor no excluye la conveniencia de su formulación, dado que en aras de la profundización en las libertades, es deseable el máximo reforzamiento del derecho de control de la persona sobre las informaciones en el ámbito informático, aunque eso no significaría que lo que se tutele sea una cualidad de la persona especial y distinta<sup>54</sup>.

Otro aspecto enfocado versa en torno a que, el punto medular de la cuestión no está propiamente en el dato en sí, ya que no todos por su contenido afectan a la intimidad. El mayor peligro de la informática, advierte Orti Vallejo<sup>55</sup>, “no proviene del almacenamiento de tales o cuales datos, sino en su tratamiento automatizado de los mismos”, a su sentir la distinción que existe entre informaciones íntimas y las que no lo son, no depende solo de ser materia informática, ya que la tecnología posee la capacidad de transformar estas últimas, en informaciones íntimas<sup>56</sup>.

Piensa Rebollo Delgado<sup>57</sup>, que el derecho al control y no ingerencia sobre los datos relativos a la persona susceptibles de tratamiento informático se encuentra dentro del contenido de un derecho a la intimidad informática. Así, para este jurista, el derecho fundamental a la autodeterminación informativa en el derecho alemán es una construcción jurídica lógica en aquél sistema, porque la Carta Magna no recoge de manera expresa el derecho a la intimidad. No obstante, en el caso concreto del derecho español, entiende, que el artículo 18.4 de la Constitución es

---

<sup>54</sup> *Ibid.*

<sup>55</sup> ORTI VALLEJO, Antonio. *Derecho a la intimidad e informática*. Granada: Comares, 1994, p. 49.

<sup>56</sup> *Ibid.*, p. 51.

<sup>57</sup> REBOLLO DELGADO, Lucrecio. *El Derecho Fundamental a la Intimidad*, Madrid: Dykinson, 2005, p. 300 y ss.

una indicación expresa del contenido esencial del derecho a la intimidad, siendo, por lo tanto, el derecho a la intimidad informática (refiriéndose a la autodeterminación informativa) “una extensión de un derecho al cual viene a completar, y que no es otro que el derecho a la intimidad”<sup>58</sup>.

## **2. El derecho fundamental autónomo a la autodeterminación informativa. La posición doctrinal y jurisprudencial.**

El derecho a la autodeterminación informativa indudablemente produce una intersección con el derecho a la intimidad. Lo que hay que indagar es en qué momento este derecho deja de ser una manifestación de aquél y pasa a tener contornos propios. Los seguidores de que se está ante un nuevo derecho fundamental, autónomo y que va más allá de la protección que puede ofrecer el derecho a la intimidad, tienen como piedra angular de su raciocinio que el bien jurídico tutelado por el derecho a la intimidad no es suficiente para proteger todos los peligros consecuentes del uso de la informática tocante a los datos personales<sup>59</sup>. En el caso de la autodeterminación informativa, su protección engloba además del control de los datos íntimos, los que también no tiene ese carácter<sup>60</sup>.

---

<sup>58</sup> *Ibid.*, p. 306.

<sup>59</sup> Para MURILLO DE LA CUEVA, si el bien jurídico por defender fuese lo que se entiende por la noción estricta de intimidad, lo que habría de resguardar del peligro informático sería muy poco. En *Informática y Protección de Datos Personales*. Madrid: Centro de Estudios Constitucionales, 1993, p. 31.

<sup>60</sup> Para el Tribunal Constitucional de España, “el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la

Para Murillo de la Cueva, no es necesario que los datos sean solamente íntimos para que estén en la órbita del derecho a la autodeterminación informativa, sino que sean personales, es decir, propios de un individuo, independientemente que sean conocidos por un determinado círculo de personas próximo al titular de estos datos<sup>61</sup>. O, por mejor decir, que sean datos que “identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo”<sup>62</sup>.

Por lo tanto, si se concibe dicha tutela dentro del contenido del derecho a la intimidad, ampliando su ámbito, se produciría como alerta con mucha lucidez González Murúa<sup>63</sup>, un gran *contradictio in terminis*, lo que ocasionaría un serio problema de aplicación práctica que sería calificar jurídicamente a dos realidades distintas bajo la misma denominación<sup>64</sup>. La respuesta jurídica para determinadas situaciones ocasionadas por el uso de la informática se quedaría restringida si dejada bajo el manto solamente del derecho a la intimidad<sup>65</sup>.

---

persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal”. STC 292/2000, fundamento 6.

<sup>61</sup> MURILLO DE LA CUEVA, Pablo Lucas. *El derecho...*, *op. cit.*, p. 117.

<sup>62</sup> STC 292/2000.

<sup>63</sup> GONZALEZ MURÚA, Ana Rosa. *El Derecho a la Intimidad, el Derecho a la Autodeterminación Informativa y la L.O. 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos Personales*. Barcelona: Institut de Ciències Polítiques i Socials, 1994, p. 22.

<sup>64</sup> *Ibid.*, p. 23.

<sup>65</sup> Subraya MURILLO DE LA CUEVA con mucha lucidez que “lo decisivo es la interacción que se da entre las normas constitucionales y la realidad que contemplan y



A entendimiento de Murillo de la Cueva<sup>66</sup>, la tutela de la intimidad pasa por el mecanismo normativo típico, es decir, se prohíbe una conducta que sería la intromisión ilegítima en la esfera protegida; se sanciona el incumplimiento de esa prohibición; se indemnizan los perjuicios originados de dicha intromisión ilícita; y, finalmente, se adoptan medidas complementarias para cesar las circunstancias que hacen posible tal intromisión, cuando es el caso. Para este autor, la protección de datos no se agota en ese itinerario, afirmando que ciertamente lo incluye pero contempla otras facultades de las personas encaminadas a asegurar el control de la información. En la opinión de Piñar Mañas<sup>67</sup>, el derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad “con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos concretados en ley”.

Sobre el artículo 18.4 de la Constitución de España, Orozco Pardo<sup>68</sup> señala que tanto la Doctrina más autorizada, el propio Tribunal Constitucional y el Legislador han sido llevados a afirmar que tal

---

el hecho de que, en esa relación emerja con claridad una necesidad básica de las personas que demande su satisfacción mediante la afirmación de un derecho fundamental”. En “La Constitución y el Derecho a la autodeterminación informativa”, *Cuadernos de Derecho Público*, Madrid: Instituto Nacional de Administración Pública, 2003, p. 41.

<sup>66</sup> MURILLO DE LA CUEVA, Pablo Lucas. *Informática y...*, op. cit., p. 32.

<sup>67</sup> PIÑAR MAÑAS, José Luis. “El derecho fundamental a la protección de datos personales”. En PIÑAR MAÑAS, José Luis (dir.). *Protección de datos de carácter personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos, La Antigua - Guatemala, 2-6 de junio de 2003*. Valencia: Tirant lo Blanch, 2006, p.

<sup>68</sup> OROZCO PARDO, Guillermo. “Notas acerca del Régimen Jurídico de los Ficheros de Datos Personales de Titularidad Universitaria”. *Informática y derecho: Revista iberoamericana de derecho informático*, nº 23-26, 1998, p. 862.

precepto “no sólo pretende promover una acción legislativa y funcional de los poderes públicos para limitar el uso de la informática (aspecto pasivo) sino que quiere garantizar al ciudadano una esfera de poder autónomo que le permita decidir acerca del tratamiento automatizado de los datos que le conciernan, no solo del nivel de conocimiento de su vida privada, sino el control de la información que le concierne y los usos que de ella se puedan realizar”.

Esta línea teórica es la que prevalece en la jurisprudencia. No obstante para que se llegara a tal entendimiento, expuesto en la sentencia 292/2000, el Tribunal Constitucional fue llamado a manifestarse en otros fallos anteriores sobre dicho derecho.

Considerada como pionera en el enfrentamiento de la aplicabilidad del artículo 18.4 de la CE, en lo que concierne la protección de datos fue la sentencia 254/1993 dictada por el Tribunal Constitucional Español. El caso que se presentaba era de un ciudadano a quien el Gobierno Civil de Guipúzcoa le había negado información sobre los datos que poseía sobre su persona. Así, aquél órgano juzgador debería decidir sobre el derecho o no del actor de la demanda de que la Administración se le suministrase la información que requería, pasando por un análisis de los efectos del Convenio del Consejo de Europa nº 108.

De este modo, con respecto a la literalidad del artículo 18.4 de la CE, en un primer momento el Tribunal manifiesta que la Constitución había incorporado una nueva garantía para una nueva forma de amenaza a la dignidad y a los derechos de la persona. Es decir, que se estaba ante un instituto “de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también, de un instituto que es, en sí mismo, un derecho o libertad fundamental”. Además, aunque no hubiera ley que desarrollase dicha garantía constitucional y el mismo Tribunal en otras ocasiones ya había decidido en sentencia que cuando se opera con una reserva de configuración legal, es posible que el mandato constitucional no tenga

más que un contenido mínimo debiendo ser completado por el legislador. En el caso analizado por este fallo, entendieron aquellos magistrados que el derecho a obtener información que pretendía el demandante del amparo formaba parte de este contenido mínimo que consagraba el artículo 18 de la CE y por lo tanto tenía eficacia directa.

Lo que se puede observar, es la dificultad que tuvo el Tribunal Constitucional en ubicar la “nueva garantía” que había sido incorporada por la Constitución. Es decir, por un lado, señala en el sentido de interpretar que se estaba delante de un nuevo derecho fundamental, lo cual se estaba originando de forma no muy diferente a como se incorporaron históricamente otros derechos fundamentales, como se observa en el fundamento 6 de la sentencia. Sin embargo, de otra parte, el mismo fundamento 6, intenta compaginarlo como un doble instituto que, por un lado sirve de garantía a otros derechos fundamentales, y a la vez, representa una libertad fundamental en si mismo. Para Orti Vallejo<sup>69</sup>, la protección de los datos es un criterio de legitimación política de los sistemas democráticos y todo lo que ello conlleva debió pesar en el ánimo del Tribunal Constitucional en esta sentencia, y en su valoración, quizás esta sea la causa de la contradicción en que incurre al afirmar, por un lado que frente a la informática se trata de tutelar derechos fundamentales ya reconocidos y, por otro, la sustantividad de un derecho en este ámbito.

Además de ello, en el fundamento 7, se identifica como garantía de la intimidad, un contenido positivo que es el control del uso de los datos insertos en un programa informático (*habeas data*). Más adelante, en el mismo fundamento se especifica que las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados, son absolutamente necesarias para que los intereses contenidos en el artículo 18 CE resulten real y efectivamente protegidos, siendo dichas facultades de información parte del contenido del derecho a la intimidad.

---

<sup>69</sup> ORTI VALLEJO, Antonio. *Cinco años... op. cit.*, p. 2.

Claramente se puede notar que en aquél momento, el propio Tribunal Constitucional no logra separar el contenido del derecho a la libertad informática del derecho a la intimidad. En nuestra opinión, aunque existan fuertes argumentos para acusar la contradicción de esta sentencia, en cuando que intenta conciliar la garantía objetiva a la protección de datos, con el derecho subjetivo a la intimidad y a la autodeterminación informativa, se debe reconocer la importancia de este fallo en el sentido de que la jurisprudencia empezaba a encaminarse hacia el reconocimiento de un derecho nuevo, fundamental y autónomo, como efectivamente se recogería en la sentencia 292/2000.

Otra sentencia importante fue la 290/2000, publicada simultáneamente con la 292/2000, en 30 de noviembre. Dicho fallo fue el resultado de la acumulación de cuatro recursos de inconstitucionalidad interpuestos por Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y por don Federico T. F. C., Comisionado por 56 Diputados del Grupo Parlamentario Popular contra algunos artículos de la Ley Orgánica 5/1992, de 29 de octubre.

Al tiempo de resolver dichos recursos sobrevino la derogación de la LO 5/1992 con la entrada en vigor de la LO 15/1999 de 13 de diciembre, de protección de datos de carácter personal. De modo que se produjo la pérdida de objeto de varios de los artículos impugnados, ya que concluidos los efectos de aquella ley en situaciones posteriores. Se quedaron solamente los que concernían a la disputa competencial entre el Estado y las Comunidades Autónomas, dado que en tres artículos el Tribunal Constitucional se entendió que subsistía la impugnación debido al grado de identidad de contenido de los preceptos de la Ley derogada con los de la nueva Ley y por lo tanto la controversia seguía viva<sup>70</sup>.

---

<sup>70</sup> Tribunal Constitucional, Sentencia 290/2000, fundamentos jurídicos 4, 5 y 6.

No obstante, la sentencia dejó consignado claramente el pensamiento del Tribunal Constitucional respecto a la autonomía del derecho a la protección de datos como un derecho fundamental. De ese modo, consignó que “en cuanto desarrollan el mandato del art. 18.4 CE, las previsiones de la LOTARD limitando el uso de la informática están estrechamente vinculadas con la salvaguardia de ese **derecho fundamental a la protección de datos** personales frente a la informática o, si se quiere, a la ‘libertad informática’ según expresión utilizada por la citada STC 254/1993”<sup>71</sup>. Y aún añade que este derecho fundamental posee un conjunto de derecho que el ciudadano puede ejercer frente a quienes sean titulares públicos o privados de ficheros de datos personales.

Otro aspecto de extremada relevancia en esta sentencia es el voto particular formulado por el Magistrado Manuel Jiménez de Parga y Cabrera, para quién el Tribunal “reconoce y protege ahora un derecho fundamental, el **derecho de libertad informática**”. El Magistrado señala la dificultad que enfrenta el Ordenamiento español en el reconocimiento de nuevos derechos fundamentales, ya que la Constitución Española no tiene una cláusula abierta como remate de la lista de los derechos fundamentales. Además, en su valoración, tiene especial relieve la última clase de derecho que son aquellos creados por la jurisprudencia, y estos derechos no-escritos han de ser tutelados por ella, ya que las Constituciones proporcionan al intérprete un punto de apoyo a través del cual se efectúa la construcción del derecho fundamental, mediante una actividad creadora.

A su sentir, continua el Magistrado, el eje vertebrador de la libertad informática en cuanto derecho fundamental no recogido expresamente en la CE, debe ser el artículo 10.1 CE, ya que es un derecho inherente a la dignidad de la persona y es tal vinculación que proporciona a la libertad informática la debida consistencia constitucional, añadiendo que

---

<sup>71</sup> Fundamento jurídico 7. En el original, está todo en negrita.

“también son preceptos que facilitan la configuración de la libertad informática los contenidos en los arts. 18.1 (derecho al honor, a la intimidad personal y familiar y a la propia imagen) y 20.1 (libertad de expresión y de información), entre otros, así como los Tratados internacionales en cuanto son guías de interpretación constitucional”. De este modo, concluye manifestando que es un cometido importante de la jurisdicción constitucional el reconocimiento y protección de nuevos derechos fundamentales ya que con esta paliación de tutela facilita la permanencia durante largo tiempo de las Constituciones.

Sin sombra a dudas, es la sentencia 292/2000 que marca en la jurisprudencia española la nueva tendencia ya anunciada de reconocimiento de un derecho nuevo y autónomo a la autodeterminación informativa. Dicha decisión fue pronunciada resolviendo el recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra algunos incisos de los artículos 21.1 y 24.1 y 24.2 de la Ley Orgánica 15/1999, por vulneración de los arts. 18.1 y 4 y 53.1 CE.

La importancia de este fallo en especial, consiste en que fue ahí donde la jurisprudencia del Tribunal Constitucional firmó claramente su entendimiento sobre el derecho a la protección de datos, logrando especificar su alcance, su contenido, su naturaleza y sus límites confiriéndole detalladamente su posición en el ordenamiento jurídico español como un derecho fundamental autónomo.

De esta forma, para el TC el derecho a la intimidad no aporta una protección suficiente frente a la nueva realidad derivada del progreso tecnológico y así quiso el constituyente garantizar un ámbito de protección más idóneo mediante el art. 18.4 CE de los que podían ofrecer aquellos derechos mencionados en el apartado 1 del mismo artículo<sup>72</sup>.

---

<sup>72</sup> Fundamento Jurídico 4.

Logra la sentencia diferenciar el derecho a la intimidad, del derecho a la protección de datos. En la valoración de aquél órgano juzgador “la peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran”. La singularidad del derecho a protección de datos reside por un lado en que su objeto es más amplio que lo del derecho a la intimidad, ya que aquél extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida, sino en ocasiones como ya había definido el TC como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal<sup>73</sup>.

Para el Tribunal Constitucional<sup>74</sup>, el contenido de este nuevo derecho garantiza a los ciudadanos un poder de control y disposición sobre los datos personales sobre su uso y destino. Dicho control se concretiza jurídicamente en las facultades de imponer a terceros algunos deberes de hacer, a través del ejercicio de derechos como el de que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a ser informado sobre el destino y uso de estos datos y el derecho a accederlos, rectificarlos y cancelarlos.

En lo que respecta a los límites de la libertad informática, la sentencia menciona lo que dice la Constitución en el artículo 105, b) que la ley regulará el acceso 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” (en relación con el art. 8.1 y 18.1 y 4 CE), así como las manifestaciones del mismo Tribunal que ha manifestado “que la persecución y castigo del delito constituye, asimismo, un bien

---

<sup>73</sup> Fundamento Jurídico 6.

<sup>74</sup> Fundamentos jurídicos 6 y 7.

digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana”<sup>75</sup>. También cumple resaltar que el fallo resalta de forma rotunda las oportunidades anteriores que el Tribunal ya había manifestado que “el derecho a la protección de datos no es limitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como lo ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos”<sup>76</sup>.

De este modo, en una sentencia de importancia notoria, el Tribunal Constitucional español asienta su jurisprudencia en el sentido de reconocer como un derecho fundamental distinto y autónomo a los que habían sido expresados en el artículo 18.1 de la Constitución de España, con todos sus aspectos jurídicos perfectamente delineados. Sin embargo, la jurisprudencia no ha dado fin a la discusión teórica de la doctrina, en la cual todavía se encuentra autores que defienden la subordinación del derecho a la protección de datos al derecho a la intimidad.

#### **IV. El derecho a la protección de datos personales y la evolución normativa y jurisprudencial en Italia.**

A pesar de la gran contribución del derecho italiano en la actualidad, con respecto a la materia de protección de datos personales, la trayectoria de aceptación de éste derecho fue marcada de un lado, por un intenso

---

<sup>75</sup> Fundamento Jurídico 9.

<sup>76</sup> Fundamento jurídico 11.



debate doctrinario y jurisprudencial, y de otro, por un rechazable retraso en la actuación legislativa. Se debe afirmar, que fue largo el camino recorrido desde la recepción en el ordenamiento jurídico italiano del derecho a la intimidad, hasta la promulgación del Código en materia de protección de datos personales.

Para empezar, la propia aceptación del derecho a la *riservatezza* fue objeto de gran controversia. Sería a partir los años treinta<sup>77</sup> cuando surgió en Italia el interés por el tema, intensificándose los debates a partir de los años cincuenta. Como subraya Nigier<sup>78</sup>, la introducción de la expresión *diritto alla riservatezza* en el lenguaje jurídico italiano se debe a las obras de Adolfo Ravà y Adriano de Cupis, aunque se encontraban otras expresiones como *derecho a la ileasa intimidad privada*, *diritto alla vita privata*, *diritto alla riservatezza* o *privatezza*. De modo que mucho antes de tener un reconocimiento legal, la doctrina ya empezaba una labor de elaboración de este derecho.

---

<sup>77</sup> Para la reconstrucción del camino histórico del debate sobre el *derecho alla riservatezza* en Italia, *vide* la sugerencia bibliográfica en CALDIROLA, Debora. *Il Diritto alla Riservatezza*. Milano: CEDAN, 2006, p. 5, notas al pié de página; PINORI, Alessandra, "La responsabilità Civile per Trattamento Illecito dei Dati Personali". En *La Politica Economica tra Mercati e Regole: scritti in ricordo di Luciano Stella*. BARBERIS, Guido, et al. (Dir.), Catanzaro: Rubbettino, 2005 p. 294, nota al pié de pagina y NIGER, Sergio, *La nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Milano: CEDAN, 2006, pp. 39-40; y, también, el interesante estudio que engloba la construcción del derecho a la *riservatezza* en el ámbito doctrinario, jurisprudencial y legal de SCALISI, Antonino. *Il Diritto alla Riservatezza*. Milano: Giuffrè, 2002, pp. 388-423.

<sup>78</sup> NIGER, Sergio, *Le nuove dimensioni... op. cit.*, p. 39. Cfr. BIANCA, Cesare Massimo. "Note Introdutive I". En BIANCA, Cesare Massimo y BUSNELLI, Francesco (Dir.). *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*. Milano: CEDAN, 2007, p. XXI.

En efecto, no existía ninguna norma específica sobre la tutela de la *riservatezza*, aunque para Franceschelli<sup>79</sup>, había numerosas disposiciones, de las cuales parte de la doctrina y algunas sentencias han deducido la existencia de un principio de tutela de la *riservatezza*. Tal ausencia, sin embargo, según Satoretti<sup>80</sup> no puede ser atribuida al desconocimiento en el ambiente académico de este derecho, sino de una libre elección del legislador constituyente de no formalizarlo en la Carta Constitucional. Una de las razones puede ser en gran parte a la época y a la cultura a la que pertenece el Código Civil italiano o a la estructura del sistema privado<sup>81</sup>.

De esta manera, las primeras discusiones a ese respecto, como observa Pardolesi<sup>82</sup>, fueron sobre cuestiones prejudiciales tocantes a la existencia de este derecho. La doctrina buscó su protección indirecta a través de la técnica de la analogía *legis*<sup>83</sup> — acercando la tutela de la *riservatezza* a las normas del derecho a la imagen y del nombre, en el Código Civil, y del derecho del autor en su normativa correspondiente; y la analogía *iuris* — ubicándole como principio general, con el objetivo de proteger un atributo fundamental de la personalidad. Ambas soluciones fueron criticadas por

---

<sup>79</sup> FRANCESCHELLI, Bruno. *Il diritto alla riservatezza*. Napoli: casa Editrice Jovene, 1960, p. 17.

<sup>80</sup> SATORETTI, Claudia. *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale*, Giappichelli, Torino, 2008, p. 49. *Vid.* la crítica de Franceschelli, Bruno. *Il diritto... op. cit.*, p. 18 y ss.

<sup>81</sup> NIGER, Sergio. *Le nuove dimensioni... op. cit.*, p. 40.

<sup>82</sup> PARDOLESI, Roberto. “Dalla Riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità”. En *Diritto alla riservatezza e circolazione dei dati personali*, PARDOLESI, Roberto (Dir.), Milano: Giuffrè, Vol. I, 2003, p. 15.

<sup>83</sup> Como bien remarca Caldirola, más que la utilización de la técnica de analogía *legis*, eran utilizados argumentos *a fortoti*, es decir si el ordenamiento tutelaba el derecho a la imagen y la imagen é una manifestación de la reserva, luego con mayor razón se debe reconocer la existencia de un interés general a la *riservatezza* en el ordenamiento. CALDIROLA, Debora. *Il Diritto alla... op. cit.*, p. 8.

sectores de la doctrina puesto que, en resumen, tocante a la analogía *legis* no se podía hallar una homogeneidad de interés entre las disposiciones comúnmente evocadas como apoyo a la existencia de un derecho general a la *riservatezza*; y respecto a la utilización de la analogía *iuris*, parecía más como un mero artificio terminológico que como instrumento de una distinta reconstrucción dogmática del derecho a la *riservatezza*<sup>84</sup>.

Igualmente controvertida fue la tentativa de fundamentar el susodicho derecho, en la concepción de la teoría monista del derecho a la personalidad, influenciada por Alemania. Como bien observa Caldirola<sup>85</sup>, esa concepción considerando la persona protegida en toda su manifestación, determinaba la ilegitimidad de cualquier intrusión, a menos que no fuera permitida por expresa y específica disposición normativa; pues para la concepción pluralista, estaría permitida la injerencia de terceros en la intimidad de vida privada, salvo expresa prohibición, todo ello interpretado en sentido amplio.

La doctrina italiana también se ve influenciada por las normativas internacionales como el artículo 12 de la Declaración Universal de los Derechos Humanos, y el artículo 8º del Convenio Europeo para la Protección de los Derechos Humanos para fundamentar el derecho a la *riservatezza*, aunque ese intento también encontró dificultades. Entre otros cuestionamientos, se suscitaba la verdadera aplicabilidad del Convenio Europeo y la cuestión de su *valor* y de su *fuerza* en el ordenamiento italiano<sup>86</sup>.

Como ya se ha señalado, no existía — ni existe — en la Constitución italiana una norma específica que expresamente tutele el derecho a la

---

<sup>84</sup> *Ibid.*, p. 11-12.

<sup>85</sup> *Ibid.*, Op. Cit., p. 13.

<sup>86</sup> Sobre la problemática involucrada en el reconocimiento internacional del derecho a la *riservatezza*, vide CALDIROLA, Debora. *Ibid.*, pp. 14-18.

*riservatezza*. Según el juicio de Satoretti<sup>87</sup>, en Italia ante esa ausencia y también debido a falta por un largo tiempo de un cuadro normativo coherente, la doctrina y la jurisprudencia han realizado un intenso trabajo a partir de los años cincuenta, para conducir a unidad sistemática el fundamento, el objeto, y los instrumentos jurídicos de garantía de este derecho

De este modo, la doctrina también encontró dificultades para ubicar su fundamento jurídico-constitucional. Para tal propósito, sirvieron las disposiciones, por ejemplo, que trataban de la inviolabilidad de domicilio (Art. 14), del secreto de la correspondencia (Art.15) y la libertad de pensamiento (Art. 21), hasta que la manifestación jurisprudencial de la *Corte*, individualizó el fundamento jurídico del citado derecho en el artículo 2º de la Constitución<sup>88</sup>.

Volviendo la mirada hacia las primeras manifestaciones sobre el derecho a la *privacy* en Europa, no es demasiado afirmar que el camino de la jurisprudencia italiana fue más largo que el de otros países en lo que concierne a la aceptación de este nuevo derecho<sup>89</sup>. De manera que, mientras la doctrina italiana se empeñaba en trazar un perfil de la *riservatezza*, contando en su contra con la limitación legal sobre el tema, la formación jurisprudencial, hasta los años setenta, obstaculizaba su entusiasmo. A este respecto, nos parece importante y tal vez necesario, hacer un recorrido histórico sobre la consideración jurisprudencial sobre tal materia.

---

<sup>87</sup> SATORETTI, Claudia. *Contributo allo... op. cit.*, p. 48.

<sup>88</sup> ELLI, Gianmario; ZALLONE, Raffaele. *Il nuovo Codice della privacy*. Torino: G. Giappichelli, 2004, p. 3. Para una lectura más actualizada del desarrollo constitucional italiano del derecho a la *riservatezza*, vid. SATORETTI, Claudia. *Contributo allo... op. cit.*

<sup>89</sup> Aunque Italia no fue el único país, como bien observa Satoretti, en el cual este derecho nace a través del trabajo doctrinario y jurisprudencial. En *Contributo allo... op. cit.*, p. 39.

De modo somero, podemos afirmar que la evolución jurisprudencial del *diritto alla riservatezza* ha atravesado dos momentos, cuyo punto de inflexión fue la sentencia nº 2129, de 27 de mayo de 1975.

Como se ha destacado anteriormente, la intensificación de los debates sobre las controversias en torno a la existencia del *diritto alla riservatezza* se remota a los años cincuenta, y por lo tanto, en esta época se encuentran las primeras decisiones sobre este tema. Justamente en el pos-guerra, lo que se observó fue que la prensa y los medios de comunicación se desarrollaran de manera muy veloz y el sistema normativo de aquella época no comportaba la debida protección para acompañar ese progreso, es decir, no existía una protección que efectivamente pudiese imponer los límites necesarios para la publicación de hechos relacionados principalmente con personas conocidas socialmente. La consecuencia primordial y directa de todo ello fue el surgimiento de nuevas exigencias sociales, derivadas del natural avance de la sociedad, que clamaba por una tutela que iba más allá de los derechos reconocidos en aquel momento.

Aunque a lo largo de los años la jurisprudencia fue paulatinamente moderando su entendimiento, ese período empezó con decisiones que negaban la existencia de un nuevo derecho. Por mejor decir, había una contraposición entre las decisiones de la *Corte di Cassazione* – más rígida para aceptar el derecho a la *riservatezza* – y los tribunales provinciales que, en cambio, estaban más receptivos.

En efecto, la primera decisión histórica que tuvo gran impacto en el medio científico sobre la materia fue dada por el Tribunal de Roma<sup>90</sup>. El hecho apreciado era un pedido de los descendientes de Enrico Caruso, para que se cesase la proyección de la película biográfica “*Leggenda di una voce*”, donde se describía su vida desde la infancia, repleta de historias de

---

<sup>90</sup> Tribunal de Roma, sentencia de 14 de septiembre de 1953, en *Foro Italiano*, 1954, I, p. 115 y ss.

sufrimiento y dolor, hasta conseguir llegar a ser una celebridad, incluyendo hechos y comportamientos relativos a su vida privada sin ningún tipo de consentimiento<sup>91</sup>.

Pese a que el Tribunal de Roma entendiera que la realización de una obra cinematográfica sobre una determinada persona conllevaba o puede conllevar la utilización de hechos y acontecimientos de su vida, que podían o implicaban derechos al nombre, a la imagen, al honor y eventualmente a aquellos de la *riservatezza*. Para este Tribunal, el nudo gordiano de la cuestión consistió propiamente en analizar si tales derechos, de la manera que estaban configurados en el ordenamiento positivo, toleraban en general la utilización de la personalidad ajena y cuáles eran los límites de esta tolerancia cuando se trataba de una persona célebre.

No obstante, y admitiendo que en el ordenamiento italiano no se reconocía el derecho a la *riservatezza*, el Tribunal romano la conceptuó como la prohibición de cualesquier ingerencia externa en la esfera de la vida privada del individuo y de cualesquier indiscreción de terceros sobre aquellos hechos o comportamientos personales que, no públicos por su naturaleza, no son destinados a la publicidad de la persona que le concierne. Por ende, a falta de un explícito reglamento legal para la construcción del citado derecho, que responda a una exigencia fundamental de la personalidad, este Tribunal se refería a la disciplina del derecho a la imagen, lo cual es tutelado como una manifestación de la *riservatezza* de la persona.

---

<sup>91</sup> Además, suscitaban otras consideraciones como la imitación de la voz de Caruso en la película, reproducida por el tenor Mario del Mónaco, cuya voz no era comparable con la del tenor napolitano; y también el hecho de que su representación fue confiada al actor Ermanno Randi que después de iniciada la difusión de la película, murió víctima de un delito que ponía de relieve la “inmoralidad de su vida íntima”.

De este modo, en base a esta analogía entre los dos derechos, el Tribunal afirmó que el derecho a la *riservatezza*, como aquél a la imagen, tolera límites cuando se trataba de persona notoria o célebre. Así, aquél órgano juzgador entendió que el interés general no podía justificar el sacrificio del individual y por lo tanto que ambos deberían ser mitigados. Esa era la exigencia de la limitación que la notoriedad imponía al derecho a la *riservatezza* de la persona celebre, aunque alertase que tal punto de equilibrio solamente podría ser alcanzado contrastando los intereses en cada caso concreto dependiendo de varios factores advenidos de las características de la persona celebre<sup>92</sup>.

No obstante este posicionamiento del Tribunal de Roma, la *Corte di Cassazione*<sup>93</sup> no compartía el mismo entendimiento. En sentencia de 22 de diciembre de 1956, n.º 4487 la Corte afirmó que en el ordenamiento jurídico italiano no existía un *diritto alla riservatezza*, pero que solamente eran reconocidos y tutelados de modos diversos derechos individuales subjetivos de la persona, por ende para aquel juzgado, no era vetado comunicar en privado o públicamente hechos de la vida ajena, sobre todo imaginarios, cuando el conocimiento de dichos hechos no hubieran sido obtenidos a través de medios ilícitos o que impusiera la obligación de secreto. Además se entendía que el tema podría ser solucionado sin la necesidad de crear un nuevo instituto, como utilizando el principio del *neminem laedere*, contenido en el artículo 2.043 del Código Civil italiano<sup>94</sup>.

---

<sup>92</sup> Al final, el fallo decidió por considerar ilícita algunas escenas de la película, aunque no acogió el pedido de resarcimiento de daños morales, ordenando la suspensión temporal de la proyección de la película hasta que fuesen depuradas las escenas ilegales, pudiendo después continuar a circular libremente.

<sup>93</sup> *Corte di Cassazione*, sentencia n.º 4487 de 22 de diciembre de 1956. Vide comentario de NIGER, Sergio. *Le nuove dimensioni... op. cit.*, p. 54 y ss.

<sup>94</sup> El Tribunal afirmó que no existía en el ordenamiento italiano ni un derecho a la fiel correspondencia de la representación artística a la verdad histórica (siempre y cuando la creación de la fantasía no denegriera la persona de cuyos acontecimientos reales o

En su momento, este hecho causó un amplio debate en la doctrina, dividiéndose la opinión de ésta en dos bloques: los que afirmaban la existencia de un derecho a la *riservatezza*, como era el caso de De Cupis, y los que la negaban, ésta última línea fue encabezada principalmente por Pugliese, que como comentario a la sentencia del Tribunal de Roma, Pugliese<sup>95</sup>, ha titulado su artículo “el **supuesto** derecho a la *riservatezza* y la indiscreción cinematográfica<sup>96</sup>”. De esta manera, como observa Cassano y Fadda<sup>97</sup>, el fallo de la *Cassazione* “reproduce casi textualmente la tesis de Pugliesi”. Por otro lado, el Tribunal de Roma, en la sentencia de primero grado acoge la tesis de De Cupis. A propósito de la sentencia de la *Corte di Cassazione*, este autor<sup>98</sup> hace una dura crítica afirmando que “la inexistencia del derecho a la *riservatezza* no está completamente demostrada en dicha sentencia y aunque el mismo derecho no existe para la *Cassazione*, continua a existir en el ordenamiento jurídico”.

---

imaginarios son narrados, mientras que el principio del *neminem laedere* podría ser aplicado incluso en el ámbito del arte), ni un derecho general a la *riservatezza* o a la *privatezza*, como límite a la libertad del arte. De este modo, declaraba que ninguna disposición de la ley autorizaba que se considerase que se había consagrado como un principio general el respeto absoluto intimidad de la vida privada, ni tampoco como forma de limitar la libertad del arte.

<sup>95</sup> En *Foro Italiano*, 1954, I, p. 116 y ss. En la misma ocasión, DE CUPIS a través de su artículo “I diritto alla riservatezza esiste”, En *Foro Italiano*, IV, 1954, p. 89 y ss., contesta a los argumentos de Pugliese.

<sup>96</sup> Subrayamos.

<sup>97</sup> CASSANO, Giuseppe, y FADDA, Stefano. *Codice in materia di protezione dei dati personali: commento articolo per articolo al Testo unico sulla privacy D. lgs. 30 giugno 2003, n. 196*. CASSANO, Giuseppe, y FADDA, Stefano (coord.), Milano: IPSOA, 2004, p. 4 y ss.

<sup>98</sup> En *Foro Italiano*, 1957, I, p. 234.



Dentro de este andamiaje, como señala Bianca<sup>99</sup>, en los años 50 la posición de los Tribunales fue demasiado rígida, mostrando que compartía la interpretación restrictiva de la norma constitucional, ya que, contenía una cláusula tan general como para convertirse en una “caja vacía” y que solamente en vía marginal podría ofrecer una tutela a posiciones subjetivas, pero que en realidad se prestaba a manipulaciones que excluían la aplicación directa de las relaciones entre los particulares.

Continuando con éste hilo conductor histórico, en 1960 el Tribunal de Milano<sup>100</sup> fue instado a pronunciarse en el famoso caso de Claretta Petacci, contra un periódico que había publicado hechos de su vida entre otros los relacionados con Benito Mussolini, especialmente sobre la última noche de la pareja antes de su ejecución. Este Tribunal reconoce el derecho a la *riservatezza* que se constituía en el variado campo de otras figuras típicas dentro de los fundamentales derechos de la personalidad, juntamente con el derecho al nombre, a la imagen, etc. Así, tal derecho debería ser respetado con amplitud autónoma y absoluta, y no sometido sino a las limitaciones que se muestran impostas por razones de orden público, o de superior interés social.

El fallo concluye<sup>101</sup> enfatizando que la investigación y la crítica histórica a veces modesta en su concreta manifestación, también tienen exigencia propia, que no conlleva el sacrificar el nombre de ese derecho personal, la *riservatezza*, incluso cuando se trata de personas que pertenecen a la

---

<sup>99</sup> En el idioma original: “La giurisprudenza italiana, sul finire degli anni '50, era invece attestata su posizioni ancora troppo rigide, mostrando di condividere l'interpretazione restrittiva della norma costituzionale, per la quale essa conteneva una clausola così generale da diventare una “scatola vuota”, una norma che soltanto in via marginale poteva offrire tutela a posizioni soggettive, ma che in realtà si prestava a manipolazioni tali da escluderne l'applicazione diretta ai rapporti tra i privati”. BIANCA, Cesare Massimo, *Note Introductive...Op. cit.*, p. LXIV.

<sup>100</sup> Corte D'appello di Milano, 26 agosto 1960, in *Foro It.*, 1961, I, c.47.

<sup>101</sup> En *Foro Italiano*, 1961, I, p. 48.

vida pública de un país, el secreto de su vida íntima debe ser respetado. No se da lugar, tampoco en este caso, a la facultad de la indiscreción y a la invasión de la curiosidad pública.

De nuevo, una vez más la *Corte di Cassazione*<sup>102</sup> se manifestó sobre el tema. Y como observa Cassano y Fadda, en esta sentencia<sup>103</sup> la *Corte*, de un lado no debía ser insensible a los cambios que se producían en la sociedad<sup>104</sup>, y de otro, tampoco podía olvidar el propio posicionamiento precedente. Por ello, este Tribunal revisó la postura asentada por su jurisprudencia<sup>105</sup> sobre el derecho a la *riservatezza* flexibilizándola, y aunque afirmó que, por la ausencia de una explícita previsión legal no se podía reconocer, estableció una premisa importante al admitir un derecho *erga omnes* a la libertad de autodeterminación en el desarrollo de la personalidad del hombre como individuo. Y de ello se derivaría la prohibición de la divulgación de aspectos relativos a la vida privada de las personas sin su consentimiento, excluyéndose los casos en que este está implícito por la actividad que desarrolla el individuo o debido a la característica de su actividad o si del hecho divulgado prevalezca un interés público.

---

<sup>102</sup> Sentencia nº 990 de 20 de abril de 1963, in *Foro Italiano*, 1963, p. 877 y ss.

<sup>103</sup> Vid. BUTTARELLI, Giovanni. *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione: commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale*. Milano: Giuffrè Editore, 1997, p. 100 y ss.

<sup>104</sup> Según estos autores, en los diez años que separaban la sentencia del caso Caruso y esta, el cuadro social y cultural experimentó una rápida evolución, así una gran parte de la sociedad civil ya clamaba por la tutela al derecho a la *riservatezza*. En *Codice in materia... op. cit.*, p. 18.

<sup>105</sup> Consigna en el fallo que frente al disenso de gran parte de la doctrina a los inconvenientes que derivan de una absoluta exclusión de la tutela jurisdiccional de la reserva de la vida privada esto Supremo colegio é impulsado al reexamen de la propia jurisprudencia. *Foro Italiano, op. cit.*, p. 877.

El segundo momento se produjo como ya se ha adelantado, con la sentencia de la *Corte de Cassazione* nº 2.129, de 27 de mayo de 1975, cuya controversia fue protagonizada por la princesa Soraya Esfandiari, contra algunos periódicos que habían publicado fotografías donde ella aparecía en el interior de su chalet romano en actitudes íntimas con el director de cine Franco Indovina.

De esta forma, fue suscitada la protección entre otros derechos, de la *riservatezza*, y el Tribunal analizó en esa ocasión su autonomía. Manifestó en la sentencia que la cuestión del entonces debatidísimo tema en el medio científico exigía una solución que, en la natural evolución jurisprudencial — mientras se quedara fijado en la norma constitucional y en otras disposiciones del ordenamiento positivo —, fuese sensible a la atemperación de la tutela de los diversos intereses a la luz de la vasta tendencia también de derecho internacional, de ampliar la defensa de la personalidad humana, tanto en la confrontación del abuso de los poderes públicos, como en las relaciones subjetivas individuales.

Para aquél Órgano juzgador, el continuo desarrollo de la moderna tecnología ofrecía tanto al sector público como al privado innúmeras posibilidades de control de cada aspecto de la vida y de rápida divulgación. Por lo que en el entendimiento de aquellos juzgadores, esa evolución no podía ser ignorada ni por el derecho privado ni en sede jurisprudencial<sup>106</sup>.

Fue en este fallo<sup>107</sup>, donde finalmente se asentó en la jurisprudencia italiana el derecho a la *riservatezza*, superando las antecedentes

---

<sup>106</sup> En *Foro italiano*, 1976, p. 2901 y 2902.

<sup>107</sup> Cassano y Fadda subrayan que a principio de los años 70 la Corte Constitucional empieza a reconocer algunas expresiones de un derecho general a la *riservatezza*, aunque no definiese con precisión sus contornos, como es el caso de la sentencia nº 122 de 9 de junio de 1970, cuando analizaba un caso de derecho del autor, dicho Tribunal afirmó que el derecho a la *riservatezza* de la propia imagen podía constituirse

orientaciones interpretativas. Reconoce por lo tanto la *Corte di Cassazione* que este derecho encuentra su fundamento no solo implícitamente en el sistema jurídico, sino también, en una serie de referencias legislativas dentro de un conjunto de normas ordinarias y constitucionales, como en las normas especiales en las cuales se evoca expresamente la vida privada del sujeto. Así, expresa la sentencia que una tutela más amplia que aquella circunscrita a la intimidad doméstica además de no ser contraria a los principios constitucionales, encuentra en ellos varios motivos de convalidación.

De modo que dicho derecho, preveía proteger los acontecimientos y hechos estrictamente personales y familiares, siempre y cuando no hubiera interés público relevante, aunque se produjeran fuera del hogar y la información fuese obtenida por medios lícitos para finalidades no especulativas y que no ofendiesen al honor, a la reputación y al decoro.

Otro punto que parece importante señalar, trata sobre la problemática terminológica de lo que se entiende en el derecho anglosajón *privacy* y su recepción por el ordenamiento jurídico italiano. En éste sentido, tenemos en primer lugar que atender a la dificultad metodológica de transferir un instituto típico de la *common law*, a un sistema jurídico diverso y atribuirle relevancia jurídica a intereses, necesidades y sentimientos que la sociedad italiana sentía en menor escala que la americana<sup>108</sup>.

Los términos usados tanto por la doctrina como por la jurisprudencia italiana para incorporar la palabra inglesa fueron *riservatezza* y *privatezza*, aunque en la valoración de Caldirola<sup>109</sup>, no son totalmente idóneos para

---

en un límite sustancial a la libertad de manifestación del pensamiento. En otra sentencia, en el año de 1972, nº 12 de 2 de febrero, el mismo Tribunal reconoció la existencia del derecho a no revelar la propia convicción. En *Codice in... op. cit.*, p. 10.

<sup>108</sup> CALDIROLA, Debora. *Il Diritto alla... op. cit.*, p. 59.

<sup>109</sup> *Ibid.*, p. 61.

abarcando todos los posibles significados de la *privacy*, por lo que es común encontrar en el ordenamiento italiano también la voz inglesa. Ahora bien, el problema conlleva algo más que una mera traducción o en una simple transcripción de ese vocablo, sino su integración como término jurídico y todo el complejo de intereses que ese derecho pretende tutelar, añadiéndose a eso la absoluta imposibilidad de transponer de un sitio a otro el ambiente cultural y jurídico en el cual nace la *privacy*<sup>110</sup>.

No obstante, hay que plantearse otro aspecto respecto a la evolución del concepto de *riservatezza* o *privacy*<sup>111</sup> frente al desarrollo de las nuevas tecnologías. Al parecer, la doctrina italiana no se ha puesto de acuerdo con la utilización de los términos y su significado actual, pudiendo encontrarlos tanto utilizados como sinónimos, o casi antónimos. Marcándose las diferencias y trazándose sus contornos específicos como es el caso de Quadri di Cardano<sup>112</sup>, para quién en el lenguaje jurídico *privacy* y *riservatezza* son conceptos distintos y los correspondientes

---

<sup>110</sup> Cfr. CALDIROLA, Debora, *Il Diritto alla... op. cit.*, p. 62. La autora aún va más allá opinando que quizás el error de la primera elaboración doctrinal y jurisprudencial fue el de haber querido buscar un fundamento jurídico al derecho a la *riservatezza* sobre la base del contenido elaborado en los países anglosajones, así que mientras en Italia en los años sesenta y hasta mediados de los años setenta se discutía aún en base a qué norma debía reconocerse, también en nuestro ordenamiento, el derecho a ser dejado solos, la *riservatezza* asumía contornos distintos y más complejos por efecto del carácter penetrante y invasivo de las tecnologías de la información.

<sup>111</sup> Vide RODOTÀ, Stefano. *Tecnologie e diritto*. Bologna: Il Mulino, 1995, p. 101 y ss.; CALDIROLA, Debora. *Il Diritto alla... op. cit.*, p. 188 y ss.

<sup>112</sup> QUADRI DI CARDANO, Gioacchino. *La privacy informatica: trattamento dei dati personali e tutela dell'affidamento*. Bologna: Librería Bonomo, 2008, p. 1. Sin embargo, es común encontrar en la doctrina italiana el término *privacy* como sinónimo del derecho a la *riservatezza* y de la protección de los datos personales. Cfr. la definición de *riservatezza* en PARADISO, Massimo. *Corso di Istituzioni di Diritto Privato*. Torino: Giappichelli, 2008, p. 119 y NIGER, Sergio. "Il diritto alla protezione dei dati personali". En MONDUCCI, Juri; SARTOR, Giovanni (coord.). *Il Codice in Materia di Protezione dei dati personali*. Milano: CEDAN, 2004, pp. 3-4.

derechos aspiran a proteger diferentes necesidades aunque para distintos aspectos parcialmente coincidentes. Por derecho a la *privacy*, continúa el autor, actualmente se entiende el derecho reconocido a cualquiera individuo a la protección de los datos<sup>113</sup> que les concierne, mientras el derecho a la *riservatezza*, anhela a tutelar la esfera privada del individuo de la ingerencia indebida de terceros.

En Italia, cuando verdaderamente se tiene un reconocimiento legal explícito de la tutela de los datos personales es con la llegada del nuevo Código de Protección de los Datos Personales, que inaugura su texto con la proclamación de dicho derecho<sup>114</sup>, ubicándole en el título dedicado a los principios generales.

Sin resquicios a duda, ello causó gran eco en la doctrina. Pues semejante declaración, introduce un nuevo derecho con la categoría de principio rector de todo el sistema normativo, sin que específicamente hiciese referencia de vinculación a cualquier otro, conduciendo el pensamiento jurídico a una nueva perspectiva.

A este respecto, haciendo un breve repaso a la doctrina en torno a tal afirmación. Merece destacarse la opinión de Piraino,<sup>115</sup> que subraya que la proclamación de este derecho constituye una novedad de absoluta relieve y que confiere una justa relevancia a una expresión polivalente que designa tanto a un conjunto complejo de poderes, como a una específica

---

<sup>113</sup> Utilizando el término en ese mismo sentido, PERRI, Pierluigi. *Privacy, Diritto e Sicurezza Informatica*. Milano: Giuffrè, 2007, p. 3.

<sup>114</sup> Art. 1º del Código intitulado “Derecho a la protección de los datos personales” dispone que cualquiera tiene derecho a la protección de los datos personales que le digan respecto.

<sup>115</sup> PIRAINO, Fabrizio. “Il codice della privacy e la tecnica del bilanciamento di interessi”. *Libera circolazione e protezione dei dati personali*. CEDON, Paolo (coord.) Milano: Giuffrè, Vol. I, 2006, p. 707.

tutela, conferida al sujeto del que va a tratar la información o informaciones de carácter personal.

Para Bardusco<sup>116</sup>, del enunciado del artículo 1º del Código emerge un principio general, proclamado de manera representativa y clara, con la afirmación del ideal de fondo con el fin de iluminar los preceptos puntuales contenidos en los distintos y numerosos artículos del Código. Remarca este autor, sin embargo, que aunque la afirmación del derecho a la protección de los datos sea formulada en términos generales y absolutos, el propio Código demuestra lo contrario. Ello porque la persona no tiene un derecho real similar al derecho de propiedad, sobre los datos que le conciernen.

En efecto, el reconocimiento rotundo del derecho a la protección de datos, demuestra una importante evolución socio-legal del concepto de intimidad que ha sido absorta en Italia; al pasar de una concepción tradicional a una más dinámica, coherente con la tendencia actual de la sistemática del ordenamiento comunitario e internacional, al igual que, con los importantes cambios realizados por las tecnologías en el seno de la sociedad. Y todo ello formulado con una autonomía, que hasta entonces no se podía observar en las normas predecesoras de aquél país.

En este sentido, Santaniello<sup>117</sup> destaca que el Código refleja la mutación profunda, por la que, desde la fórmula original de la intimidad, desde el inicio del siglo XX, entendida como el derecho del individuo a la inviolabilidad de su esfera privada, a una perspectiva más avanzada, en

---

<sup>116</sup> BARDUSCO, Aldo. "Articolo 1 (Diritto alla protezione dei dati personali)". En *Codice della Privacy: Commento al Decreto Legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative*. VITORIO, Italia (coord.). Milano: Giuffrè, Vol. I, 2004, p. 12.

<sup>117</sup> SANTANIELLO, Giuseppe. *I fattori evolutivi della codificazione concernente la protezione dei dati personali* [en línea]. Roma: Interlex. 07.10.04.

<http://www.interlex.it/675/santaniello11.htm> [Consulta: 16 mar. 2009].

la cual la protección de los datos personales no se conecta tanto al momento del aislamiento de la persona como al de su proyección participativa en la amplia red de relaciones de la sociedad civil. A éste tenor, para Viterbo<sup>118</sup>, una de las principales novedades del Código, es la afirmación del derecho a la protección de los datos personales como concreta y autónoma especificación de la categoría de los derechos y de las libertades fundamentales<sup>119</sup>.

La evolución de la doctrina italiana, al igual que la española, conlleva dos tesis opuestas en lo que respecta a la autonomía del derecho a la protección de los datos personales, en relación al derecho a la *riservatezza*. Algunos autores defienden que existe una confluencia entre el derecho a la protección de datos y la nueva acepción del derecho a la *riservatezza*. Así, para Bianca<sup>120</sup>, el derecho a la *riservatezza* sufrió una transformación en lo que concierne al alcance de su sentido, al abarcar no solamente el **derecho a la no divulgación de hechos personales**, como el **derecho a la vida privada**, ese comúnmente expresado con el termino *privacy*. Frente a la primera concepción del derecho a la *riservatezza*, ha perdido autónoma relevancia, al encontrarse en la actualidad inserto dentro del derecho a la protección de datos personales. No obstante, la acepción de la *riservatezza*

---

<sup>118</sup> VITERBO, Francesco Giacomo. *Protezione dei dati personali e autonomia privata: profili di interferenza e di reciproca funzionalizzazione*. Napoli: Edizioni Scientifiche Italiane, 2008, p. 110

<sup>119</sup> Para Vincenzo Cuffarro la colocación de la norma en la abertura del catálogo de los principios generales del Código confirma que el enunciado quiere expresar un fuerte grado de tutela que el ordenamiento pretende perseguir respecto a las actividades de tratamiento de datos, mientras la comparación con la Carta de Niza, cuando la homóloga disposición es colocada entre los derechos y libertades fundamentales, constituye una señal inequívoca del significado del enunciado, el cual viene de tal modo a asumir una especie de valor constitucional. “Il Principio di Protezione dei Dati”. En *Il Codice del Trattamento dei Dati personali*. RICCIUTO, Vincenzo; D’ORAZIO, Roberto; CUFFARO, Vincenzo (coord.). Torino: G. Giappichelli, 2007, p. 11.

<sup>120</sup> BIANCA, Cesare Massimo. *Note... op. cit.*, p. XX y ss.



como derecho a la vida privada conservan su importancia, como aparece reflejada en la Carta de los Derechos Fundamentales de la Unión Europea, en un artículo separado (art. 7) del derecho a la protección de los datos personales (art. 8).

También Bianca, cree que el derecho a la *privacy*, puede sufrir varias formas de ingerencia, pero es principalmente amenazado a través del tratamiento abusivo de los datos personales. Por todo ello, en su valoración, el *Codice* hizo referencia a la *riservatezza*, como el respecto a la vida privada, al afirmar que el tratamiento de los datos personales deberá desarrollarse en el respecto “de los derechos y de la libertad fundamentales con particular referencia a la *riservatezza*”.

Asimismo, para este autor, la previsión del derecho a la tutela de los datos personales en la nueva reglamentación sobre este tema ubicado en un artículo separado que dispone sobre la *finalidad* del tratamiento, le configura como objeto de un autónomo derecho de la personalidad (posición esa no pacífica en la doctrina) y se constituye en una **especificación** del derecho a la *riservatezza*<sup>121</sup>, ampliamente entendido como derecho al respecto de su vida privada, pero derecho que se ciñe más a del secreto y a de la imagen. No obstante, esto no excluye su autonomía de contenido y de disciplina, es decir, “la tutela de los datos personales, precisamente, es uno de los modos a través del cual el ordenamiento realiza el respecto de la vida privada”<sup>122</sup>. Por lo que, a su parecer, la autónoma identidad estaría ratificada por el hecho de que su

---

<sup>121</sup> Es la misma opinión de Fioriglio, para quién “el referimiento explico sea al derecho a la *riservatezza* como al derecho a la protección de datos personales hace surgir el carácter general del derecho a la *riservatezza*, del cual el derecho a la protección de los datos personales constituye, sin embargo, una especificación”, FIORIGLIO, Gianluigi. *Temì di Informatica Giuridica* [en línea], [http://www.informaticagiuridica.com/temiig/fioriglio-temi\\_di\\_informatica\\_giuridica.pdf](http://www.informaticagiuridica.com/temiig/fioriglio-temi_di_informatica_giuridica.pdf), p. 210.

<sup>122</sup> BIANCA, Cesare Massimo. *La protezione... op. cit*, p. XXIII.

violación es punible, independientemente de la determinación de la lesión a otros derechos; asimismo el entendimiento del derecho a la protección de los datos personales como autónomo derecho a la personalidad no es incompatible con la graduación de su tutela, encontrando explicación en la peculiaridad de su objeto, más o menos sensible.

Ahora bien, desde la perspectiva adoptada por otra parte de la doctrina, como es el caso de Melchiona<sup>123</sup>, el nuevo Código, afirma la existencia de un derecho a la protección de los datos personales, distinto de la *riservatezza*, al cualificar como derecho positivo autónomo, aquél que hasta entonces era considerado como una acepción más moderna del concepto de *diritto alla riservatezza*. La autora<sup>124</sup> considera que el derecho a la protección de datos personales debe ser valorado incluso normativamente de forma distinta de la libertad negativa de no sufrir interferencia en la propia vida privada, significado éste que se constituye actualmente como el principal del derecho a la *riservatezza*, convirtiéndose precisamente en la libertad positiva para ejercer un control sobre el flujo de la propia información.

En la misma línea de pensamiento, se manifiesta Ninno<sup>125</sup>, al resaltar que la protección de datos personales es un derecho nuevo y autónomo, y por esta razón su tutela no se consigue solamente a través de la extensión de derechos como los del respeto a la vida privada y familiar, del

---

<sup>123</sup> MELCHIONNA, Silvia. “Principi generali”. En *Il Diritto alla protezione dei Dati Personali: La disciplina sulla privacy alla luce del nuovo Codice*. ACCIAI, Riccardo (Dir.), Santarcangelo di Romagna: Maggioli, 2004, p. 32.

<sup>124</sup> La autora aún añade que en el sistema de garantía del Código el derecho a la protección de los datos personales sigue siendo estrictamente conexo al derecho a la *riservatezza* e al de dignidad y identidad personal, constituyéndose junto a estos el límite insuperable del tratamiento de datos. Op. Cit., p. 33.

<sup>125</sup> NINNO, Alessandro del. “Nuove tecnologie e tutela del diritto alla protezione dei dati personali”,. En *I Diritto Della Persona: Tutela Civile, Penale, Amministrativa*, CEDON, Paolo (coord.). Torino: UTET, 2006, pp. 367-368.

domicilio o de la propia comunicación, pero erigiéndose como un nuevo derecho constitucional específico.

No obstante, ya era posible encontrar en la doctrina trazos de esa misma tendencia en la anterior ley 675/96. En torno a ésta cuestión, merece destacarse la opinión de Giannantonio<sup>126</sup>. Este autor va más allá de una mera discusión de ubicación del derecho a los datos personales como un derecho de la personalidad, sino que, aunque no hable de un derecho autónomo de protección de datos, identifica en la finalidad de la ley la tutela de un derecho independiente del propio derecho a la *riservatezza*. De modo que él parte del principio que la ley<sup>127</sup> había introducido un derecho nuevo y *sui generis*, diverso de los tradicionales derechos de la personalidad<sup>128</sup>. Así, a su sentir, “la tutela de la *riservatezza*, no tiene por objeto un bien externo a la persona, pero encuentra en la misma persona el punto de referencia objetiva. En particular, los derechos al honor, a la *riservatezza*, a la identidad personal tienen por objeto el valor del individuo en su consideración social, y regulan los datos personales no en sí, sino en cuanto su comunicación o su difusión hayan lesionado este valor”.

---

<sup>126</sup> En el idioma original, este autor así registra: “La tutela della riservatezza, infatti, non ha per oggetto un bene esterno alla persona, ma trova nella stessa persona il punto di riferimento oggettivo. In particolare i diritti all’onore, alla riservatezza e all’identità personale hanno per oggetto il valore dell’individuo nella considerazione sociale e disciplinano i dati personali non in sé, ma in quanto la loro comunicazione o la loro diffusione abbiano leso tale valore”. En GIANNANTONIO, Ettore. LOSANO, Mario. ZENO- ZENCOVICH, Vincenzo (Coord.). *La tutela dei Dati Personali. Comentario alla Ley 675/1996*, Padova: CEDAN, 1999, p. 5.

<sup>127</sup> En este caso, la ley 675/1996.

<sup>128</sup> Para el autor en cita, “sería un error pensar que de este modo la norma haya querido reconocer legislativamente derechos de la personalidad de creación jurisprudencial, como el derecho a la *riservatezza* o el derecho a la identidad personal, o haya querido disciplinar aspectos particulares”. GIANNANTONIO, Ettore; et al. *Comentario... op. cit.*, p. 4.

Por ende, en su valoración, cuando un individuo recopilaba o elaboraba un conjunto de datos personales de otros sujetos, tanto fuesen datos íntimos, como socialmente irrelevantes, no cometería ningún perjuicio al derecho a la identidad o a la *riservatezza*, máxime que no comunicase o difundiese dichos datos. La ley de protección de datos italiana, en cambio, tutela los datos personales con independencia de su comunicación o difusión, de modo que llega a afirmar que el objeto de la norma es cualquier actividad que tenga por objeto los datos personales, aunque no haya difusión o comunicación, puede conferir a quien la efectúa un poder que es necesario regularlo. Para el autor en cita, la protección principal de la ley era la transparencia y no la *riservatezza*.

Además, el autor insiste, que el derecho sobre los datos personales debe ser considerado como un verdadero y propio derecho de la personalidad, aunque diferente de los tradicionales derechos de la personalidad elaborados por la doctrina y jurisprudencia, y más similar a aquellos de origen legislativo como es el caso del derecho al nombre o a la imagen. Eso porque tales derechos aunque tengan como objeto un bien distinto de la persona, es estrictamente conexo a ella: su reglamentación es mucho más de imposición de conducta que sancionadora de hechos ilícitos<sup>129</sup>.

En su juicio la tradicional disciplina del derecho a la personalidad estuvo por un largo tiempo identificada con la responsabilidad civil, siendo el reconocimiento del derecho de la personalidad un modo de determinar el daño injusto y, así, resarcible. El autor observa que tanto la tutela inhibitoria como la resarcitoria están presentes en todos los derechos de la personalidad. Sin embargo, la disciplina de sobre los datos personales es directa, no tanto a sancionar un hecho ilícito, sino más bien a imponer una determinada conducta. No obstante asevera que la

---

<sup>129</sup> *Ibid.*, p. 6.

prevalencia de una no significa necesariamente la exclusión de la otra tutela<sup>130</sup>.

## V. El derecho a la autodeterminación informativa en el derecho brasileño.

La cuestión que se debe plantear en este apartado es: ¿existe en el sistema jurídico brasileño el derecho autónomo a la autodeterminación informativa? En el caso de que sea afirmativa la respuesta, ¿sería este considerado como un derecho fundamental?. A partir del análisis detenido de tales interrogantes se pueden plantear nuevas perspectivas para el sistema jurídico brasileño sobre el tema de protección de datos personales.

La concepción tocante a la libertad informática en éste país todavía es muy incipiente no solamente en el medio jurídico sino también en el social, principalmente cuando se le vislumbra de modo autónomo a los derechos de intimidad y honor fundamentalmente. Es decir, se aprecia que la sociedad brasileña todavía no ha despertado a la importancia de controlar sus datos personales, independiente de su naturaleza (si íntimos o no). En lo que respecta al derecho a la protección de datos ocurre un fenómeno semejante a lo que sucedió en Italia en el momento de la recepción del derecho a la *privacy*. El interés social en Brasil sobre los datos personales no parece darle una importante relevancia jurídica al tema, siempre que este no interfiera en los derechos al honor e intimidad. Cuando se suscita alguna cuestión sobre este tema, generalmente se le

---

<sup>130</sup> *Ibid.*, pp. 6-8.

vincula a la ofensa de estos dos derechos, y la consecuencia jurídica es, muy a menudo, la petición indemnizatoria en el ámbito de la responsabilidad civil, de manera que la tutela resarcible aplasta la preventiva.

Así como los sistemas jurídicos más modernos, el brasileño también protege el derecho a la intimidad en su texto constitucional. En el artículo 5º, ubicado en el Título II “*De los Derecho y Garantías Fundamentales*”, que inicia el Capítulo I “*De los derechos y deberes individuales y colectivos*”, que taxativamente en su línea X preceptúa que son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurado el derecho a la indemnización por el daño material o moral derivada de su violación. De modo que la Constitución brasileña consagró la tutela de dichos derechos al nivel de fundamentales.

El Supremo Tribunal Federal brasileño (STF), responsable, precisamente, de la guardia de la Constitución, ya tuvo oportunidad de manifestarse en diversas ocasiones sobre la tutela jurídica de la intimidad. Para aquél Tribunal<sup>131</sup>, ésta se constituye como una de las expresiones más significativas en que se pluralizan los derecho de la personalidad y su protección busca erigir y reservar siempre al individuo contra la acción expansiva del arbitrio del poder público, una esfera de autonomía intangible por la actividad desarrollada por el Estado.

Cumple resaltar que en el derecho brasileño, tanto la doctrina mayoritaria como la jurisprudencia hacen distinción entre el derecho a la intimidad y a la privacidad, sin que esto sea excluyente de encontrar los términos utilizados como sinónimos. La diferencia entre ambos vocablos, residiría en la amplitud del contenido del concepto, él de la privacidad es más amplio que el de la intimidad. De modo somero, este último se refiere a la persona en sí misma, mientras que en la privacidad este campo

---

<sup>131</sup> STF. MS 22801/DF, Rel. Min. Alberto Menezes Direito, 17/12/2007.

alberga también las relaciones con sus familiares y amigos. Por mejor decir, nos valemos de la lección de Sampaio Ferraz Junior<sup>132</sup> para quién la intimidad es el ámbito exclusivo que alguien reserva para sí, sin ninguna repercusión social, siquiera alcanzado por su vida privada que por más aislada que sea ésta es siempre un vivir entre los otros (en la familia, en el trabajo, en el ocio común). Ya la vida privada, a su sentir, protege formas exclusivas de la convivencia, o sea algunas situaciones en que no se puede evitar la comunicación de una persona a otra, donde ahí estén excluidos terceros.

No obstante, también hay quien vislumbre, así como lo hacen en España con el derecho a la intimidad, el contenido positivo del derecho a la privacidad y de la intimidad. Aunque ora lo hacen como institutos jurídicos sinónimos, ora como distintos, considerando la intimidad como especie del genero de la privacidad<sup>133</sup>.

Pese a que nuestra posición en este tema sea la de que son dos institutos jurídicos distintos, pero conexos, tal afirmación no nos ayuda en la búsqueda de donde supuestamente se ubicaría el fundamento jurídico autónomo del derecho a la autodeterminación informativa en el sistema jurídico brasileño.

---

<sup>132</sup> SAMPAIO FERRAZ JUNIOR, Tercio. *Sigilo de dados: o Direito à privacidade e os limites à função fiscalizadora do Estado* [en línea]. 24/08/2006. <http://www.terciosampaioferrazjr.com.br/?q=/publicacoes-cientificas/49>. [Consulta: 10 jul. 2009].

<sup>133</sup> Vide el estudio de MALTA VIEIRA, Tatiana. *O Direito à privacidade na sociedade da informação*, Porto Alegre: Sergio Antonio Fabris Editor, 2007, p. 29 y ss.

## 1. El derecho brasileño y la tutela de los datos personales.

Si pudiese hablarse de un sistema de protección de datos en Brasil, este estaría estructurado de manera dispersa en leyes sectoriales, que por lo general no tratan de la temática de modo directo, sino siempre como auxilio a la tutela de otros derechos.

De modo que se puede encontrar en ese sistema jurídico normas que versen sobre el tratamiento de informaciones en el ámbito de su área de actuación<sup>134</sup>, como la ley 5.250 de 9 de febrero de 1967 y el Estatuto de la Crianza y del Adolescente, ley 8.069 de 13 de julio de 1990, pero indudablemente carentes de garantías individuales del interesado,

---

<sup>134</sup> La ley 5.250 de 9 de febrero de 1967, llamada ley de Imprenta que reglamenta la libertad de manifestación del pensamiento y de la información que en su artículo 7 prohíbe el anonimato en el ejercicio de estos derechos pero asegura el sigilo de los datos relativamente a las fuentes o origen de las informaciones; La Ley 8.069 de 13 de julio de 1990, el Estatuto de la Crianza y del Adolescente que prevé en su artículo 94 la manutención de un banco de datos por las entidades responsables por los programas de internación de los niños allí enviados. Dichas entidades tiene la función, según su naturaleza, de ejecución de programas socio-educativos destinados a niños y adolescentes en régimen que van desde orientación y apoyo socio familiar, socio educativo, colocación familiar y abrigo hasta medidas judiciales por delitos cometidos como la libertad asistida, semilibertad y internación. Pues bien, en estas base de datos de tales entidades deben constar la fecha y la circunstancia por las cuales fue presentado el menor, su nombre, el nombre de sus padres o responsables, de parientes, dirección, sexo, edad y demás datos que posibiliten su identificación y la individualización en su atención. Y hasta ahí hemos llegado, porque aparte de la creación de estos ficheros, no existe ninguna otra referencia legal sobre como tales datos deberán ser tratados o cualquier sombra de los derechos que pueden ser ejercidos por los interesados.



aunque, algunas veces las más básicas que se pueden exigir. Son normas que por lo común, no tratan de temas importantes relativos a la protección de los datos como la divulgación, la seguridad, el consentimiento, etc.

Esa es una característica muy fuerte que está presente en prácticamente todas las normas. Y, como ya se ha advertido, la tutela no aparece regulada dentro de un determinado sector de la materia de derecho, sino en, algunas disposiciones sobre los archivos, datos e informaciones que se puedan necesitar para facilitar el cumplimiento de la ley. Por tanto sólo hay una reglamentación parcial de lo que sería la protección de datos, como medio en sí para alcanzar una determinada finalidad legislativa. No obstante, hay normas, aunque raras, que preceptúan algunos derechos de los afectados.

Otro ejemplo de ley en cuanto a la protección de datos, es el Código Tributario Nacional<sup>135</sup>, cuyo artículo 198<sup>136</sup> prevé la prohibición de que la Hacienda Pública o sus funcionarios, divulguen informaciones obtenidas en razón de su labor sobre la situación económica o financiera del sujeto pasivo, o de terceros, así como, la naturaleza y el estado de sus negocios o actividades. Aunque la citada prohibición no es absoluta, ya que no se aplica si es solicitada por la autoridad judicial en el interés de la justicia o por petición de la autoridad administrativa en el interés de la Administración Pública. En este último caso, se ha de probar que fue abierto un proceso administrativo por práctica de infracción administrativa en la entidad, con el objetivo de investigar el sujeto pasivo a que se refiere la información. Además, su intercambio deberá ser realizado a través de procedimiento, y la entrega será efectuada personalmente a la autoridad administrativa solicitante, mediante recibo que formalice la transferencia y asegure la preservación de la información.

---

<sup>135</sup> Ley n° 5.172, de 25 de octubre de 1966.

<sup>136</sup> Este artículo fue modificado por la Ley Complementar n° 104 de 10 de enero de 2001.

La crítica, sin embargo, que se puede realizar sobre este procedimiento, afecta al párrafo 3º del artículo que estamos analizando, que permite la divulgación de informaciones relativas a registros de deudas contra la Hacienda, su aplazamiento o moratoria. Dicha norma no hace ninguna mención sobre los aspectos más relevantes de la comunicación de estas informaciones. No obstante, el silencio en éste sentido también se aprecia en otros preceptos, al no contemplarse en ellos la explícita posibilidad del ciudadano ejercer sus derechos, y tampoco sobre la seguridad y calidad de los datos.

Otra ley importantísima que versa sobre protección de datos, más específicamente sobre el sigilo de las operaciones de las instituciones financieras es la Ley Complementar nº 105, de 10 de enero de 2001. Tanto las operaciones pasivas como activas son protegidas y el artículo 1º, párrafo 1º que enumera los órganos que son considerados instituciones financieras, llegando a un número de doce, aparte de los que pueden ser considerados como tal, si en razón de la naturaleza de sus operaciones sea así consideradas por el *Conselho Monetario Nacional*<sup>137</sup>.

No obstante, dicha norma restringe sus disposiciones nada más que a la vigilancia y cuidado de las informaciones que habitualmente tienen las instituciones financieras, derivadas de su función, y no al resto de los supuestos ajenos a ella. Sin embargo, lo que podría ser una gran garantía a los interesados (esa restricción), no se le exige a los propios órganos financieros. Es decir, que el cambio de informaciones para finalidad de registro entre todas las instituciones listadas en el artículo 1º párrafo 1º de la susodicha ley, no constituye violación del deber de sigilo. Eso es lo que

---

<sup>137</sup> El *Conselho Monetário Nacional* es el órgano deliberativo máximo del Sistema Financiero Nacional, lo cual compete establecer las directrices generales de las políticas monetarias, cambiaria y crediticia, reglamentar las condiciones de constitución, funcionamiento y fiscalización de las instituciones financieras y disciplinar los instrumentos de política monetaria y cambiaria. En <http://www.fazenda.gov.br/portugues/orgaos/cmn/cmn.asp> [Consulta 10 jul. 2009].

determina el párrafo 3º, línea I del mismo artículo 1º, añadiendo incluso en su rol las centrales de riesgos.

La consecuencia de este dispositivo es que la central de riesgo en Brasil puede poseer en su base de datos todas las informaciones, sin ningún tipo de restricción, que puedan ser generadas por las instituciones financieras, sean advenidas de operaciones pasivas o activas, transformándose en el mayor fichero sobre datos financieros antes visto. Este hecho nos parece de extrema relevancia resaltarlo — aunque ésta cuestión no sea objeto de nuestro estudio —, y a la vez consignar nuestro rechazo a lo que entendemos sea la peor violación a los derechos de privacidad y autodeterminación informativa del ciudadano.

Aparte de lo ya consignado, también cumple resaltar que el hecho de que las instituciones financieras suministren informaciones constantes en el fichero de los libradores de cheques sin fondos y deudores morosos a los ficheros de solvencia patrimonial y crédito tampoco se considera como una inobservancia al deber de sigilo.

Lo que ocurre con esta y las demás leyes que versan más o menos sobre la protección de datos en Brasil es que se olvidan completamente de los afectados. Es decir, se enclaustran demasiado en su finalidad a punto de apartar cualquier mención a temas no solamente correlativos, sino también, congénitos y fundamentales con respecto a la protección de los derechos del individuo, como debería ser, si hubiese efectivamente una cultura jurídica o incluso social de protección de datos en Brasil.

La única ley a nuestro entender que comparte sus dispositivos a los responsables del fichero y a las garantías de los ciudadanos interesados es el Código de Defensa del Consumidor, pero aquí se observa el efecto inverso con relación a otras normas anteriormente citadas. En éste sentido, el artículo 43 trata de modo general, de los ficheros de morosos y registros de consumidores, enumerando en sus cinco párrafos derechos de

los afectados y deberes de los responsables del fichero. Entre ellos prevé el acceso a las informaciones, el derecho de ser comunicado, dispone sobre la calidad de los datos, la permanencia del registro, en fin, con la intención de crear en un único artículo un micro sistema legal de protección de datos en el ámbito de actuación del Código. Hasta ahora simplemente se ha enunciado el tema, pues su estudio será objeto de análisis, en su capítulo correspondiente.

## **2. El fundamento jurídico-constitucional del derecho a la autodeterminación informativa en el sistema jurídico brasileño.**

La Constitución regula en el artículo 1º línea III la dignidad de la persona<sup>138</sup> como uno de los fundamentos del Estado brasileño. Así, como fundamento que es, se comprende dentro de lo que se entiende como las razones que justifican y que legitiman la existencia del Estado Democrático de Derecho de la República brasileña. Por lo tanto se afirma como principio político-constitucional, funcionando como criterio de interpretación y integración de las normas, incluso las constitucionales.

De suerte que, como observa Afonso da Silva, estamos ante “un valor supremo que atrae el contenido de todos los derechos fundamentales del hombre, desde el derecho a la vida”. De hecho, es el principio que orienta

---

<sup>138</sup> Art. 1º La Republica Federativa de Brasil, formada por la unión indisoluble de los Estados y Municipios y del Distrito Federal, constituyese en Estado Democrático de Derecho y tiene como fundamentos:

(...)

III. La dignidad de la persona humana.

la interpretación jurídica, fundado en la propia naturaleza humana — innata — siendo un fin en si misma y tiene como objeto promover la auto realización del individuo. Y al comprender elementos que armonizan las relaciones socio-jurídicas, emana un conjunto de facultades que, una vez reconocidas, permite el libre desarrollo del hombre en su convivencia sea individual, sea colectiva.

En el caso de la República Federativa de Brasil, la dignidad ha sido reconocida por la Constitución y alzada a principio constitucional, aunque es un valor que antecede al ordenamiento jurídico, y su consideración jurídica es estimada como un valor supremo que se materializa como uno de los fundamentos de éste país.

En torno a esta cuestión, defiende Moraes<sup>139</sup>, que la dignidad “es un valor espiritual y moral inherente a la persona, que se manifiesta en la autodeterminación consciente y responsable de la propia vida y trae con él la pretensión al respeto por parte de los demás, constituyéndose un mínimo invulnerable que todo estatuto jurídico debe asegurar (...)”. De suerte que la medida en que la sociedad cambia es natural que sus valores puedan ser alterados y con ello tanto la evaluación de algunos derechos como el surgimiento de otros puedan ser consecuencias de esa transformación, sin embargo siempre con la mirada dirigida hacia la protección de la dignidad de la persona.

Uno de los objetivos fundamentales de la República Federativa de Brasil establecidos en su Constitución es la construcción de una sociedad libre, justa y solidaria, así como la promoción del bien de todos sin preconcepción de origen, raza, color, edad y cualesquier otras formas de discriminación<sup>140</sup>. Son a través de estas finalidades especificadas en un rol,

---

<sup>139</sup>MORAES DE, Alexandre, *Direito Constitucional*, São Paulo: Atlas, 2005, p. 16.

<sup>140</sup> Artículo 3º de la CF, líneas I y IV.

en nuestra opinión, no exhaustivo, donde se busca la realización y legitimación del Estado democrático de Derecho.

Repetidas veces se ha dicho que hoy por hoy información es poder, y sería excesivo aquí comprobar lo obvio. No se puede hablar de una sociedad justa y libre sin que en los días actuales no exista una serie de garantías que aseguren a los individuos frente aquellos que se dedican al acopio de datos. Como se sabe, la recopilación, la retención de diversos registros, su tratamiento, el intercambio de informaciones entre ficheros, la posibilidad de trazar perfiles individuales de cualquier naturaleza y que pueden destinarse a diversas finalidades son actividades que a diario ocurren en cualquier país mínimamente desarrollado.

No se puede admitir que el individuo en su imprescindible desarrollo natural en la vida social, conviviendo con los diversos aspectos a ella innatos — y entre ellos el uso de datos —, no sepa quién posee informaciones sobre él y sobre lo que versa esa información. Pues ello provoca una inadmisibles desigualdad que no es comprensible en lo que apreciamos o entendemos como una sociedad que tiene como fundamento la justicia y la libertad. Por ello resulta totalmente inverso, que se le imposibilite al individuo su disfrute. De manera que las mencionadas actividades merecen control por parte del Estado, o por mejor decir, forman parte de sus principales deberes con el ciudadano, y así se asegura el equilibrio, y que las relaciones sociales puedan darse en un ambiente justo y no discriminatorio.

En la Constitución Federal de Brasil por tanto, el derecho a la privacidad se encuentra plenamente protegido en el artículo 5º, línea X, como ya se ha indicado. Al margen de aludido, es fácil apreciar sin mucho esfuerzo, además de su protección directa, que la Ley Fundamental también prevé diversas situaciones que se vinculan con el derecho de la privacidad. Algunas de ellas se relacionan con el derecho a la información y a la comunicación. Nos referimos, en este último caso a la línea XII del

artículo 5º de la Constitución brasileña<sup>141</sup> que declara la inviolabilidad del sigilo de la correspondencia y de las comunicaciones telegráficas, de los datos y de las comunicaciones telefónicas.

Inicialmente esta norma provocó dudas tocante al alcance que quiso dar el legislador cuando mencionó la inviolabilidad del sigilo de los datos. Para Sampaio Ferraz Junior<sup>142</sup>, “el objeto protegido en el derecho a la inviolabilidad del sigilo no son los datos en sí, sino que su comunicación restringida. (...) el cambio de informaciones (comunicación) privativa no puede ser violada por un sujeto extraño a la comunicación”.

Este mismo entendimiento fue manifestado por Tribunal Constitucional brasileño (el *Supremo Tribunal Federal*), que en sentencia<sup>143</sup> de 10 de mayo de 2006 consignó que sería poco razonable la interpretación de que se tratara de sigilo de datos, porque ello correspondería al reconocimiento de que cualquier registro que no gozara del sigilo, desde que fuese puesto dentro del ordenador, pasaría a serlo con carácter absoluto. De modo que se ha manifestado de manera muy aclaradora el Magistrado Cesar Peluzo, cuando consignó en la oportunidad de su voto, que lo inviolable en los términos de la Constitución era el proceso de comunicación en sí, es decir, el objeto tutelado era el proceso de comunicación independiente de su contenido, porque se trataba de resguardar la privacidad de los interlocutores en acto típico de intersubjetividad. Esta interpretación — con la que estamos totalmente de acuerdo — no permite cualquier ilación sobre una posible ubicación del fundamento jurídico de la libertad

---

<sup>141</sup> CF, art. 5º, XII – es inviolable el sigilo de la correspondencia y de las comunicaciones telegráficas, de los datos y de las comunicaciones telefónicas, salvo, en el último caso, por orden judicial, en las hipótesis y en la forma que la ley establecer para fines de investigación criminal o instrucción procesal penal.

<sup>142</sup> SAMPAIO FERRAZ JUNIOR, T. *Sigilo de dados... op. cit.*

<sup>143</sup> En el voto del Ministro Cesar Peluzo en la sentencia HC 83.168-1/SC, Rel. Min. Sepulveda Pertence.

informática constituyéndose una protección más bien del derecho a la privacidad.

La Constitución brasileña surgió en una época de muchos cambios políticos, cuando Brasil dejaba a tras un régimen dictatorial y pasaba definitivamente a una democracia. Todo ello conllevó al legislador constituyente a dar más atención a las garantías fundamentales y las libertades, entre ellas las de expresión, pensamiento, comunicación y la libertad de información<sup>144</sup>. Para lograr esta última garantía, el Texto Constitucional se ha valido de preceptos como, los que se hallan en el artículo 5º, línea XXXIII, que confiere a todos los ciudadanos el derecho a recibir de los órganos públicos informaciones de su interés particular o de interés colectivo o general, excluyendo solamente aquellas en las cuales sea imprescindible a la seguridad del Estado y de la sociedad. Además, la línea siguiente, letra b, asegura el derecho a la obtención de certificado en los órganos públicos para la defensa de derechos y aclaración de situaciones de interés personal.

---

<sup>144</sup> Para Afonso da Silva la Constitución Federal brasileña ha distinguido la libertad de información del derecho a la información. El primero comprendería la búsqueda, o acceso, o recibimiento y la difusión de informaciones o ideas por cualquier medio de comunicación, sin censura, respondiendo cada uno por los abusos que pudiera cometer. En AFONSO DA SILVA, José. *Curso de Derecho Constitucional*. São Paulo: Malheiros, 1998, p. 249. Para ese constitucionalista, el derecho a informar — como aspecto de la libertad de manifestación del pensamiento — es un derecho individual contaminado por el interés colectivo. En su opinión, la Constitución Federal brasileña acogió esta distinción, ya que en el artículo 5º, alineas XIV y XXXIII es notoria la dimensión colectiva del derecho a la información. *Idem*, p. 263.



### 3. El “Habeas Data”.

No obstante estas normas anteriormente citadas, en Brasil, la Carta Política de 1988 prevé la acción de naturaleza constitucional, el *Habeas Data*, en su artículo 5º, inciso LXXII. Mucho antes de promulgada la Constitución brasileña, ya se podía encontrar en la doctrina el fundamento del *habeas data*, como es el caso de lo que consigna Frosini<sup>145</sup>, cuando manifiesta que: “el ciudadano tiene el derecho de disponer libremente de los propios datos personales, salvo los límites y las obligaciones previstos por la ley, así como tiene derecho de disponer libremente del propio cuerpo (en conformidad con el clásico principio del *Habeas Corpus Act* de 1679), y del propio pensamiento en sus distintas formas de expresión; pues, si alguien detiene abusivamente y utiliza a su arbitrio los datos concernientes a un ciudadano (que pueden también ser de naturaleza delicada, como aquellos sobre sus condiciones físicas o psíquicas), ejerce, en realidad, sobre éste un poder basado en la información”.

En efecto, el instituto procesal que se nombró *habeas data* surgió justamente para intentar facilitar al ciudadano recurrir a la justicia cuando se encontrase en situaciones que marcasen un desequilibrio injusto entre éste y los poseedores de informaciones sobre su persona.

Es importante resaltar que el artículo que hoy prevalece en la Constitución fue alterado de modo sustancial de lo que previa su anteproyecto<sup>146</sup>. En el texto de este documento, se dedicaba un artículo<sup>147</sup>

---

<sup>145</sup> FROSINI, Vittorio. *Banco de datos... op. cit.*, p. 24.

<sup>146</sup> <http://www.senado.gov.br/sf/publicacoes/anais/constituente/AfonsoArinos.pdf>  
Acceso en 10 de julio de 2009.

<sup>147</sup> Art. 17 – Todos têm direito de acesso às referências e informações a seu respeito, registradas por entidades públicas ou particulares, podendo exigir a retificação de

(art. 17), a garantizar el derecho al acceso a las informaciones personales registradas por entidades públicas o particulares y se vedaba el registro de datos sensibles. Así, el *Habeas Data*, que estaba ubicado en otro precepto, y servía para “asegurar los derechos tutelados en el artículo 17”. No obstante, como afirma Afonso da Silva<sup>148</sup>, el citado artículo 17 surgió de la influencia que tuvo las Constituciones de España y Portugal sobre el control del uso de la informática. Incluso en el texto que había sido propuesto<sup>149</sup> a la Comisión del Anteproyecto, se añadía un párrafo en lo cual se fijaba que solamente una ley federal determinaría quién podría mantener registros informáticos, con los respectivos fines y contenidos. Pero, la misma *Comissão Provisória de Estudos Constitucionais*, al transponer ese artículo al anteproyecto, desafortunadamente suprimió este precepto.

Después de otras modificaciones, el texto final reunió — o por lo menos intentó reunir — los dos preceptos en uno sólo, lo que en nuestra opinión fue un grave equivoco legislativo. Primero porque perdió la oportunidad de aprovechar la experiencia de leyes constitucionales como la portuguesa y la española y legislar en el ámbito constitucional el tema de la informática y de la protección de datos. Segundo, porque hubiese ampliado ya en la Constitución el alcance del *Habeas Data*, sin la necesidad de interpretación doctrinal o jurisprudencial. Consiguiéndose lo contrario, es decir, se ha transformado la innovación constitucional de la creación de

---

dados, com sua atualização e supressão dos incorretos, mediante procedimento judicial sigiloso.

§ 1º – É vedado o registro informático sobre convicções pessoais, atividades políticas ou vida privada, ressalvado o processamento de dados não identificados para fins estatísticos.

§ 2º – A lesão decorrente do lançamento ou da utilização de registros falsos gera a responsabilidade civil, penal e administrativa.

<sup>148</sup> AFONSO DA SILVA, José. *Curso de... op. cit.*, p. 454.

<sup>149</sup> Fue el constitucionalista José Afonso da Silva quién propuso a la Comisión del anteproyecto la inserción del *habeas data* en el texto de la Constitución.

un fuerte instrumento de protección de un derecho fundamental, en una herramienta que se ha mostrado en la práctica demasiado restricta, inusual y de equivocada aplicabilidad.

Para muchos autores que tratan de ese tema, como Arruda Alvim Wambier<sup>150</sup>, este instituto fue entendido, tanto en las discusiones en el Congreso Constituyente, como después de algún tiempo de la vigencia del Texto Constitucional, como instrumento del cual podrían servirse las víctimas del régimen político no democrático, para acceder a datos constantes en los registros de órganos de inteligencia e información, principalmente en el área de la llamada seguridad nacional. Quizás por esa razón hubieron tantas modificaciones en el texto que instituía el *habeas data*, resquicios aún de un sistema político militar dictatorial que hacía muy poco dejaba de existir.

De modo que, muchos doctrinadores han criticado muy seriamente este instituto, como es el caso de Ribeiro Bastos<sup>151</sup>, que lamenta que el constituyente no haya aprovechado la ocasión para poner la temática en un nivel más alto de lo que se encuentra en algunas Constituciones, donde el instituto trasciende las dimensiones de un simple medio de acceso a las informaciones personales, para transformarse en un contrapeso eficaz a la utilización de la informática por el Estado moderno. Pese las críticas y los cambios efectuados en el instituto del *habeas data*, el mismo, fue indudablemente una innovación de la Carta Política brasileña, al margen de la importancia que tal instrumento aún puede adquirir en el orden jurídico.

Actualmente, el texto que preceptúa el *habeas data* en la Constitución brasileña está así redactado: "Se concederá "habeas data": a) para asegurar

---

<sup>150</sup> En: ARRUDA ALVIM WAMBIER, Teresa. *Habeas Data*, São Paulo, Revista dos Tribunais, 1998, p. 6-7.

<sup>151</sup> RIBEIRO BASTOS, Celso. "Habeas Data". En: ARRUDA ALVIM WAMBIER, Teresa (coord.) *Habeas Data.. op. cit.*, p. 90.

el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo”. No obstante la redacción constitucional, tanto la doctrina como la jurisprudencia habían hecho eco de la necesidad de la edición de una norma específica para disciplinar ese instituto. Aunque se prevé en la Constitución brasileña en el mismo art. 5º, línea LXXVIII, párrafo 1º, que las normas que definen los derechos y garantías fundamentales tienen aplicación inmediata; incluyéndose el *habeas data*.

De este modo, surge la ley del *habeas data*, nº 9.507/97, que regula el derecho de acceso a informaciones y disciplina su rito procesal<sup>152</sup>. El artículo 7º determina tres hipótesis en las cuales éste puede ser concedido, repitiendo en las dos primeras líneas lo que dice la Constitución y añadiendo la posibilidad de anotación en los registros del interesado de contestación o explicación sobre dato verdadero, pero justificable y que esté sobre pendencia de resolución judicial o amigable. Ni la Constitución ni la ley que desarrolla el instituto exigen que sea necesaria la unión de los tres supuestos para legitimar su uso, es decir, conocer, rectificar y añadir registros son tres posibilidades independientes.

Determinado ya por la Constitución, el *habeas data* solamente podrá ser interpuesto contra banco de datos públicos o que tengan este carácter. La ley 9507/97 comienza su texto aclarando — por no decir, desde nuestro punto de vista, infringiendo la Constitución — que se consideran de carácter público todos los registros o banco de datos que puedan ser transmitidos a terceros y que no sean del uso privado del órgano o entidad productora o depositaria de las informaciones.

---

<sup>152</sup> Vid. sobre el rito procesal del *Habeas Data*: BARBOSA MOREIRA, José Carlos. “O Habeas Data Brasileiro e a sua Lei Regulamentadora” [en línea]. Disponible en: [http://www.senado.gov.br/web/cegraf/ril/Pdf/pdf\\_138/r138-09.pdf](http://www.senado.gov.br/web/cegraf/ril/Pdf/pdf_138/r138-09.pdf)

En efecto, el legislador desafortunadamente ha conseguido con esa regla restringir aún más y sin ninguna necesidad el alcance del *habeas data*. Si se constata que no existe cambio de informaciones entre entidades públicas o terceros, en las informaciones contenidas en los ficheros, no se puede utilizar el *habeas data*. Pero de ser así, la propia Carta Política habría registrado tal impedimento, lo que nos hace pensar que dicho precepto es inconstitucional.

Lo cierto es que puede que en algunas situaciones los ciudadanos no sepan si los datos que están en determinados ficheros son o no transmitidos a terceros, porque la ley no exige la notificación del interesado. Es más, la ausencia en Brasil de una entidad reguladora similar a la Agencia de Protección de Datos de España y de un mandamiento legal que discipline los bancos de datos son indudablemente obstáculos para los ciudadanos que no tienen conocimiento siquiera de la existencia del determinado fichero y consecuentemente si están sus datos allí o no. De hecho, cuando el tema es protección de datos, Brasil acumula una sucesión de equívocos legislativos, aparte de perder, una y otra vez, grandes oportunidades de legislar de una manera mínimamente “honesta” tal materia.

Se podría suponer que cuando promulgase la ley del *habeas data*, que engloba no solamente procedimientos judiciales pero también administrativos, fuese una norma que revolucionaria el escenario de la protección de datos en aquél país, incluyendo conceptos importantes como de *informaciones*, *banco de datos*, etc., los principios generales, reglas sobre los derechos de los individuos y obligaciones de los responsables por los bancos de datos, aunque solamente lo hiciera para aquellos que fuesen considerados de carácter público. Ya habría sido un gran paso, pero no fue así. Quizás los mejores artículos de esta norma fueron los que sufrieron los vetos<sup>153</sup>.

---

<sup>153</sup> Disponible en [http://www.planalto.gov.br/ccivil/Leis/Mensagem\\_Veto/anterior\\_98/VEP-LEI-9507-1997.pdf](http://www.planalto.gov.br/ccivil/Leis/Mensagem_Veto/anterior_98/VEP-LEI-9507-1997.pdf)

La ausencia legal de matices tan importantes se refleja en la jurisprudencia. Actualmente el citado instituto ha sido utilizado como sustituto a otros procedimientos judiciales: “*exibição de documentos*” o “*mandado de segurança*”, ora aceptados por los tribunales, ora no. En efecto, se observa el uso del *habeas data* como instrumento procesal para finalidades como el pedido de acceso a los contenidos, o incluso fotocopias de procedimientos administrativos, o acceso a exámenes de selectividad etc. Y si puede causar sorpresa la elección del aludido instrumento procesal para satisfacer tales pedidos, mayor extrañeza origina como deciden los tribunales sobre el tema.

El *Tribunal Regional Federal* de la 4ª Región ha emitido fallos entendiendo que el *habeas data* no se presta a obtener copias de procesos administrativos. Es el caso de la sentencia<sup>154</sup> de 18 de agosto de 2009, donde se afirma que el *habeas data* no es el medio adecuado para la obtención tales documentos. Así como esa, otras diversas decisiones<sup>155</sup> del mismo tribunal firmando el mismo entendimiento, sobretodo consignando, que “la naturaleza del *habeas data* no se confunde con el derecho constitucional para obtener certificados. La pretensión de cada impetrante es siempre de obtener todas las informaciones objetivas o subjetivas que consten a su respecto, en registros o banco de datos gubernamentales<sup>156</sup>”.

No obstante, lo que no se puede comprender si comparamos las decisiones anteriormente expuestas es que del mismo tribunal se emita un fallo aceptando el uso del *habeas data* como instrumento hábil, en la

---

<sup>154</sup> TRF, 4ª R., AC nº 2008.72.004430-0, Rel. Romulo Pizzolatti, DEJF 25/08/2009.

<sup>155</sup> TRF 4ª R., AI nº 2008.04.00.041892-3/SC, Rel. Celso Kipper, DEJF 07/04/200; TRF 4ª R., AC nº 2007.70.06.002062-0, Rel. Celso Kipper, DEJF 18/11/2008;

<sup>156</sup> TRF, 4ª R., AC nº 2005.71.00.003081-0/RS, Rel. Victor Luiz dos Santos Laus DJU 30/11/2005.

obtención de copia de un examen de selectividad. Para la juez<sup>157</sup>, el precepto inscrito en el artículo 5º, LXXII de la Constitución brasileña (*habeas data*) “asegura el conocimiento de informaciones relativas a la persona del impetrante, que están en el poder de entidades gubernamentales o de carácter público por medio de *Habeas Data*, viabilizando la utilización de este instrumento para amparar el derecho vindicado en los autos”. Asimismo, se puede encontrar en otros tribunales decisiones siguiendo la misma línea argumentativa<sup>158</sup>. De otra parte, hay otras sentencias que expresan opiniones justamente opuestas a esta. Por poner un ejemplo, el fallo del *Tribunal Regional Federal* de la 1ª Región<sup>159</sup> deja bien consignado que el acceso a los exámenes de la selectividad no es equivalente a la exigencia legal para el uso del instituto que es el conocimiento de informaciones relativas al impetrante y de modo que el *habeas data* no es la vía procesal adecuada para proporcionar la tutela postulada.

Desde nuestro punto de vista, el problema principal de todo ello está en la ausencia del análisis de conceptos esenciales como banco de datos. Si la información no se encuentra en un fichero, el *habeas data* no puede ser utilizado. En algunas ocasiones se tienen emitidos fallos, aparte de las situaciones anteriormente expuestas, que vislumbran no sólo la perspectiva del acceso a la información sino que van más allá de lo que la propia ley regula, entrando en el aspecto más subjetivo del afectado, como la finalidad que éste desea dar, a las informaciones obtenidas<sup>160</sup> y según dichas finalidades, se juzga el acierto en la elección del instrumento

---

<sup>157</sup> TRF 4ª R., AC nº 2007.71.02.001229-8/RS, Rel. Marga Inge Barth Tessler; DEJF 02/03/2009.

<sup>158</sup> TRF 5ª R., AC nº 2007.84.00.000789-1/RN, Rel. Barros Dias, DJU 09/03/2009.

<sup>159</sup> TRF 1ª R., AC 2007.38.13.004331-4/MG, Rel. Selene Maria Almeida, DJF 22/05/2009.

<sup>160</sup> TRF, 2ª R., RHD 2007.51.01.021645-9, Rel. Raldênio Bonifacio Costa, DJU 17/06/2009.

procesal. Si por un lado el *habeas data* no puede servir para satisfacer la curiosidad de nadie, por otro el juzgador no puede negar el pedido que fundamenta el uso del instituto, de informaciones que consten en banco de datos públicos, basado en el único argumento de que existen otros medios procesales para alcanzarlas<sup>161</sup>.

De manera que, entendemos que el análisis de la adecuación del instrumento procesal y el pedido es esencialmente objetivo, es decir, el examen de la legitimidad activa y pasiva, la negativa del órgano administrativo en suministrar las informaciones, si estas se encuentran en un banco de datos, si es público o tiene ese carácter, y si lo que se quiere es conocer, rectificar o añadir informaciones. En el caso de que se quiera conocerlas, no hay condición legal ni siquiera de rango constitucional que limite el uso del *habeas data* a la presentación de motivos que fundamentan el pedido de informaciones<sup>162</sup>, asimismo como el uso posterior de dichas informaciones por el interesado<sup>163</sup>.

Quizás por el caos legislativo y jurisprudencial, la doctrina ha criticado bastante el instituto, así, la que hace Ribeiro Bastos<sup>164</sup>, que suscita un cuestionamiento sobre la utilidad del *habeas data* en un régimen democrático. Aunque el autor resalte la importancia del ciudadano en tener derecho al acceso, a la rectificación y a la complementación de sus propios datos que están en el poder del Estado, critica el instituto por haberse olvidado de ciertas cuestiones como el derecho al sigilo en relación a terceros, o incluso la prohibición de tratamiento informático de ciertos tipos de datos personales. En su opinión, el *habeas data* es un

---

<sup>161</sup> TRF 2ª R., RHD nº 2007.51.01.028690-5, Rel. Poul Erik Dyrland, j. 03/06/2008.

<sup>162</sup> TRF 2ª R., RHD nº 762008.51.10.001149-1, Rel. Antonio Cruz Netto, DJU 06/08/2009.

<sup>163</sup> TRF 5ª R., AC nº 2008.82.00.001275-8/PB, Rel. Margarida Cantarelli, DJU 09/07/2009.

<sup>164</sup> RIBEIRO BASTOS, Celso. *Habeas Data... op. cit.*, p. 93.



instrumento desnecesario para un orden democrático de un Estado que procura ser transparente con la *res publica*, concluyendo que el instituto, a pesar de la ley 9.507/90, continua padeciendo de un distanciamiento de lo que hubiese sido su finalidad útil, es decir, la de constituirse en un instrumento en condiciones de enfrentar el uso de la informática por el Estado, concluyendo con, “tenemos lo que no precisamos y no tenemos lo que precisamos”. Una opinión muy similar parece ser la de Lauria Tucci<sup>165</sup>, para quién el *habeas data* en el ordenamiento jurídico brasileño es redundante y innecesaria.

No llegaríamos tan lejos de etiquetar el *habeas data*, como un instrumento inútil, pero quizás, tal como se interpreta y se perfila, hoy por hoy, diríamos restricto. Restricto no en su concepción, pero sí en su sistematización, como antes hemos mencionado, desde el momento de configurarse en la Constitución descartando los ficheros particulares, mezclando conceptos, y dificultando su aplicación al incluir los de “carácter público”.

Es perfectamente comprensible que en el instante de transición política, el poder legislativo constituyente aunque hubiera la posibilidad de estar todavía bajo la influencia del régimen anterior, no podía disminuir derechos, pero sí debería de haberlos aumentado, como medio de ahuyentar los fantasmas del pasado. Aunque todo ello podría de algún modo ser la explicación del cambio de sentido dado por el instituto del *habeas data*, de un instrumento procesal de protección contra los avances informáticos en las libertades individuales, a un instituto que evita la colecta por el Estado de datos personales para finalidades de toda suerte<sup>166</sup>. Sin embargo, las mismas razones no se pueden atribuir al

---

<sup>165</sup> LAURIA TUCCI, Rogério. “Processo e Procedimento da Ação de *Habeas Data*”. En: ARRUDA ALVIM WAMBIER, Teresa (coord.). *Habeas Data. Op. cit.*, p. 322.

<sup>166</sup> BARBOSA MOREIRA, observa que en Brasil durante los gobiernos dictatoriales, algunas informaciones aleatoriamente recogidas en fuentes de discutible idoneidad, muchas veces manipulados sin escrúpulos o incluso fabricadas por los órganos

legislador en 1997, casi diez años después de promulgada la Constitución brasileña, dentro de un régimen democrático ya consolidado. La Ley del *Habeas Data*, aparte de reglamentar algunos aspectos procesales y administrativos sirve muy poco al ciudadano para protegerle de los abusos de la informática y banco de datos, dependiendo este, por lo tanto, de la labor jurisprudencial y de la doctrina para corregir la imperdonable omisión legislativa.

Nos parece oportuno destacar otros aspectos de la Ley 9.507/97. Por ejemplo, el artículo 8º, párrafo único, línea I, determina que en el momento de la proposición de la demanda, la petición inicial deberá contener la recusa del acceso a las informaciones, lo que quiere decir, que antes de utilizarse el instrumento constitucional, el afectado deberá solicitarlas primeramente a la entidad responsable por el banco de datos. La no observancia de este precepto podrá ser motivo de denegación de la petición inicial, conforme se puede leer en el artículo 10.

En lo que concierne a los sujetos activos, pueden ser la persona física, brasileña o extranjera, o persona jurídica a que se refiere la información.

---

represivos eran incorporadas a registros oficiales o “paraoficiales” que pasaron a establecer criterios de evaluación para la imposición de medidas punitivas o discriminatorias. Tales criterios, dice el autor, no podía ser objetados o discutidos, incluso porque los interesados no tenían acceso a los datos constantes en los registros. En *O Habeas... op. cit.*, p.126. Señala BARROSO, sobre el mismo tema, que desde el punto de vista histórico uno de los grandes estigmas del régimen dictatorial, al lado de la violencia física era la malversación de informaciones sobre la vida privada de los ciudadanos. Inicialmente, según el autor, tales datos muchas veces obtenidos de manera ilegal suministraba materia-prima que alimentaba la persecución política, mismo cuando no había cualquier imputación formal de la violación del orden jurídico. Más adelante el uso indebido de las informaciones compraba el silencio y la adhesión de los disidentes del propio régimen, con la amenaza de hacer publica hechos de su vida privada. BARROSO, Luis Roberto. “Viagem Redonda: Habeas Data, Direitos Constitucionais e Provas Ilícitas”. En: ARRUDA ALVIM WAMBIER, Teresa (coord.). *Habeas Data. Op. cit.*, p. 204.

Mientras que los sujetos pasivos son las entidades u órganos públicos responsables por los ficheros, incluyéndose los privados siempre que sus bancos de datos sean de carácter público.

Es importante resaltar que con el *habeas data* solamente se puede requerir informaciones que se refieran a la persona del demandante, con el objetivo de que este la conozca y, si es necesario, la rectifique. Como advierte Alexandre de Moraes<sup>167</sup>, el carácter personalísimo de esa acción constitucional deriva de la propia amplitud del derecho defendido, ya que, el derecho de saber de los propios datos y registros constantes en las entidades gubernamentales o de carácter público comprende el derecho de que esos datos no sean devastados o difundidos a terceros.

Los tribunales también se han hecho eco de esta concepción. La sentencia del Tribunal de Justicia del Distrito Federal<sup>168</sup> entendió que, según lo que dispone la Constitución Federal, en su artículo 5º, LXXII apartados "a" y "b", el *Habeas Data* será concedido para asegurar el conocimiento de informaciones relativas a la persona del impetrante, constante en los registros o banco de datos de entidades gubernamentales o de carácter público o para la rectificación de datos cuando no se prefiera

---

<sup>167</sup> DE MORAES, Alexandre. *Direito Constitucional... op. cit.*, p.129. La misma posición defiende Abreu Dalari, cuando consigna que “se trata de un pedido hecho por el interesado sobre antecedentes que consten en los registros a su respecto. Evidentemente todas las informaciones serán de su conocimiento, todos los datos, si fueren verdaderos, serán de su conocimiento, porque él participó de los hechos que están registrados. Y si los datos almacenados en los registros no son verdaderos, no conviene al Estado mantener informaciones erradas o falsa. Entonces no conviene o no corresponde este sigilo – también – para el interesado, que se mantenga in sigilo para otras personas puede ser razonable. Pero si se trata de una información de carácter personal, no hay ninguna justificación para que se niegue a información al propio interesado”. ABREU DALARI, Dalmo. *Derecho a la autodeterminación informativa y acción de Habeas Data en Iberoamérica* [en línea]. Disponible en [http://derecho.utralca.cl/pgs/revistas/ius/3-1-97/071\\_080\\_abreu.pdf](http://derecho.utralca.cl/pgs/revistas/ius/3-1-97/071_080_abreu.pdf)

<sup>168</sup> TJDF, nº 20050111155592, Relator BENITO TIEZZI, juzgado en 04/10/2006.

hacer por proceso sigiloso, judicial o administrativo. Así, continua la sentencia, para que se le conceda el remedio constitucional es necesario que las informaciones pleiteadas digan respecto a la propia persona del demandante, no estando comprendida en el mandamiento constitucional la hipótesis de obtención de informaciones de interés del impetrante, pero relativa a terceros.

Ahora bien, terceros es un término que se relativiza cuando se da el caso de que pleitee la viuda el acceso a informaciones de su fallecido marido, como ya decidió el Superior Tribunal de Justicia<sup>169</sup>, para quien el pedido deberá ser concedido, ya que negarle tal derecho conllevaría una ofensa a la propia finalidad de la norma constitucional, cuyo conocimiento de las informaciones podría reflejarse, en este caso, en el patrimonio moral y financiero de la familia del fallecido.

Con respecto al objeto del *Habeas Data*, según José Afonso da Silva<sup>170</sup>, citando Firmin Morales Prats, sería la protección de la esfera íntima de los individuos contra: a) el uso abusivo de los registros de datos personales, recabados en fuentes ilícitas; b) el registro de datos sensibles; y c) permanencia de datos falsos con fines distintos de los autorizados en ley. Sin embargo, también es objeto del *Habeas Data* asegurar el derecho de acceso y rectificación de datos personales, almacenados en ficheros públicos, o que tengan este carácter<sup>171</sup>, así como insertar anotación de esclarecimiento o justificativa en el registro de datos<sup>172</sup>.

---

<sup>169</sup> STJ, HD nº 147-DF (2006/0224991-/DF); Rel. Min. Arnaldo Esteves Lima; Julg. 12/12/2007.

<sup>170</sup> AFONSO DA SILVA, José. *Curso... op. cit.*, p. 453.

<sup>171</sup> DE MORAES, Alexandre. *Direito Constitucional Administrativo*. São Paulo: Atlas, 2002, p 256; y, también, AFONSO DA SILVA, José. *Curso... op. cit.*, p. 455.

<sup>172</sup> ZANELLA DI PIETRO, Maria Sylvia. *Direito Administrativo*. São Paulo: Atlas, 2001, p. 617.

En la valoración de Ribeiro Bastos<sup>173</sup>, su objeto es asegurar el acceso a las informaciones personales del demandante, que conste en los registros o banco de datos de entidades gubernamentales o de carácter público con la finalidad de rectificarlos. Además, opina que el instituto presupone que la información a que se desea obtener guarde relación con la preservación de la intimidad y que el objetivo del *Habeas Data* es la rectificación de los datos, expresión esa que debe ser entendida de manera más amplia, comprendiendo también la supresión de los datos cuando se trate de informaciones pertinentes a la vida íntima de la persona, así como, cuando se trate de las hipótesis en las cuales los datos personales no tengan relación con las finalidades legalmente definidas del órgano colector<sup>174</sup>. En este mismo sentido, el Superior Tribunal de Justicia de Brasil<sup>175</sup> consignó en Sentencia ésta otra función del *habeas data* que es la supresión de informaciones del siguiente modo: el *habeas data* pretende garantizar el acceso a las informaciones referentes a la persona del impetrante y desconocidas por el mismo. De esto se deriva la posibilidad de rectificación o mismo la excusión de los datos.

En efecto, el país creador del procedimiento *habeas data* desafortunada y paradójicamente tiene todavía un sistema muy débil de protección de datos. Sin embargo, la observación de Garcia<sup>176</sup>, retrata un poco la situación del citado instituto en el sistema jurídico de Brasil, al afirmar que la cultura brasileña no ha atingido la plenitud del trato constitucional y democrático, que es un proceso constante y “por eso las medidas del alcance del *habeas data* son incomprendidas y entendidas inocuas y de inicio se tiene revelada como tales; no obstante, mejor para la salud

---

<sup>173</sup> RIBEIRO BASTOS, Celso. *Habeas... op. cit.*, p. 84.

<sup>174</sup> Idem, p. 86

<sup>175</sup> STJ. Recurso Especial nº 781.969-RJ. Rel. Min. Luiz Fux, Juzgado en 08/05/2007.

<sup>176</sup> GARCIA, Maria. “Habeas Data. O Direito à Informação. O Direito Fundamental à Intimidade, à Vida Privada, à Honra e à imagem das pessoas. Um Perfil Constitucional”. En ARRUDA ALVIM WAMBIER. Teresa (coord). *Habeas Data...*, op. cit., p. 241.

constitucional de la sociedad brasileña es que estén consagradas en el texto constitucional, ya que el tiempo y la experiencia harán con que sean ejercitada en su justa medida”.

Es cierto que la Constitución Federal brasileña en lo que concierne a derechos y garantías individuales fundamentales no se quedó en la mera declaración de derechos materiales. De modo que consagró en su texto algunos instrumentos procesales, que tiene por finalidad promover la defensa de los derechos allí enunciados. Éste es, precisamente, el caso del *habeas data*.

No obstante, no somos de la opinión que este instituto sirva en su concepción primaria al derecho a la intimidad. Es decir, el *Habeas Data*, fue estructurado como un instrumento procesal con el que se pretende que el individuo pueda tener acceso a sus informaciones personales. Ocurre que la naturaleza de tales datos no es necesariamente íntima. De esta manera, a nuestro juicio, el *habeas data* es la garantía constitucional que tiene como objeto proteger el derecho a la autodeterminación informativa de la persona, con todo el respaldo y sistema protectivo que este conlleva.

La Constitución brasileña habla de asegurar el conocimiento de informaciones relativas a la persona del demandante, lo que no se confunde con satisfacer la simple curiosidad de uno. De modo que *conocer* se entiende desde una perspectiva más amplia, previendo el texto constitucional la rectificación de los registros y la ley que disciplina el *habeas data*, añadiendo la inserción de informaciones con el objetivo de aclarar algún dato. Ese conjunto derechos que protege el instrumento procesal constitucional podría ser perfectamente resumido como el *control de los datos*. El individuo que puede acceder, rectificar, suprimir, añadir informaciones, tiene sobre su dominio y sobre su vigilancia sus datos personales, que se encuentren en un banco de datos público o que tenga ese carácter, es decir, tiene su control. Además, como bien destaca Murillo

de la Cueva<sup>177</sup>, algunos de los contenidos activos del derecho a la autodeterminación informativa son precisamente estos: acceso, rectificación, complementación y cancelación.

Es principalmente por esa razón que a nuestro parecer el *habeas data*, pese surgir como un derecho procesal, guarda el fundamento del derecho a la libertad informática en el sistema jurídico brasileño<sup>178</sup>.

No se puede imaginar una garantía procesal sin su respectivo derecho material que le proteja. Y si el instituto surge como pretenden algunos para protección de la intimidad, cualquier otro dato que no sea íntimo no podría ser objeto de impetración del *habeas data*. Y aceptarlo de ese modo es forzar una restricción que no existe en el cuerpo constitucional. Sin embargo, eso no quiere decir que de algún modo, en algunas situaciones, el derecho a la intimidad no sea también protegido por el mismo instituto, y ese hecho de ninguna manera negaría su configuración. Ahora bien, la utilización del instrumento procesal no puede ser confundida con el derecho material. Las restricciones que contiene el *habeas data*, como por ejemplo que solamente puede ser utilizado contra banco de datos públicos, o que tengan ese carácter, no debe ser entendido como obstáculo al fundamento constitucional de la libertad informática. Es cierto, que este principio no puede permitir tal distinción. Esta acción constitucional de hecho posee sus peculiaridades lo que no significa que, por otra vía

---

<sup>177</sup> MURILLO DE LA CUEVA, Pablo Lucas. "Perspectivas del derecho a la autodeterminación informativa". En: "III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas" [monográfico en línea]. IDP. Revista de Internet, Derecho y Política. n.º 5. UOC. <http://www.uoc.edu/idp/5/dt/esp/lucas.pdf> [Consulta: 29 feb. 2009].

<sup>178</sup> Para Nojiri, "la matriz constitucional de ese derecho está en el artículo LXXII, de la Ley Mayor, que ha traído a la nuestra sistemática jurídica el instrumento del *habeas data*". NOJIRI, Sergio. "O Habeas Data e o Direito à Autodeterminação Informativa". En ARRUDA ALVIM WAMBIER. Teresa (coord). *Habeas Data...*, op. cit., p. 362.

procesal no se pueda exigir la garantía del derecho material que guarda el *habeas data*, que es la autodeterminación informativa.

En nuestra opinión, la libertad informática se encuentra perfectamente respaldada en la Constitución brasileña, sobre todo cuando interpretado y integrado con los artículos 1º, línea III y 3º, líneas I y IV de la Constitución. Es necesario resaltar que el conjunto de derechos y garantías fundamentales inscritos en el artículo 5º de la Carta Política es abierto, tanto que en la línea LXXVIII, párrafo 2º explícitamente manifiesta que los derechos y garantías expresos en la Constitución no excluyen otros decurrentes de régimen y de los principios por ella propia adoptados, o de tratados internacionales en los que Brasil sea parte.

## VI. Toma de Posición.

Niger<sup>179</sup>, cuando trata del *diritto alla riservatezza*, afirma que el objeto de este derecho es tutelar la necesidad del sujeto a que los hechos de su vida privada no sean públicamente divulgados, añadiendo que éste protege al sujeto contra la curiosidad individual. De hecho, y así considerado, aquí residiría la separación de los dos derechos: la autodeterminación informativa no tiene la pretensión principal de proteger el afectado de la curiosidad individual, tutela esa típica del derecho a la intimidad, pero permitirle controlar sus propias informaciones.

En definitiva, a nuestro sentir, el derecho a la intimidad y el de la autodeterminación informativa se encuentran en una zona de intersección

---

<sup>179</sup> NIGER, Sergio. *Le nuove... op. cit.*, p. 41.



en la cual confluyen una pluralidad de situaciones jurídicas que podrían incluso confundir la protección de uno y otro derecho. No obstante, eso no puede significar la inexistencia de un más allá de este punto, donde se distancian y se tornan independientes, y donde paralelamente recurrirán a ellos otras distintas situaciones jurídicas que no necesariamente requieren la tutela de ambos derechos a la vez y por tanto, tampoco se mezclarán<sup>180</sup>. Aunque se considere que el contenido del derecho a la intimidad sea negativo –de exclusión– y positivo, –de control–, no se puede pretender que el segundo sea extendido a punto de beneficiarse de un alcance más amplio que el propio continente. En efecto, señala con mucha lucidez Orozco Pardo<sup>181</sup> que “existen datos relativos a la vida de las personas que no entran dentro del ámbito de lo íntimo, tales como domicilio, hábitos de consumo, profesión, etc. Que incluso responden a actividades *públicas*, sobre los cuales el Derecho reconoce la posibilidad de permitir o no que sean, no tanto conocidos, como recabados, tratados y utilizados en ficheros, manuals o automatizados”.

Además, la tendencia a vincularse con otros derechos no ocurre solamente entre el de la intimidad y el de la autodeterminación informativa, como destaca Serrano Pérez<sup>182</sup>, pero también con otros como

---

<sup>180</sup> Sobre ese tema, la postura adoptada por el Tribunal Constitucional es la de que: “El derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, **con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar**, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática (...)” pero que uno y otro derecho poseen distinta función, objeto y contenido. STC 292/2000. Subrayamos.

<sup>181</sup> OROZCO PARDO, Guillermo. “La protección de datos en Derecho español a la luz de la reciente jurisprudencia constitucional”. Aranzadi. Actualidad civil, nº 1, 2002, p. 213.

<sup>182</sup> Así afirma Serrano Pérez, que “en nuestro Texto Constitucional el art. 18 de la Constitución recoge la protección de la intimidad personal y familiar y la propia

lo de inviolabilidad del domicilio y el secreto a la correspondencia, sin que dicha relación implique una la pérdida de la autonomía de los citados derechos.

De modo somero, el fundamento social de la autodeterminación informativa reposaría en el derecho que tiene cualquier ser humano a no ser procesado, juzgado y a veces incluso condenado por los sistemas informáticos; por mejor decir, de no someterse a una forzosa institucionalización de estos sistemas que al fin y al cabo e irónicamente no tiene más que informaciones que respectan al propio individuo<sup>183</sup>. En definitiva, permitir que se pueda vivir y convivir en una sociedad donde esté asegurada su plena libertad incluso de las modernas técnicas de interferencias.

En la convivencia de una sociedad organizada bajo el manto del Estado Democrático, no es posible permitir el planteamiento sobre derechos

---

imagen, la inviolabilidad de domicilio, y el secreto de la correspondencia, todos ellos como derechos tendentes proteger el núcleo más íntimo de la persona, pero reconocidos también con sustantividad propia frente a la intimidad. La intimidad o su sentido de salvaguarde de todo aquello que guarda relación con los actos mas personales del individuo parece latir en el sentido de todo el precepto. Esa función de vínculo entre todo el precepto que parece desempeñar la intimidad no implica su transformación en un derecho aglutinador de todos los demás”. SERRANO PÉREZ, María Mercedes. “El derecho fundamental a la protección de datos. Su contenido esencial”. *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, Sevilla, núm. 1, 2005, pp. 249-250.

<sup>183</sup> Para el Tribunal Superior de Justicia de Andalucía, “las novedades informáticas y telemáticas están obligando a una nueva clasificación de los derechos fundamentales, no bastando la distinción entre derechos individuales o libertades y derechos sociales o prestacionales, naciendo así derechos o libertades llamados de “tercera generación”, constituidos por las garantías del individuo frente a la contaminación o deterioro que las libertades pueden sufrir por las nuevas tecnologías. Entre esos derechos se incluirían el secreto de las comunicaciones informáticas y telemáticas, la intimidad informática y el derecho a la autodeterminación informativa, formando un conjunto que me atrevería a denominar de “libertades informáticas”. TSJ Andalucía, 1691\2003.

absolutos, sean ellos fundamentales o no, porque todos ellos encuentran sus límites unos en los otros, aspecto ese, ya por reiteradas veces pronunciado por el Tribunal Constitucional español<sup>184</sup>.

Sin embargo, como hemos comentado hasta la saciedad, es imposible imaginar la sociedad actual sin la tecnología que se tiene a disposición. No es otra la razón por la cual se denomina esta actual fase social como “sociedad de la información”. Es innegable que el desarrollo de la informática ha modificado acentuadamente las relaciones sociales. En esta perspectiva, se puede afirmar que ese cambio en el *modus vivendi* supone alteraciones o incluso surgimiento de nuevas relaciones jurídicas y, con ellas, sus conflictos.

Por consiguiente, entendemos, que el apareamiento de nuevos derechos establece siempre un dialogo con las nuevas necesidades humanas, la etapa social de (r)evolución tecnológica exigía la respuesta adecuada a las nuevas intromisiones ilícitas sobre las libertades y derechos individuales y también colectivos. En este sentido destacó Pérez Luño<sup>185</sup>, con mucha lucidez que “el estudio actual de los derechos

---

<sup>184</sup> STC 2/1982: “No existen derechos ilimitados. Todo derecho tiene sus límites”. RTC 2000\186: “es doctrina reiterada de este Tribunal que ‘el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho’ (SSTC 57/1994, F. 6, y 143/1994, F. 6, por todas)”. Igualmente, la Audiencia Nacional declaró “(...) como ya se ha adelantado **y como acontece con cualquier derecho, tenga éste la calidad que tenga**, ni el derecho fundamental a la intimidad personal, ni el derecho a ver protegidos los datos de tal carácter, son absolutos, pudiéndose y debiéndose, dentro de la relación jurídico-laboral, modularse e incluso limitarse (...)”, Sentencia núm. 38/2006 de 28 abril. Subrayamos.

<sup>185</sup> PÉREZ LUÑO, Antonio Enrique. “Internet y los derechos humanos”. *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, nº. 2, Huelva, 2002, p. 102.

humanos no puede omitir esa referencia contextual, ni puede abdicar del juicio crítico de sus implicaciones. Se trata de lograr que los desarrollos tecnológicos no menoscaben ni se alcancen a costa de las libertades cívicas”. De otra parte, merece destacarse la observación de Viterbo<sup>186</sup>, cuando afirma que en la actual configuración del mercado la libre circulación de los datos de carácter personal es funcionalmente conectada a la libre circulación de personas, de las mercancías, servicios y capitales. No obstante, continúa el autor en cita, el interesado independientemente de la relación que puede haber dado causa al tratamiento de sus datos, está tutelado por el ordenamiento en cuanto persona, titular de una situación subjetiva de relevancia fundamental y, en particular, de una imprescindible libertad de autodeterminación.

No es nuestro deseo, aquí, profundizar en esta cuestión, lo que excedería el propósito de este estudio. Sin embargo, previa advertencia no obstaría señalar que coincidimos con la línea argumentativa moderada de Murillo de la Cueva. Si es verdad que no se puede transformar todas las pretensiones existentes en la categoría de derechos humanos, gozando así de la máxima protección dentro de un sistema jurídico, desde otra óptica no se puede permanecer ciego ante las nuevas exigencias que nacen paralelamente al natural desarrollo social. Es decir, hoy por hoy, no se concibe por lo menos en los países desarrollados o en desarrollo un cuerpo institucional – público o privado – sin que el flujo de datos sea el cimiento fundamental de su actuación.

En nuestro modesto juicio, con el más profundo respecto a la gran e indiscutible contribución científica de los seguidores de la tesis de la no autonomía del derecho a la autodeterminación informativa, no entendemos que tal derecho está en el rol de aquellos que carecen de los requisitos que se hacen necesarios para la consideración de un derecho como fundamental. Además, es un derecho que traspasa las fronteras de

---

<sup>186</sup> VITERBO, Francesco Giacomo. *Protezione... op. cit.*, p. 107.

desarrollo tecnológico. Por mejor decir, opinamos que el entorno en el cual se ubica la discusión es tan universal<sup>187</sup>, tanto en el sentido lógico cuanto cuantitativo, como lo son, actualmente, las plataformas sobre las cuales se sitúan los responsables por posibles intromisiones ilegítimas a la autodeterminación informativa. Podríamos incluso afirmar que jamás en otra época estuvimos discutiendo un fenómeno tan global.

No obstante en algunas sociedades todavía no se han iniciado debates sobre la necesidad de protección especial de este derecho, sea porque efectivamente aún no hayan afrontado el problema (por ausencia de voluntad política o incluso social), sea por su etapa de desarrollo tecnológico<sup>188</sup>, ello no implica en “punirlas” por el hecho de que todavía no hayan despertado para pretensiones de esta naturaleza; así como no se puede “sacrificar” a otras sociedades que por un conjunto de factores político-sociales ya reclaman una protección especial de este derecho.

---

<sup>187</sup> Para Ferrajoli, tocante a la universalidad de los derechos humanos, esta debe ser entendida “en el sentido lógico y no valorativo de la cuantificación universal de la clase de sujetos que, como personas, ciudadanos o capaces de obrar, sean sus titulares”. FERRAJOLI, Luigi. “Los Fundamentos de los Derechos Fundamentales”. En *Los fundamentos de los derechos fundamentales*, FERRAJOLI, Luigi. Debate con Luca Baccelli et al. Madrid: Trotta. 2001, p. 291.

<sup>188</sup> Hay que tenerse en cuenta que, a depender del interés de una sociedad, determinada tecnología puede o no desarrollarse. Es decir, generalmente las necesidades sociales son responsables por mover el rumbo tecnológico. La Internet es un buen ejemplo: surgió en un ambiente militar, en medio a la Guerra Fría, estimulada principalmente por la comprensión de la necesidad, en aquella época, de fortalecer los medios de comunicación para asegurar que informaciones sigilosas no se perdiesen y pudiesen ser transmitidas, en caso de ataque militar. Como resalta Heilbroner, el hecho de que la tecnología avance en determinado sector depende, en parte de las recompensas, alicientes e incentivos que ofrezca la sociedad. Así, concluye el autor, el rumbo del avance tecnológico es en parte el resultado de la política social. HEILBRONER, Robert L. “¿Son las maquinas el motor de la historia?”. En MARX, Leo; SMITH, Merritt Roe. *Historia y determinismo tecnológico*. Madrid: Alianza, 1996, p. 78.

Además, es de extrema importancia resaltar que con independencia del interés de quienes usen los sistemas informáticos, este tipo de distinción puede ser completamente irrelevante. Así, es muy aclarador el planteamiento de Frosini<sup>189</sup>, al investigar sobre la problemática del flujo internacional de datos, cuando resalta que “los países con civilización tecnológica avanzada son capaces de coleccionar, acumular y distribuir informaciones con los sistemas informáticos; mientras que los países con civilización tecnológica atrasada sólo pueden recibir y consumir las informaciones”. Es decir, el problema de la protección de datos va más allá de las fronteras y de la identificación de las condiciones tecnológicas de uno u otro país, ya que esto puede ser fácilmente superado, como es el caso, de cuando se está delante de la relación proveer-consumir informaciones incluso entre Estados.

Es indiscutible que el debate sobre la protección jurídica de las personas, referente a sus datos de carácter personal representa una evolución tocante a las garantías y derechos fundamentales del ciudadano. O, aun mejor, significa decir que el Estado no se encuentra adormecido ante su función de intervenir y tutelar sus ciudadanos contra

---

<sup>189</sup> FROSINI, Vittorio. *Banco de datos... op. cit.*, p. 38. El mismo autor pone de relieve un caso muy interesante sobre la problemática del cambio de datos entre países, que nos parece conveniente exponerlo como modo de reforzar la irrelevancia de la desigualdad tecnológica para el afrontamiento de la protección de datos: “Un ejemplo muy significativo de las diferentes situaciones entre países productores y países informadores nos fue dado por una ponencia en el Simposio organizado en Viena en septiembre de 1977 por la OCDE y dedicado justamente al ‘flujo de datos transfronteros y a la protección de la privacidad’. **El delegado de un Estado de Europa oriental reveló que su país, al no disponer de un sistema adecuado de equipos electrónicos, se valía para las reservaciones de viajes aéreos de una conexión internacional con una agencia con sede allende el Atlántico, ésta desempeñaba su actividad mediante la transmisión telemática. Por esto, se conocía mejor en el extranjero que en el país mismo la fecha, la destinación y los acompañadores eventuales de los viajes de los hombres políticos de ese país**”. Subrayamos. *Ibid.*, p. 39.

las más diversas formas de intrusión ilegítima de sus derechos, aunque ésta sea patrocinada por la mala utilización de las nuevas tecnologías<sup>190</sup>.

Todo ello porque, como ya hemos tenido oportunidad de resaltar, el reconocimiento de los cambios introducidos por el desarrollo tecnológico dentro del cuerpo social se revela a través de una visión bipartida, de efectos positivos por un lado y potencialmente lesivos por otro, a depender de cómo se conduzca su utilización.

En realidad, los datos - y con ellos las informaciones que contienen - y su circulación, favorecida por la evolución tecnológica, se constituyen en la espina dorsal de nuestra sociedad. Sin embargo, la configuración actual y todo lo que se comprende por Estado Democrático de Derecho<sup>191</sup> no puede permitir que haya desproporcionalidad entre el libre y pleno ejercicio de los derechos de los ciudadanos, y el uso de lo que se concibe como factor esencial de la sociedad. Ya había advertido Pérez Luño<sup>192</sup>, que una de las funciones de los derechos fundamentales es establecer un equilibrio de poder y eso exige que las relaciones entre Estado y sociedad, y entre los miembros de esta no se den situaciones de marcada desigualdad en el acceso al poder que impliquen para determinadas personas o grupos humanos una marginación de la libertad”.

---

<sup>190</sup> Desde esta perspectiva, nos parece conveniente subrayar que la Carta de los Derechos Fundamentales de la Unión Europea, en el artículo 8, capítulo II, dedicado a la libertad, expresa taxativamente que toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Declara en esta oportunidad los derechos a la adecuación de los datos, al acceso, a la rectificación, además de establecer el consentimiento como la base de esta protección u otro fundamento previsto por ley.

<sup>191</sup> Sobre todo entendido en una óptica de que el Estado protege la libertad de la persona humana de cualquier forma de opresión reconociendo los derechos individuales, así como ofreciendo las condiciones necesarias para que los ciudadanos disfruten de su pleno ejercicio.

<sup>192</sup> PÉREZ LUÑO, Antonio Enrique. *El Derecho... op. cit.*, p. 301.

Ineludiblemente estamos ante una nueva forma de poder<sup>193</sup>, con perfiles distintos a los que suelen influir en la convivencia social y que además no está accesible a todos. El manejo y el coste de un sistema informático que permita el acopio, almacenamiento, el enlazamiento y la circulación de datos aún no está al alcance de toda la sociedad.

Dicho esto, vislumbrar esa problemática ubicándola dentro de esa necesidad de sopesar tales elementos, no corremos el riesgo de distanciar Estado y ciudadanos de la realidad de una “sociedad de la información”, con todo lo que implica su concepto para que verdaderamente, se pueda convivir según los criterios de un Estado Social y Democrático de Derecho.

En esta perspectiva, resulta importante subrayar la interesante observación de Toniatti<sup>194</sup>, cuando manifiesta que si la nuestra es una “*information intensive society*”, sería ilusoria la (falsa) alternativa de intentar atenuar la demanda de información, que es, hoy por hoy, vital para el buen funcionamiento del sistema. En su opinión, sería más realista y funcional reglamentar y racionalizar los flujos informativos, protegiendo su calidad y estableciendo aquellas restricciones y solamente aquellas que mejor correspondan a la exigencia de reequilibrar, en beneficio del segundo, la contraposición entre el interés por la intimidad.

---

<sup>193</sup> Para Martin Pallín, “la tecnología es poder o, si prefiere, sirve al poder dotándole de más posibilidades de información insospechadas en época anteriores” y sigue afirmando que “la técnica, como todo medio instrumental puede ser puesta al servicio de una idea o de un sistema político determinado y de sus valores esenciales”. MARTIN PALLÍN, José Antonio. “Protección de los derechos y libertades individuales frente al uso de la informática y las telecomunicaciones”. *Anuario de jornadas 1989-1990*. Bilbao: Servicio de Estudios del IVAP, 1991, pp. 336-337.

<sup>194</sup> TONIATTI, Roberto. “Libertad Informática y Derecho a la Protección de los Datos Personales: Principios de Legislación Comparada”. *Anuario de jornadas 1989-1990*. Bilbao: Servicio de Estudios del IVAP, 1991, p.261.



No cabe duda que se puede afirmar que el riesgo de la mala utilización de la tecnología puede alcanzar y debilitar los pilares del sistema democrático. A nuestro juicio, es innegable que somos protagonistas y a la vez espectadores de un nuevo capítulo de la historia de los derechos fundamentales.

Otra cuestión que entendemos que no es ociosa destacar, es la necesidad de perfilar los contornos del derecho subjetivo de la libertad informática y del derecho objetivo que sirve para su efectividad. A este respecto, a nuestro sentir, se debe superar cualquier discusión más profundada sobre nomenclatura, que al fin y al cabo, es menos relevante de lo que se pretende verdaderamente proteger. Lo principal es garantizar la efectividad de los derechos tutelados, independientemente de cómo se quiera denominarlos. Y exactamente sobre esa importancia tuvo oportunidad de manifestarse el jurista italiano Ferrando Mantovani<sup>195</sup>, para quién las dos condiciones fundamentales para que estos derechos sean una “efectiva realidad” son su *reconocimiento jurídico-formal* y la garantía de la *efectividad* de su goce, necesitando además de su proclamación, su concreto disfrute. El citado autor, observó que la efectividad de estos derechos en el actual modelo social “se ve cada vez más puesta en entredicho por el *uso destructivo de la ciencia y la tecnología*, amparada por los ‘totalitarismos de la economía y la tecnología’, las dos fuerzas principales que guían las sociedades modernas, y por la propia ‘miopía de un cientifismo’ afectado por la limitada capacidad de prever y controlar como mucho los micro-efectos de las micro-causas, pero no los macro-efectos de las micro-causas, que no son otra cosa sino el resultado del conjunto de los micro-efectos de las micro-causas, puestos

---

<sup>195</sup> MANTOVANI, Ferrando. “La proclamación de los derechos humanos y la ineffectividad de los derechos humanos”. Trad., Peris Riera, Jaime M. (inédito), conferencia realizada en la Facultad de Derecho de la Universidad de Granada, en 9 de abril de 2006.

cotidianamente en entredicho por el desarrollo económico y tecnocientífico”.

Así, siguiendo esta línea de raciocinio, la distinción a la que antes hemos hecho referencia, parece ser de extremada importancia. Para eso, vamos diferenciar aquí, aunque no sea ninguna innovación, el derecho subjetivo denominándolo *libertad informática*, o como preferimos más, la *autodeterminación informativa*, y para la garantía objetiva de este, utilizaremos *protección de datos*, ya que son términos bastante difundidos en la doctrina y jurisprudencia.

Este enfrentamiento que se pretende hacer, se justifica por la observación de cierta tendencia de parte de la doctrina científica y de la jurisprudencia, en limitar la interpretación del derecho a la autodeterminación informativa en lo que se comprende por *habeas data*, es decir, el control de datos personales que son tratados por programas informáticos.

A nuestro juicio, la autodeterminación informativa, como se concibe actualmente, corre el serio riesgo de verse condicionada a una concepción restricta y fácilmente superable con la evolución tecnológica y social. Hecho que, *mutatis mutandi*, fue presenciado con el derecho a la intimidad, cuando fue necesaria la reevaluación de su noción, progresando de un contenido únicamente negativo hacia la elaboración de un positivo, tal y como ya se ha comentado anteriormente.

La interrogante estaría en si ¿el derecho a la libertad informática se agota únicamente en el alcance fornecido por la garantía objetiva de la protección de datos personales en el ámbito de los ficheros informáticos<sup>196</sup>,

---

<sup>196</sup> Según Downing, Covington y Mauldin Covington, la informática es definida como el estudio científico y matemático de los posibles usos de las computadoras, que abarca un amplio campo incluyendo las matemáticas pura, la ingeniería (arquitectura informática), la gestión (ingeniería de software) y el estudio de la mente humana (inteligencia artificial). Según estos autores, los científicos de la computación trabajan

como hoy se presentan?. Entendemos que no. Ha sido reconocido el derecho subjetivo de protección de las informaciones personales (íntimas o no) de los individuos frente a cualquier forma de amenaza. Es el poder de control, uso y destino de informaciones que no pueden restringirse a banco de datos sean informáticos o manuales. Es decir, la limitación del modo de tornar efectivo el derecho subjetivo no puede ser en si su propio condicionante.

El Derecho no puede dar por hecho que la única forma de reunir informaciones personales sobre alguien sea a través de ficheros controlados por programas informáticos sobre todo cuando la evolución tecnológica se opera con una velocidad cada vez más intensa, eso si miramos hacia el futuro. Ya se sabe que la transmisión de datos se puede operar de las más diversas formas, debiéndose tal hecho al desarrollo de las comunicaciones. En lo que se refiere al almacenamiento de datos, aunque actualmente las plataformas de los programas informáticos sean las más utilizadas, no se puede garantizar que será siempre inmutable, y el único medio usado para tal fin. Y si no se puede garantizar que no habrá cambios operados por las nuevas tecnologías en la forma de almacenamiento de datos, como de hecho ya lo hay en la transmisión, no se debe limitar el derecho subjetivo al control de datos personales fundado en las tecnologías actuales. Pero sí, dejar dicha limitación para el derecho objetivo.

---

frecuentemente sobre los problemas en casi cualquier campo en los cuales las computadoras pueden ser aplicadas. Éste es un concepto más restricto de la informática ya que según los mismos autores en cita, ésta ciencia comprende algo más que la capacitación en el uso actual de las computadoras y software; ella incluye la preparación para comprender la tecnología del futuro y sus fundamentos teóricos. En: DOWNING, Douglas A.; COVINGTON, Michael A. y MAULDIN COVINGTON, Melody. *Dictionary of Computer and Internet Terms*. Hauppauge: Barron's, 10ª Edición, 2009, p. 108.

Por lo tanto, entender esto de otra manera, pensamos que se podría disminuir la importancia de la información ante la forma de su acopio y restringir esta última, a una única manera de actuar, así como, rechazar la idea de que puedan existir almacenamientos de informaciones utilizándose otras técnicas. Y, aún más, mirar el fenómeno de las nuevas tecnologías con tal inocencia como si la etapa actual de desarrollo no estuviese susceptible a cambios — y de hecho, estos no solamente son susceptibles sino que pueden ser inminentes — tornándose el derecho inflexible desde su concepción.

El derecho a la autodeterminación informativa preserva los datos de cualquier naturaleza desde que son personales; asegura por regla general el consentimiento del afectado<sup>197</sup>. Su contenido descansa en garantizar un poder de control<sup>198</sup> sobre los datos personales: su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del afectado, aunque eso no signifique de ninguna manera su incondicional propiedad. Es decir, la posibilidad de tener el control del uso por terceros de información personal que sean relevantes para el

---

<sup>197</sup> Para MURILLO DE LA CUEVA, "... la forma de operar de las normas dedicadas a proteger la autodeterminación informativa es distinta de la que adoptan las que se encargan de asegurar la intimidad. En este caso, basta con observar lo que dispone la Ley Orgánica 1/1982, es la noción de intromisión ilegítima la pieza central del sistema de protección y la publicidad, el desvelamiento por el afectado de parcelas de su intimidad, excluye tal legitimidad, sin embargo, en el caso de la autodeterminación informativa, es el consentimiento del afectado la piedra angular del conjunto incluso cuando se pretenda tratar datos relativos a conductas o hechos que se han realizado públicamente". *La Constitución... op. cit.*, p. 37

<sup>198</sup> A este respecto, muy interesante el posicionamiento del Tribunal Constitucional cuando afirma que, "ha de tenerse presente, (...), que el derecho fundamental al que estamos haciendo referencia garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos". STC 290/2000

pleno ejercicio de los derechos de la persona. Además asegura que el sujeto tenga conocimiento del acopio de sus datos independiente del medio utilizado para este almacenamiento, garantizando su seguridad, la lealtad en el momento en que son recogidos y la veracidad de su contenido.

Ahora bien, todo ello es parte de la esencia del derecho a la autodeterminación informativa. El Tribunal Alemán<sup>199</sup>, tuvo la oportunidad de manifestar que éste derecho no sólo depende del dato sino de su elaboración, y lo que decide si es digno de ser protegido es el contexto de su uso. Por ende, las especificidades para tornarlo efectivo formará parte del derecho objetivo.

Actualmente, la protección de los datos de carácter personal dirigen su tutela hacia los ficheros manuales o bien automatizados a través de las tecnologías que presentemente están a disposición de la sociedad, estableciendo las reglas más específicas para garantizar el real ejercicio de la libertad informática.

No obstante ello, también sirve para impedir que se afecten a otros derechos como al honor, a la imagen, a la intimidad, etc. La no observancia legal de cómo se deben recabar los datos, su uso desviado de la finalidad para lo cual fueron obtenidos o su circulación indebida son conductas que en sí mismas ya afrontan al derecho fundamental a la autodeterminación informativa. El problema no reside en los efectos posteriores porque es imposible vislumbrar en un futuro próximo la intención del presunto autor al practicar dichas acciones ilegales — o aunque su ejecución sea viciada solamente por la culpa — todas las secuelas del acto. Por eso, pensamos que no son las consecuencias que ese hecho puede conllevar, pero lo que el derecho a la protección de datos pretende evitar es la propia acción ilícita.

---

<sup>199</sup> Vid. Denninger, Erhard. *El derecho... op. cit.*, p. 273.

Para finalizar, cumple subrayar aún que este derecho es también una tutela preventiva, que al fin y al cabo, salvaguarda igualmente otros derechos fundamentales, porque están integrados sistemáticamente en ellos. Como manifiesta Rodotá<sup>200</sup>, la protección de datos como derecho fundamental “se expresa también como condición preventiva para poder ejercer de modo efectivo otros derechos y libertades fundamentales, como la libertad de expresión, la libertad de organización política y sindical, el derecho a la salud”. Sin embargo, si restringimos la tutela a los datos, cualquier información, aunque personal, que no tuviese vínculo con estos derechos (intimidad, honor, imagen) podría circular libremente porque huye del ámbito de sus tutelas, hecho que se lo impide la autodeterminación informativa, motivos por los cuales a nuestro juicio debe ser considerado como un derecho autónomo.

---

<sup>200</sup>RODOTÁ, Stefano. *Democracia y Protección de Datos Personales* [en línea]. Agencia Española de Protección de Datos. Disponible en [https://www.agpd.es/portalweb/.../DemocraciaMadrid\\_mayo\\_05.pdf](https://www.agpd.es/portalweb/.../DemocraciaMadrid_mayo_05.pdf) . [Consultado en 15 jun 2009].

**CAPITULO SEGUNDO: LEYES DE PROTECCIÓN DE  
DATOS. PERSPECTIVA HISTÓRICA Y CONCEPTOS  
ACTUALES.**

## I. La evolución legislativa de la protección de los datos personales en Europa.

Con los avances tecnológicos y por ello la posibilidad de crecimiento de acopio de información sobre las personas, los países europeos han iniciado una fuerte discusión sobre la respuesta jurídica necesaria para la protección de los derechos de los ciudadanos frente a los avances de las nuevas tecnologías<sup>201</sup>.

Como ha puesto de manifiesto Freixas Gutiérrez<sup>202</sup>, “el contundente desarrollo tecnológico de esta materia provoca la utilización de datos y más datos que actualmente ya va más allá de lo que es la intimidad, afectando la privacidad, concepto ese mucho más extenso que el primero. Y estas parcelas de privacidad e intimidad requerían una protección. Aunque la dificultad estaba en cómo hacer frente a una actividad que evolucionaba constantemente, y cómo hacerlo de una manera paralela con una reglamentación jurídica que evitase también una monopolización de las bases de información, que, a la larga, podían constituir poderes fácticos y reales en contraposición de los constitucionalmente previstos”.

---

<sup>201</sup> Vide DAVARA RODRIGUEZ, Miguel Angel. “Derecho y Tecnología de la Información”. BECERRIL RUIZ, Diego (coord.). TIC y sociedad en el siglo XXI. Granada: Editorial Universidad de Granada *TIC y Sociedad en el Siglo XXI*, 2007; CLIMENT BARBERÁ, Juan. *Derecho y nuevas tecnologías: lección magistral leída en la apertura del curso 2001-02*. Valencia: Universidad Cardenal Herrera-CEU, 2001.

<sup>202</sup> FREIXAS GUTIERREZ, Gabriel. *La protección de los datos de Carácter Personal en el Derecho Español*. Barcelona: Editorial Bosh, 2001, p 18.



En efecto, la posibilidad de almacenamiento de los datos personales en los bancos de datos automatizados<sup>203</sup>, el volumen que pueden ser registrado, la velocidad de transmisión<sup>204</sup>, en suma la proliferación del uso de la informática generó una preocupación continental, tocante sobre todo al derecho a la intimidad, que incluso hoy todavía implica a diversos sectores de la Comunidad Europea. Sobre la importancia de la reglamentación de tales cuestiones señala Orozco Pardo<sup>205</sup>, que “el volumen de información que hoy se genera y procesa en los diversos ámbitos de las relaciones sociales, ha tenido como primera consecuencia la necesidad de aplicar los medios informáticos a la recogida, almacenamiento, proceso y transmisión de información (v.gr. tratamiento) y, dentro de esta, la más importante está referida a los datos personales de diverso orden que las Administraciones, empresas y profesionales poseen relativos a los administrados, trabajadores, clientes y terceros que con ellas entran en relación. Ésta dinámica ha ido generando la aparición de ficheros automatizados que sirven para el tratamiento de esos datos

---

<sup>203</sup> El Consejo de Europa justifica el Convenio 108, en su informe explicativo al decir, “hay una necesidad de tales reglas legales debido al aumento de los ordenadores para los propósitos administrativos. Comparado con los archivos manuales, los archivos automatizados tienen una capacidad de almacenaje sumamente superior y ofrecen la posibilidad de una variedad mucho más amplia de transacciones, que pueden realizar en gran velocidad”.

<sup>204</sup> Losano destaca cuatro elementos que compone lo que nombra de “técnica particularmente adecuada para el tratamiento electrónico de datos jurídicos”, a saber: “la eficiencia (es decir, el porcentaje de informaciones pertinentes recuperadas respecto a las efectivamente memorizadas); el aprovechamiento (es decir, la relación entre el uso efectivo de informaciones recuperadas y el máximo uso posible del propio sistema informático); la accesibilidad (es decir, el grado de dificultad que el usuario encuentra al dirigir preguntas al sistema informático); la velocidad operativa (es decir, el tiempo que transcurre entre el momento en que el usuario plantea la pregunta y el momento en que recibe la respuesta)”. LOSANO, Mario. *Curso de Informática Jurídica*. Madrid: Tecnos, 1987, p. 212.

<sup>205</sup> OROZCO PARDO, Guillermo. “Los derechos de las personas frente al tratamiento de datos personales: un análisis crítico”. En: BECERIL, Diego. *TIC... op.cit.*, p. 85

personales y que han de estar necesariamente sometidos al régimen jurídico general establecido por el Ordenamiento para regular tales cuestiones. Dichas normas pretenden, como objetivo básico, asegurar que estos tratamientos y cesiones no vulneren en ningún caso los derechos y libertades de las personas concernidas”.

En el año de 1968, la Asamblea del Consejo de Europa editó la Recomendación 68/509 sobre “los derechos humanos y los nuevos logros científicos y técnicos”, considerada como el germen institucional, en el marco europeo, de lo que adelante se conocería como protección de datos<sup>206</sup>. Mientras los países, individualmente, se empeñaban en estructurar en su ordenamiento jurídico las leyes de protección de datos.

La primera legislación nacional fue formulada en Land de Hesse<sup>207</sup>, el 9 de octubre de 1970, seguida por la ley Sueca nº 289 de 11 de mayo de 1973, aunque esta última, para Frosini<sup>208</sup>, fue la primera norma efectivamente orgánica y completa sobre la protección de la privacidad y sobre el control de los bancos de datos, públicos y privados, compuesta por veinticinco artículos y varias disposiciones transitorias. El autor<sup>209</sup> en cita, también

---

<sup>206</sup> DAVARA RODRIGUEZ, Miguel Angel. *Manual de Derecho Informático*. Navarra: Aranzadi, 2006, p. 56.

<sup>207</sup> Frosini explica que esta ley era “bastante esquemática, ya que estaba compuesta por diecisiete artículos (el último de estos fijaba la fecha de la entrada en vigor), pero presentaba algunas novedades muy importantes: pues no sólo regulaba la utilización de los centros de información electrónica administrados por las autoridades públicas de Hesse, con una referencia precisa al respecto del secreto (art. 3), y al derecho de control sobre los datos (artículo 4), sino también instituía por primera vez un órgano de vigilancia adecuado, el *Datenschutzbeauftragter* o comisario para la protección de los datos (art. 7.15), es decir, un magistrado público con una competencia específica en el campo de la gestión pública de los ordenadores electrónicos y de la aplicación de la ley”. FROSINI, Vittorio. *Banco... op. cit.*, p. 27.

<sup>208</sup> *Ibid.*, p. 29.

<sup>209</sup> *Ibid.*, pp 26 y 27.

recuerda que el gobierno de Land de Bavaria (República Federal Alemana) en 1969 editó un acta administrativa que establecía una disciplina reglamentar para la “redacción de normas con sistemas automatizados” (ley 27 de agosto de 1969, núm. 1552-2-75), y tenía carácter vinculante sólo para los órganos administrativos de ese mismo *Land*. Según su planteamiento, “tratábase, sin embargo, de un documento sobre el nuevo interés por las innovaciones tecnológicas en el campo del procesamiento informático de los datos, y no de un reconocimiento abierto del nuevo problema de la tutela de la privacidad como control sobre los bancos de datos personales”.

Tras dichas normas, se manifiesta, otra vez, el Consejo de Europa, a través de su Comité de Ministros, sugiriendo algunos aspectos que los países deberían tener en cuenta, en orden a su política legislativa sobre la creación de bancos de datos. Estas recomendaciones se centraron en dos importantes resoluciones: la primera en el 26 de septiembre de 1973, resolución (73) 22 sobre la regulación jurídica de los ficheros electrónicos en el sector privado, y la segunda un año después, en el 26 de septiembre de 1974 la resolución (74) 29 sobre “la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público”<sup>210</sup>.

Continuando el recorrido histórico, también se puede citar la ley alemana de 27 de enero de 1977 de protección de datos (*Bundesdatenschutzgesetz*), seguida por la ley francesa de Informática, Ficheros y Libertades, nº 78-17 de 6 de enero de 1978. En el año subsecuente, el Parlamento Europeo publica otra resolución aprobada en

---

<sup>210</sup> Sobre este aspecto, Tellez Aguilera, señala que “la doctrina más cualificada ha visto en estas Resoluciones el verdadero origen del movimiento legislativo que a partir de entonces recorrerá Europa en materia de protección de datos”. TELLEZ AGUILERA, Abel. *Nuevas Tecnologías. Intimidación y Protección de Datos*. Madrid: Edisofer, 2001, p. 93.

8 de mayo de 1979 “sobre la tutela de los derechos del individuo frente al creciente progreso técnico en el sector de la informática”.

Asimismo, se debe tener en cuenta en este entorno la edición de un importantísimo documento si se tiene en cuenta la influencia política del órgano que lo ha emanado, la Organización para la Cooperación y el Desarrollo Económico (OCDE) denominado de las “Directrices de la OCDE que Regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales”, de 23 de septiembre de 1980. Según la síntesis del texto<sup>211</sup>, dichas directrices representaban un consenso internacional sobre la orientación general respecto a la colecta y administración de la información personal, y sus principios eran caracterizados por la claridad, flexibilidad de aplicación y por la formulación suficientemente amplia para posibilitar la adaptación a los cambios tecnológicos.

Al estudiar ese documento y su comparación con las legislaciones posteriores, se aprecia, notase la gran influencia que estas han sufrido de aquella. El texto aludido está dividido en cinco partes: la primera se ocupa a breves “Definiciones Generales”, como la de “inspector de datos”, que sería la persona competente para decidir sobre el contenido y el uso de dato; “datos personales” como toda información relativa a un individuo identificado o identificable (sujeto de los datos); y por “flujos transfronterizos de datos personales” se entiende, para los efectos de aquél documento, como los desplazamientos de datos personales más allá de las fronteras nacionales.

La segunda parte se dedica a delimitar el alcance de las Directrices, pormenorizando que estas se referían tanto a los datos personales del sector público como del privado. La tercera especifica los principios básicos de aplicación nacional que serían: principio de limitación de

---

<sup>211</sup> Texto disponible en <http://www.oecd.org> , acceso en 05 de julio de 2009.

recogida; principio de calidad de los datos; principio de especificación de los fines; principio de limitación de uso; principio de salvaguarda de la seguridad; Principio de transparencia; Principio de participación individual, que reconocería muchos de los derecho de los interesado; y el principio de responsabilidad que sería destinado al inspector de datos para exigirle el cumplimiento de las medidas que permiten la aplicación de los demás principios. Es decir, ya formaba una estructura sistemática que más adelante sería fuente de fuerte influencia en la Directiva del Consejo 95/46.

De modo somero, la tercera parte de la directriz establece los principios básicos de aplicación internacional: libre flujo y restricciones legítimas que según expone el apartado 16, los Países Miembros deberían adoptar todas las medidas oportunas y razonables para garantizar que los flujos transfronterizos de datos personales, incluido el tránsito a través de un País Miembro, sea continuado y seguro. La cuarta parte cuida de recomendar la implantación nacional de los principios establecidos en la Directriz y la quinta y última parte se ocupa de la cooperación internacional. Como se ve, es un documento que para su época era muy completo, con una sistemática legislativa extremadamente elogiabile, y que de ningún modo sorprende que haya sido llevada en consideración por las leyes internacionales sucesivas.

Tras dichas normas y recomendaciones, aún a nivel internacional se debe citar el Convenio 108 del Consejo de Europa "Para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal", en el ámbito comunitario la Directiva 46/95 "relativa a la protección de las personas físicas en lo que atañe al tratamiento de datos personales y a la libre circulación de estos datos" que serán más adelante analizados, y el tratado de Schengen, cuyo objetivo es la creación de una zona de libre circulación, suprimiendo las fronteras comunes de los países signatarios. Asimismo, El Tratado de Funcionamiento de la

Unión Europea<sup>212</sup> que dedica su artículo 16 a declarar que “Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan”, comprometiéndose a que el Parlamento y el Consejo establecerán las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos.

Cabe subrayar, también, la Carta de los Derechos Fundamentales de la Unión Europea, cuyo artículo 8 ocupase de la protección de datos de carácter personal, estableciendo, así como el Tratado de Funcionamiento de la Unión Europea, el derecho de todas las personas a la protección de los datos personales. Además, dispone en su texto algunos principios de su tratamiento como la lealtad, la finalidad, el consentimiento de la persona afectada, y también los derechos de acceso y rectificación.

No resulta extemporáneo señalar que como no se puede prever hasta dónde llegará el desarrollo tecnológico, actualmente es difícil afirmar con exactitud el grado de madurez y alcance de las actuales legislaciones sobre el tema. No obstante, tocante a las legislaciones sobre protección de datos, es común encontrar en la doctrina una clasificación en generaciones<sup>213</sup>. De modo que para Pérez Luño<sup>214</sup>, se pueden separar las

---

<sup>212</sup> Documento en versión consolidada, Diario Oficial n° C115 de 09/05/2008 p.1–388, texto disponible en <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0001:01:ES:HTML>.

<sup>213</sup> *Vide*. PUENTE ESCOBAR, Agustín. “Breve descripción de la evolución histórica de y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal”. PIÑAR MAÑAS, José Luis (dir.). *Protección de datos de carácter personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos, La Antigua - Guatemala, 2-6 de junio de 2003*. Valencia: Tirant lo Blanch, 2006, pp. 40-47.

<sup>214</sup> PÉREZ LUÑO, Antonio Enrique. *Manual de Informática y Derecho*. Barcelona: Editorial Ariel, 1996, pp. 51 y 52.

leyes de protección de datos en tres generaciones, siendo la primera basada en la autorización previa de los banco de datos, “en una época en que los equipos de informáticos eran escasos, voluminosos y fácilmente localizables”; las de segunda generación se caracterizan por tener como principal objetivo los datos sensibles y finalmente las de tercera generación que son las que “se han hecho cargo de la revolución microinformática con la consiguiente difusión capilar de los banco de datos”, lo que supuso la imposibilidad de control previo de los equipos informáticos, como lo hacen la de primera generación; así como no pueden reducirse a la calidad de la información, como era el criterio utilizado por las leyes de segunda generación. Pare este autor, las leyes de tercera generación deben hacerse extensivas “a la dinámica de su uso o funcionalidad”.

### **1. El Consejo de Europa: el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.**

En enero de 1981, el Consejo de Europa aprueba su Convenio nº 108, “Para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal”, considerado por la doctrina española como “respaldo definitivo a la protección de la intimidad”<sup>215</sup>.

---

<sup>215</sup> Para Serrano Pérez, “el Convenio representa un importante punto de partida de cooperación, entre los países europeos y a nivel internacional, en el terreno de la protección de la vida privada de los individuos ante el creciente fenómeno informático”, y acrecienta que “el Convenio se convirtió, a partir de su existencia, en el

El citado Convenio nació de la preocupación del Consejo de Europa con los peligros que puede entrañar el avance de la informática y su impacto en la vida privada de los ciudadanos, especialmente tocante al tratamiento automatizado de datos de carácter personal, y de la pretensión en desarrollar el artículo 8-1 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales<sup>216</sup>.

Ahora bien, lo que ha de tenerse en cuenta es que el Convenio 108 es un documento resultado de varios estudios anteriormente desarrollados, que se inician, como advierte Serrano Pérez<sup>217</sup>, en 1967, año en el que se constituye la Comisión Consultiva para abordar el estudio del tema de la defensa de las libertades frente al avance de las nuevas tecnologías. Culminando, estas pesquisas, en la citada Recomendación 509, y las Resoluciones (73)22, de 26 de septiembre, (74)29, de 20 de septiembre, y desagan en el Convenio 108. Como subraya Puente Escobar<sup>218</sup>, sólo desde 1967 cabe hablar de la existencia de una preocupación de los

---

texto inspirador y modélico acerca del contenido que debía reunir una legislación sobre protección de datos y en el primer documento internacional importante sobre la materia". SERRANO PÉREZ, Maria Mercedes. *El Derecho Fundamental a la Protección de Datos, Derecho Español y Comparado*. Madrid: Editorial Civitas, 2003, pp. 94 y 99.

<sup>216</sup> Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales, de 4 de Noviembre de 1950, ratificado por España con fecha 26 de septiembre de 1979, y publicado en el Boletín Oficial del Estado de 10 de octubre de 1979. El informe explicativo del Convenio 108 consignó que en 1968, la Asamblea Parlamentaria del Consejo de Europa envió la recomendación 509 al Comité de los Ministros, solicitando examinar si la convención europea de los derechos humanos y la ley de cada uno de los Estados miembros ofrecían una adecuada protección al derecho de la privacidad en vista de la ciencia y tecnología modernas. Posteriormente, un estudio realizado en respuesta a esa recomendación demostró que las legislaciones nacionales existentes no habían dado la protección suficiente a privacidad y otros derechos e intereses de los individuos tocante a los bancos de datos automatizados.

<sup>217</sup> SERRANO PÉREZ, Maria Mercedes. *El Derecho... op. cit.*, p. 90.

<sup>218</sup> PUENTE ESCOBAR, Agustín. *Breve descripción... op. cit.*, p. 38.



legisladores internacionales e nacionales por la protección, en principio, de la intimidad o privacidad de las personas en relación con los avances producidos en el campo de la informática.

Resulta oportuno subrayar la observación de Orozco Pardo<sup>219</sup> sobre el aludido convenio, que destaca entre otras cuestiones que este texto sirvió de motor para impulsar la promulgación de leyes sobre la materia en diversos países así como de precedente para la normativa comunitaria. Además, señala que “por su carácter vinculante, ha servido como un instrumento inmediato de defensa de tutela de los ciudadanos en los países signatarios que aún no poseían una normativa específica sobre la materia”.

Como ya se ha mencionado, existían leyes en Europa que trataban de la materia, pero la ausencia de identidad resultaba en diferentes disposiciones legales y consecuentemente no existía uniformidad para los movimientos transfronterizos de datos entre los países, interfiriendo en la protección de aquellos relativos a las personas. Todo ello afectaba el buen funcionamiento del mercado europeo interno, como lo dejó patente la Recomendación de la Comisión 81/679/CEE, de 29 de julio de 1981<sup>220</sup>, que entendía necesaria la aproximación legal de los países sobre el tema de protección de datos para también “evitar situaciones desiguales de competencia que puedan dar lugar a distorsiones de la competencia en el mercado común”, aconsejando así, a que los Estados miembros de la Comunidad, que todavía no hubiesen hecho, firmasen el Convenio 108 en el mismo año de 1981 y lo ratificasen antes de terminar el año de 1982.

---

<sup>219</sup> OROZCO PARDO, Guillermo. “Notas acerca de la L.O. 15/1999 de protección de datos de carácter personal: ¿una reformatio in peius?”. En HERRERA CAMPOS, Ramón (coord.). *Homenaje al profesor Bernardo Moreno Quesada*. Almería, Universidad de Almería (coeditado), Servicio de Publicaciones, Vol. 3, 2000, p. 1394.

<sup>220</sup> Recomendación de la Comisión de 29 de julio de 1981 relativa al Convenio del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

España lo firmó en el 28 de enero de 1982 y lo ratificó en 31 de enero de 1984, habiéndose publicado en el BOE el 15 de noviembre de 1985. En el caso de Italia, la firma ocurrió un año después de España, en 2 de febrero de 1983, pero su ratificación tardó más de diez años desde cuando lo firmó, siendo en 29 de marzo de 1997.

## **2. La Directiva del Consejo 95/46, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos.**

Según consta en el primer informe de la Comisión sobre la aplicación de la Directiva sobre protección de datos 95/46 del Parlamento Europeo y del Consejo, esta “consagra dos de las ambiciones más antiguas del proyecto de integración europea: la realización del mercado interior (en este caso, la libre circulación de datos personales) y la protección de los derechos y libertades fundamentales de las personas”.

La aprobación de esta norma, relativa a la protección de las personas respecto a los datos personales, se hizo el 24 de octubre de 1995<sup>221</sup>. Su nacimiento se explica principalmente por la patente necesidad de aproximación del tratamiento legal por los Estados miembros sobre

---

<sup>221</sup> DIRECTIVA 95/46/CE del Parlamento Europeo y del Consejo 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 el 23 de noviembre de 1995, en el Diario Oficial de la Unión Europea (DOUE) serie L nº 281, entró en vigor el 13 de diciembre de 1995.

protección de los datos personales<sup>222</sup>, hecho que facilitaría su circulación y transmisión entre los países de la Comunidad, aumentando su flujo transfronterizo, beneficiando, así, el mercado común, concomitante a la protección adecuada de los derechos fundamentales individuales en esta materia. Respecto a ello, destaca Serrano Pérez<sup>223</sup>, que “con las miras puestas al espacio colectivo, la Directiva aborda la armonización de las legislaciones de todos los países para contar con un ámbito jurídico unificado, superando así en este terreno la permisividad del Convenio”.

Efectivamente, los países integrantes de la Comunidad han tenido que adaptar su ordenamiento con a llegada de la nueva normativa internacional<sup>224</sup>, y aunque las legislaciones internas de cada uno de ellos, comparadas entre si, puedan tener diferencias más o menos relevantes, lo cierto es que tal Directiva ha venido a armonizar la materia de protección de datos en los Estados miembros, siendo considerada actualmente como la más importante referencia legislativa en el ámbito comunitario en este tema.

Según el artículo 3 del citado texto legal, su ámbito de aplicación sería el tratamiento total o parcialmente automatizado de datos personales, así como aquél no automatizado, cuyas informaciones están contenidas o destinadas a ser incluidas en un fichero. Exceptuándose, sin embargo, al tratamiento de datos efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad

---

<sup>222</sup> Muchos de los países comunitarios, antes de la aprobación de la Directiva, ya tenían leyes de protección de datos y era el Convenio 108, a su época, la referencia legal internacional sobre la materia.

<sup>223</sup> SERRANO PÉREZ, Maria Mercedes. *El Derecho... op. cit.*, p. 95.

<sup>224</sup> El estado de la aplicación de la Directiva 95/46 se muestra bastante desarrollado, consoante datos de la Comisión Europea disponibles en línea:

[http://ec.europa.eu/justice\\_home/fsj/privacy/law/implementation\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm) .

pública, la defensa, la seguridad del Estado y sus actividades en materia penal. Así como no será aplicable al tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

Además, la Directiva dedica un capítulo al que nombra de “Condiciones generales para la licitud del tratamiento de datos personales”, estableciendo principios de la protección de datos que se refieren a la calidad, a la legitimación del tratamiento, a los datos sensibles, a la información al afectado, al derecho de acceso, al derecho de oposición, a la confidencialidad y seguridad del tratamiento, la notificación del tratamiento a la autoridad de control, así como define las excepciones y limitaciones del alcance de los principios.

Otro punto importante de ser comentado es de la similitud de la Directiva con el Convenio 108, aunque la primera haya venido a mejorar el texto legal del último, como dicen innumerables voces doctrinales. En efecto, sobre este aspecto se destaca en el documento de trabajo sobre *transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE* que “las obligaciones y los derechos establecidos en la Directiva 95/46/CE se basan en aquellos dispuestos en el Convenio nº 108 (1981) del Consejo de Europa, que a su vez no son diferentes de los incluidos en las directrices de la OCDE (1980), o en las directrices de la ONU (1990).

Por ello, parece que existe un alto grado de consenso en relación con el contenido de las normas de protección de datos que traspasa los límites del espacio ocupado por los quince estados de la Comunidad<sup>225</sup>. El propio

---

<sup>225</sup> Vid. Comisión Europea. Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Documento de Trabajo: *Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE*. DG XV D/5025/98. WP 12. Aprobado por el Grupo de Trabajo el 24 de julio de 1998.

Considerando 11 de la Directiva aclara que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, allí contenidos, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales.

Además, la norma comunitaria en cita prevé que los Estados miembros en sus legislaciones nacionales establezcan un recurso judicial en caso de violación de sus derechos, garantizando a la reparación debida cuando sufra perjuicio en consecuencia de tratamiento ilícito de sus datos personales, así como la adopción de las sanciones aplicables en caso de incumplimiento de las disposiciones adoptadas en la Directiva.

También regula las transferencias de datos personales de los Estados miembros a países terceros autorizando cuando este tercer país garantice un nivel adecuado de protección y desautorizando, evidentemente, en el supuesto de disparidad de nivel de protección, salvo las excepciones allí enumeradas. Pretende también la Directiva alentar elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros así como códigos de conducta comunitarios.

Para finalizar con los aspectos más importantes recogidos en la norma comentada, es necesario destacar el precepto que reglamenta la creación por los Estado miembros de una o varias autoridades públicas de control, órganos independientes que se encargan de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la Directiva. Además, la normativa crea un grupo para la protección de las personas en lo que respecta al tratamiento de datos personales, que estará compuesto por representantes de las autoridades de control nacionales, por representantes de las autoridades de control de las instituciones y

organismos comunitarios y por un representante de la Comisión, cuyas funciones se hallan en su artículo 31.

## II. La ley de protección de datos de carácter personal en España.

### 1. Evolución legislativa.

El artículo 18.4 de la CE establece que “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”. Conviene resaltar que España fue uno de los primeros países<sup>226</sup> a elevar como un derecho fundamental la protección de las personas frente al progreso de la informática (artículo 18.4). Aunque un representativo segmento de la doctrina critique el texto de la Constitución Española<sup>227</sup>, sobre todo cuando comparan con la portuguesa, no se debe olvidar que, aparte de las

---

<sup>226</sup> La primera manifestación constitucional de Europa a la protección de datos fue de Portugal, en el año de 1976, seguida de España y Austria, en 1978. En el caso de Austria, hay que tenerse en cuenta que su sistema normativo permite la adopción leyes que, aunque sean ordinarias, son “provisiones constitucionales” (Verfassungsbestimmungen). Estas provisiones son parte de la Constitución, es el núcleo de lo que es la Ley Federal Constitucional (Bundes-Verfassungsgesetz). Cfr.:

<http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83545>

<sup>227</sup> Entre otros, *vid.* PÉREZ LUÑO, Antonio Enrique. *Derechos humanos... op. cit.*, p. 334-346; FREIXAS GUTIERREZ, Gabriel. *La protección... op. cit.*, pp. 33-37; SERRANO PÉREZ, Maria Mercedes. *El Derecho..., op. cit.*, pp. 123-126.

discusiones de técnica legislativa<sup>228</sup>, esa actitud ha representado un avance con respecto a la manera de tratar el tema en relación a los demás países de Europa. Es reseñable la importancia de una orientación constitucional de este derecho para el posterior tratamiento por las legislaciones de rango inferior<sup>229</sup>.

Sin embargo, es relevante recalcar que hubo un gran retraso del legislador español para implementar una norma que realmente respondiese a los problemas que empezaban a hacerse más evidentes con lo avance de las nuevas tecnologías. Respecto a ese tema, en artículo publicado en 1979, Pérez Luño<sup>230</sup>, ya había advertido que el legislador español tenía la importante e insoslayable tarea de dar una respuesta rápida a las apremiantes cuestiones que suscitaba la informática tocante al efectivo disfrute de los derechos fundamentales.

Mientras no se desarrollaba el artículo 18.4 con su normativa correspondiente, la Ley Orgánica 1/82, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia

---

<sup>228</sup> Pérez Luño observa que “el encuadre del precepto en el marco de las libertades públicas y el restringido alcance expreso de su contenido a la órbita personal y familiar supone un planteamiento fragmentario e individualista de la compleja serie de cuestiones de matiz personal y social que hoy se debaten y suscitan en el marco de las relaciones entre intimidad e informática. En efecto, entiendo que en la redacción de este párrafo el bien jurídico protegido –la intimidad– aparece concebido dentro de unas coordenadas individualistas, como un derecho del individuo a la soledad “a tener una esfera reservada en la cual desenvolver su vida sin que la indiscreción ajena tenga acceso a ella” (...). Quedan por tanto, fuera de esta norma constitucional los aspectos sociales y colectivos de la cuestión tendentes a posibilitar a las personas y a los grupos el acceso a las informaciones que directamente les afectan”. PEREZ LUÑO, Antonio Enrique. “La protección de la intimidad frente a la informática en la Constitución Española de 1978”. REP, 1979, nº. 9, pp. 61 y 62.

<sup>229</sup> Vid. PÉREZ LUÑO, Antonio Enrique. *Derechos humanos... op. cit.*

<sup>230</sup> Pérez Luño, Antonio Enrique. *La protección..., op. cit.*, p. 71

imagen intentaba realizar lo que adelante se constató insuficiente<sup>231</sup>: hacer frente al vertiginoso avance de la informática producido en España y sus consecuencias tocante a la protección de datos. Efectivamente Murillo de la Cueva<sup>232</sup>, alertaba que dicha norma solamente protegía el ámbito más estricto de la intimidad pero era inútil ante la captación, el acopio, la relación y transmisión de los datos personales que no necesariamente habían de pertenecer a este reducto último de la vida privada. Aun añade el citado autor, que las diversas leyes sectoriales, el artículo 1.902 del Código Civil y la ratificación de España al Convenio 108 del Consejo de Europa tampoco eran suficientes para ofrecer la cobertura legal necesaria para proteger los datos personales ante el uso de la informática<sup>233</sup>.

La misma línea de raciocinio sigue el planteamiento de Orozco Pardo<sup>234</sup>, para quién esta norma era insuficiente para resolver la variada problemática que este tema estaba ya suscitando y ello no escapa a la percepción del legislador. Según su valoración, la prueba de tal afirmación son las diversas iniciativas parlamentarias que se siguieron desde 1979 hasta 1992, año en que se aprobó una ley específica desarrolladora del precepto constitucional.

De suerte que, en el año de 1992, y por lo tanto con un retraso de catorce años desde la aprobación de la Constitución, fue promulgada la Ley Orgánica de Tratamiento Automatizado de Datos de Carácter Personal (5/1992, de 29 de octubre), la primera ley específica en España

---

<sup>231</sup> La Disposición Transitoria Primera de la citada ley, establecía que “En tanto no se promulgue la normativa prevista en el artículo dieciocho, apartado cuatro, de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley”. El citado dispositivo sería, con la promulgación de la LORTAD, derogado.

<sup>232</sup> MURILLO DE LA CUEVA, Pablo Lucas. *Informática ...op. cit.*, p. 17.

<sup>233</sup> *Ibid.*, pp. 19 y 20.

<sup>234</sup> OROZCO PARDO, Guillermo. *Los derechos... op. cit.*, pp. 94-95.



que disciplinaba la materia. En este contexto, hay que recordar, como observa González Méndez<sup>235</sup>, que un impulso importante para la elaboración de la normativa especial lo representó la adhesión de España en 1991 al Acuerdo de Schengen, relativo a la supresión gradual de los controles en las fronteras comunes que obligaba al país a poner en marcha una legislación sobre protección de datos.

Tocante al objeto de la LORTAD, según el artículo 1º, es limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos<sup>236</sup>.

La ley fue objeto de algunos recursos de inconstitucionalidad y críticas doctrinales. Con la aprobación de la Directiva 95/46 y la necesidad de transponerla al ordenamiento jurídico interno, la LORTAD no era suficiente para abarcar todos los reclamos de la Directiva. Según observa

---

<sup>235</sup> GONZALÉZ MÉNDEZ, Amelia. *La Protección de Datos Tributarios y su Marco Constitucional*. Valencia: Tirant lo Blanch. Consultado a través de Tirant On Line (370.005). En este mismo sentido, Murillo de la Cueva señala que el motivo inmediato de la aprobación de la LORTAD no fue el propósito de cumplir la Constitución y ofrecer mayores garantías a los ciudadanos respecto a los avances tecnológicos. Asegura el autor que la razón no fue otra que “la necesidad de contar con ese instrumento legislativo para que España pudiera integrarse en el grupo de países que, conocido como Grupo de Schengen, suprimió los controles fronterizos interiores, pues lo exigían las reglas de los acuerdos que lo crearon”. En “La Constitución y el Derecho...”, *op. cit.*, p. 30.

<sup>236</sup> En el apartado segundo de la exposición de motivos sobre la finalidad de la norma manifiesta que: “Partiendo de que su finalidad es hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos, la ley se nuclea en torno a los que convencionalmente se denominan “ficheros de datos”: Es la existencia de estos ficheros y la utilización que de ellos podría hacerse la que justifica la necesidad de la nueva frontera de la intimidad y del honor”.

Navalpotro Navalpotro<sup>237</sup>, en un principio la idea no era la de publicar una nueva ley, pero sí reformar la ya existente y adaptarla a la Directiva, pero el texto de reforma presentado por el Gobierno sufrió tantas enmiendas (ciento catorce) que provocó que se propusiera un nuevo texto legal con el objetivo de derogar el anterior.

En este enredo, surge la nueva Ley Orgánica de Protección de Datos de Carácter Personal, 15/1999, de 13 de diciembre (LOPD), actualmente en vigor. No obstante su publicación, que venía a sustituir otra tan criticada, no parece que haya calmado los ánimos de la doctrina científica percibiéndose claramente una gran resistencia de esa sobre dicha norma<sup>238</sup>. Conforme consignó Freixas Gutiérrez<sup>239</sup>, algunas opiniones solicitaban una nueva ley ya que la anterior no lograba contentar ni a los afectados, que no se sentían protegidos, ni a los que ejercían la actividad informática, que se sentían a menudo en entredicho además, en su opinión, a pesar de todo ello, la nueva ley padece de los mismos defectos que la anterior. Orozco Pardo<sup>240</sup> señala que el texto de la LOPD pervive las

---

<sup>237</sup> NAVALPOTRO NAVALPOTRO, Yolanda. “Antecedentes de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (LOPD)”. En ALMUZARA ALMAIDA, Cristina (coord.). *Estudio Práctico sobre la protección de datos de carácter personal*. Lex Nova, Valladolid, 2007, p. 44.

<sup>238</sup> Aunque como señala Orozco Pardo, “se trata de un texto consensuado, no solo dentro del Ejecutivo sino también con otras fuerzas sociales que fueron tenidas en cuenta a la hora de su preparación y redacción final”. En “La protección de datos en Derecho español a la luz de la reciente jurisprudencia constitucional”. Aranzadi. *Actualidad civil*, nº 1, 2002, p. 211.

<sup>239</sup> FREIXAS GUTIERREZ, Gabriel. *La protección... op. cit.*, p. 84.

<sup>240</sup> OROZCO PARDO, Guillermo. *La protección de datos... op. cit.*, p. 174. Como bien señala Martínez Martínez, “ninguna norma nace del vacío. Todas ellas incorporan un conjunto de decisiones políticas y jurídicas socialmente relevantes o demandadas”. MARTÍNEZ MARTÍNEZ, Ricard. “El Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Consideraciones generales”. *Revista de Protección de Datos*. Madrid: Agencia de Protección de Datos de la Comunidad de Madrid, 2007, nº 2, p. 89.

mismas lagunas y *zonas grises* existentes en su predecesora, “pues el nuevo texto no incorpora significativos avances en la materia, salvo lo que supone adaptar la Directiva de la que trae causa el proceso de reforma, y las aportaciones que introduce no son tan positivas como el legislador ha querido hacer creer”.

En el año de 2007, se aprueba el Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la Ley Orgánica 15/1999. Es de subrayarse que la Disposición Final Primera de esta última contempla que el Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la aludida Ley.

De modo que tal reglamento (en adelante, RPD), como bien explicita su exposición de motivos, no ha nacido con la finalidad de reiterar los contenidos de la LOPD, pero de la necesidad de “dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y desarrollar los aspectos novedosos de la LOPD”, así como aquellos contenidos que se demostraran a través de la experiencia de casi diez años de vigencia de esta ley que necesitan de una mayor atención legal y de un mayor grado de precisión que dote de seguridad jurídica al sistema. En efecto, como señala Piñar Mañas<sup>241</sup>, dotar el sistema de mayor seguridad jurídica (así como dar cumplimiento a la antes citada Disposición Final de la LOPD era sin duda el más importante de los motivos que entonces se tuvieron en cuenta para acometer tan necesaria empresa”, aunque añade el autor que había otros de menor alcance como la conveniencia de adaptar el incompleto y fragmentario marco reglamentario existente, aclarar diversas cuestiones relativas a la adecuación de la legislación española al derecho comunitario así como

---

<sup>241</sup> PIÑAR MAÑAS, José Luis. “El porqué de un Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos”. *Revista de Protección de Datos*. Madrid: Agencia de Protección de Datos de la Comunidad de Madrid, 2007, nº 3, pp. 30-31.

recoger los criterios interpretativos de la LOPD consolidados por la AEPD y los Tribunales.

No obstante, voces doctrinales<sup>242</sup> ya advertían desde hace mucho que la LOPD no hacía frente a diversas cuestiones como por ejemplo los ficheros sobre menores, los que contienen datos sobre personas fallecidas, etc. En la opinión de Brines Almiñana<sup>243</sup>, se hacía necesario la aprobación de un reglamento “a fin de cubrir la laguna normativa, que, recogiendo los criterios interpretativos y sancionadores de la norma emanados desde su aprobación, otorgara mayor seguridad jurídica a los destinatarios de las obligaciones establecidas en la LOPD y garantizara la efectividad de los derechos de los titulares de datos”. En efecto, es un reglamento que tiene un ámbito de tutela muy amplio, cuyo objeto es no solamente el desarrollo de la LOPD, pero también abarca las tutelas de otras normas como los reales decretos 1332/1994<sup>244</sup>, de 20 de junio y 994/1999<sup>245</sup>, de 11 de junio, la atribución de la Agencia Española de Protección de Datos por la ley 34/2002, de 11 de julio, la Ley 32/2003, de 3 de noviembre, de Servicios de la Sociedad de la Información y de Comercio Electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

---

<sup>242</sup> Vide la crítica de OROZCO PARDO, Guillermo. *La protección de datos...* op. cit., p210 y ss.

<sup>243</sup> BRINES ALMIÑANA, Javier. *Novedades más significativas del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos*. Editorial LA LEY. *Diario La Ley*, nº 6921, Sección Doctrina, 9 Abr. 2008, Año XXIX, p. 4-13.

<sup>244</sup> Por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal.

<sup>245</sup> Por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Sobre este aspecto, apunta Martínez Martínez<sup>246</sup> que el Reglamento es una norma muy extensa y aunque la cantidad de artículos no revele un indicador cualitativo de nada, la “simple referencia de la extensión del texto constituye un primer indicio de su importancia”. Para éste autor, el Reglamento trata de resolver una clara dispersión normativa, “que obligaba a acudir a dos normas reglamentarias preexistentes, el Real Decreto 1332/1994 y el Real Decreto 994/1999, completando los criterios de interpretación con determinadas instrucciones de entre las que cabe destacar la relativa a la solvencia patrimonial y el crédito — Instrucción 1/1995 — la relativa a los derechos de acceso, rectificación, cancelación y oposición al tratamiento — Instrucción 1/1998 —, y, finalmente, la que se refiere a los movimientos internacionales de datos”.

El RD 1720/2007 se estructura en nueve títulos, que tratan de diversos aspectos que, como ya se ha mencionado, merecieran destaques tanto en la jurisprudencia, como en la doctrina y en los pronunciamientos de la Agencia Española de Protección de Datos Personales. De modo que así constituido, el Título I se dedica a las disposiciones generales, contemplando su objeto y ámbito de aplicación, desarrollando fundamentalmente el apartado 2 del artículo 2 de la LOPD, aparte de aportar algunas definiciones que facilitan la interpretación de la Ley y fija el criterio a seguir en materia de cómputo de plazos. El Título II trata de los principios de la protección de datos, con énfasis a lo de calidad de los datos y del consentimiento y su respectiva captación y el Título regula III los derechos del interesado y su ejercicio. Las disposiciones aplicables al régimen de algunos específicos ficheros de titularidad privada, entre ellos los de solvencia patrimonial y crédito es el objeto de que se ocupa el Título IV. Además, el reglamento se refiere a las obligaciones previas al

---

<sup>246</sup> MARTÍNEZ MARTÍNEZ, Ricard. “Prólogo”. En MARTÍNEZ MARTÍNEZ, Ricard (coord.). *Protección de datos Comentarios al Reglamento de Desarrollo de la LOPD*. Comentarios al Reglamento de Desarrollo de la LOPD. Valencia: Tirant lo Blanch, 2009, pp. 17-18.

tratamiento de datos incluido ahí los ficheros de titularidad pública y privada (Titulo V), transferencia internacionales de datos (Titulo VI), Códigos tipos (Titulo VII), medidas de seguridad en el título VIII y finalmente los procedimientos tramitados por la Agencia Española de Protección de Datos.

De suerte que con solamente un somero repaso estructural del reglamento comentado se puede observar que España tiene hecho un esfuerzo para garantizar la seguridad jurídica tocante a la aplicación práctica del conjunto normativo que trata de protección de datos de carácter personal.

La promulgación del RDP se asemeja mucho a lo que pasó en Italia con la ley de 1996, que era muy general, pero en éste caso, la opción legislativa italiana no fue solucionar el problema con un reglamento, pero sí con la derogación de la ley y la emanación de una nueva norma y posteriormente los Códigos de buena conducta. A nuestro sentir, leyes que son demasiado generales de hecho terminan por no alcanzar la efectividad deseada, aunque si no fuera así, corren el riesgo de tornarse ultrapasadas. De todos los modos, es posible constatar que las normas con esa característica después de un tiempo de vigencia necesitará una reformulación legislativa, independiente del medio que se elija para tal fin. En nuestra opinión, se entiende perfectamente que en España la vía reglamentaria fuese políticamente más plausible, sin embargo, la ampliación de la adopción de los Códigos deontológicos como hechos en Italia nos parece ser una posición más adecuada y democrática para los sectores específicos.

## 2. La Ley Orgánica de protección de datos personales nº 15/1999.

### 2.1 Objeto de la ley y su ámbito de aplicación.

La Ley Orgánica de Protección de Datos Personales (LOPD) expresa su objeto en el artículo 1º que es garantizar y proteger, en lo que concierne a tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Acompañando indudablemente el objetivo expuesto en la Directiva 95/46, la finalidad de la LOPD notadamente es más amplia que de la ley derogada, además de observarse una destacable mejora en su redacción, especificando con más claridad su objetivo. De manera que la nueva norma no centra su garantía en restringir el uso de la informática, de hecho suprime la referencia al artículo 18.4 de la CE, pero fundamentalmente pone de relevo la protección a los derechos fundamentales de las personas, destacando el honor y la intimidad personal.

La redacción del artículo 1º de la LOPD aunque general y ambiciosa, en nuestra valoración no es criticable. El conjunto de intenciones que abarca dicho precepto sobre todo cuando generaliza los derechos fundamentales y las libertades públicas de ningún modo debilita el alcance de la norma. Es decir, si se encuentra violación a un derecho fundamental sea cual sea — y la propia especificación legal al honor y a la intimidad nos sirven de argumento — por el uso indebido del tratamiento de datos, aunque carezca de mecanismos prácticos para asegurar toda y cualquier injerencia ilegal, la norma cuenta con principios que pueden facilitar la interpretación legal para cada caso concreto, utilizándose, como es obvio,

la observancia en la aplicación de la ponderación y proporcionalidad de los derechos que estén implicados.

Asimismo, cuida el legislador de adelantarse, en lo que está a su alcance, a los cambios tecnológicos, y aunque no pueda deducir todas las posibles infracciones a todos los derechos fundamentales, puede, eso sí, ofrecer mecanismos al intérprete. Todo ello no es más de lo que pretende el derecho fundamental a la autodeterminación informativa: la creación de un sistema de principios y garantías que pueda asegurar al ciudadano su dignidad, sus libertades y sus derechos, fundamentales o no, en lo que concierne al tratamiento de sus datos personales.

Desde nuestra perspectiva, cuando resalta la ley los derechos a la intimidad y al honor, que en efecto son los más susceptibles a las violaciones con el tratamiento de datos personales, deja claro que el su objeto sirve a estos y otros derechos, pero que no se confunde con ellos.

Tocante al ámbito de aplicación, la LOPD establece en su artículo 2º que la “Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”. La primera observación que debe ser resaltada es sobre la generalidad que el artículo analizado propone en lo que respecta al soporte donde estarían registrados los datos. Ya hemos tenido la oportunidad de manifestarnos, en el capítulo anterior de este trabajo de investigación, la nuestra profunda inquietud con relación a que las leyes restrinjan su protección, sea en el enunciado de su objeto, sea en el ámbito de aplicación, por el exceso de preocupación con los matices tecnológicos.

A nuestro parecer, fue muy acertada la elección del legislador español en utilizar la expresión genérica *soporte físico*. Ahí, no se restringe desde nuestro punto de vista solamente a si son ficheros automatizados o manuales, pero dentro de lo que se entiende por automatizado, cualquier



tipo de soporte que exista actualmente, así como aquellos que puedan surgir en el futuro, desde que los datos que allí se encuentren sean, por supuesto, de carácter personal y que estén susceptibles al tratamiento.

En efecto, si lo que pretende la ley es proteger los derechos de los individuos contra el uso abusivo de los datos, no interesa cual medio utilizado, porque ello huye de lo que se tiene como parámetro legal fundamental, dejando tal tarea al intérprete. De ésta manera, la norma puede sobrevivir un tiempo más largo acompañando, si es el caso, el desarrollo tecnológico.

Además de ello, cumple destacar que no son todos los datos que cuida la ley, pero solamente aquellos que sean de carácter personal, concepto ese que tendremos oportunidad de analizar pormenorizadamente más adelante. Cabe consignar aún que se extiende la aplicabilidad de la norma asimismo a los momentos posteriores al tratamiento de los datos, o por mejor decir, de toda modalidad de uso ulterior, incluyéndose ahí tanto los ficheros de titularidad pública como privada.

Otro criterio que adopta la ley para delimitar su ámbito de aplicación es el territorial, estableciendo como pauta de sus supuestos la localización del tratamiento de los datos. De modo que las hipótesis que se rigen por esta norma son: todo tratamiento de datos de carácter personal realizados en el territorio español que estén en el marco de las actividades de un establecimiento del responsable del tratamiento; cuando, aunque el responsable del tratamiento no esté establecido en territorio español, la norma española le sea aplicable, de acuerdo con las leyes de Derecho Internacional público; y, finalmente, cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se usen únicamente con fines de tránsito.

## 2.2. Los principios de la protección de datos en la LOPD.

Como no podía ser diferente, la Directiva 95/46 establece los principios que, como consigna el considerando 25, tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, a las autoridades públicas, a las empresas, a las agencias u otros organismos que efectúen tratamientos — obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento — y, por otro lado, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento, como el derecho a ser informadas, de poder acceder a los datos, de solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias.

La LOPD dedica el Título II para consagrar, siguiendo la Directiva, los principios que sirven de fundamento para la protección de datos de carácter personal. Parte de la doctrina critica el citado Título por no estar ordenado sistemáticamente<sup>247</sup> y tampoco estar coordinado con los derechos de los ciudadanos, ofreciendo un tratamiento legal compartimentado, como observa Freixas Gutierrez<sup>248</sup>, lo que, en su opinión, provocaría una regulación ilógica.

---

<sup>247</sup> Cfr. TÉLLEZ AGUILERA, Abel. *Nuevas Tecnologías. Intimidación y Protección de Datos*, Madrid, 2001, p 127; ORTI VALLEJO, Antonio. *Derecho a la intimidad... Op. Cit.*, p. 109.

<sup>248</sup> FREIXAS GUTIERREZ, Gabriel. *La protección... op. cit.*, p. 151.

### 2.2.1 La Calidad de los datos.

Este principio protege los datos en las fases de su vida física, a saber la recogida, el registro y la conservación<sup>249</sup>. Su aplicación exige que las informaciones sean obtenidas por medios lícitos, no fraudulentas y desleales. Además, que sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades determinadas, expresas y legítimas para las cuales fueran recabados. Dispuesto en el artículo 4 de la LOPD y en el reglamento de desarrollo de la misma, nº 1720/2007, en el artículo 8, dicho principio es orientativo, o sea, la calidad de los datos está ligada al principio de la proporcionalidad, es decir, utilizarse los datos recabados con un criterio de racionalidad, preservando su uso solamente para las finalidades compatibles con las que motivaran su recogida. En definitiva, esa relación estrecha entre el dato y la finalidad es lo que legitimará su registro, tratamiento y conservación. En nuestra opinión, si en algún momento se rompe esa conexión, se habrá aniquilado el fichero por ausencia de legitimidad para existir.

Como se ha comentado, tocante a las otras fases de la vida física de los datos, el principio también protege su exactitud y su actualización para que siempre respondan con veracidad a la situación presente del afectado. El apartado 4 del artículo 4 de la LOPD va más allá, cuando determina que en el supuesto de que los datos registrados sean inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes, rectificadas o completados. El reglamento 1720/2007 establece un plazo de diez días desde que se tuviese conocimiento de la exactitud para que se proceda la rectificación oportuna, excluyendo la hipótesis de que la legislación aplicable al fichero sea específica y establezca un procedimiento o un plazo para ello. Sobre el particular,

---

<sup>249</sup> Cfr. SERRANO PÉREZ, María Mercedes. *El Derecho... op. cit.*, p. 433

acrecienta, aún, que también será de diez días el plazo para que el responsable del fichero notifique al cesionario de la rectificación o cancelación siempre que el ese sea conocido y cuando los datos hubiesen sido comunicados. Dicho plazo igualmente se fija para el cesionario que mantenga el tratamiento de los datos, contados a partir de la recepción de la notificación para proceder la a la rectificación y cancelación notificada. No obstante ello, esa actualización no necesitará ser comunicada al interesado, así como no perjudica en absoluto el ejercicio de ninguno de los derechos reconocidos por la LOPD.

Es importante resaltar que el Reglamento 1720/2007 aclara que en el caso de que sea el afectado quien informe directamente sobre los datos, estos serán considerados exactos. Es una puntualización a nuestro parecer obvia y sobrante. Sin embargo aunque su inserción no represente un gran cambio en la lógica interpretativa, mejor que esté ahí especificado.

A más, en lo que concierne a su conservación, no permite dicho principio que continúen a figurar en el fichero cuando dejen de ser necesarios y pertinentes para la finalidad para la cual fueran recabados o registrados. Así como no podrán conservarlos de manera que se permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido obtenidos o registrados<sup>250</sup>. Otra vez el reglamento viene a esclarecer que en los casos en que se pueda exigir algún tipo de responsabilidad derivada de una relación u obligación jurídica, o de la ejecución de un contrato, o incluso de la aplicación de medidas precontractuales solicitadas por el interesado, podrán conservarse durante el tiempo en que perdure tales supuestos. No obstante, después de cumplido estos plazos, la conservación solo será lícita si hubiere la disociación de los datos.

---

<sup>250</sup> Como explicita el apartado 5 del artículo 4 de la LOPD.

Cumple resaltar, aún, que el artículo 4, en su apartado 6, protege el ejercicio de derecho de acceso, ya que obliga que los datos sean almacenados de forma que permita al afectado ejercerlo. En este punto, añade el reglamento de desarrollo de la LOPD que estos derechos pueden ser ejercido hasta que no se haya procedido la cancelación de los datos.

### *2.2.2. Principio del consentimiento.*

El principio del consentimiento es de carácter general, y legitima el tratamiento de los datos. El artículo 6 de la LOPD, en el apartado 1 dispone que salvo la Ley diga otra cosa, su tratamiento requerirá el consentimiento inequívoco del afectado. Ya el reglamento 1720/2007, en el artículo 10, apartado 1, complementa tal precepto estableciendo que los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello, así como el artículo 12 del mismo RDP determina al responsable del tratamiento el deber de obtener el consentimiento del interesado para el tratamiento de sus datos, salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

Como se sabe, el consentimiento es la piedra angular del derecho a la autodeterminación informativa. Sin embargo la LOPD solamente dedica un artículo con cuatro apartados para tratar de este principio y por tal razón, el reglamento tuvo que detenerse en este aspecto, dedicando en el capítulo II (Consentimiento para el Tratamiento de los Datos y Deber de Información) una sección exclusivamente para tratar de la obtención del consentimiento. En efecto, la LOPD no se ocupó como debería del consentimiento y como consecuencia ello trajo muchas controversias las cuales se espera que gran parte se haya sanado con la entrada en vigor del Reglamento.

Se ha dicho anteriormente, que por ser el consentimiento el nudo gordiano del sistema de protección de datos, todos los supuestos en los que él no sea determinante para el tratamiento de datos deberán estar especificados en la norma, siendo, de este modo, su silencio interpretado como la necesidad de obtención del consentimiento, que es la regla general. De manera que por ser una característica esencial, su manifestación debe ser inequívoca, libre e informada. Igualmente es necesario que se informe al afectado de forma clara y fácilmente comprensible los datos que van a ser objeto de tratamiento y la finalidad a que van a ser destinados y de ese modo pueda el interesado consentir o se oponer a su tratamiento.

La LO 15/1999 claramente especifica los supuestos en los cuales no será necesario el consentimiento para el recabo de los datos. Así el apartado 2 del artículo 6 determina que estos casos serán: a) para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; b) cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; c) cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de LOPD, o d) cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Por regla general, a tenor del epígrafe 3 del artículo en comento, el consentimiento podrá ser revocado en el caso de que exista causa justificada para ello y no se le atribuyan efectos retroactivos. Para Vizcaino Calderón<sup>251</sup>, por causa justificada se entiende una razón

---

<sup>251</sup> VIZCAINO CALDERÓN, Miguel. *Comentarios a la Ley Orgánica de protección de datos de carácter personal*. Madrid: Civitas, 2001, p. 119.

adicional de singular entidad que tenga que esgrimir el afectado para legitimar su revocación. Orti Vallejo<sup>252</sup> opina que además de parecerle desacertada la introducción en la ley de la “justa causa”, éste es un típico concepto jurídico indeterminado. Explica el autor, citando Doral que tal concepto puede entenderse tanto como algo negativo, “ausencia de impedimentos o prohibiciones, que no contradiga lo convenido a la *aequitas*, ausencia de lesión a otro en la toma de posesión” y también como algo positivo, “límites de la autonomía privada sin invadir la esfera de otro y sobre todo, los principios de la buena fe negocial”. Por tanto, concluye que la elasticidad del concepto acarrea una censurable inseguridad jurídica en el ejercicio de la facultad revocatoria. Vizcaino Calderón<sup>253</sup>, se inclina por una concepción más amplia y flexible. En su opinión, si con carácter general el consentimiento se dio libremente, también debe ser razonablemente libre la revocación, máxime cuando el tratamiento no produce especiales beneficios al afectado.

En nuestra opinión, la norma reglamentaria debería haber solventado el problema del alcance del concepto de “causa justificada” cuando estamos hablando de la regla general del consentimiento. Es decir, por más que el legislador quiera limitar la revocación, estará también limitando el derecho al consentimiento. Entendemos que quien puede libremente consentir, puede a cualquier momento revocarlo. Porque si no es así, lo que se entiende por consentimiento como manifestación de la voluntad pierde su sentido semántico y jurídico. Estaríamos delante de otra situación jurídica que no es el consentimiento, en la cual la libre voluntad para aceptar no es la misma para revaluar y cambiar la situación anterior. La ausencia del factor “voluntad” es por regla general la justa causa de la revocación del consentimiento.

---

<sup>252</sup> ORTI VALLEJO, Antonio. *Derecho... op. cit.*, p. 147.

<sup>253</sup> VIZCAINO CALDERÓN, Miguel. *Comentarios... op. cit.*, p. 121.

Ahora bien, revocar no significa retrotraer los efectos del primer acto libre de la voluntad, y por lo tanto solo se opera a partir del conocimiento de su manifestación. Además, como advierte Vizcaíno Calderón, el problema del resarcimiento por eventuales daños causado por la revocación será resuelto con arreglo a los principios generales de la responsabilidad civil. De todo ello, corresponderá al interprete la labor de limitar la revocación observando el principio de la razonabilidad.

El párrafo 4 del artículo 6 ocupase de establecer el derecho del afectado en oponerse al tratamiento de datos en los casos en los que no sea necesario su consentimiento, siempre que una Ley no disponga lo contrario, y cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero deberá excluir del tratamiento los datos relativos al afectado.

Es importante remarcar que según preceptúa el Reglamento (art. 10, apartado 2) es innecesario el consentimiento tanto para el tratamiento cuanto para la cesión de los datos cuando así lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando el tratamiento y la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, o sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de las citadas leyes.

Además, en el caso de tratamiento de los datos especialmente protegidos, la LOPD dedica en el artículo 7 a establecer la forma de obtención del consentimiento para aquellos que revelen ideología, afiliación sindical, religión y creencias. De modo que deberá ser expreso y por escrito, no siendo aplicable tal regla para los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, aunque



para su cesión siempre será necesario el previo consentimiento del afectado.

Cumple subrayar, asimismo, que aquellos que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos con el consentimiento expreso del interesado.

Lo que nos parece curioso, es lo que estatuye el apartado 6 del mismo artículo 7, que dispone que en que pese lo que determina los apartados anteriores, “podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto”.

El precepto en análisis, por excelencia, es un punto absolutamente neurálgico. Porque allí los datos tratados son esencialmente íntimos, en el sentido más reservado que se pueda uno tenerlo. Son datos que su naturaleza exige una protección más firme que cualquier otro y justamente por eso tiene una denominación propia — “datos sensible” — y una consideración normativa especial<sup>254</sup>. Además toda excepción que se

---

<sup>254</sup> Nos parece interesante señalar el planteamiento de Stefano Rodota sobre la tutela de los datos sensibles y la función de la privacidad. Para el autor en cita, “Dotar a estos datos de una protección específica contra los riesgos de su tratamiento es consecuencia de su posible aptitud de ser utilizados con fines discriminatorios. De aquí deriva una aparente paradoja: a estos datos típicamente públicos se le atribuye el máximo de protección privada. Y esto conlleva una substancial mutación de las razones de la tutela : el fin ya no es estimar el secreto como un bien en si mismo, sino impedir posibles discriminaciones, hacer que la igualdad sea efectiva”. Para el autor en cita, ello conlleva a un cambio profundo en “la función socio-política de la privacidad, que de esta manera sobrepasa la esfera privada, confirmándose como elemento

lo haga a su recabo, tratamiento o cesión debe tener una razón de índole más fuerte y superior que la propia tutela de los datos para que se la justifique.

Por todo ello, es comprensible, por lo menos en parte, que en algunos raros casos la religión y creencias del ciudadano puedan auxiliar — pero a nuestro sentir, jamás ser determinante — a definir la forma por la cual se encaminará determinado tratamiento médico, o incluso ayude a encontrar el diagnóstico de alguna enfermedad. Porque sí, es verdad, que algunas creencias y religiones nos conducen a actuar de cierta manera en nuestras vidas que pueden influir en la salud de uno, y consecuentemente estarse delante de un riesgo para la propia vida. Aunque opina Vizcaíno Calderón<sup>255</sup>, que “en primero término no se aprecia qué tenga que ver los datos a que se refiere el apartado 2 (ideología, afiliación sindical, religión y creencias) con la hipótesis de diagnóstico, tratamiento o asistencia médica o sanitaria a que se refiere el número 6”. A su sentir, la Ley no ha querido abordar en esta norma el tema delicado y profundo, del tratamiento condicionado por determinadas creencias.

No obstante, una inquietante cuestión que nos surge es la siguiente: ¿en cuál tratamiento médico o diagnóstico se hace necesario tomar conocimiento de la ideología y afiliación sindical? O, aún mejor, ¿en qué momento se puede relegar la protección de estos datos para la tutela de

---

constitutivo de la ciudadanía. Y su definición, durante largo tiempo únicamente conexas al ‘derecho de ser dejado solo’, se dilata y dirige hacia la idea de tutela global de las opciones de vida contra toda forma de control público y de estigmatización social, en un marco caracterizado por la libertad de las opciones existenciales y políticas. Estamos frente a una perfecta correspondencia entre la regulación de tales datos sensibles y las normas constitucionales sobre la igualdad”. RODOTÁ, Stefano. *Democracia y Protección de Datos*, texto disponible en

[https://www.agpd.es/portalweb/.../DemocraciaMadrid\\_mayo\\_05.pdf](https://www.agpd.es/portalweb/.../DemocraciaMadrid_mayo_05.pdf) , acceso 10 de enero de 2009.

<sup>255</sup> VIZCAINO CALDERÓN, Miguel. *Comentarios... op. cit.*, p. 130.

otro bien mayor?. ¿Cual bien jurídico tiene, por su naturaleza, la fuerza de aplastar dicha garantía para que se le salvaguarde? No pretendemos de ningún modo alargar la discusión del tema, lo que extrapola el objeto de nuestra investigación, pero lo cierto es que se siembra la duda cuando se intenta imaginar alguna hipótesis de subsunción de la norma a un supuesto real.

Para Vizcaíno Calderón<sup>256</sup>, la interpretación más razonable probablemente sea la de entender que el tratamiento de los datos del apartado 3 del artículo 7 de la LOPD (y los del apartado 2) requiere siempre el consentimiento expreso (apartado 3, origen racial, a la salud y a la vida sexual) o el consentimiento expreso y por escrito (apartado 2, ideología, afiliación sindical, religión y creencias) salvo en las hipótesis de la prevención y diagnóstico médico prevista en el apartado 6, “sin que se entienda bien, pese a la redacción textual de éste último qué tiene que ver en su contexto los datos de religión y creencias y, menos aún, los de ideología y afiliación sindical”. Concluye el autor que si lo que quiere la Ley, como parece, en los supuestos del artículo 7.6 no es necesario el consentimiento del afectado para el tratamiento de sus datos de salud o vida sexual, nada hubiera costado precisarlo en la norma.

Otro punto que ha merecido nuestra atención, pero igualmente sin ánimo de profundizar la materia, es la redacción del apartado 2 del artículo 7 de la LOPD. Lo que se entiende que el legislador pretendía, por la lógica legal, era que los ficheros de un partido político no necesiten del consentimiento del afectado para tratar sus datos sobre su ideología política, así como aquellos mantenidos por la iglesia sobre la religión y creencia del interesado, y así sucesivamente con todos los ficheros de los cuales hace la ley excepciones. Pero en ningún momento se ha especificado la innecesidad del consentimiento a cada uno de los ficheros

---

<sup>256</sup> *Ibid.*, p. 131.

allí excluidos se refiere al ámbito de su finalidad restricta, hecho que se lo arreglaría con una sencilla mención en el precepto.

El otro supuesto del consentimiento que la LO 15/1999 trata con detenimiento es en los casos de la comunicación de los datos. El artículo 11 de la LOPD establece la necesidad del previo consentimiento del interesado para que puedan ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario. Las excepciones legales para la ausencia del consentimiento son las siguientes: a) cuando la cesión está autorizada en una Ley; b) cuando se trate de datos recogidos de fuentes accesibles al público; c) cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En esta hipótesis la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique; d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas; e) cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica y, como el apartado 6 del mismo artículo determina: f) si la comunicación se efectúa previo procedimiento de disociación.

Además de estos supuestos, también determina el artículo 11 el caso en que la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. El Reglamento en su artículo 8, apartado 4, línea

c agrega sobre esta hipótesis que no es necesario el consentimiento para la cesión entre las Administraciones Públicas cuando los datos de carácter personal hayan sido recogidos o elaborados por esa con destino a otra igualmente pública; también si la comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

Asimismo, el RPD repite la permisión de la comunicación de datos de fuentes accesibles al público, no obstante acrece que las Administraciones públicas solo podrán comunicarlos a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley (art. 10, apartado 2, alinea b).

Importa añadir que podrá padecer del vicio de la nulidad el consentimiento para la comunicación de los datos a un tercero cuando la información que se facilite al afectado no le permita conocer la finalidad a que se destinarán los datos o el tipo de actividad de aquél a quien se pretende comunicar (art. 11, apartado 3 de la LOPD). Además, el consentimiento para la comunicación de los datos de carácter personal también posee un carácter revocable (art. 11, apartado 4 de la LOPD). Hay que añadir también que, el mero hecho de recibir la comunicación de los datos ya obliga a quien se hubiere comunicado la observancia de las disposiciones de la LOPD (art. 11, apartado 5 de la LOPD). Sobre ese último aspecto, el artículo 12 del reglamento también considera nulo el consentimiento si en la comunicación el interesado no fue informado de modo que conozca incontrovertiblemente la finalidad a que se destinarán sus datos, respecto de cuya comunicación se solicita además del tipo de actividad que el cesionario desarrolla.

El mismo artículo 12 del Reglamento dispone sobre la forma de obtener el consentimiento. De esta manera, establece que la solicitud debe ir referida a un tratamiento o serie de tratamientos concretos, delimitándose la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamiento. También

determina que recae al responsable del tratamiento la carga probatoria de la existencia del consentimiento del interesado por cualquier medio de prueba admisible en derecho. Este último aspecto nos ha llamado la atención. Porque no obstante entendemos que la ley abre muchas concesiones para la innecesidad del consentimiento, creemos que nada más que fijar claramente a quién cabe la carga probatoria, ello fortalece de manera notable la protección del individuo.

Al dirigirse al afectado con la finalidad de recabar su consentimiento, según dispone el artículo 14 de la aludida norma, el responsable deberá concederle un plazo de treinta días para manifestar su negativa, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos. Aquí, en este punto, volvemos a la misma discusión que ya se tenía antes de la entrada en vigor del reglamento sobre el silencio del interesado.

Es cierto que, como observa Puente Escobar<sup>257</sup>, tanto la doctrina como la jurisprudencia “han venido a considerar que el hecho de que el consentimiento del afectado haya de ser inequívoco no implica que aquél no pueda ser obtenido tácitamente”. Aunque el autor subraya que hay que establecer una serie de normas que regulen un procedimiento estándar para que se evite situaciones que pueden ser consideradas abusivas hacia el afectado. Y desde el punto de vista del responsable, hay que establecer mecanismos que faciliten la prueba de la obtención del consentimiento prestado evitando reclamaciones del afectado basadas en la mera negativa de éste a la efectiva recepción de la solicitud formulada. También el mismo autor<sup>258</sup> subraya que “el consentimiento no habrá de

---

<sup>257</sup> PUENTE ESCOBAR, Agustín. “Consentimiento del afectado y deber de información”. En MARTÍNEZ MARTÍNEZ, Ricard (coord.). *Protección de datos Comentarios al Reglamento de Desarrollo de la LOPD*. Comentarios al Reglamento de Desarrollo de la LOPD. Valencia: Tirant lo Blanch, 2009, pp. 45-46.

<sup>258</sup> PUENTE ESCOBAR, Agustín. *Consentimiento... op. cit.*, p. 40.

ser necesariamente expreso; es decir, podrá derivarse de una manifestación positiva de voluntad, pero también podrá entenderse prestado cuando se ofrezca al interesado la posibilidad de manifestarse en contra del tratamiento de los datos y éste no se niegue a ello”.

Desde nuestra perspectiva, primeramente el plazo concedido no debería ser de manera general para la manifestación de la negativa al tratamiento pero sí para que el afectado preste inequívocamente su consentimiento. Y en lo que respecta al silencio, si quisiera dar una connotación jurídica, que esta fuese la oposición al citado tratamiento. En efecto, la representación que se pretende conferir al silencio en las más diversas situaciones legales es todavía muy problemática. Aunque su naturaleza sea fundamentalmente una acción negativa, es decir, cuando se silencia, el sujeto se abstén de expresarse, esa su esencia no puede confundirse con el contenido de lo que eventualmente se desearía decir, si fuese el caso. De manera general el silencio es neutral, porque inexistente la exteriorización de la manifestación del individuo, y tampoco no es posible por lo menos en un primero momento de hacer cualquier conjetura. Si a ello no acompaña actos que revelen que el interesado ha dado el consentimiento, el silencio únicamente, desde nuestra perspectiva no puede ser entendido como una aceptación.

En el supuesto que hemos analizado, si la regla general es que para recabar, tratar y comunicar datos es necesario el consentimiento, ¿como puede el silencio corresponder justamente lo opuesto a la regla general del principio? Cual la naturaleza de la fuerza jurídica que se le otorga para que un elemento neutral se transforme en la excepción a la regla?

Además, otro problema que se puede plantear es la dificultad practica de comprobar el consentimiento dado a través del silencio, aunque se permita todas las pruebas admitidas en derecho. Y, a nuestro sentir, el RPD empeora aún más en el apartado 3 del artículo 14 estableciendo que en todo caso será necesario que el responsable del tratamiento pueda

conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos. De suerte que, en nuestra opinión, todo ello refuerza la importancia de que se haya especificado en la ley el destinatario del *onus probandi* porque así, aunque en silencio, este deberá ser comprobado si es el caso, sus razones. Además de lo que determina el siguiente apartado cuando preceptúa que será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

Habría sido indudablemente más fácil para todos los involucrados si hubiese sido respetado el principio general del consentimiento o que por lo menos el silencio fuese entendido tal y como lo es: silencio.

El apartado 4 del mismo artículo exige que se facilite al interesado un medio sencillo y gratuito para manifestar su negativa, sea mediante un envío pre franqueado al responsable del tratamiento o la llamada a un número de teléfono gratuito. El siguiente apartado añade la imposibilidad de solicitarse el consentimiento nuevamente a través del mismo procedimiento respecto a los mismos tratamientos y finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

La solicitud del consentimiento en las relaciones contractuales para fines no relacionadas directamente con las mismas es también objeto de apreciación por el Reglamento. Dispone en el artículo 15 que el responsable del tratamiento “deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos”. Lo que nos parece un poco ilógico en este precepto es lo que viene después, cuando la norma dice que se entiende cumplido tal deber cuando permita al afectado la marcación de una casilla claramente visible **y que no se encuentre ya marcada en el documento que se le entregue para la**



**celebración del contrato**, o en su caso, un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

A nuestro juicio la ley fue poco afortunada con tal disposición. Primero porque únicamente marcar una casilla para expresar el consentimiento, es un instrumento muy frágil que puede, indudablemente, dar lugar a muchísimos fraudes. La ley ya ha determinado su extenso rol donde se encuentra los supuestos de excepción al consentimiento, así que cuando se le exige que su manifestación sea *expresa*, no debería permitir que se le hiciera a través de una sencilla marcación de una casilla. Segundo porque desde nuestra perspectiva, ya que fue opción del legislador regular la forma que se debe obedecer para recabar el consentimiento en esta hipótesis, obviamente para que no haya — o por lo menos disminuyan — los problemas concernientes a ella sobretodo cuando se trata del consentimiento, lo debería haber hecho de modo taxativo y no sin dejar espacio para interpretaciones. Desde nuestro punto de vista no debería primero determinar que el responsable permita “al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos”, y acto seguido especificar una manera de solicitar tal consentimiento (marcando una casilla) y en la misma oportunidad autorizar que se pueda establecer “un procedimiento equivalente que le permita manifestar su negativa al tratamiento”. Este espacio interpretativo nos parece criticable, por decirlo de algún modo: es por lo menos contradictorio que la norma una vez decida determinar los instrumentos y el procedimiento del recabo del consentimiento, no puede “medio legislar”, no fijando una forma eficaz de procederlo, y a la vez ser permisiva. Se ya nos parece absurdo que el discutido y discutible precepto permita que sea una casilla la expresión del consentimiento, nos resulta más aún sorprendente el margen interpretativo concedido, cuando la misma ley permite un “procedimiento equivalente”.

El Reglamento trae una novedad importantísima que es el artículo 13 dedicado a las disposiciones sobre el consentimiento del tratamiento de

datos de menores. Al respecto, señala Orozco Pardo<sup>259</sup>, “hoy los menores participan cada vez más en el mercado de bienes y servicios, incluidos los negocios relativos a las vertientes patrimoniales de sus derechos a la intimidad, la imagen y la protección de datos”.

La citada norma es muy contundente al decretar que solamente se puede manejar los datos de los menores de 14 años con el consentimiento de sus padres o tutores. Ya para los mayores de 14 años, determina que se puede proceder con el tratamiento de sus datos personales, con su consentimiento, salvo que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela.

De todos los modos, el aludido reglamento prohíbe que se obtenga a través del menor información sobre los datos de los demás miembros del grupo familiar, o sobre características del mismo sin el consentimiento de los titulares de dichos datos, aunque excluye los datos de identidad y dirección de los padres o tutor con la finalidad única de recabar la autorización del consentimiento para tratar los datos del menor.

Además, cuando el tratamiento de los datos se refiera a los menores, la norma exige que la información dirigida a ellos deberá ser expresada en un lenguaje fácilmente comprensible por aquellos, con indicación de lo dispuesto en el artículo 13 del RPD. Asimismo, son los responsables del fichero o tratamiento a quienes les corresponde comprobar de modo efectivo la edad del menor y la autenticidad del consentimiento prestado, en su caso los padres o representantes legales.

De hecho, este artículo es de gran valía cuando se imagina la cantidad de datos que son fornecidos por menores sobre todo a través de Internet

---

<sup>259</sup> OROZCO PARDO, Guillermo. “Intimidad, privacidad «extimidad» y protección de datos del menor ¿Un cambio de paradigma?. En BOIX REIG, Javier (Dir.). *La protección Jurídica de la Intimidad*, Madrid: lustel, 2010, p. 402.

y, en ésta, en las llamadas redes sociales. Moreno Navarrete<sup>260</sup> ha señalado con mucha propiedad que tales redes sociales son un fenómeno cuyo alcance aún está por determinar y que afecta de forma muy importante a la esfera jurídico personal de los sujetos, a su esfera de su personalidad, muy especialmente a su intimidad. En efecto, específicamente a lo que atañe a los menores de edad, advierte Morillas Fernández<sup>261</sup> que el uso de las redes sociales por parte de estos se ha convertido en una parte más de sus vidas y no obstante tengan los menores ciertas nociones de seguridad, descuidan algunos aspectos y, en ocasiones, no otorgan la importancia que merecen los datos personales.

Pero no solamente ahí se quedan los riesgos a que están sometidos los menores. Un ejemplo de lo que puede pasar con aquellos no se restringe al ámbito de Internet es lo que sucedió en diciembre de 2008 con la empresa Telefónica Móviles, que fue multada por la Agencia Española de Protección de Datos en 230 mil euros por uso irregular de datos de menores. En el caso, Telefónica propuso a niños que usaban teléfonos prepagos a cambiarlo a contrato. Los menores aceptaron y la empresa no solicitó el consentimiento de los padres o tutores. Como consecuencia, hubo la natural imposibilidad de los menores cumplir con el pagamiento de las facturas advenidas del contrato. Ello ocasionó la inclusión por parte de Telefónica de sus nombres en el registro de morosos ASNEF. Además de haber hecho un contrato telefónico no obstante la edad de los contratantes, de lo que consta, la empresa no realizó las comprobaciones necesarias en lo referente a sus edades, no requirió la autorización a sus

---

<sup>260</sup> MORENO NAVARRETE, Miguél Ángel. “Aspectos Jurídicos privados de las tecnologías Web 2.0 y su repercusión en el derecho de la intimidad”. En BOIX REIG, Javier (Dir.). *La protección Jurídica de la Intimidación*, Madrid: lustel, 2010, p. 335.

<sup>261</sup> MORILLAS FERNÁNDEZ, Marta. “La protección jurídica del menor ante las redes sociales”. En BOIX REIG, Javier (Dir.). *La protección Jurídica de la Intimidación*, Madrid: lustel, 2010, p. 365.

representantes legales y usó indebida y ilícitamente los datos de los menores<sup>262</sup>.

El último aspecto que nos parece relevante subrayar, tocante al Reglamento, es la forma de revocación del consentimiento, regulada en el artículo 17. El responsable del fichero o tratamiento deberá poner a disposición del afectado un medio sencillo, gratuito y que no implique ingreso para nadie, pudiendo ser considerados lícitos, entre otros, un envío pre franqueado al responsable del tratamiento, la llamada a un número de teléfono gratuito o a los servicios de atención al público que hubiere sido puesto a disposición por el mismo. De manera que no se podrá establecer cualquier medio que implique en un coste al interesado. Desde la recepción de la revocación, el responsable tiene diez días para cesar el tratamiento, sin perjuicio de su obligación de bloquear dichos datos conforme lo dispuesto en el artículo 16.3 de la LOPD. En el caso de que los datos hubieren sido cedidos, también el mismo plazo se observará para informar a los cesionarios que estos deben suspender el tratamiento, en el caso de que aún se mantuviese. Además, si el interesado solicita la confirmación del cese del tratamiento de sus datos, es obligación de esto responder expresamente su solicitud.

Sobre el tema del consentimiento de menores Grimald<sup>263</sup>, no considera adecuado al principio de reserva de ley orgánica de los derechos fundamentales fijar mediante reglamento la edad a partir de la cual los menores pueden prestar válidamente su consentimiento para el tratamiento de sus datos. A su sentir, si por un lado se puede afirmar que

---

<sup>262</sup> Información disponible en la pagina web:

[http://www.elpais.com/articulo/sociedad/Multa/Telefonica/hacer/contratos/mobiles/ninos/elpepisoc/20081209elpepisoc\\_2/Tes](http://www.elpais.com/articulo/sociedad/Multa/Telefonica/hacer/contratos/mobiles/ninos/elpepisoc/20081209elpepisoc_2/Tes) . [Consulta en 9 de dez. 2008].

<sup>263</sup> GRIMALD, Pedro. “El consentimiento y el tratamiento con fines publicitarios y prospección comercial”. En MARÍ, Joana, VILASAU, Mònica (coord.). *El Reglamento de protección de datos de carácter personal. Aspectos clave*. Barcelona: UOC, 2008, p. 71.

ello garantiza la seguridad, por otro el autor citado entiende que el principio de la seguridad jurídica no debe ser aplicado en detrimento de reglas constitucionales concreta (la reserva de ley orgánica), además dicho principio no se consigue desde el momento en que el propio reglamento hace excepción a aquellos casos en los que la Ley exija para su prestación “la asistencia de los titulares de la patria potestad o tutela” y ello obliga a acudir a unas normas legales que tampoco están muy claras.

### *2.2.3. Información en la recogida de datos.*

Este principio es una obligación que tienen los responsables del fichero y por lo tanto a su vez es un derecho del interesado a lo que se soliciten datos personales. La finalidad de tal obligación puede ser extraída de la Sentencia del Tribunal Constitucional de 30 de noviembre (STC 292/2000), que ha dejado consignado que parte del contenido del derecho fundamental a la protección de datos reside en un poder de disposición y control sobre los datos personales, que se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero. Por lo tanto, continua explicando el fallo “...es evidente que el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de estos, pues solo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales (...) De suerte que sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD ) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de datos personales, pues es claro

que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia”.

De suerte que los afectados, a tenor del artículo 5.1, deberán ser **previamente** informados de modo expreso, preciso e inequívoco de lo siguiente: a) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y e) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

También exige la LOPD en el apartado 2 del artículo 5 que cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado 1. Es interesante señalar a este respecto que la Audiencia Nacional<sup>264</sup> entiende que la LOPD ha querido imponer una formalidad específica en la recogida de datos que garantice el derecho a la información de los afectados. Así, en los casos de cuestionarios u otros impresos, “si esa información no es legible (por ejemplo cuando se incluyen leyendas informativas con una letra de tamaño minúsculo) se frustra la finalidad del derecho a la información en la recogida de los datos al no poder llegar a un verdadero conocimiento de sus destinatarios, con lo que se conculca tal deber de información previa”.

En el supuesto de que los datos no hayan sido recabados del propio interesado, aun así este deberá ser informado por el responsable por el fichero o su representante, en un plazo de tres meses a contar desde el momento del registro de los datos salvo que ya hubiera sido informado

---

<sup>264</sup> Por todas, la Sentencia de 19 noviembre 2009 (JUR 2010\18130).

con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras *a)*, *d)* y *e)* del apartado 1 del artículo 5.

Además de todo ello, ha de destacarse las excepciones al deber de informaciones que son cuando los datos proceden de fuentes accesibles al público y se destinan a la actividad de publicidad o prospección comercial, aunque se exija en este último caso que en cada comunicación al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten. Así como se exceptuará cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados.

El Reglamento 1720/2007, artículo 18, añade que la información deberá llevarse a cabo a través de un medio que se pueda acreditar su cumplimiento, debiendo ser conservado mientras persista el tratamiento de los datos. El soporte de conservación de dicha acreditación podrán ser medios informáticos o telemáticos, y si se procede al escaneado de la documentación en soporte papel, se debe garantizar que en dicha automatización no ha mediado alteración alguna de los soportes originales. Además de ello, en los casos en que se produzca una modificación del responsable del fichero como consecuencia de alguna operación contemplada por la normativa mercantil, para que se produzca la cesión deberá ser observado lo que dispone el artículo 5 de la LOPD, sobre información del interesado.

#### 2.2.4. Seguridad de los datos.

Este principio también establece obligaciones a los responsables por el fichero y el responsable por el tratamiento para que adopten las medidas técnicas y organizativas adecuadas a los riesgos que pueden presentar su tratamiento. Así, no se podrá registrar datos de carácter personal en los ficheros que no adopten algunas medidas de seguridad cuyos requisitos y condiciones se establecen reglamentariamente. Todo ello para que se eviten alteración, pérdida, tratamiento o acceso no autorizado a los datos de carácter personal almacenados en un fichero.

El artículo 9 de la LOPD determina que el responsable por el fichero — o por su tratamiento — está obligado a tomar las medidas necesarias para la seguridad de los datos registrados. Como seguridad de los datos de carácter personal entendemos, según el RD 994/1999, artículo 1º señala, como aquellas medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal, en el caso sujetos al régimen de LOPD y de su Reglamento. Según Freixas Gutiérrez<sup>265</sup>, la define como “aquellas medidas de carácter técnico, a través de la adopción de mecanismos o dispositivos que eviten su alteración, pérdida, tratamiento o acceso no autorizado”.

Efectivamente, los responsables por los ficheros deberán adoptar todas las medidas necesaria que garanticen la seguridad de los datos registrados pues las informaciones allí registradas se refieren a los individuos, por consiguiente los derechos de intimidad y privacidad de las personas. Para

---

<sup>265</sup> FREIXAS GUTIERREZ, Gabriel. *La protección... op. cit.*, p. 206.



Martínez Martínez<sup>266</sup>, “la implementación de medidas de seguridad permite depositar la suficiente confianza sobre la capacidad de dicha información y de los sistemas para sostener el funcionamiento adecuado de las funciones y los valores de la organización”. Por lo tanto, dichas informaciones no deben ser del conocimiento de las personas que no tienen un interés real y concreto sobre ellas, y las citadas medidas de seguridad sirven para evitar el desvío de la información hacia sitios no previstos<sup>267</sup>.

Las medidas de seguridad estaban anteriormente reglamentadas en el RD 994/1999, y según el artículo 3 de esta norma, pueden ser clasificadas en tres niveles: básico, medio y alto, establecidos atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

El Reglamento 1720/2007 también la engloba su disciplina, la reordena, la amplía y la sistematiza. De modo que dedica el Título VIII “De las medidas de seguridad en el tratamiento de datos de carácter personal” compuesto por 35 artículos (art. 79 al art. 114) divididos en cuatro capítulos. El primero se dedica a las disposiciones generales que deben cumplir todos los ficheros. El segundo capítulo trata del documento de seguridad; los siguientes capítulos se ocupan de las medidas de seguridad aplicables a ficheros y tratamientos automatizados no automatizados. De hecho, la grande novedad del Reglamento en éste punto son las medidas de seguridad específica para los ficheros no automatizados.

---

<sup>266</sup> MARTÍNEZ MARTÍNEZ, Ricard. “Las Medidas de Seguridad”. En MARTÍNEZ MARTÍNEZ, Ricard (coord.). *Protección de datos Comentarios al Reglamento de Desarrollo de la LOPD*. Comentarios al Reglamento de Desarrollo de la LOPD. Valencia: Tirant lo Blanch, 2009, pp. 91.

<sup>267</sup> Vide DAVARA RODRIGUEZ, Miguel Angel. “El nuevo Reglamento de Medidas de Seguridad de la ley de Protección de Datos”. WESTLAW [en línea]. *Actualidad Jurídica Aranzadi*, núm. 690/2005.

En lo que concierne a los niveles de seguridad, el artículo 81 mantiene la clasificación en tres: básico, medio y alto. Según el artículo 81 del RPD, todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico. En los casos de los ficheros de solvencia patrimonial, se requiere un nivel medio, como determinaba el apartado 2 del artículo 4 del mismo Real Decreto, que disponía que deberían reunir, además de las medidas de nivel básico, las calificadas como de nivel medio de seguridad aquellos ficheros en los cuales contengan datos que se rijan por el artículo 28 de la Ley Orgánica 5/1992, que se referían en la derogada ley, aquellos objeto de nuestra investigación. El Reglamento actualiza éste dispositivo, determinando explícitamente que deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en aquellos ficheros cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, es decir, los ficheros de solvencia patrimonial y crédito.

Es importante ubicar la clasificación de seguridad ya que el artículo 9 de la LOPD prohíbe el registro de datos en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad<sup>268</sup>, es decir, es una condición de licitud para el tratamiento de los datos.

---

<sup>268</sup> Vid. MARTÍNEZ SÁNCHEZ, M., “La notificación de ficheros para su inscripción en el Registro General de Protección de datos y la seguridad de las bases de datos”, en *Protección de Datos de carácter personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos, celebrado en La Antigua-Guatemala del 2 al 6 de junio de 2003*, Valencia, 2005.

### 2.2.5. *Deber de secreto.*

Como establecido en el artículo 10 de la LOPD, el deber de secreto es la obligación que corresponde al responsable del fichero o cualquiera que intervenga en cualquier fase del tratamiento de los datos estando obligados al secreto profesional respecto de los mismos y al deber de guardarlos. Dicho deber subsistirá aun después de terminada la relación con el titular o el responsable del fichero.

La importancia de este deber fue manifestada por la Audiencia Nacional<sup>269</sup>, en Sentencia de 24 octubre 2007, donde define dicha obligación como “una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000”. Señala aún este Tribunal que “este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE”.

Es necesario añadir que el incumplimiento a este principio está tipificado como infracción. De un lado, el artículo 44.2.e) de la LOPD, tipifica como infracción: “incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave”. Por otro lado, el artículo 44.3.g) establece que son infracciones graves “la vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la

---

<sup>269</sup> Audiencia Nacional. Sentencia de 24 octubre 2007 (JUR 2007\346164).

personalidad del individuo”. Aparte de la condición legal y objetiva de la tipificación de la infracción como grave cuando los datos de carácter personal estén incorporados a ficheros que contengan un conjunto de datos suficientes para obtener una evaluación de la personalidad del individuo, especificado en el propio artículo 44.3.g), la determinación de infracción como leve o no del incumplimiento del deber de secreto viene de la propia Audiencia Nacional en el fallo citado anteriormente donde señala que “resulta que la diferencia la infracción correspondiente a la omisión del deber de secreto considerada grave ó leve procede del hecho de que pueda dar lugar a elaborar un perfil de la persona”.

En efecto, en Sentencia anterior este órgano juzgando la gravedad de la infracción del caso que en aquél momento se apreciaba, comparativamente a otro apreciado por el mismo Tribunal, refuerza la importancia de que la violación del deber de secreto tenga como consecuencia la proyección de un perfil de la persona: “en la línea de razonamiento de la demandante, esta Sala apreció que la infracción no era subsumible en el tipo de la infracción grave en un caso en el que los datos a los que indebidamente había tenido acceso un tercero fueron el número de cuenta y el saldo existente pero no el nombre del titular de dicha cuenta, pues entendíamos que la información proporcionada no aparecía vinculada a una persona determinada ni permitía, por tanto, hacer valoración alguna sobre el perfil o personalidad del titular de tales datos (SAN, 1ª, de 17 de enero de 2003 en Recurso 1000/00). Sin embargo, las cosas son bien distintas en el caso que nos ocupa pues en las facturas remitidas por la demandante aparecen asociados el nombre de la persona con el de la cuenta bancaria y con ello se está dando una información indudablemente relacionada con el servicio bancario pues se da noticia de que una determinada persona es titular de una cuenta corriente de la que se facilitan todos los datos de identificación”.

### III. La ley de protección de datos de carácter personal en Italia.

#### 1. Evolución legislativa

Hasta el año de 1996 Italia era un país huérfano de una ley específica sobre la protección de datos, no obstante la labor jurisprudencial y de la doctrina, y también de algunas propuestas legislativas iniciadas desde el 1981<sup>270</sup>, pero que nunca fueron aprobadas y de leyes como la n° 300 de 20 de mayo de 1970 y la n° 121 de 1° de abril de 1981 que en algunos puntuales artículos tratan de algunos perfiles del derecho a la *riservatezza*. Como resalta Satoretti<sup>271</sup>, el cuadro jurídico-normativo que se presentaba ante los ojos de los estudiosos se caracterizaba de un lado por la ausencia de una disciplina orgánica y de otro por la presencia de una multiplicidad de normas sectoriales que necesitaban ser unificadas. Según la autora en cita, el primer paso del legislador para reunirla lo cumple con la adopción de la ley 675/96 y sucesivamente con el Código en materia de protección de los datos personales. No obstante, en la opinión de Niger<sup>272</sup>, la falta de una normativa sobre ese tema se debe justamente al intenso debate doctrinario y a las “oscilantes orientaciones jurisprudenciales” sobre la existencia y el fundamento del *diritto alla riservatezza*.

---

<sup>270</sup> Vid. BUTTARELLI, Giovanni. *Banche... op. cit.*, p. 110 y ss.; y también PARDOLESI, Roberto. *Dalla Riservatezza... op. cit.*, p. 40 y ss.; y PERRI, Pierluigi. *Privacy... op. cit.* p. 4 y ss.

<sup>271</sup> SATORETTI, Claudia. *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale*. Torino: Giappichelli, 2008, p. 39.

<sup>272</sup> NIGER, Sergio, *Le nuove dimensioni... op. cit.*, pp. 40-41.

Resalta Zeno-Zenconvich<sup>273</sup>, que Italia era, en estas fechas, el último país de la Unión Europea que todavía no tenía una legislación específica en materia de datos personales. Para el autor en cita<sup>274</sup>, sería casi inútil preguntarse el motivo de tanto retraso sobre todo en un país sensible a los derechos fundamentales y profundamente europeo, no fuese por señalar que la “agenda política” — tanto ayer, como hoy — parece a menudo más centrada en temas marginales si no ajenos al resto de Europa y precisamente ello justifica a la frecuente “diferencia de velocidad” entre Italia y los demás países en algunos asuntos.

Se puede afirmar que los motivos que principalmente impelieron el surgimiento de la primera legislación unificada sobre este tema (la ley nº 675/96) fueron la aprobación de la Directiva del Consejo 95/46 — y consiguientemente la necesidad de transponerla al ordenamiento jurídico interno —, la Convención de Estrasburgo, ratificada por Italia en 1989 que exigía que los países adoptasen las medidas internas necesarias para dar efectos a sus principios fundamentales, y, finalmente, la adhesión italiana al Tratado de Schengen.

Es importante recordar que cuando dicho tratado ha empezado a tener efecto, aquél país aún no había aprobado su ley de protección de datos, lo que motivó su exclusión temporaria de la área de actuación de la frontera Schengen<sup>275</sup>. Como subraya Butarelli<sup>276</sup>, este hecho repercutió fuertemente

---

<sup>273</sup> ZENO-ZENCOVICH, Vincenzo. “Dieci anni di legislazione sui dati personali: tentativo di un bilancio”. En: *La legge sulla privacy dieci anni dopo*. FRANCO FERRARI, Giuseppe (coord.). Milano: Egea, 2008, p. 35.

<sup>274</sup> *Ibid.*, p. 35.

<sup>275</sup> *Vide* GALETTA, Diana-Urania. “La cooperazione fra polizie e il Sistema informativo Schengen (SIS) per una sicurezza e una giustizia europee” En: LOSANO, Mario. *La legge Italiana sulla privacy: un bilancio dei primi cinque anni*, Laterza, 2001, Bari, p. 189 y 190.

<sup>276</sup> BUTTARELLI, Giovanni. *Banche dati... op. cit.*, p. 119.

en la prensa y opinión pública y por eso dejó de ser un mero empeño formal para transformarse en un tema de especial atención en la agenda política.

Aún sobre ese tema, según lo que consta en la nota introductiva del documento del *Comitato Parlamentare Schengen-Europol* de controle sobre la actuación y funcionamiento de la Convención de aplicación del Acuerdo de Schengen y de vigilancia sobre la actividad de la unidad nacional Europol<sup>277</sup>, y a pesar de que Italia había ratificado desde 1993<sup>278</sup> el Acuerdo y el Convenio, no pudo unirse, a nivel operativo, al sistema de Schengen, que había entrado en vigor el 26 marzo de 1995, por razones de orden político y organizativo que consistieron, en primero lugar en la no aprobación por el Parlamento de una ley sobre protección de datos, y el artículo 117 del Tratado disponía que tocante al tratamiento automatizado de datos de carácter personal cada país signatario debería adoptar, a más tardar en el momento de la entrada en vigor del citado Convenio, las disposiciones nacionales necesarias para conseguir un nivel de protección que fuese al menos igual a los que derivan de los principios del Convenio del Consejo de Europa de 28 de enero de 1981. El Convenio de Schengen, cuya ratificación había sido autorizada por las Cámaras desde 1989, a través de la Ley 98/1989, aún no había completado su proceso de depósito de los instrumentos, porque Italia todavía no había cumplido tal compromiso.

En segundo, la participación italiana en el Sistema de Información de Schengen (SIS). El artículo 92 del Convenio de Aplicación del Acuerdo de

---

<sup>277</sup> Comitato parlamentare di controllo sull'attuazione ed il funzionamento della Convenzione di applicazione dell'Accordo di Schengen e di vigilanza sull'attività dell'unità nazionale Europol, documento disponibile en

[http://www.camera.it/\\_bicamerale/schengen/notaintro/introfr.htm](http://www.camera.it/_bicamerale/schengen/notaintro/introfr.htm) [consulta en 05 feb. 2009].

<sup>278</sup> Ley nº 338, de 30 de septiembre de 1993.

Schengen establecía que fuese creado un sistema común de información, constituido de una Sección Nacional, establecida en cada Estado y responsable de crear y mantener en un archivo de datos sobre una base nacional; y de una Unidad de Apoyo Técnico, con sede en Estrasburgo, con la tarea de gestionar un fichero de datos con los cuales fuese garantizada la identidad y, por tanto, la homogeneidad de los archivos nacionales a través de la transmisión de información en línea.

Los dos obstáculos fueran sanados desde el momento en que, como apunta el citado documento, terminada la fase de prueba denominada "*data loading test*" para verificar la idoneidad y la compatibilidad del sistema nacional con la central en Estrasburgo desde el punto de vista puramente técnico, fue completada la fase de descarga de los datos procedentes de los países en los cuales el acervo Schengen eran ya operativos en el SIS nacional.

Con respecto a la ausencia normativa sobre protección de datos, esta fue remediada con la promulgación de la Ley nº 675, de 31 de diciembre de 1996<sup>279</sup>, de modo que el Consejo Ejecutivo, en reunión del 7 de octubre de 1997, aprobó la entrada de Italia en el espacio Schengen en 26 de octubre de ese mismo año. Por todo ello, la importancia de la citada ley no puede ser vista solamente desde un punto de vista jurídico-formal, pero también político ya que fue la responsable por la inserción de Italia en el espacio Schengen.

De manera que la aludida norma entró en vigor en 8 de mayo de 1997, visiblemente inspirada en la Directiva Comunitaria 46/95, hecho que no sorprende debido a la aproximación temporal entre una y otra reglamentación. Sin embargo, aparte de que carecía de muchos ajustes a todos los principios dictados por la Directiva y por lo tanto no servía integralmente como la norma de transposición, se puede detectar

---

<sup>279</sup> Para los aspectos más importantes del régimen jurídico de la ley 675/96, vide SCALISI, Antonino. *Il Diritto alla Riservatezza*. Milano: Giuffrè, 2002, pp. 188-203.



diferencias muy importantes entre ambas legislaciones como por ejemplo en el ámbito de protección: mientras la Directiva solamente tutela las personas físicas, la ley italiana la amplia para las personas jurídicas y otros entes y asociaciones<sup>280</sup>.

Para Fioriglio<sup>281</sup>, la importancia de ley 675/96 reside en el reconocimiento de un nuevo derecho que permite proteger aquellos valores fundamentales de la persona humana que, en virtud de su carácter, no pueden permanecer privados de protección. No obstante el retraso para promulgar una norma específica sobre el tema, lo que debería suponer — en tesis — en una norma más elaborada, y la reacción positiva de la doctrina con su llegada<sup>282</sup>, esta recibió diversas críticas. La más dura era sobre el problema de su generalidad. Como no disciplinaba la materia en muchos de los sectores específicos de la economía, para algunos eso hizo con que la ley encontrase en su primera fase de vigencia un problema de actuación práctica. Ello porque, como advierte Imperiali<sup>283</sup>, ni todos los dispositivos que contenían los principios generales eran de aplicación inmediata en diversos contextos. En la opinión de este autor, por esta razón el legislador, ya previamente advertido, también promulgó juntamente con esta norma, una otra “gemela”, nº 676/96, que implicaba la posibilidad fundamental de delegar poderes al gobierno para integrar y adecuar el reglamento principal, en el decorrer de su empleo practico.

---

<sup>280</sup> Artículo 1º de la Ley 675/96.

<sup>281</sup> FIORIGLIO, Gianluigi. *Il Diritto alla privacy. Nuove frontiere nell'era di Internet*. Bologna: Bononia University Press, 2008, p. 16.

<sup>282</sup> Vid. KIRSCHEN, Sabina. “Il Codice della privacy, fra tradizione ed innovazione”. En: *Libera circolazione e protezione dei dati personali*. PANETTA, Rocco (coord.). Milano: Giuffré, Tomo I, 2006, p. 6.

<sup>283</sup> IMPERIALI, Riccardo. y IMPERIALI, Rosario. *Codice della privacy. Commento alla normativa sulla protezione dei dati personali*. Milano: Il sole-24 ore, 2005, p. 10.

En efecto, la ley 676/96 estaba compuesta de tres artículos que conferían al Gobierno el poder de emitir uno o más decretos legislativos que contuviesen disposiciones correctivas e integrativas de la legislación sobre la protección de las personas y de otras materias relativas al tratamiento de datos personales, en un plazo de dieciocho meses a partir de la fecha de entrada en vigor de la susodicha norma<sup>284</sup>. Así que esta fue largamente aplicada<sup>285</sup>, mostrándose por un lado un instrumento muy válido y por otro corroborando con las críticas de la doctrinas sobre la problemática de la aplicación práctica de una norma tan general.

En los siete años en que estuvo en vigor la ley 675/96, ésta sufrió diversas modificaciones, que fueran efectuadas a través de dos decretos presidenciales y nueve decretos legislativos. En la opinión de Imperiali<sup>286</sup>, se trataran de una serie de normas algunas veces incoherentes, otras de naturaleza transitoria, que fueron sobreponiéndose en el tiempo, promulgadas debido a las exigencias consideradas, en su momento, primordiales. Por lo tanto, si por un lado estos cambios conferían una mayor aplicabilidad a la estructura legal sobre protección de datos, por otro causó una confusión y descentralización de la sistemática legislativa,

---

<sup>284</sup> En la valoración de Caldirola, la ley 675/96 fue una “norma experimental” y que el intento no era aquello de fijar una vez por todas la disciplina del tratamiento de los datos personales, sino de trazar los principios rectores y de comprobar la compatibilidad del sistema de garantías en ella definido, respeto a los distintos ámbitos sobre los cuales la ley afectaría. Además, a su juicio, añade que la peculiaridad de la ley delegada no estaba en el carácter integrativo y correctivo, más bien en el papel central confiado al *Garante* que debía ser oído en fase de preparación de los decretos legislativos, y la falta de una clara delimitación de la función delegada. En *Il Diritto... op. cit.*, p. 93.

<sup>285</sup> Vide sobre ese tema LUPPO, Nicola. “Le fonti della *privacy*”. En: CUFFARO, Vincenzo. *Il Codice... op. cit.* p. 785 y ss.; CASUCCI, Felice. *Tutela della privacy e misure di sicurezza dei dati personali*. Napoli: Edizioni Scientifiche Italiane, 2006, p. 16 y ss.

<sup>286</sup> IMPERIALI, Riccardo. *Codice... op. cit.*, p. 10.

ya que existían diversas reglamentaciones esparzas que trataban de la materia.

No obstante la fijación de un tiempo determinado para que fuesen concretizadas las alteraciones integrativas y correctivas de la norma principal, el legislador se utilizó de la edición de otras leyes que concedían aplazamientos del tiempo indicado originariamente por la 676/96, siendo que el último de estos estaba previsto en la ley 127/2001 y tenía como fecha final en 31 de diciembre de 2001.

Además de establecer el último plazo para la modificación del texto de la ley 675/96, la ley 127/2001 previa la adopción por parte del gobierno de un texto único con las disposiciones sobre la protección de las personas y de otros temas en relación al tratamiento de los datos personales, conteniendo aquellas normas conexas, coordinando las ya existentes, procediendo con las incorporaciones y modificaciones necesarias para garantizar su aplicación<sup>287</sup>. Según observa algunos sectores de la doctrina italiana<sup>288</sup>, dicha previsión legal no se refería a la confección de un instrumento meramente compilado de las leyes ya existentes, sino de un texto innovador.

De manera que se inicia una labor para reunir las normas que eran directamente relativas a la protección de datos personales o bien relacionadas a estas. Como destaca el informe parlamentario de acompañamiento del nuevo Texto Único<sup>289</sup>, el trabajo de unificar tales normas no era solamente un examen recopilatorio de las disposiciones

---

<sup>287</sup> Ley 127/2001, de 24 de marzo, artículo 1º, apartado 4.

<sup>288</sup> Vid. CIRILLO, Gianpiero Paolo. *La Tutela della Privacy nel Sistema del Nuovo Codice sulla Protezione dei Dati Personali*, Milan, CEDAM, 2004, p. 3; e IMPERIALI, Riccardo. *Codice... op. cit.*, p. 11;

<sup>289</sup> Disponible en

<http://www.privacy.it/codprivacyattiparl.html> . Acceso en 21 de diciembre de 2008.

vigentes, pero también de adecuación e intervenciones parciales de armonización de la norma reunida en uno solo texto, respetando las ponderación del Parlamento, los principios conexos, su ámbito de aplicación y la estructura de garantía derivada de la ley en aquél entonces vigente.

## **2. El Texto Único en materia de protección de datos personales italiano**

El denominado *Codice in Materia di Protezione dei Dati Personali*, tiene su germen, de hecho, en la ley 127/2001. En el mismo año de 2001, el Gobierno instituye una comisión de expertos presidida por el Prof. Cesare Massimo Bianca, responsable por redactar “el esquema del Texto Único, en los límites y según los principios de la delega parlamentaria<sup>290</sup>”.

Como bien señala Kirschen<sup>291</sup>, una labor de ésta envergadura iba a requerir un largo tiempo. Así, por esta razón, con la demora de la confección del Texto Único, se elaboró el Decreto Legislativo 28 diciembre 2001, nº 467, que daba aplicación a algunas disposiciones contenidas en la Ley nº 127/2001. El aludido Decreto, que entró en vigor en su totalidad el 1 de febrero 2002, simplificó diversos trámites para las empresas y para los sujetos públicos que trataban datos personales, aclarando algunos aspectos de la aplicación de la normativa, en particular en lo que respecta a la información de los interesados y la notificación de los tratamientos; además, como bien observa la autora, ha ampliado los poderes del

---

<sup>290</sup> IMPERIALLI, Riccardo. *Codice... op. cit.*, p. 5.

<sup>291</sup> KIRSCHEN, Sabina. *Il Codice... op. cit.* 10.

supervisor italiano para la protección de los datos personales (en adelante *Garante*) y reescrito en gran parte el aparato sancionador inicialmente previsto en la Ley nº 675/96.

Cumple resaltar aún que en este entretiempos de la constitución del grupo de expertos y la conclusión de su trabajo, hubo una modificación en la orientación administrativa de la simplificación normativa en algunos sectores del ordenamiento italiano. Es decir, con la llegada de la nueva Ley de *Semplificazione*<sup>292</sup>, el Parlamento opta por una solución diferente. Las leyes que antes eran aprobadas siguiendo la técnica de textos mixtos — que contenía juntamente normas primarias y secundarias —, a partir de entonces como subraya Imperiali<sup>293</sup>, han pasado a utilizar un sistema bipartido, donde el Texto Único é norma delegada con fuerza de ley, que viene seguido por reglamentos de ejecución. Por mejor decir, el Código tiene naturaleza de texto legislativo (norma primaria) que determina las reglas generales y las directrices fundamentales; de ello se derivan reglamentos (normas secundarias) en sectores específicos. Dicho Código en materia de protección de datos personales es el primero ejemplo de la nueva tendencia<sup>294</sup>.

Las ventajas de la adopción de un texto exclusivamente legislativo son acentuadas por Kirschen<sup>295</sup> para quien desde un punto de vista técnico jurídico, eliminando las distintas referencias a las disposiciones reglamentarias se ha asegurado una mayor "legibilidad" de las nuevas disposiciones, también reducidos considerablemente en número, además

---

<sup>292</sup> Ley n. 229, de 29 de julio de 2003. Sobre ese tema, vide el comentario de IMPERIALI, Riccardo. *Codice... op. cit.*, p. 4 y ss.; y LUPO, Nicola. *Le fonti... op. cit.*, p. 800 y ss.

<sup>293</sup> IMPERIALI, Riccardo. *Codice... op. cit.*, p. 6.

<sup>294</sup> KIRSCHEN, Sabina. *Il Codice... op. cit.*, p. 11.

<sup>295</sup> *Ibid.*, p. 11.

de una más sencilla articulación de las mismas, con los consiguientes beneficios en el plano sistemático.

Finalmente en el año de 2003 fue aprobado el Texto Único en materia de protección de datos y a través del Decreto ley nº 196 de 30 de junio, considerado por la doctrina como un instrumento flexible y a la vez completo<sup>296</sup>. Sobre este aspecto, Kirschen<sup>297</sup> remarca que por primera vez a nivel internacional viene un texto único redactado con todas las disposiciones legislativas y reglamentarias sobre protección de datos que unifica una materia caracterizada por su extrema transversalidad, capaz de influir sobre los más diversos sectores públicos y privados.

Con 186 artículos, el Código sobre protección de datos se divide en tres partes, a saber: la primera versa sobre los principios rectores, las disposiciones generales que se aplican a todos los tratamientos de datos personales, exceptuándose aquellos relativos a sectores particulares, que son objeto de disciplina particular; La segunda, como ya adelantado, se ocupa las normas que disciplinan los sectores como los datos sanitarios, los de solvencia patrimonial, tratamiento de datos con la finalidad estadística, histórica y científica, datos del ámbito judicial y de la fuerza policial, etc.; y la tercera que concierne a la tutela del interesado, contempla normas sobre los instrumentos jurídicos y administrativos puesto a su disposición, además del aparato sancionador.

Un gran progreso de la nueva legislación italiana fue englobar el contenido de las Directivas europeas 95/46/CE y 2002/58/CE, de la anterior ley de protección de datos, de los decretos y los reglamentos responsables por las modificaciones de la ley 675/96, de la jurisprudencia de los Tribunales y las decisiones del Garante — es decir, de los varios años de

---

<sup>296296</sup> CIRILLO, Gianpedro Paolo. *La Tutela... op. cit.*, p. 3. Vide, también, la observación de PIRAINO, Fabrizio. *Il codice... op.cit.*, p. 707 a 710.

<sup>297</sup> KIRSCHEN, Sabina. *Il Codice... op. cit.*, p. 12.

experiencia en tutela de los datos personales que separan las dos leyes sobre el tema. En definitiva, el Texto Único nace armonizando un cuadro normativo antes totalmente fragmentado<sup>298</sup>.

En la valoración de Imperiali<sup>299</sup>, lo que quiso el legislador fue hacerse cargo de las críticas a la normativa de *privacy* en sus primeros siete años de vida que se resumen en la complicación, en el retraso y en la ineficacia. Y es justamente ahí, para este autor, donde reside el carácter innovador y no sólo ordenador la nueva ley. Eso porque un texto puede limitarse a agrupar normas dispersas, o bien podrá, además de reagrupar, modificar e introducir normas nuevas y este último caso es el del Código, fruto de una doble exigencia: reorganización de una normativa que creció exageradamente y un primer balance, y nuevo inicio, después de siete años de aplicación e de experiencia.

### 3. La finalidad de la ley.

O artículo 2º del Código<sup>300</sup> se dedica a especificar la finalidad de la ley. Con un texto muy similar a la norma antecesora, este artículo garantiza

---

<sup>298</sup> Según destacan Cassano y Fadda, el Texto Único constituye el presupuesto necesario para conferir organicidad a una disciplina excesivamente fragmentada y para atribuir eficacia normativa a algunas indicaciones del *Garante* en el decorrer de casi diez años de actividad, hasta la promulgación del Código. CASSANO, Giuseppe, y FADDA, Stefano. *Codice... op.cit.*, p. 9.

<sup>299</sup> IMPERIALI, Riccardo. *Codice... op. cit.*, p. 11.

<sup>300</sup> Decreto legislativo 30 de junio de 2003, n. 196, *Codice in materia di protezione dei dati personal*, Artículo 2º, párrafo I: "Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti

que el tratamiento de los datos personales se desarrolle en el respeto de los derechos y libertades fundamentales, así como de la dignidad del interesado, con particular referencia a la *riservatezza*, a la identidad personal y al derecho a la protección de los datos personales.

La única, pero importantísima diferencia respecto a la ley 675/96<sup>301</sup> es que el nuevo Código hace una referencia genérica al interesado, eliminando los términos específicos que existía como personas físicas, jurídicas, ente y asociaciones. De modo que refuerza, así, la tutela a cualquier interesado los cuales sean sus datos sujetos a tratamiento. Aparte, por supuesto, de lo que ya se ha comentado en el capítulo anterior sobre la declaración específica del derecho a la protección de los datos personales de modo autónomo en el rol de los derechos especificados en el marco de su finalidad.

Otro aspecto que merece ser resaltado es el planteamiento de Vecchi<sup>302</sup>, respecto a los artículos en comento. Comparando los textos legales italianos – en vigencia y el derogado – con la normativa comunitaria 95/46, destaca el autor en cita, que mientras la atención del legislador comunitario se centraba sobre la garantía de la tutela de los derechos y de la libertad fundamentales, tocante a la protección de datos personales, dando particular relieve a la tutela de la vida privada, con una clara referencia al derecho a la *riservatezza*, el texto del Código italiano

---

e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali”.

<sup>301</sup> Ley 675/96, artículo 1º: “La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle **persone fisiche**, con particolare riferimento alla riservatezza e all'identità personale; garantisce altresì i diritti delle **persone giuridiche** e di ogni altro **ente o associazione**”. (Subrayamos)

<sup>302</sup> VECCHI, Paolo Maria. “Comentarios a los artículos 1º y 2º”. En: BIANCA, Cesare Massimo. *La protezione... op. cit.*, p. 3 y ss.



(inalterado respecto a la ley predecesora) contraponen algunas situaciones jurídicas subjetivas seguramente individualizadas, es decir los derechos, la libertad fundamentales y, ahora, el derecho a la protección de los datos personales, de los intereses no cualificados formalmente, o sea, la dignidad, la *riservatezza* y la identidad personal.

La preocupación de este autor era la de que si la dignidad de la persona tiene una segura relevancia jurídica en cuanto valor consagrado a nivel constitucional, y puede ser considerada en el mismo grado que los derechos y las libertades fundamentales, el problema aflora tocante a la *riservatezza* e identidad personal, que vienen tomándose en cuenta, al menos desde el punto de vista literal, no como objeto de derechos cuya protección debe ser garantizada por el Código, pero como intereses, aunque fundamentales de la persona que pueden estar implicados en tratamiento de datos personales.

Por todo ello, la duda sería de que como la ley de 1996 y también el Código no dieron lugar a un reconocimiento jurídico de los derechos a la *riservatezza* y a la identidad personal, así como individualizados por la jurisprudencia, pero les indica más bien como momentos en los cuales la protección de los derechos y las libertades fundamentales deben ser especialmente garantizada, sin con ello proteger el interés mediante el reconocimiento de especificaciones situaciones jurídicas subjetivas. Restaría saber de este modo si las lesiones al derecho a la *riservatezza* y a la identidad personal se detectarían sólo en cuanto puedan ser al mismo tiempo calificadas como una violación de derechos o libertades fundamentales consagrados por textos normativos o como atentados a la dignidad personal. Para superar tal dilema, se ha propuesto una lectura interpretativa conjunta entre los artículos 1º e 2º del Código, fundada, como resalta Viterbo<sup>303</sup>, sobre la previsión sistemática del artículo 2º y

---

<sup>303</sup> VITERBO, Francesco Giacomo. *Protezione dei dati personali e autonomia privata: profili di interferenza e di reciproca funzionalizzazione*. Napoli: Edizione Scientifiche Italiane, 2008, pp. 110-111, comentarios al pie de página.

dejando al artículo 1º el papel de un *incipit* declamatorio de todo el complejo normativo.

#### 4. El Código en Materia de protección de datos personales italiano y los Códigos de Buena Conducta.

Otra importante novedad del Código de protección de datos personales italiano es, como destaca Bianca<sup>304</sup>, el amplio espacio conferido a los códigos de deontológicos<sup>305</sup>, no obstante la ley de 1996 ya previera entre las atribuciones de la Agencia de Protección de Datos (*Garante*) la adopción de código de buena conducta para sectores específicos (art. 31, letra h). Ellos representan, en la valoración de Santaniello<sup>306</sup>, una nueva área de la instrumentación normativa y una nueva estructura del sistema de las fuentes de derecho. A su parecer, la flexibilidad que les caracterizan les dan la gran ventaja de que pueden ser fácilmente modificados, pues cada eventual cambio e integración de las normas no exige los largos tiempos de un complicado procedimiento de reforma legislativa; y por lo tanto son particularmente idóneos para disciplinar también materias que pasan por una fuerte dinámica innovadora como la de comunicaciones en línea y las incesantes innovaciones tecnológicas.

---

<sup>304</sup> BIANCA, Cesare Massimo. *La protezione... op. cit.*, p. XXVI.

<sup>305</sup> Vide SILEONI, Serena, SIMONCINI, Andrea. “I codici deontologici di buona condotta”. En: CUFFARO, Vincenzo. *Il Codice... op. cit.*, p. 812 y ss.

<sup>306</sup> SANTANIELLO, Giuseppe. “Le nuove garanzie nell'era del diritto alla protezione dei dati personali” [en línea]. Roma: Interlex. 07.10.04. <http://www.interlex.it/675/santaniello9.htm> [Consulta: 13 mar. 2009].

En el mismo sentido Piraino<sup>307</sup>, destaca que la casi totalidad de los autores que afrontaron la temática de la tutela de la persona frente a los tratamientos de datos de carácter personal ya habían alertado sobre las constantes mutaciones repentinas así como el progreso tecnológico que la suporta. Para este autor<sup>308</sup>, el problema no es sectorial, pero de amplio alcance porque invierte el tradicional desequilibrio que pasa entre la norma jurídica y la realidad social, que sin resquicio a duda es más aguda en los lugares donde en el curso de la historia resulta acelerado el ritmo de la innovación científica y tecnológica.

Es especialmente notable y demuestra la operatividad de los códigos de buena conducta son la confluencia de la participación de las categorías interesadas y del *Garante* para la emanación de normas de auto reglamentación, específicas y sectoriales, hasta entonces inexistentes<sup>309</sup>. Todo eso aporta una flexibilidad a la norma principal y por otro lado confiere a los códigos deontológicos los detalles importantes para la disciplina sobre el tema que tratan.

El artículo 12, párrafo 2º del nuevo *Codice* innova respecto a la antecesora norma al elevar la observancia a dichos códigos de buena conducta a condición esencial para la licitud del tratamiento de los datos. Así, aunque guarden una subordinación con otras normas dentro del ordenamiento jurídico, son ellos también fuentes de derecho, siendo una de las funciones del *Garante* verificar la compatibilidad entre estos códigos

---

<sup>307</sup> PIRAINO, Fabrizio. *Il codice... op. cit.*, p. 708.

<sup>308</sup> En el idioma original, este autor así registra: “Il problema non è però settoriale, ma di ben più vasta portata poiché investe la tradizionale discrasia che corre tra le norme giuridiche e la realtà sociale, che si rivela certo più acuta in quei luoghi in cui il corso della storia risulta accelerato dal ritmo impressogli dall’innovazione scientifica e tecnologica”. PIRAINO, Fabrizio. *Il codice... op. cit.*, p. 708.

<sup>309</sup> *Vid.* DEL NINNO, Alessandro. *Nuove... op. cit.*, p. 373.

y la ley. Por todo ello, “debe considerarse inaplicable las disposiciones de los códigos que son contrarias a las normas legales de orden superior”<sup>310</sup>.

En definitiva, la experiencia italiana con los códigos de buena conducta es la comprobación práctica de la necesidad de dinamizar y flexibilizar la tutela en tema de datos personales. El sistema creado por el ordenamiento de aquél país a través de la nueva sistemática legal introducida por el Código de protección de datos personales consiguió superar o por lo menos disminuir, hasta el presente momento, la diferencia entre el desarrollo tecnológico y las diversas maneras de que estos puedan lesionar los derechos individuales tocante al tratamiento de datos personales.

## **VI. Las definiciones generales en las leyes de protección de datos española e italiana.**

El *Codice* italiano y la Ley de Protección de Datos de Carácter Personal de España tiene una clara diferencia en lo que concierne a la estructura general de las definiciones. La norma italiana divide su artículo 4 en cuatro apartados, dedicándose en el primero a los conceptos generales. Ya el segundo cuida de las definiciones relativas a servicios de comunicación electrónica. Dicho apartado se hizo necesario, como señalan Cassano y Fadda<sup>311</sup>, por la imposición de coordinamiento del Código con las disposiciones que regula la materia en general y aquellas establecidas en el decreto legislativo nº 171 de 13 de mayo de 1998, sobre “*Disposiciones en*

---

<sup>310</sup> BIANCA, Cesare Massimo. *La protezione... op. cit.*, p. XXVII

<sup>311</sup> CASSANO, Giuseppe, y FADDA, Stefano. *Codice in materia... op. cit.*, p. 52.

*Materia de la tutela de la vida privada en el sector de las comunicaciones, en cumplimiento a la Directiva 97/66/CE del Parlamento Europeo y del Consejo, y en materia de la actividad periodística*”, ley esta derogada por dicho Código. Además, también por la necesidad de transposición de la Directiva 2002/58, de 12 de julio de 2002<sup>312</sup>, que se hizo oportuna la introducción de algunas definiciones, específicamente dedicadas a los servicios de comunicación electrónica, que complementan y acompañan las de alcance general.

El tercer párrafo se ocupa de aquellas definiciones concernientes a las medidas técnicas informáticas y de seguridad, y por último, el cuarto párrafo contempla las nociones respecto a las finalidades, contando de éste modo con más de treinta conceptos. En cambio, la LOPD se dedica únicamente a definiciones generales, ubicadas en el artículo 3 y las diez líneas siguientes.

El primer vocablo que aparece definido en el artículo 4 del Código italiano es el *tratamiento*. Esto no pasó desapercibido por la doctrina, como bien apunta Vecchi<sup>313</sup>, para quien ello la elección de ubicar la definición de tratamiento primero, relegando a de banco de datos en la sucesiva alinea p) del párrafo primero del artículo 4 encuentra plena justificación ya que el citado tratamiento parecer ser la noción central de toda la disciplina, pudiendo ser considerado el efectivo objeto, mientras que el hecho que los datos personales sean organizados en bases de datos resulta bastante secundario.

Diferentemente, la LOPD inicia sus definiciones por datos de carácter personal, lo que nos parece muy interesante elección, ya que desde el

---

<sup>312</sup> Relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

<sup>313</sup> VECCHI, Paolo Maria. “Comentario al artículo 4º”. En: BIANCA, Cesare Massimo. *La protezione... op. cit.*, p. 44.

primero momento se acota el objeto de la norma, se tiene en cuenta que no es el tratamiento de cualesquier datos que serán su objeto, pero solamente aquellos que tengan la especial característica de ser *personales*. El reglamento de desarrollo de esta ley amplia de manera significativa las definiciones, además de mejorar y especificar las que ya se encontraban en la Ley 15/1999. De hecho, todas las definiciones contenidas en el apartado 2 del artículo 5, que son aquellas referentes al título VIII del reglamento (Las medidas de seguridad en el tratamiento de datos de carácter personal), no existían en la LOPD, además de añadir otras figuras como el exportador (apartado 1 línea j. del artículo 5) y el importador (apartado 1, línea ñ. del artículo 5) de datos personales.

## 1. Datos de carácter personal.

### 1.1. Concepto y características en la LOPD.

La Ley Orgánica de Protección de Datos, nº 15/1999, conceptúa datos de carácter personal como *cualquier información concerniente a personas físicas identificadas o identificables*. Es interesante subrayar la similitud entre esta definición y la del Convenio 108. Así mismo, la Directiva 95/46 CE, en la misma línea del Convenio, añade que *se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*. El Reglamento de desarrollo de la LOPD especifica el concepto “cualquier información” añadiendo que esta puede ser numérica, alfabética, gráfica, fonográfica, acústica o de cualquier otro tipo.

Parece oportuno resaltar la diferencia que hace Davara Rodríguez<sup>314</sup> entre datos, información e informática. El autor en cita parte de la hipótesis de que si por dato se entiende “el antecedente o noticia cierta que sirve de punto de partida para la investigación de la verdad y aceptamos que ese datos se encuentran en un documento o soporte — físico o lógico — con la calidad de testimonio, debemos distinguirlo de información, entendiendo por tal acción de informar o dar noticia de alguna cosa”, de modo que así comprendido, en su valoración, sería difícil que el dato por sí solo cause una grande o grave incidencia en la privacidad. Desde la perspectiva del autor, solamente se convierte un dato en información cuando éste da respuesta a una consulta determinada, o sirve a un fin. Por lo tanto, concluye que información sería el resultado orientado a un fin determinado. E informática, conceptúa el autor, como el tratamiento automático de la información.

Convendría con respecto a este punto hacer la siguiente pregunta: ¿se puede afirmar que los datos por si solo efectivamente no son hábiles a violar el principio de la autodeterminación informativa? En este debate no nos parece oportuno discutir si pueden ser medios a operar intromisiones ilegítimas en los derechos de intimidad (o mismo privacidad), porque en materia de protección de datos, como tuvimos oportunidad de manifestarnos en el capítulo anterior, entendemos que el derecho que está en evidencia es la libertad informática. De modo que no habrá injerencia en los derechos a la intimidad, al honor o mismo a la imagen, si antes, o a la vez, no hubiere existido violación a la autodeterminación informativa del individuo.

En la definición somera y de uso actual de los científicos informáticos resaltada por TANG, XI, e YOU<sup>315</sup>, datos son símbolos sin procesos

---

<sup>314</sup> DAVARA RODRÍGUEZ, Miguel Angel. *La Protección de Datos en Europa*. Madrid: Editorial Grupo Asnef Equifax, 1998, p. 15.

<sup>315</sup> TANG, Deyou; XI, Jianqing; YOU, Jinguo [et. al.]. “Data Evolution and Its Modeling” [en línea]. En IEEE Computer Society. *Proceedings of the 2008 Fifth international*

derivados. Añaden aún, los autores en cita, que su concepto implica: que éstos son sólo una combinación de símbolos adecuados para el tratamiento por ordenador, sin capacidades interactivas; que la semántica de los datos se limita al significado de la información, es decir, los datos son la abstracción de los contenidos de la información sin un proceso de derivación y, finalmente, que la semántica de los datos se mantiene inalterada a menos que se cambie la combinación de los símbolos. Para Setzer<sup>316</sup>, datos son una secuencia de símbolos cuantificados y cuantificables, que pueden ser descritos a través de representaciones formales o los “bloques de construcción de la información”<sup>317</sup>. Ya las informaciones serían el producto de los datos procesados, revelando el significado de los datos<sup>318</sup>. La distinción fundamental entre uno y otro, como apunta Setzer, es que el dato es puramente sintáctico, mientras la información contiene necesariamente la semántica.

Ahora bien, partiendo de estas definiciones, datos son el continente limitado por su propio contenido que son las informaciones. Aunque éstas solo podrán ser comprensibles una vez sean los datos procesados por el ordenador. De ésta manera, aunque la composición de los datos sea una combinación de símbolos, esta guarda una “abstracción de la información”. De hecho, aún considerados aisladamente, éstos no pierden sus características de modo que si no fueron modificados, deteriorados,

---

*Conference on Fuzzy Systems and Knowledge Discovery Volume 05* (18-20 Octubre 2008). Washington: 2008. [Consulta en 19 oct. 2008].

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4666596&isnumber=4666476> .

<sup>316</sup> SETZER, Valdemar W. “Dado, Informação, Conhecimento e Competência” [en línea]. Disponible en

<http://www.ime.usp.br/%7Evwsetzer/dado-info.html> . [Consulta en 14 set 2009].

<sup>317</sup> PETER, Rob; CORONEL, Carlos. *Sistemas de bases de datos: diseño, implementación y administración*. México D.F.: Thomson Editores, 2004, p. 7.

<sup>318</sup> *Ibid.*, p. 7.



cancelados o borrados, estarán aptos a descodificar la información que guardan.

Por lo tanto, desde que adecuados para el procesamiento y para su transferencia, nos parece que los datos pueden incidir en el derecho a la autodeterminación informativa. Una vez reducida la información a datos, estos podrán traficar entre diversas base de datos, estando a cualquier momento la información susceptible de ser traducida. En efecto, lo que no tiene la capacidad de generar alguna violación al derecho a la autodeterminación informativa son informaciones fuera de contexto<sup>319</sup>. No datos. Cabe destacar que, como advierte Serrano Pérez<sup>320</sup>, toda información puede convertirse en delicada a depender del contexto de su uso. Además, la legislación no especifica *numerus clausus* los datos que estarán sobre su tutela. Al optar por un sistema más abierto a interpretaciones, la ley se flexibiliza, tornándose siempre actual, permitiendo adaptarse a posibles y, porque no decir, inminentes cambios debido a evolución tecnológica.

El concepto de la LOPD de datos personales desde nuestro punto de vista es en realidad la definición de información. Es decir, para que sean considerados como personales, ya han pasado por el procesamiento. Pero del mismo modo que los datos se transforman en información, ésta igualmente vuelve a ser un dato después de utilizada.

De lo que se extrae del contenido legal, para que el dato sea considerado como “de carácter personal”, debe de reunir tres elementos que: la generalidad de la información, una persona física y la conexión

---

<sup>319</sup> Para DRUMOND, “...en cuanto información aislada, un dato (puesto que está fuera de contexto) no significa nada. Acaba por ser un elemento único de información inoperante, no siendo suficiente, por lo tanto, para permitir cualquier identificación relevante”. DRUMOND, Victor. *Internet, Privacidad y Datos Personales*, Madrid: Reus, 2004, p. 50.

<sup>320</sup> SERRANO PÉREZ, Maria Mercedes. *El Derecho... op. cit.*, p. 379.

entre el contenido de la información y la persona a que se refiere. De modo que la primera característica destacable de los *datos personales* es la generalidad. **Toda**, como pretende la Directiva, o **cualquier** información, como en los textos del Convenio y de la LOPD, pueden ser de “carácter personal”, de modo que, *a priori*, ninguna información será desconsiderada.

Estas normas parten del principio de que cualquier información puede ser objeto de su protección. Ahora bien, la “generalidad” legal de los datos está delimitada por otros dos elementos que, complementando este último, componen la adjetivación de “carácter personal”, que son la **conexión** y una **persona física**. Es importante subrayar que en dicha correlación es necesario que exista el reconocimiento individualizado de la persona. Por mejor decir, las informaciones que contienen el dato deben ser suficientes para identificar a un sujeto o que permitan tal posibilidad<sup>321</sup>. Añade Freixas Gutiérrez<sup>322</sup> que no se podrá obtener un concepto de dato personal disociándolo del concepto de identificación del afectado cuando de una manera individualizada o coordinados entre sí puedan dar un perfil concreto, identificando a alguien. Siguiendo ese mismo raciocinio, Aparicio Salom<sup>323</sup> considera que si el dato de carácter personal constituye siempre información relativa a personas físicas, cabe entender que para que sea de carácter personal es preciso que existan dos elementos: la información y la persona a la que concierne dicha información. En el supuesto que no concurren ambas circunstancias habrá que entender que no se trata de datos de carácter personal.

---

<sup>321</sup> MESSIAS DE LA CERDA BALLESTROS, Jesus Alberto. *La Cesión o Comunicación de Datos de Carácter Personal*, Madrid: Civitas, 2003, p. 30.

<sup>322</sup> FREIXAS GUTIERREZ, Gabriel. *La protección... op. cit.*, p. 120.

<sup>323</sup> APARICIO SALOM, Javier. *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Navarra: Aranzadi, 2000, p. 43.

Por lo tanto, su destinatario es el afectado siempre y cuando este pueda ser identificado a través del tratamiento que se dé a los datos. Pretende la ley, en virtud de lo dicho anteriormente, por un lado establecer una protección preventiva evitando que se trace perfiles de determinados aspectos de la vida personal de los afectados, como en los casos de los datos sensibles<sup>324</sup>, y por otro, en los casos que sea posible tal identificación, prevé los límites que ha entendido el legislador necesarios y suficientes para resguardar los derechos de los afectados. Ante dicha perspectiva, la ausencia de un elemento identificador que lo interrelacione con una persona, directa o indirectamente, no se reconoce el dato como de “carácter personal”<sup>325</sup>.

Nos parece importante señalar, el posicionamiento del Tribunal Supremo, en Sentencia de 31 de octubre de 2000<sup>326</sup> en el cual diferencia el “dato personal” de “datos de carácter personal”, clasificando estos últimos en tres: a) “*strictu sensu*” que son los existenciales que pueden ser asociados a una persona determinada o determinable (nacimiento, muerte, matrimonio, domicilio y análogos), los datos referentes a la actividad profesional, al patrimonio, a la pertenencia a una confesión religiosa, a un partido político, las enfermedades, etc.; b) la “información sobre las condiciones materiales”; y c) evaluaciones y apreciaciones que puedan figurar en el fichero y que hagan referencia al afectado. Así, los datos personales serían una especie del género “datos de carácter personal”. Tal postura del Tribunal fortalece la interpretación amplia, siempre considerando no la naturaleza del dato, sino su capacidad de identificación.

---

<sup>324</sup> Sobre ese tipo de datos, vid. SERRANO PÉREZ, María Mercedes. *El Derecho... op. cit.*, pp. 377-341.

<sup>325</sup> O como prefiere Vizcaíno Calderón, “... entendida dicha relación no como necesaria identificación actual sino como una posibilidad real de identificación”. VIZCAÍNO CALDERÓN, Miguel. *Comentarios... op. cit.*, p. 72.

<sup>326</sup> STS, Recurso de casación n. 6188/1996.

Según La Directiva 95/46/CE, en su considerando 26, tocante a como determinar si una persona es identificable o no, recomienda que para ello sea considerado el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o cualquier otra persona para distinguir a alguien. Efectivamente, solamente a través del análisis individualizado del conjunto de datos utilizado es que se podrá saber si dicha persona es identificable. Ahora bien, entendiéndose identificable (o indentificabilidad), en la lección de Vizcaíno Calderón<sup>327</sup>, “como la posibilidad de ser atribuido o imputado cualquiera de los aspectos de la personalidad descritos en la norma”.

Otra novedad que trajo el Reglamento fue la inclusión de dato disociado y datos de carácter personal relacionados con la salud en la lista de definiciones. El primero es descrito como aquél que no permite identificación de un afectado o interesado; el segundo son aquellas informaciones sobre la salud física o mental de un individuo no importando para la ley la cuestión temporal, es decir, si se refieren al pasado, presente o futuro del interesado. Añade también que aquellos datos que se refieran a su porcentaje de discapacidad y a su información genética también se consideran como tales.

## 1.2. Concepto y características de dato personal en el *Codice in materia di protezione dei dati personali*

El artículo 4, párrafo 1, alinea b define *dato personal* como cualquier información relativa a persona física, persona jurídica, ente o asociación, identificada o identificable, también indirectamente, a través de referencia

---

<sup>327</sup> VIZCAÍNO CALDERÓN, Miguel. *Comentarios... op. cit.*, p. 73.

a cualquier otra información, ahí incluido un número de identificación personal.

Como se puede percibir, la expresión *cualquier información* también está presente en el precepto del Código italiano. El *Garante*<sup>328</sup> señaló que ello quiere atribuir a la definición de "dato personal" la máxima amplitud, incluyendo también cualquier noticia, información o elemento que tenga una eficacia informativa que aportar, es decir una contribución adicional de conocimiento respecto a un sujeto identificado o identificable.

A diferencia de la LOPD, en la estructura jurídica de protección de datos italiana, los entes, asociaciones y personas jurídicas también están tutelados por su disciplina. Cumple resaltar que el precepto no hace ninguna diferencia entre la persona jurídica de derecho público o privado. Todo ello, sin ninguna duda, genera una serie de interrogantes sobre la teoría general de los derechos humanos o fundamentales y su titularidad, de naturaleza jurídico-formal, técnica y también de conceptual que por su complejidad sería imposible en el marco de esta investigación un estudio más profundado.

No obstante tal ponderación, a nuestro parecer, es una opción bastante notable del legislador italiano. Primero porque se la propuesta legislativa era de un texto único, que se denomina *Código*, que nada más es que un conjunto normativo sobre una determinada materia, éste debe preocuparse con todos los aspectos a ella concernientes. Ahora bien, tocante a la posibilidad de personas jurídicas ser titulares de derechos fundamentales, es un tema que causa mucha divergencia doctrinal. De hecho, analizando en el sistema constitucional español, algunos autores

---

<sup>328</sup> Garante per le Protezione dei Dati Personali, *Bolletino* nº 9, 34, de 2 de junio de 1999 (Doc. Web. nº 40261), disponible en

[www.garanteprivacy.it](http://www.garanteprivacy.it).

como Díez Picazo<sup>329</sup>, alertan para la dificultad en encontrar una respuesta en la Constitución de España al cuestionamiento de la posibilidad de las personas jurídicas ostentaren derechos fundamentales, diferentemente de la Ley Fundamental Alema que hace referencia directa a la extensión de los derechos fundamentales a las personas jurídicas nacionales que según su respectiva naturaleza les sean aplicables.

En efecto, la concepción originaria de los derechos fundamentales nos remite a la idea de que estos son destinados a los individuos, a las personas que los posee por el mero hecho de serlos. Es decir, es una concepción innata del ser humano<sup>330</sup>. Dado esto por sentado, el problema que surge en la afirmación de la posibilidad de personas jurídicas ser titulares de estos derechos, diagnosticado por Díez-Picazo, es que ello conllevaría a una extensión o ampliación de la originaria razón de ser de estos derechos. Sin embargo, el autor en cita plantea algunos argumentos a favor de ésta extensión. El primero sería vislumbrarlos desde una concepción institucional, o sea, dichos derechos también dan vida “a un orden objetivo de valores cuya efectividad debe ser asegurada por todos los poderes del Estado”, y siguiendo el precepto alemán, algunos bienes jurídicos de los derechos fundamentales no solamente son predicables a los seres humanos pero también merecen protección respecto de las personas jurídicas. Otro razonamiento expuesto por el autor es la visión de que la consideración de la persona jurídica como una entidad instrumental que usan los seres humanos para lograren determinados

---

<sup>329</sup> DÍEZ-PICAZO, Luis Maria. *Sistema de Derechos Fundamentales*, Madrid: Thomson/Civitas, 2008, p. 141.

<sup>330</sup> Según el concepto fornecido por Naciones Unidas, “los derechos humanos son derechos inherentes a todos los seres humanos, sin distinción alguna de nacionalidad, lugar de residencia, sexo, origen nacional o étnico, color, religión, lengua, o cualquier otra condición”. In

<http://www.ohchr.org/SP/Issues/Pages/WhatareHumanRights.aspx> , acceso en 20 de julio de 2009.

fines<sup>331</sup>. No obstante estos fundamentos, lo que siempre hay que llevarse en cuenta en el tema de la titularidad de los derechos fundamentales a las personas jurídicas es la reflexión ya citada, inscrita en la Constitución Alemana de que dicha extensión solo se concretizan en la medida en que les sean aplicables considerando siempre su respectiva naturaleza.

Tocante a las personas jurídicas públicas, algunos comentarios merecen atención. La historia del surgimiento de los derechos fundamentales está marcada por la constante “hombre *versus* Estado”. Resulta repetitivo afirmar que en la historia siempre que el individuo se revelaba contra las amenazas del gigante estatal a si mismo, considerado como persona, surgiendo una nuevas declaraciones de derechos, formando sus generaciones. Así que el carácter de persona jurídica no es tan problemático como su condición de *público*. De suerte que la titularidad de los derechos fundamentales por las personas jurídicas publicas es un planteamiento que en la doctrina todavía no hay unidad. Como bien apunta Díez-Picazo<sup>332</sup>, “en la lógica profunda de los derechos fundamentales, está la convicción de que entre gobernantes y gobernados existe, por definición, una situación de desequilibrio a favor de los primeros, por lo que los segundos han de ser compensados con especiales garantías”. El citado autor continúa su planteamiento afirmando que si ello es así, desde su perspectiva no tiene sentido sostener que los entes públicos han de estar protegidos por garantías similares a las de los particulares, por mucho que se aprecien los méritos de la dimensión constitucional.

---

<sup>331</sup> DÍEZ-PICAZO, Luis Maria. *Sistema... op. cit.*, pp. 141-142.

<sup>332</sup> *Ibid.*, p. 143.

De otra parte, según el planteamiento de Dabove<sup>333</sup>, lo nuevo del cuestionamiento sobre la titularidad de los derechos fundamentales por las personas jurídicas no parte de la esfera privatista del concepto de persona sino de su *dimensión pública*. Para la autora en cita, la osadía filosófica de la postmodernidad consiste en saber si las personas jurídicas públicas, pueden ser titulares de derechos "humanos" y en qué medida pueden serlo efectivamente. Concluyendo su trabajo, deja a entender la autora que sí es posible que algunos derechos fundamentales sean ejercidos por personas jurídicas públicas, siempre dependiendo de una interpretación casuística, ya que en estos casos ocurriría lo mismo supuesto de las personas jurídicas privadas, es decir, hasta donde lo permita la concepción jurídica y política de los derechos humanos de que se trate. Además la autora cita algunas sentencias del Tribunal Constitucional español en las cuales a su sentir fueron analizados y admitidos los de derechos fundamentales ejercidos por personas jurídicas públicas<sup>334</sup>, aunque sostiene que la lista puede incluso llegar a ampliarse, pese a que es un catalogo mucho más limitado que las de personas jurídicas privadas.

Desde la perspectiva de la autora citada, actualmente existe una preocupación con las personas jurídicas publicas porque quizás la duda gire en torno la fuerza o debilidad real que existe detrás del concepto de soberanía estatal, complementando que "tal vez este interrogante no sea

---

<sup>333</sup> DABOVE, Maria Isolina. "Personas Jurídicas Publicas: ¿Titulares de Derechos Humanos? Algunas reflexiones desde la Filosofía del Derecho en España" [en línea], disponible en

<http://www.cartapacio.edu.ar/ojs/index.php/iyd/article/view/770/575> , [Consulta en 20 jul. de 2009].

<sup>334</sup> Entre ellos el derecho de tutela judicial efectiva, los derechos derivados de la actuación de la Administración en forma privada, los derechos de las Corporaciones de Derecho Público, Colegios, Cámaras, Universidades además de la igualdad ante la ley y el derecho a la autonomía universitaria.



más que otro indicio de la transformación que se está operando en el seno internacional y comunitario, acerca de la concepción misma del Estado”.

De todo ello, a nuestro parecer, entendemos que no hay ningún obstáculo para que las personas jurídicas privadas puedan gozar de la protección de los datos que les conciernen, extendiéndose por supuesto, a lo que sea aplicable de acuerdo con su naturaleza, lo que no quiere decir que deba necesariamente ser ubicada dicha protección, en el caso de España, en la LOPD. No obstante, en lo que concierne a las personas jurídicas de carácter público, a nuestro juicio, es absolutamente impracticable. El complejo de principios administrativos que las envuelven funcionarán como obstáculo al ejercicio de un derecho a la protección de datos tal y como se entiende en la normativa comunitaria, internacional y nacional. La esencia de la Administración Pública es la transparencia, y la convivencia de este principio con la protección de datos resulta antagónica.

Ahora bien, el hecho de que sea contra la naturaleza de la persona jurídica pública el goce de un derecho como el de la protección de datos ello no es un obstáculo a que se confiera dentro de la normativa de protección de datos un tratamiento normativo diferenciado respecto a otras personas jurídicas cuando su posición legal sea la del sujeto activo, es decir, en los supuestos en que actúan como titulares o responsables de ficheros de datos de carácter personal.

Dicho esto, analizando el específico caso de Italia, nos encontramos con algunas dificultades interpretativas. Por un lado, el artículo 1º declara que **cualquiera** tiene derecho a la protección de datos personales que le conciernan. Después, en la definición de datos personales incluye las personas físicas y jurídicas, los entes y las asociaciones sin expresar claramente la Administración Pública. Luego, en el mismo artículo 4, alineas *f)* y *g)*, al definir los titulares y los responsables por el fichero

declara pormenorizadamente que estos pueden ser las personas físicas y jurídicas, los entes, las asociaciones y la Administración Pública.

Para Cassano y Fadda<sup>335</sup>, la palabra *cualquiera* debe ser interpretada teniendo en cuenta el contexto general de la ley en la cual es utilizada y por lo tanto, en el caso del Código, esa se refiere tanto a las personas físicas como las personas jurídicas. No obstante, añade los autores en cita, que no os parece que sea posible ampliar su alcance a incluir también la Administración pública.

De otra parte, Giofrè<sup>336</sup>, entiende que la norma italiana, diferentemente de la Directiva 95/46, no limita la definición de datos personales a las personas, sino se ha extendido a las personas jurídicas, entidades, asociaciones, por lo que en el ordenamiento jurídico italiano es cualquier información personal que se refiere a instituciones, asociaciones y a la Administración pública. A su sentir, la dirección del Ministerio del Interior, por ejemplo, “es un dato personal y de confidencial no hay nada, todos lo saben, todos lo pueden saber; sin embargo es un dato personal”.

En nuestra opinión, la ausencia de la Administración pública en el rol de los interesados y en la definición de dato personal no fue involuntaria o fruto del olvido legal. Hubiera deseado proteger los datos personales de los organismos públicos, la ley lo habría hecho como lo hace con los entes y asociaciones, y también en los demás dispositivos. Seguimos pensando que proteger datos de la Administración es exactamente el opuesto de lo que se exige del Estado en una sociedad democrática que es la transparencia.

---

<sup>335</sup> CASSANO, Giuseppe, y FADDA, Stefano. *Codice... op.cit.*, p. 40.

<sup>336</sup> GIOFRÈ, Giovanni. “La privacy nella Pubblica Amministrazione e la sua tutela” [En línea], disponible en

<http://www.diritto.it/art.php?file=/archivio/26450.html> , [Consulta en 03 feb. de 2009].

La definición de dato personal en el nuevo Código es idéntica a la ley derogada. Como se puede observar, el concepto de dato personal es muy amplio, según lo que observa Melchionna<sup>337</sup>, incluye cualquier información que pueda derivar de datos alfanuméricos, imágenes, sonidos independientemente del soporte que les contiene (carta, videocasete) y la forma en que se utilizarán (informaciones numéricas, digitales). Para Cassano y Fadda<sup>338</sup>, la importancia de la definición de dato personal es no solamente contribuir en la individualización del ámbito de aplicación normativo pero también sobre otro perfil, en cuanto se refiere a una multiplicidad de casos en los cuales la aplicación del Código puede ser dubitativa.

El legislador, al conceptualizar datos personales incluyó también en las alineas subsecuentes la definición de “datos de identificación”, que son aquellos que permiten la identificación directa de los sujetos. Para Melchionna<sup>339</sup>, dicha previsión no se radica en la voluntad de dictar una peculiar disciplina para estas informaciones, sino en mejor aclarar que deben ser considerados como datos personales también aquellos que no identifican de forma directa el interesado y que, subsistiendo distintas tipologías de información, el titular debe preferir las que sólo proporcionan los elementos estrictamente necesarios a alcanzar la finalidad de recabo.

Además, así como la norma española y en la Directiva, inserta en su texto la noción de datos sensibles precisando que son aquellos que permite la divulgación del origen racial o étnico, las creencia religiosas, filosóficas o de otro tipo, opiniones políticas, afiliación a partidos, sindicatos, asociaciones u organizaciones de carácter religioso, sindicalista

---

<sup>337</sup> MELCHIONNA, Silvia. *I principi...*, op. cit., p. 38.

<sup>338</sup> CASSANO, Giuseppe, y FADDA, Stefano. *Codice... op.cit.*, p. 54.

<sup>339</sup> MELCHIONNA, Silvia. *I principi...*, op. cit., p. 39.

filosófico, político o sindical, así como los datos personales que revelan la salud y la vida sexual del individuo.

Asimismo, incluye la ley los “datos judiciales”, confiriéndole una definición más bien técnica, que no permite mayores dilaciones, siendo aquellos capaces de revelar, como bien sintetiza Resta<sup>340</sup>, las medidas inscritas en los antecedentes penales; las sanciones administrativas dependientes de delito y relativos cargos pendientes; los datos personales que pueden detectar la calidad del investigado o imputado. Están excluidas de esta definición las informaciones relativas a medidas civiles o administrativas no relacionados con delitos.

## **2. Tratamiento de datos personales.**

### **2.1. La noción de tratamiento de datos personales en la LOPD.**

A tenor del artículo 3 línea c) de la LOPD, tratamiento consiste en las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. El reglamento 1720/2007 añade a la lista de actividades que compone el tratamiento la elaboración, modificación, consulta, utilización, o supresión de los datos personales.

---

<sup>340</sup> RESTA, Fabio di. *Protezione delle informazioni: privacy e sicurezza*. Torino: G. Giappichelli, 2008, p. 23.

E efecto, el Reglamento de desarrollo se acercó más a la Directiva 95/46. El concepto de tratamiento es muy amplio y algunas veces puede involucrar otros términos que viene definidos en la ley. Es el caso de fichero, recogida e incluso cesión, como bien advierte Vizcaíno Calderón<sup>341</sup>. Acentúa Freixas Gutiérrez<sup>342</sup>, que dicho concepto incluye todas las actuaciones técnicas necesarias tanto con la utilización de los datos como las que conciernen a los derechos del ciudadano como es el caso del bloqueo o cancelación.

## 2.2. La noción de tratamiento de datos personales en el *Codice in materia di protezione dei dati personali*.

El tratamiento es el término que inaugura el artículo 4, del Código italiano de protección de datos, que se ocupa de las definiciones. La norma citada, le conceptúa como cualquier operación o conjunto de operaciones, efectuadas incluso sin ayuda de instrumentos electrónicos, relativas a la recogida, el registro, la organización, la conservación, la consulta, la elaboración, la modificación, la selección, la extracción, la comparación, la utilización, la interconexión, el bloqueo, la comunicación, la difusión, la cancelación y la destrucción de datos, incluso si no registrados en un banco de datos. Como se puede notar, la definición es muy semejante a de la Directiva Comunitaria 95/46, apenas suprimiendo que todo el rol de las actividades es aplicada a los datos personales. Sin

---

<sup>341</sup> VIZCAÍNO CALDERÓN, Miguel. *Comentarios... op. cit.*, pp. 77-78.

<sup>342</sup> FREIXAS GUTIERREZ, Gabriel. *La protección... op. cit.*, p. 121.

embargo, es un concepto muy amplio, y según Vecchi<sup>343</sup>, la absoluta generalidad de la previsión normativa permite considerar la lista de las actividades sobre los datos personales meramente ejemplificativa.

Este autor, aún advierte que por lo que respecta al enfoque general del Código, la amplitud de la finalidad de la tutela que se propone a aplicar no permite excluir que un acción aislada que tenga por objeto datos personales pueda ser considerado tratamiento, de lo contrario sucedería la disminución de toda la previsión legal para éste, dando lugar a claras incongruencias<sup>344</sup>. Además, en su opinión<sup>345</sup>, concluye que la interpretación más fiel al texto legal esaquella “que identifica un tratamiento de datos personales en cada operación, aunque aislada, que tenga por objeto información sobre personas físicas o jurídicas idónea a constituirse, precisamente, en un dato personal”.

El Título III del Código se ocupa en disciplinar los principios generales para el tratamiento de datos, dividiéndose en: reglas generales para todos los tipos de tratamientos (Capítulo I), reglas suplementarias para los sujetos públicos (Capítulo II) y, finalmente, reglas adicionales para los sujetos privados y entes públicos económicos (Capítulo III).

A tenor del artículo 11, en lo que respecta a la modalidad de tratamiento y de los requisitos de los datos, estos deben ser tratados de modo lícito (principio de la buena fe), recabados y registrados para finalidad determinada, explícita y legítima y si utilizados en otras operaciones de tratamiento en términos que sean compatibles con tales fines (principio de la finalidad). Deben también ser exactos y, si fuera necesario, actualizados (principio de la exactitud), además de pertinentes,

---

<sup>343</sup> VECCHI, Paolo Maria. “Comentario al artículo 4º”. En: BIANCA, Cesare Massimo. *La protezione ... op. cit.*, p. 44.

<sup>344</sup> *Ibid.*, pp. 49-50.

<sup>345</sup> *Ibid.*, p. 50.

completos y no excesivos con relación a la finalidad para las cuales son recogidos o tratados posteriormente (principio de la pertinencia) y, finalmente, deberán ser conservados de manera que permita la identificación del interesado por un período de tiempo no superior a lo necesario para los fines para los cuales fueron recogidos o posteriormente tratados (principio de la conservación de los datos).

Es importante añadir que el artículo 13, párrafo 1, dispone que son presupuestos de licitud de tratamiento de datos que el interesado, o la persona ante la que se recogen los datos personales, sea previamente informado de manera verbal o escrita respecto a la finalidad y las modalidades de tratamiento que se destinan los datos; a la naturaleza obligatoria o facultativa de cederlos; a las consecuencias de un eventual rechazo de responder; a los sujetos o las categorías de sujetos a los cuales los datos personales pueden ser comunicados o que pueden tener conocimiento en calidad de responsables o encargados, y el ámbito de difusión de estos datos; y, por fin, informar de los derechos del afectado contemplados en el artículo 7 del Código. Asimismo, la observancia a los Códigos de Buena Conducta, según el artículo 12, párrafo 3 constituye condición esencial para la licitud y exactitud del tratamiento de datos personales efectuado por sujetos privados y públicos. No obstante todo ello, según lo que consta del párrafo 2, del mismo artículo 13 en la notificación al afectado se puede dejar de incluir elementos ya conocidos por este, así como aquellas informaciones cuyo conocimiento puede obstaculizar el cumplimiento, por parte de un sujeto público, de funciones de inspección o de control llevadas a cabo para fines de defensa o seguridad del Estado, o de prevención, detección y represión de delitos.

En el caso de que los datos personales no hayan sido suministrados directamente por el interesado, el párrafo 4 del artículo en cita establece que éste deberá ser informado sobre la existencia y tipología de los datos tratados en el momento de sus registros, pero en el supuesto de que estuviere prevista la comunicación de los mismos, le deberá ser notificado

en la primera comunicación y no en las posteriores. Esta regla, no obstante, no se aplica cuando: a) los datos son tratados según una obligación prevista por la ley, por un reglamento o por la normativa comunitaria; b) para la finalidad de desarrollo de una investigación de defensa, a cual se refiere la ley nº 3977 de diciembre de 2000, o para hacer cumplir o defender un derecho en juicio, siempre que los datos sean tratados exclusivamente para tal finalidad y por el periodo estrictamente necesario para ello c) la notificación al interesado implica un uso de medios que el *Garante*, al determinar eventualmente las medidas apropiadas, declare manifiestamente desproporcionadas en relación al derecho protegido, o se revela imposible, a juicio del *Garante* (párrafo 5 del artículo 13).

El Código igualmente prohíbe que los actos o disposiciones judiciales o administrativas que impliquen una evaluación del comportamiento humano no podrá ser basado únicamente en un tratamiento automatizado de datos personales destinados a definir el perfil o la personalidad del interesado, siendo conferido a éste oponerse a cualquier otro tipo de decisión adoptada sobre la base del tratamiento mencionado, salvo que esta haya sido adoptada en ocasión de la celebración o de la ejecución de un contrato, en aceptación de una propuesta del interesado, o sobre la base de las garantías adecuadas establecidas por el presente código o por una disposición del *Garante* en virtud del artículo 17, que trata de los datos que presentan riesgos específicos<sup>346</sup>.

En lo que concierne a los daños causado por el tratamiento de datos, el Código determina la obligación de aquél que lo produjo de resarcirlo conforme el artículo 2.050 del Código civil, asimismo el daño no patrimonial es resarcible también en caso de violación de los principios

---

<sup>346</sup> El artículo 17 prevé que el *Garante* sea responsable en trazar las medidas y disposiciones para el tratamiento de datos que presentan riesgos específicos.



generales para el tratamiento de los datos, ubicados en el artículo 11 del *Codice in Materia de Protezione dei dati personali*.

Cuando se opere el cese del tratamiento de los datos personales, por cualquier causa, la norma establece cuatro hipótesis de destinación de los mismos, siendo estas: la destrucción de estos datos, la cesión a otro titular, siempre que el tratamiento sea destinado a las finalidades compatibles por las cuales fueron recabados; conservarlos para fines exclusivamente personales y no destinados a una comunicación sistemática o difusión; o entonces conservarlos o cederlos a otro titular para finalidades estadísticas o científicas, de acuerdo con la ley, el reglamento, a la normativa comunitaria y a los códigos de buena conducta.

### **3. Fichero.**

#### 3.1. El concepto de fichero en la LOPD.

La LOPD, en su artículo 3, apartado *b)*, define fichero como todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. En la Directiva 95/46/CE se conceptúa como todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica. Entendemos que la LOPD no sólo cogió el sentido de la Directiva, como es natural, sino que ha ampliado de modo notable la conceptualización de los ficheros.

En la opinión de Vizcaíno Calderón<sup>347</sup>, “el fichero es el registro en el que se recoge y almacena el conjunto de datos que integra la información. Es la colección ordenada de aquéllos susceptibles de acceso, localización y tratamiento en términos más o menos sencillos según las circunstancias de cada caso. Naturalmente, los datos han de estar organizados aun cuando dicha ordenación u organización responda a sencillos parámetros”. De manera que su característica principal es reunir, almacenar y recuperar datos, además de auxiliarlo en su transformación en información, así como en el manejo tanto de esos datos como de la propia información<sup>348</sup>. A efectos de la ley, los ficheros deben reunir datos de carácter personal.

La diferenciación entre fichero de titularidad pública y privada ha sido realizada por el reglamento 1720/2007. En dicha definición la ley marca la

---

<sup>347</sup> VIZCAÍNO CALDERÓN, Miguel. *Comentarios... op. cit.*, p. 76.

<sup>348</sup> Vide PETER, Rob; CORONEL, Carlos. *Sistemas de bases de datos: diseño, implementación y administración*. México D.F.: Thomson Editores, 2004, p. 320. Creemos que es conveniente registrar los conceptos de base de datos en la Informática. Según DATE un sistema de base de datos, “es básicamente un sistema computarizado para guardar registros; es decir, es un sistema computarizado cuya finalidad general es almacenar información y permitir a los usuarios recuperar y actualizar esa información con base en peticiones. La información en cuestión puede ser cualquier cosa que sea de importancia para el individuo u organización; en otras palabras, todo lo que sea necesario para auxiliarlo en el proceso general de su administración”. DATE, C. J.. *Introducción a los sistemas de bases de datos*. México: PEARSON EDUCACIÓN, 2001, p. 5. Desde el punto de vista de ELMASRI y NAVATHE, “una base de datos es un conjunto de datos lógicamente coherente, con cierto significado inherente. Una colección aleatoria de datos no puede considerarse propiamente una base de datos. Toda base de datos se diseña, construye y puebla con datos para un propósito específico. Está dirigida a un grupo de usuarios y tiene ciertas aplicaciones preconcebidas que interesan a dichos usuarios. En otras palabras, una base de datos tiene una fuente de la cual se derivan los datos, cierto grado de interacción con los acontecimientos del mundo real y un público que está activamente interesado en el contenido de la base de datos”. ELMASRI, Ramez, NAVATHE, Shamkant B. *Sistema de base de datos. Conceptos fundamentales*. Mexico: Addison-Wesley Iberoamericana, 1997, p. 2.

figura del responsable como elemento caracterizador de uno u otro. De suerte que, independientemente del factor económico de procedencia de recursos, los ficheros privados son aquellos cuyos responsables son personas, empresas o entidades de derecho privado, o en su caso, mismo cuando sean responsables las corporaciones de derecho público, mientras los ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica. Para gozar de la consideración de ficheros públicos, los responsables deberán ser los órganos constitucionales o con relevancia constitucional del Estado, o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público, salvo que su finalidad sea el ejercicio de potestades de derecho público.

Además de eso, los ficheros no automatizados fueron incluidos en el reglamento, definidos como aquellos que están organizados de forma no automatizada y estructurados conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica. Lo que nos llama positivamente la atención en este precepto es que la única particularidad que podría ser elemento descaracterizador de dicho fichero es la forma de acceso, y pormenoriza la independencia de la centralización o no del conjunto de datos, siguiendo lo que dispone la Directiva 95/46.

3.2. El concepto de fichero en el *Codice in materia di protezione dei dati personali*.

El Código italiano de protección de datos define de manera muy objetiva el *banco de datos* como cualquier conjunto organizado de datos personales, repartido en una o más unidades, desplazados en uno o más sitios.

Según la doctrina italiana<sup>349</sup>, esta conceptualización además de representar una mejora en relación a la ley derogada, está más cercana al modo en que normalmente se entiende los bancos o archivos de datos, como lo hace, por ejemplo la Directiva 95/46. En lo que se refiere comparativamente a la ley anterior nº 675/1996 y la actual norma es que aquella definía los banco de datos como cualquier conjunto organizado de datos personales, repartido en una o más unidades, desplazados en uno o más sitios pero incluía en la parte final del dispositivo que estos deberían estar *organizados según una pluralidad de criterios determinado*.

Como bien apunta Vecchi<sup>350</sup>, esa noción dada por la antigua ley era peligrosamente susceptible de excluir una gran parte de ficheros. Así, por ejemplo, los ficheros manuales que no utilizan medios automatizados y difícilmente permiten ordenar la información según una pluralidad de criterios, no obstante deben ser incluidos en la disciplina de la tutela de los datos personales, o asimismo los ficheros automatizados que no necesariamente deban estar organizados según una pluralidad de criterios.

Sin embargo, la actual norma no se refiere a una pluralidad de criterios ordenadores para identificar el banco de datos, siendo suficiente que consista en un complejo organizado de datos personales, de manera que tal organización de dicho complejo pueda derivarse del hecho de que éste haya sido ordenado según un único criterio. Es importante añadir que la

---

<sup>349</sup> Vid. VECCHI, Paolo Maria. "Comentario al artículo 4º". En: BIANCA, Cesare Massimo. *La protezione... op. cit.*, p. 81.

<sup>350</sup> *Ibid.*, pp. 81-83.

ley italiana no hace ninguna diferenciación entre los banco de datos públicos o privados.

#### 4. Cesión o comunicación de datos.

Se entiende por cesión o comunicación de datos, según lo que dispone el artículo 3, i, de la LOPD, toda revelación de datos realizada a una persona distinta del interesado. El Reglamento de desarrollo de la LOPD repite en los mismos términos tal definición.

Vale recordar que el artículo 11 de la LOPD y el artículo 10 del RD 1720/2007 establecen algunos requisitos para que sea válida la cesión, supuestos esto ya analizados en el tópico referente al principio del consentimiento. De modo somero, es necesario primero que la cesión se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario y segundo que por regla general exista previo consentimiento del interesado.

El Código italiano utiliza solamente la expresión *comunicazione* para identificar el hecho de dar conocimiento de los datos personales a uno o más sujetos determinados, distintos del interesado, del representante del titular en el territorio del Estado, del responsable y por los encargados, en cualquier forma, incluso mediante su disposición o consulta. También define el legislador la *diffusione* como dar conocimiento de los datos personales a sujetos indeterminados, también mediante su disposición o consulta.

La diferencia entre uno y otro término está en los sujetos destinatarios. O por mejor decir, el momento que los distinguen es representado por la

mayor o menor determinabilidad del destinatario<sup>351</sup>. Vecchi<sup>352</sup>, plantea que puede surgir una duda tocante a la expresión “dar conocimiento” usada en una y otra definición, si ello debe consistir en el efectivo acceso a la información o es suficiente revelar a tercero de la sola existencia del dato personal, sin transmitirle la información en este contenida. Observa el autor en cita que se podría sostener que en cuanto el dato personal es la información relativa a la persona, si ésta no viene transmitida, no habría el conocimiento de ésta por parte de tercero o terceros en el cual consiste la comunicación y la difusión. No obstante ello, el autor añade que lo que se debe tener presente es la extrema penetración de la noción de dato personal, que se refiere cualquier información relativa a una persona, con la consecuencia de que ya el hecho que exista una información archivada relativa a un sujeto determinado es un dato personal cuyo transmisión a tercero puede ser calificada como comunicación o difusión.

## **5. Los responsables del fichero o tratamiento y los encargados del tratamiento.**

### 5.1. Los conceptos en la LOPD.

Segundo la LOPD, en el apartado d) del artículo 3, el responsable del fichero o del tratamiento es la persona física o jurídica, de naturaleza

---

<sup>351</sup> VECCHI, Paolo Maria. “Comentario al artículo 4º”. En: BIANCA, Cesare Massimo. *La protezione ... op. cit.*, p. 76.

<sup>352</sup> *Ibid.*, p. 77.

pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido o uso del tratamiento. Como advierte Freixas Gutiérrez<sup>353</sup>, aunque la ley defina el responsable del fichero y el responsable del tratamiento en la misma oportunidad, dichos conceptos no tienen porque coincidir, sobre todo al proceder el análisis de la responsabilidad compartida, tocante a las infracciones y sanciones de uno y otro cuando sus actos puedan ser diferenciados de manera clara.

El Reglamento que desarrolla la LOPD, en el artículo 5º, línea *q*), podría haber separado los dos conceptos, pero ha dejado pasar la oportunidad, prefiriendo utilizarse de la misma técnica que la LOPD, manteniéndolos juntos. No obstante, dicho reglamento acierta cuando mejora la redacción del dispositivo, acercándose más a lo que establece la línea *d*) del artículo 2 de la Directiva 95/46.

En efecto, dicha Directiva no conceptúa el responsable del fichero, pero sí del tratamiento como la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales. El Reglamento, a su turno, define responsable del fichero o del tratamiento como la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Además, dicho precepto añade que los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados podrán ser también considerados como tales.

Lo que se debe tener en cuenta y es de fundamental importancia, como señala Orozco Pardo<sup>354</sup>, analizando la ausencia de la definición de “titular del fichero” en la LOPD, es que ésta opta — en nuestra opinión

---

<sup>353</sup> FREIXAS GUTIERREZ, Gabriel. *La protección... op. cit.*, p. 121.

<sup>354</sup> OROZCO PARDO, Guillermo. *Los derechos... op. cit.*, p. 99.

acertadamente — por hacer hincapié en la responsabilidad por la gestión del mismo, antes que por la relación de pertenencia o titularidad. En éste mismo sentido Vizcaíno Calderón<sup>355</sup>, afirma que la ley conecta el responsable del fichero con el poder de decisión sobre la finalidad, contenido y uso del tratamiento. Efectivamente, esta es la figura que representa indudablemente el principal sujeto pasivo de las relaciones jurídicas que emanan de la LOPD.

Encargado del tratamiento es conceptualizado por la LOPD como la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento. El Reglamento 1720/2007 añade que la naturaleza de la persona jurídica puede ser pública o privada y acrece a la lista de aquellos que pueden ser encargados del tratamiento los órganos administrativos y los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados. Merece resaltar que en la parte final del precepto, dicho reglamento especifica que las personas capaces de tener la consideración de encargado pueden actuar por cuenta — además del responsable del fichero — del responsable del tratamiento como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Chaveli<sup>356</sup>, señala objetivamente que lo que en efecto define al encargado es que preste un servicio al responsable del fichero o del tratamiento y que para la prestación de los mismos tenga que tratar datos.

En lo que concierne a las relaciones entre el responsable y el encargado del tratamiento, el RPD estableció en el artículo 20 y sus respectivos

---

<sup>355</sup> VIZCAÍNO CALDERÓN, Miguel. *Comentarios... op. cit.*, p. 79.

<sup>356</sup> CHAVELI, Eduard. “El estatuto del encargado del tratamiento en el Reglamento de Desarrollo de la LOPD”. En MARÍ, Joana, VILASAU, Mònica (coord.). *El Reglamento de protección de datos de carácter personal. Aspectos clave*. Barcelona: UOC, 2008, p. 132.



apartados algunas reglas específicas. De modo que la primera disposición legal sobre el tema es la desconsideración del acto de comunicación de datos cuando su acceso por parte de un encargado del tratamiento resulte necesario para la prestación de un servicio al responsable. Vale resaltar que para la ley en lo que respecta al servicio contratado entre el responsable y el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante ello, el precepto determina que se considerará la existencia de comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado, es decir, como ya señaló la AEPD<sup>357</sup>, será preciso que la actuación del encargado del tratamiento se limite a la prestación de los servicios objeto de la contratación.

El Reglamento también fija como deber del responsable del tratamiento, cuando este contrate la prestación de un servicio que comporte un tratamiento de datos personales, velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo que dispone la citada norma. Además, tocante a la responsabilidad del encargado, dispone el reglamento que en el supuesto que éste destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, tendrá la consideración de responsable del tratamiento, y por lo tanto responderá a las infracciones en que hubiera incurrido éste personalmente. La excepción sería en la hipótesis de que el encargado del tratamiento, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio.

---

<sup>357</sup> AEPD, Informe nº 17/2009.

## 5.2. Los conceptos en el *Codice in materia di protezione dei dati personali*.

El Código en materia de protección de datos personales de Italia distintamente de la Directiva y de la LOPD, ha preferido separar los conceptos de responsable del fichero, responsable del tratamiento y encargado del tratamiento, utilizándose también de términos diverso de los que utiliza las citadas normas para indicar estos sujetos.

De suerte que, según apunta Vecchi<sup>358</sup>, el texto italiano identifica al sujeto que elabora y se sirve del tratamiento de los datos personales y aquél que materialmente efectúa el mismo tratamiento por petición del primero. El Código usa el vocablo titular (*titolare*) para definir la persona física, la persona jurídica, la administración pública y cualquier otra entidad, asociación u organismo a los cuales corresponden sólo o conjuntamente con otros titulares, las decisiones sobre la finalidad, las modalidades del tratamiento de datos personales y a los instrumentos utilizados, incluido el perfil de la seguridad. Esta figura, en la Directiva, correspondería al responsable del tratamiento (alineación *d*) del artículo 2).

Para el texto italiano el responsable (*responsabile*) es la persona física, la persona jurídica, la administración pública y cualquier otra entidad, asociación u organismo encargado por el titular<sup>359</sup> del tratamiento de datos personales. Como señala Melchionna<sup>360</sup>, el responsable se trata de una figura no obligatoria a cual es conferido un mandato muy amplio, que nace de la voluntad del legislador en individualizar, en el ámbito del

---

<sup>358</sup> VECCHI, Paolo Maria. "Comentario al artículo 4º". En: BIANCA, Cesare Massimo. *La protezione ... op. cit.*, p. 69.

<sup>359</sup> El responsable según el texto comunitario.

<sup>360</sup> MELCHIONNA, Silvia. *I principi...*, *op. cit.*, p. 60.

la actividad de gestión de los tratamientos, centros precisos de autonomía y, consecuentemente, de imputación de responsabilidad.

Lo que considera la norma en comento como encargado (*incaricato*), según el artículo 4, letra *h*), es la persona física autorizada a realizar operaciones de tratamiento por el titular o por el responsable, o sea, el sujeto que materialmente opera sobre los datos personales, siguiendo las instrucciones del titular o del responsable<sup>361</sup>. Vale subrayar que en la Directiva comunitaria 95/46 no existe ninguna referencia a tal figura<sup>362</sup>.

Para Vecchi<sup>363</sup> el responsable es una figura original de la disciplina italiana, y no parece ser posible considerarla como equivalente a lo que la Directiva denomina de encargado. Ello porque, según el planteamiento del autor<sup>364</sup> en cita, el Código considera el responsable como un “encargado” del titular, de manera que individualiza una relación que por un lado permite imputar la actividad relativa al tratamiento al titular, y por otra parte, también en consecuencia de esta imputación, pone en evidencia como el tratamiento sucede para satisfacer intereses no del responsable, sino del titular, cuyas instrucciones, independientemente de su especificidad, el primero debe seguir.

Esta, no obstante, no parece ser la opinión de Melchionna<sup>365</sup>, para quien tal precepto reproduce íntegramente la definición ya contenida en el artículo 2, párrafo 2, letra *e*) de la ley derogada 675/1996, que recoge del

---

<sup>361</sup> VECCHI, Paolo Maria. “Comentario al artículo 4º”. En: BIANCA, Cesare Massimo. *La protezione ... op. cit.*, p. 69.

<sup>362</sup> MELCHIONNA, Silvia. *I principi...*, *op. cit.*, p. 63, nota el pie de página nº 94.

<sup>363</sup> VECCHI, Paolo Maria. “Comentario al artículo 4º”. En: BIANCA, Cesare Massimo. *La protezione ... op. cit.*, pp. 70-72.

<sup>364</sup> *Ibid.*, p. 70.

<sup>365</sup> MELCHIONNA, Silvia. *I principi...*, *op. cit.*, p. 59, nota al pie de página n. 79.

artículo 2 letra e) de la Directiva, donde, sin embargo, esta figura es indicada como encargado del tratamiento.

## 6. Afectado o interesado.

### 6.1. España.

Define la LOPD el afectado o interesado como la persona física titular de los datos que sean objetos del tratamiento a que se refiere el apartado c) del artículo 3. La Directiva 95/46/CE, sin embargo, aunque no lo conceptúe directamente, alude el interesado como una persona física identificada o inidentificable haciendo dicha remisión al definir datos personales.

El legislador español ha decidido seguir la línea restrictiva de la Directiva comunitaria en lo que concierne a los interesados, y de hecho el Reglamento 1720/2007 aunque repita la definición de la LOPD, parece ser redactada de manera más objetiva como “la persona física titular de los datos que sean objeto de tratamiento”.

La Agencia Española de Protección de Datos ya ha decidido por varias veces que la LOPD no se aplica a las personas jurídicas. Incluso después de la entrada en vigor del Reglamento, la AEPD<sup>366</sup> consignó en informe jurídico que “la protección conferida por la Ley Orgánica 15/1999 no es

---

<sup>366</sup> Informe Jurídico n. 42/2008, disponible en

<https://www.agpd.es>.

aplicable a las personas jurídicas, que no gozarán de ninguna de las garantías establecidas en la Ley, sin perjuicio de que los Tribunales puedan atender las reclamaciones de responsabilidad que pudieran exigirse en el caso de que el uso de información relativa a las empresas les cause algún perjuicio. En consecuencia, las previsiones de la Ley Orgánica 15/1999 no serían de aplicación a los datos referidos a personas jurídicas”.

En los casos de los empresarios individuales, el en mismo documento la AEPD explicita que mismo cuando los datos referidos a estos, o que les identifican, aparecen ligados a su actividad mercantil, aunque con su nombre o apellido identificando un establecimiento o una marca de un producto o servicio, como consecuencia de una libre decisión empresarial adoptada en este sentido, no serán sometidos a las reglas establecidas por la LOPD. No obstante ello, los profesionales y los comerciantes individuales sí gozarían de la protección de la Ley Orgánica 15/1999 cuando los primeros no tuvieran organizada su actividad profesional bajo la forma de empresa, no ostentando la condición de comerciante, como es el caso de los profesionales liberales y en el caso de los segundos cuando no fuera posible diferenciar su actividad mercantil de la propia actividad privada.

## 6.2. Italia.

En lo que concierne a esta materia en Italia, como ya tuvimos oportunidad de remarcar cuando del examen de datos personales, el Código acrece a la lista de los interesados los entes, asociaciones y personas jurídicas, diferenciándose, de este modo, de la Directiva Comunitaria y de la LOPD. Dicha definición se encuentra en la alinea *i*)

del artículo 3, de la ley 196 de 30 de junio de 2003, conceptuando el interesado como la persona física, la persona jurídica, el ente o asociación a cuyos datos personales se refieren.

## 7. Fuentes accesibles al público

### 7.1. España.

De lo que se extrae de la letra j) del artículo 3 de la LOPD, son fuentes accesibles al público aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencias que, en su caso, el abono de una contraprestación. La segunda parte del apartado especifica que ficheros tienen este carácter, de manera que son así considerados el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

El Reglamento de desarrollo de la LOPD no solamente repite el texto de la citada ley, pero añade en el artículo 7 como fuentes accesibles al público las guías de servicio de comunicaciones electrónicas. Además, determina que en la lista de personas pertenecientes a grupos de profesionales, la dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica y en el

caso de los Colegios profesionales podrán indicarse como datos de pertenencia al grupo los números de colegiados, fecha de incorporación y situación de ejercicio profesional.

En definitiva, como señala Puente Escobar<sup>367</sup>, “dicha norma introduce una importante aclaración en relación con las fuentes accesibles al público, al regular detalladamente su concepto en el artículo 7”. Hay que recalcar el importante refuerzo que hace el artículo 7, apartado 2 del Reglamento en lo que concierne a la consideración de fuente accesible al público, que no reside solamente en ubicarse en la enumeración del artículo 3 j) de la LOPD, pero que también “será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación”. Respecto a este tema, la Agencia de Protección de Datos<sup>368</sup> se manifestó en el sentido de que no necesariamente todos los ficheros que contengan los datos enumerados en el artículo han de ser considerados fuentes accesibles al público, “sino que para que dicha circunstancia pueda tener lugar, será indispensable que tales ficheros puedan ser libremente accesibles por cualquier persona, bien gratuitamente, bien mediante el abono de una contraprestación. Los ficheros que conteniendo los datos enumerados sean utilizados internamente por el Colegio Profesional o sean de acceso restringido, por ejemplo, a los propios colegiados, exclusivamente, no tendrán la condición”.

---

<sup>367</sup> PUENTE ESCOBAR, Agustín. “Legitimación para el tratamiento”. En MARTÍNEZ MARTÍNEZ, Ricard (coord.). *Protección de datos Comentarios al Reglamento de Desarrollo de la LOPD*. Comentarios al Reglamento de Desarrollo de la LOPD. Valencia: Tirant lo Blanch, 2009, p. 27.

<sup>368</sup> AEPD. Informe Jurídico nº. 234/2008.

En lo que concierne a las páginas web<sup>369</sup>, la Agencia Española de Protección de Datos no las considera como fuentes accesibles al público. En Informe Jurídico<sup>370</sup>, este órgano consignó que tanto la definición del artículo 3. j. De la LOPD como la del artículo 7 del Reglamento “tienen una enumeración taxativa respecto a lo que cabe considerar como fuentes accesibles al público, lo que impide que consideremos a las páginas *web* como fuentes accesibles al público. Por ello, para tratar la información contenida en dichas páginas debería de obtenerse el consentimiento de los afectados”. De este modo, concluye la Agencia que la creación de un fichero que contenga información obtenida de páginas *web* resulta contraria a la Ley Orgánica 15/1999, dado que se carece de legitimación para tratar los datos personales contenidos en las mismas. Siguiendo el mismo entendimiento, la Audiencia Nacional en Sentencia de 5 noviembre 2008, cuyo objeto analizado era la resolución del Director de la Agencia Española de la Protección de Datos que desestimaba el recurso de reposición interpuesto contra la resolución de la misma Agencia de fecha 7 de mayo 2007 que acordaba imponer a una empresa una sanción de multa por haber tratado datos personales recabados de Internet, sin el consentimiento del interesado. El fallo concluye que Internet no constituye una fuente de acceso al público. En lo que concierne a la equiparación entre Internet como medio de comunicación, y ahí se

---

<sup>369</sup> El Tribunal de Justicia de las Comunidades Europeas en el Caso contra Bodil Lindqvist, señaló que la difusión de los datos personales en Internet constituye un tratamiento total o parcialmente automatizado, en los siguientes términos: “la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales» en el sentido del artículo 3, apartado 1, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 (LCEur 1995, 2977), 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. Sentencia 6 de noviembre de 2003 (TJCE 2003\368).

<sup>370</sup> AEPD. Informe Jurídico nº. 0342/2008.



justificaría como fuentes accesible al público, la Audiencia Nacional<sup>371</sup> ha señalado se entiende como medio de comunicación aquellas estructuras “que se dedican de forma profesional a obtener, procesar y difundir de forma masiva información o cualquier otro tipo de contenidos siempre que gocen de relevancia pública, cualquiera que sea el soporte que utilicen para el desarrollo de dicha actividad (audiovisual, escrita, digital a través de Internet, etc.)”. En efecto, este Tribunal<sup>372</sup> viene interpretando que aparte de aquellos que están enumerados en la ley, no hay más fuentes accesibles al público.

También merece destacar la problemática de los datos que contienen los Boletines y Diarios Oficiales, principalmente en su versión electrónica, ya que el propio medio utilizado facilita la localización de las informaciones personales allí registradas, a través de buscadores de Internet. El reto está en equilibrar la obligatoriedad de la publicación en el BOE y garantizar los derechos del interesado según la Ley de Protección de Datos. En la Memoria de 2007<sup>373</sup>, la Agencia Nacional de Protección de Datos ya había advertido que “el desarrollo de la sociedad de la información ha generalizado la posibilidad de acceder a ediciones digitales de los Boletines y Diarios Oficiales. La información publicada suele incluir datos personales y es también captada por los motores de búsqueda en Internet, multiplicando las posibilidades de acceso y dificultando el ejercicio de los derechos de cancelación y oposición. Esta situación aconseja impulsar los procedimientos que, sin afectar la función propia de los diarios oficiales, limite su captación por los motores de búsqueda en Internet”. En efecto, las Agencias de Protección de Datos de Cataluña y Madrid han editado Recomendaciones (Recomendación nº 1/2008 y Recomendación nº 2/2008,

---

<sup>371</sup> Audiencia Nacional. Sentencia de 10 julio 2008 (JUR 2008\291771)

<sup>372</sup> Audiencia Nacional. Sentencia de 3 septiembre 2007 (JUR 2007\276044)

<sup>373</sup> AEPD. Memoria 2007. Texto disponible en

[http://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/memoria\\_AEPD\\_2007.pdf](http://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/memoria_AEPD_2007.pdf).

respectivamente) en las cuales sugieren la colaboración entre las instituciones implicadas para que se adopte las medidas tecnológicas que eviten recopilación de los datos personales para finalidades diferentes de aquéllas a la cual obedece la publicación.

Es interesante subrayar lo que la Agencia de Protección de Datos de Madrid en la Recomendación nº 2/2008 consigna respecto al acceso de informaciones publicas en el contexto de las fuentes accesibles al público fundamentalmente aquellas disponibles en Internet: “el acceso a información pública tiene en nuestro país un sólido fundamento constitucional, aunque no ha sido expresamente reconocido como derecho como ocurre en otros países. En cualquier caso, no es un derecho absoluto sino que está sometido a límites, unos límites que deben encontrarse establecidos en una Ley, ser legítimos — apoyarse en otro bien o valor constitucional — y ser proporcionales”. De este modo, el acceso cuando indiscriminado a la información pública puede suponer transparencia absoluta, tanto de la Administración cuanto del ciudadano ante la sociedad, “lo que vulnera no sólo nuestro derecho fundamental a la protección de datos personales sino también nuestro derecho a la intimidad que es un presupuesto para una mínima calidad de vida para la dignidad y para la libertad personal”.

La citada Recomendación hace un análisis muy minucioso de la problemática entre los límites de los derechos a la protección de datos y la publicación de información administrativa. El nudo gordiano residiría en las publicaciones de datos personales en un Boletín Oficial, incluyéndose la publicación en Internet, ya que esto, en la opinión de éste Órgano, supone un elevado nivel de intromisión en el derecho de protección de datos personales. Ello porque se atribuye a dicha publicación el carácter de fuente accesible al público, implicando en la permisión de la consulta por cualquier persona “sin más límite que el abono, en su caso, de una contraprestación y con un conjunto de consecuencias en materia de publicidad y prospección comercial – art. 30 LOPD - y en relación con los

servicios de solvencia patrimonial y de crédito – art. 29 LOPD -, unos efectos que no tiene aquello que se publica simplemente en Internet y que no alcanza el carácter de fuente accesible al público”. De suerte que dicho documento pretende establecer directrices para equilibrar los derechos fundamentales implicados, prescribiendo respuestas a ésta problemática.

## 7.2. Italia.

Tocante a éste apartado, el Código italiano no trae en su rol de definiciones ninguna relativa a fuentes accesibles al público. No obstante, el *Codice* en el Título IV (*Trattamenti in ambito pubblico*), Capítulo II (*Registri pubblici e albi professionali*), artículo 61 establece algunas reglas que deben ser observadas cuando los datos tratados hayan sido recogidos de fuentes públicas. De suerte que el citado artículo establece que el *Garante* deberá fomentar la adopción de un código de ética y de buena conducta para el tratamiento de los datos personales procedentes de archivos, registros, listas, actos o documentos en poder de sujetos públicos.

Además, el Código de buena conducta que reglamenta los ficheros de información crediticia, en su artículo 10 trata de los datos que son recabados de fuentes accesibles al público, y aunque tampoco los defina, en la letra *a*), los identifica asimismo como registro públicos, listas, actos o documentos públicamente disponibles. Algunas de estas fuentes públicas serían el registro de protesto y el registro inmobiliario, como señala Imperiali<sup>374</sup>.

---

<sup>374</sup> IMPERIALI, Riccardo. *Codice... op. cit.*, p. 996.

**CAPITULO TERCERO: ASPECTOS GENERALES DE LOS  
FICHEROS DE SOLVENCIA PATRIMONIAL Y CREDITO**

## I. Cuestiones preliminares.

Antes de adentrarnos en el tema, creemos necesario hacer algunas consideraciones preliminares, fundamentalmente en lo relativo a la nomenclatura que será utilizada en el objeto de este trabajo. Las leyes española, italiana y brasileña usan cada una expresiones distintas para conceptuar el mismo fichero, objeto de esta investigación.

En España, la Ley Orgánica de Protección de Datos denomina de modo general 'ficheros de solvencia patrimonial y crédito' y el Reglamento 1720/2007 introduciendo el término 'fichero común' para especificar aquellos que tratan los datos recabados directamente por el acreedor; el Código en Materia de Protección de Datos Personales italiano designa su Capítulo I del Título IX de *sistemi informativi*. Ya el código de buena conducta que reglamenta tales ficheros emplea la expresión *sistema di informazioni creditizie*, aunque en algunos reglamentos se puede encontrar el término *centrali rischi*. Finalmente, la ley brasileña usa un vocablo más general, *banco de dados de consumo*. Aparte del nombre elegido por la técnica legislativa, estos tipos de ficheros reciben distintas denominaciones no solamente por los ciudadanos sino también por los medios de comunicación, e incluso por la doctrina y la jurisprudencia.

De forma tal que en España se puede encontrar 'ficheros o registro de moroso', 'fichero o registro de impagado', 'lista de deudores', etc.; en Italia, son comunes las expresiones *banche dati dei cattivi pagatori*, *lista nera* y en Brasil, *banco de dados, órgão o serviço de proteção ao crédito, cadastro de devedores o insolventes, lista negra*, etc.

Desde nuestro punto de vista, la denominación utilizada por la Ley Orgánica española 15/1999 es la que más se adecua a los fines pretendidos

por tales ficheros. Es decir, banco de datos que tienen como objetivo determinar tanto cuanto sea posible la solvencia patrimonial de un individuo, analizando su capacidad de crédito, para que a partir de ese conjunto de información se pueda considerar el riesgo que implicaría llevar a cabo una operación crediticia con dicho sujeto. En tal acepción, el centro de atención no es el crédito, sino el interesado en relación a su situación de solvencia. En nuestra opinión, la énfasis dada al crédito en las expresiones italiana “sistema de información crediticia” y la brasileña “sistema de protección al crédito” no nos parecen la más adecuada, dado que en dichos ficheros confluyen datos personales individualizados de los interesados en relación a una solicitud o relación de crédito y la finalidad va siempre dirigida a operaciones individuales, en las que se analiza caso por caso.

A pesar de estas consideraciones, consideramos importante advertir que durante este trabajo se utilizarán las expresiones definidas por las leyes de cada país, conjuntamente con aquellas que aunque no sean empleadas por esas legislaciones, son ampliamente utilizadas en la doctrina y jurisprudencia.

## **II. Marco normativo de los ficheros de solvencia patrimonial y crédito.**

Cada país ha elegido una manera distinta de ubicar la normativa sobre los bancos de datos objeto de esta investigación. La única similitud que se puede encontrar sobre este punto es la existencia de leyes generales de protección de datos en España e Italia y por lo tanto se ubica ahí la principal referencia legislativa de estos ficheros. Tal hecho está

plenamente justificado teniendo en cuenta que en materia de protección de datos los países pertenecientes a la Comunidad Europea tienen prácticamente unificada la disciplina ya que están obligados a seguir las determinaciones de la Directiva Comunitaria 95/46. Así, los ficheros de solvencia patrimonial y crédito en España e Italia encuentran su principal marco normativo en sus leyes generales de protección de datos.

### **1. Marco normativo español.**

Específicamente en España, la Ley Orgánica de 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal dedica su artículo 29 a una disciplina general de dichos banco de datos. Ocho años después, es promulgado el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, en el Título IV, denominado “Disposiciones aplicables a determinados ficheros de titularidad privada”, Capítulo I, “Ficheros de Información sobre Solvencia Patrimonial Y Crédito”, dividido en dos secciones: la primera, regula las disposiciones generales y está constituida por un único artículo (art. 37); y la segunda sección, “Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés”, formada por siete artículos (arts. 38 a 44). De modo que es ahí donde se encuentra la mayor parte de la disciplina específica relativa a este banco de datos, y de modo general regula los requisitos para la inclusión de los datos; el deber de la información previa al interesado de la posibilidad de ser los datos comunicados a un fichero; la notificación de su inclusión; la conservación de los datos; el acceso a la información contenida en el fichero; la responsabilidad del acreedor y, finalmente, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Efectivamente, en esta ley se encuentran más detallados varios de los aspectos no tratados por la norma principal, y refuerza aquellos ya existentes. Tal disciplina es fruto de la experiencia y del trabajo de la Agencia de Protección de Datos, de la doctrina y de la jurisprudencia, como ya mencionado anteriormente. Según Prats Albentosa<sup>375</sup>, “en tanto que la regulación contenida en la LOPD no descendía a detalles relativos a la prestación de este servicio y la tutela de los derechos de los particulares, esta carencia redundaba no sólo en contra de estos, sino también, en detrimento del adecuado ejercicio por la AEPD de su competencia, y por tanto y de nuevo, de los particulares, que por esta carencia no podían recibir todo el amparo posible de la Agencia”.

## 2. Marco normativo italiano

Italia ubica la disciplina de estos bancos de datos en el artículo 117 del Capítulo I del Título IX del *Codice*. A diferencia de la elección del legislador español, el citado artículo ordena al *Garante* la creación del Código de Deontología y Buena Conducta, que en efecto ha entrado en vigor el 1º de enero de 2005<sup>376</sup>, para reglamentar todos los aspectos concernientes al sistema de información al crédito, siendo por lo tanto, la norma más importante de nuestra investigación.

---

<sup>375</sup> PRATS ALBENTOSA, Lorenzo. “Ficheros de información sobre solvencia patrimonial y crédito”. En: MARTÍNEZ MARTÍNEZ, Ricard (coord.). *Protección de datos Comentarios al Reglamento de Desarrollo de la LOPD*. Comentarios al Reglamento de Desarrollo de la LOPD. Valencia: Tirant lo Blanch, 2009, p. 220.

<sup>376</sup> *Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti*.



Entendemos oportuno hacer un somero comentario respecto a los artículos 118 (*Informazioni commerciali*) y 119 (*Dati relativi al comportamento debitorio*) del *Codice*. El primer dispositivo enunciado reglamenta la creación de un código de buena conducta para la información comercial y el segundo determina que el mencionado código deberá establecer períodos de conservación de los datos personales contenidos, en particular, en los bancos de datos, registros y listas mantenidas por órganos públicos y privados en lo que concierne al pago de deudas por parte de los titulares de las informaciones en otros supuestos diversos de aquellos disciplinados por el artículo 117.

Ahora bien, por información comercial<sup>377</sup> no se entiende aquellas relativas a la actividad publicitaria, de marketing directo o indirecto, la promoción comercial, etc., de suerte que, como subraya Imperiali e Imperiali<sup>378</sup>, dicho artículo se refiere a la actividad de información comercial llevada a cabo por sociedades especializadas en proporcionar información sobre las empresas (volumen de actividad, volumen de negocios, pendencies judiciales, etc.), de manera que éstas son informes detallados que representan la fotografía o la radiografía del “estado de salud” de una empresa, por mejor decir, de su situación económica. Para Rossi<sup>379</sup>, la expresión “información comercial” es término por si mismo muy genérico y elástico y se presta a ser interpretado según el contexto de su uso: son informaciones económicas o comerciales tanto el número de

---

<sup>377</sup> Vide IMPERIALI, Riccardo. y IMPERIALI, Rosario. *Codice della privacy. Commento alla normativa sulla protezione dei dati personali*. Milano: Il sole-24 ore, 2005, p. 641; VOTANO, Giulio. “Sistema Bancario, Finanziario ed Assicurativo”. En *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*. BIANCA, Cesare Massimo y BUSNELLI, Francesco (Dir.), Milano: CEDAN, 2007, p. 1511.

<sup>378</sup> IMPERIALI, Riccardo, IMPERIALI, Rosario. *Codice... Op. Cit.*, p. 641.

<sup>379</sup> ROSSI, Valentina. “Art. 117. Affidabilità e puntualità nei pagamenti”. En: CASSANO, Giuseppe, y FADDA, Stefano (coord.). *Codice in materia di protezione dei dati personali: commento articolo per articolo al Testo unico sulla privacy D. lgs. 30 giugno 2003, n. 196*. Milano: IPSOA, 2004, p. 534.

referencia de una cuenta corriente bancaria como los datos relativos a un usuario telefónico y los datos relativos a una tarjeta de crédito.

En lo que concierne a la relación entre el artículo 118 y el 119 para *Imperiali e Imperiali*<sup>380</sup>, la categoría de *informaciones comerciales* no es lo suficientemente amplia como para incluir los datos del registro público de protesto, los datos de la Secretaria del juzgado civil competente responsable por los pagos y requerimientos de pagos, bien como aquellos de la Secretaria del juzgado competente en materia concursal, para la quiebra y los procedimientos concursales. Esto concierne también a la información de los registros inmobiliarios, que no serían informaciones comerciales en sentido estricto, aunque su recogida y su circulación obedezcan a fines comerciales, es decir, en el comercio como base de partida para una transacción. Por todo ello, para este autor, viene en ayuda el artículo 119 que determina que el Código deberá disponer de modalidades de tratamiento y plazos de conservación de los datos uniformes y armonizados también en relación a las informaciones sobre el comportamiento de la deuda del sujeto en cuestión.

El artículo 118 del *Codice* en cambio regula los bancos de datos que tratan informaciones comerciales de empresas y personas físicas, dentro del ámbito mercantil; Por lo que no corresponde al objeto de estudio de esta investigación, centrándonos en el fichero que regula el artículo 117.

### 3. Marco normativo brasileño.

---

<sup>380</sup> *Ibid.*, p. 641.

En el caso de Brasil, por la inexistencia de una ley general de protección de datos, la norma que se ha encargado de reglamentar los ficheros objetos de nuestro estudio ha sido el *Código de Defesa do Consumidor*, ley nº 8.078, de 11 de septiembre de 1990, en su artículo 43. Teniendo en cuenta la mencionada ausencia de una ley general en el sistema jurídico de este país, no nos ha parecido del todo equivocada la inclusión de estos dispositivos en el Código del Consumidor, en su momento. Pues como la protección de las operaciones de crédito se destina a las personas físicas, y a las relaciones de consumo, de ellas que nacen toda la problemática que implica el ámbito del cumplimiento o incumplimiento de las obligaciones contractuales referentes al crédito. Aunque el CDC no pueda solucionar los numerosos aspectos a los que actualmente se enfrentan los derechos de los ciudadanos en materia de protección de datos.

Aparte del citado Código, el principal fichero de solvencia patrimonial de Brasil, el *Serviço de Proteção ao Crédito* (SPC) posee un Reglamento interno que establece algunas directrices sobre su constitución, finalidad, criterios sobre el registro de los datos, acceso, además de otros preceptos relativos al funcionamiento interno de dichos ficheros, sin embargo, esto no es vinculante para otros bancos de datos, tratándose de una norma de autorregulación interna del SPC.

Es cierto que en este país, también existen las centrales de riesgos públicas, o por mejor decir, el *Sistema de Informações de Crédito do Banco Central*<sup>381</sup>, cuyos datos son cedidos mensualmente por las instituciones

---

<sup>381</sup> Según el propio Banco Central, tal sistema de informaciones de crédito tiene el objetivo de reforzar los mecanismos de supervisión bancaria, con el aumento de la eficacia de evaluación de los riesgos inherentes a la actividad, además de auxiliar las instituciones financieras en la gestión de sus carteras de crédito, subsanando una laguna en la obtención de informaciones sobre las características y evaluación de la capacidad de pagamiento de los deudores, objetivando disminuir las tasas de insolvencia. Banco Central do Brasil

<http://www.bcb.gov.br/fis/crc/ftp/cartilhascr.pdf> .[Consulta en 30 Octubre 2009].

financieras, de las operaciones de crédito concedidas sobre un valor estipulado igual o superior a R\$ 5 mil, sean vencidas o a vencer, además de los avales y las fianzas prestadas por las instituciones financieras a sus clientes. El marco normativo de este sistema es especial y distinto de los ficheros que analizamos, siendo la Ley Complementar 105/01 y la Resolución 2.724 del Banco Central las dos normas que reglamentan en dichos bancos de datos.

Al margen de todo ello, en el Senado Federal se está tramitando el Proyecto de Ley nº 85/2009 que disciplinan el funcionamiento de los bancos de datos y servicios de protección al crédito y congéneres y da otras providencias. Es un texto que por un lado es estructuralmente muy parecido a las normas de protección de datos europeas, y que de otro se diferencia de la disciplina del Código del Consumidor, ya que se centra en los aspectos de la protección de datos, aunque desafortunadamente no haga ninguna mención sobre tal derecho. De modo que una vez más, al que parece, el legislador perderá la oportunidad de empezar una nueva directriz en esta materia en el ordenamiento jurídico brasileño.

### **III. La finalidad de los ficheros.**

La Directiva Europea 45/96, en su artículo 6, apartado 1, b), establece que los Estados miembros dispongan en sus legislaciones, además de otras exigencias, que los datos personales sean recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichas finalidades. El principio de la calidad de los datos conlleva una importancia fundamental en la aplicación práctica del derecho a la protección de los datos personales. Podríamos afirmar,

incluso, que la relación que guarda uno y otro es comparable con la que respecta al vínculo entre el consentimiento y la autodeterminación informativa. Es decir, en el momento que nace el fichero, ese solamente puede estar justificado si su ámbito de aplicación o su finalidad están bien definidos. No se puede concebir que un registro trate datos de todas las especies, porque contraría no solamente el principio de la autodeterminación informativa como otros derechos fundamentales así, el de la intimidad. De este modo, entendemos que en el momento que se haga necesario la interpretación legal tocante a su alcance y en lo que concierne a la finalidad de un fichero, ésta debería ser siempre restrictiva, ya que los derechos fundamentales naturalmente tienen preponderancia sobre el derecho a la creación de un banco de datos.

La obligatoriedad de la definición de la finalidad de un fichero es el punto de partida fundamental para el ejercicio de control de los datos. Es ahí donde se enmarcan sus fronteras de actuación y los límites del tratamiento de las informaciones. Esta exigencia es lo que garantiza que la libertad de información no se transforme en institucionalización de un poder que siquiera el Estado puede tenerlo: una dictadura informativa, es decir, la libre e indiscriminada detención de todos los tipos de informaciones sobre cada uno de los ciudadanos concentrados en un único banco de datos. De manera que, como hemos tenido la oportunidad de opinar en los capítulos anteriores, pensamos que lo que legitima el registro de un dato, no es solamente la propia existencia del fichero, sino el fiel cumplimiento de sus funciones en el ámbito de sus finalidades.

Ahora bien, la tarea de trazar límites estableciendo sus objetivos no puede surgir solamente de la mera voluntad del responsable del fichero. Por mejor decir, crear un fichero, determinando su contenido a partir de la elección de una finalidad debe de obedecer a ciertos parámetros. De esta manera creemos que, primeramente hay que tener en cuenta la conformidad del objeto del fichero al Derecho. No se puede admitir que su contenido sea de informaciones que afronten al Estado Democrático de

Derecho. Así que sería inadmisibles el mantenimiento de un particular de un banco de datos que reuniera informaciones, *v. gr.*, sobre compradores y vendedores de narcóticos, o armas ilegales, o incluso que tratase de compilar informaciones sobre terroristas y su red de actuación, porque tales informaciones *a priori* no resultarían en una finalidad legítima de un fichero privado. En estos casos expuestos, el recibo de ese tipo de datos solamente serviría, en último caso, al Estado para que ejerciera sus funciones institucionales, fundamentalmente aquella de seguridad pública. Merece destacarse sobre este aspecto que lo que ha dejado consignado el Tribunal Supremo de España en la Sentencia núm. 292/2000 de 30 noviembre, cuando señaló con mucha lucidez que “el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos”.

Además de estas consideraciones, desde nuestra perspectiva entendemos que esa finalidad también debe asumir una función social. Cuando se vislumbra el objetivo de un banco de datos, no se puede permitir que su creación sea fruto únicamente del interés exclusivo y propio del responsable, pero exigir que dicho fichero asuma una utilidad social. Con eso no se quiere decir que estos deban de estar directamente relacionados a una actividad pública, ya que por poner un ejemplo los ficheros que tratan los datos de los trabajadores de una empresa sirven en un primer momento al propio funcionamiento interno de la misma, no obstante es un instrumento importantísimo para el desarrollo del negocio y por lo tanto, aunque de uso directo privado, indirectamente contribuye a una función de interés social. No se quiere decir aquí, que el banco de datos deba ser socialmente aceptable, desde la perspectiva de su función. Puede que un fichero sea socialmente aceptable, pero carezca de utilidad. En efecto, el considerando 30 de la Directiva Europea 95/46 consigna que “para ser lícito el tratamiento de datos personales debe basarse además en el consentimiento del interesado o ser necesario con vistas a la celebración

o ejecución de un contrato que obligue al interesado, o para la observancia de una obligación legal o **para el cumplimiento de una misión de interés público** o para el ejercicio de la autoridad pública o incluso para la realización de un interés legítimo de una persona, siempre que no prevalezcan los intereses o los derechos y libertades del interesado que, en particular, para asegurar el equilibrio de los intereses en juego, garantizando a la vez una competencia efectiva, los Estados miembros pueden precisar las condiciones en las que se podrán utilizar y comunicar a terceros datos de carácter personal, en el desempeño de actividades legítimas de gestión ordinaria de empresas y otras entidades”.

Así como el principio de la autodeterminación informativa no sirve al individuo como un mecanismo para satisfacción de su curiosidad, la creación de un fichero no puede estar vinculada a la voluntad injustificada de obtención de un conjunto aleatorio de información por su responsable. Es decir, cuando se permite el ejercicio al derecho a la creación de un banco de datos, que implica informaciones personales de particulares, hay que exigir que su ejercicio por un lado sea compensado desde la perspectiva de un beneficio o interés social, y por otro, no sea un instrumento de abuso del poder que se supone poseen aquellos que tienen informaciones de carácter personal sobre los individuos. Si recurrimos otra vez a ley Comunitaria, el artículo 7, letra f) de la Directiva 95/46 establece que los Estados miembros deben disponer que el tratamiento de datos personales sólo pueda efectuarse en el caso de que sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la misma Directiva.

De este modo, cuando se exige que exista un grado de interés social para la creación de un banco de datos, lo que ocurre es un equilibrio entre aquellos que tienen la posibilidad material de desarrollar un labor de

creación de un fichero que tratará datos más o menos sensibles, pero que dicen respecto a las personas, y la propia sociedad que en último término es para quien deben servir dichos ficheros. Si la finalidad es únicamente privada, sin que sea socialmente aceptable, como ya hemos dicho anteriormente, no tiene el banco de datos razón de existir porque tales informaciones almacenadas confieren a quien las detiene la posibilidad de un altísimo grado de manipulación sea individual sea social, en definitiva un inaceptable “asalto al poder”.

De manera que desde nuestra perspectiva, creemos que ese compromiso social también legítima, conjuntamente con la característica anteriormente comentada, la existencia del fichero y del propio ejercicio del derecho a su creación.

Además de ello, es interesante recordar otro aspecto. La Directiva Comunitaria nº 95/46 en su considerando 28 manifiesta que “todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados”. Aún en el mismo texto normativo citado, el artículo 6 determina que los Estados miembros dispondrán que los datos personales sean recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines;

Siguiendo el texto comunitario, el Código italiano de protección de datos establece el mismo principio en su artículo 11, cuya línea *b)* establece que los datos personales objetos de tratamiento deberán ser recabados y registrados para finalidad determinada, explícita y legítima y



si usados en otra operación de tratamiento, deberá ser en términos compatibles con tal finalidad.

Asimismo, el artículo 4, apartado 1 de la LOPD establece que las finalidades para el tratamiento de los datos deben ser determinadas, explícitas y legítimas, así como en el apartado 2 del mismo artículo prohíbe su uso para finalidades incompatibles con aquellas para las cuales los datos hubieran sido recogidos.

La Agencia de Protección de Datos de España<sup>382</sup> tuvo la oportunidad de dejar consignado sobre el citado apartado, que dichas finalidades allí referidas “han de ligarse o conectarse siempre con el principio de pertinencia o limitación en la recogida de datos regulado en el artículo 4.1 de la misma Ley. Concluye este órgano si la finalidad debe ser determinada, será difícil encontrar una utilización del dato para una finalidad distinta sin incurrir en la prohibición del artículo 4.2, aunque este utilice el término ‘incompatible’.

## **1. La finalidad de los ficheros de solvencia patrimonial y crédito**

Mayoritariamente la doctrina tiene enfatizado que la finalidad de los ficheros objeto del presente trabajo de investigación es asegurar el buen funcionamiento del mercado de crédito, a través de la cesión de informaciones sobre el cumplimiento o incumplimiento de las obligaciones dinerarias, o de la solvencia patrimonial del afectado que pueden ayudar a definir el grado de riesgo de una operación financiera

---

<sup>382</sup> Resolución: R/00326/2004 de la AEPD.

crediticia a un potencial cliente, siendo estas razones los principales pilares decisorios a la hora de concederle un crédito.

De hecho, el sistema financiero se mueve a través de redes de informaciones. Pero especialmente en el mercado de crédito estas son la fuente fundamental de su ejercicio. Segundo Mormile<sup>383</sup>, este es uno de los sectores de la economía en el cual la circulación de la información representa un requisito esencial para su propia existencia. Como el citado mercado tiene como característica la cesión temporal por parte del acreedor de recursos financieros — a cambio del pago de un tipo de interés — a un posible deudor, en teoría el intercambio de información confiere a los partícipes de ese mercado la posibilidad de una mejor valoración de la seguridad de la operación, disminuyendo así los márgenes de errores de sus operaciones, aumentando su lucro. Es necesario añadir que cuando se estima el riesgo de cada operación, en esta labor puede también incluirse eventualmente un análisis del porcentual de interés a ser cobrado a depender del grado de riesgo que uno posee, aunque en la práctica cuando son consumidores (persona física) los destinatarios del crédito, la disminución de ese porcentaje de interés raramente sucede.

La doctrina brasileña se manifiesta en este mismo sentido, así, Herman de Vasconcelos Benjamin<sup>384</sup>, entiende que la finalidad única de lo que

---

<sup>383</sup> MORMILE, Lalage. “Il Sistema di Informazioni Creditizie”. En *Libera circolazione e protezione dei dati personali*. PANETTA, Rocco (coord.), Milano: Giuffré, Tomo II, 2006, p. 1847.

<sup>384</sup> PELEGRINI GRINOVER, Ada; HERMAN DE VASCONCELOS BENJAMIN, Antonio; et al. *Código Brasileiro de Defesa do Consumidor: comentado pelos autores do anteprojeto*. Rio de Janeiro: RT, 2004, p. 377. En el idioma original: “o fim único dos arquivos de consumo é necessariamente prospectivo: um olhar para frente, dedicado a alertar credores potenciais sobre os riscos envolvidos ao negociarem com esse ou aquele consumidor” (...) “os arquivos de consumo destinam-se a auxiliar o funcionamento do mercado de consumo, facilitando as operações contratuais entre consumidores e fornecedores”.

denomina de manera genérica “ficheros de consumo” es necesariamente prospectiva para alertar a los acreedores sobre los riesgos potenciales al negociar con el consumidor. Además, añade que dichos bancos de datos se destinan a auxiliar el funcionamiento del mercado de consumo, facilitando las operaciones contractuales entre consumidores y empresarios<sup>385</sup>.

En esta línea de pensamiento parece seguir Roscoe Bessa<sup>386</sup>, para quien el objetivo de los bancos de datos de protección al crédito es proveer información a terceros que permitan un mejor análisis de los riesgos en la concesión de crédito a alguien. Por lo tanto, para este autor, se presupone que quien siempre cumplió con sus obligaciones contractuales en el pasado, va a mantener la misma postura en relación a nuevas concesiones de crédito.

Graciano Regalado<sup>387</sup> divide la importancia de los ficheros de morosos desde la perspectiva de las partes involucradas. De este modo, el autor opina que “para las entidades de financiación lo fundamental es que estos ficheros contengan información veraz —y en tiempo real— sobre la solvencia de sus potenciales clientes, impidiendo u obstaculizando la realización de operaciones fallidas o aquellas en las que el cliente pueda devenir moroso”. De otra parte, especifica que para el cliente es

---

<sup>385</sup> *Ibid.*, p. 389, “os arquivos de consumo destinam-se a auxiliar o funcionamento do mercado de consumo, facilitando as operações contratuais entre consumidores e fornecedores”.

<sup>386</sup> ROSCOE BESSA, Leonardo. *O Consumidor e os Limites dos Bancos de Dados de Proteção ao Crédito*. São Paulo: RT, 2003, p. 32. En el idioma original: “o objetivo dos bancos de dados de proteção ao crédito é fornecer informações a terceiros que permitam uma melhor análise dos riscos na concessão de crédito a alguém. Pressupõe-se que quem sempre cumpriu com suas obrigações contratuais no passado irá manter a mesma postura em relação a novas concessões de crédito”.

<sup>387</sup> GRACIANO REGALADO, Juan Carlos. “Ficheros de información sobre solvencia patrimonial y crédito: los ficheros RAI y ASNEF”. *Diario La Ley*. 2005, nº 6223, p. 1722.

igualmente importante que “la información proporcionada sea veraz, y también en este caso, que responda fielmente a la realidad del momento considerado, puesto que en esta información se fundamenta su credibilidad y con ello la posibilidad de obtener la financiación solicitada”.

El Código de buena conducta italiano establece para los ficheros de solvencia patrimonial y crédito en el artículo 2º que el tratamiento efectuado en estos es exclusivo para la finalidad relacionada a tutela del crédito y a la contención de los relativos riesgos, además de la evaluación de la situación financiera y el merito crediticio de los interesados o, en cualquier caso, su fiabilidad y puntualidad en los pagos.

El incumplimiento relativo a operaciones de crédito es un problema que puede a largo plazo afectar seriamente la economía de un país. Los datos que presentamos abajo nos revela, aunque desde la perspectiva del ámbito de su metodología y de su objeto, un panorama que nos permite visualizar la cantidad de pérdida de capital que se puede tener, mes a mes, por el impago de operaciones crediticia.

En España:

**Efectos de Comercio Impagados<sup>388</sup>**

---

<sup>388</sup> Según el INE, “el objetivo de la Estadística de Efectos de Comercio Impagados (ECI) es determinar mensualmente el número y el importe de los efectos comerciales de las entidades de crédito, en cartera y recibidos en gestión de cobro de clientes, que hayan vencido durante el mes de referencia y de éstos, los que hayan resultado impagados. Se obtienen datos sobre número y cuantía de los diferentes efectos, desagregados por clase de entidad: bancos, cajas de ahorros y cooperativas de crédito”. Acrescenta, aún, que son efectos de comercio vencidos, tanto en cartera como en gestión de cobro de clientes: recibos y otros documentos que vencen en el mes de referencia no se incluyendo en todo caso los recibos de servicios (luz, agua, gas, electricidad, colegios, etc.).

# ESTUDIO COMPARADO DEL RÉGIMEN JURÍDICO DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO EN ESPAÑA, ITALIA Y BRASIL

Ludmila Albuquerque Douettes Araújo

Jun. 2008	Dic. 2008	Mar. 2009	Jun. 2009	Set. 2009	Dic. 2009
1.640,57	1.762,00	1.529,82	913,72	673,13	644,75

Notas:  
Valores en millones de euros

Fuente de información: INE. Boletín Mensual de Estadística

## En Italia:

### Total de *Sofferenze*<sup>389</sup>

Jun. 2008	Dic. 2008	Mar. 2009	Jun. 2009	Set. 2009	Dic. 2009
95.042	100.735	106.720	108.412	113.719	118.921

Notas:

Valores en millones de euros

Fuente de información: Segnalazioni di Vigilanza y Centrale Rischi (Ene. 2010). Valores registrados en la *Centrale dei Rischi* de responsabilidad del *Comitato Interministeriale per il Credito e il Risparmio*. [www.bancaditalia.it](http://www.bancaditalia.it)

## En Brasil:

### Incumplimiento en Operaciones de Crédito del Sistema Financiero<sup>390</sup>

Jun. 2008	Dic. 2008	Mar. 2009	Jun. 2009	Set. 2009	Dic. 2009
30.850	38.697	46.058	55.012	61.054	60.831

<sup>389</sup> *Sofferenze*: comprende la totalidad de las relaciones de caja pendientes con sujetos en estado de insolvencia o en situaciones sustancialmente comparables, independientemente de las garantías que les asisten, al bruto de las devaluaciones y al neto de los pasos a pérdida eventualmente efectuados.

<sup>390</sup> Estos datos se refiere a las series del saldo de las provisiones relativas a los créditos de liquidación dudosa. No abarcan la totalidad de las operaciones de crédito, pero solamente un conjunto formado por las principales modalidades de crédito con recursos libres (correspondiendo en conjunto a aproximadamente 55% del crédito total del sistema financiero). Las informaciones presentadas representan el valor total de los créditos en mora por más de noventa días.

# ESTUDIO COMPARADO DEL RÉGIMEN JURÍDICO DE LOS FICHEROS DE SOLVENCIA PATRIMONIAL Y CRÉDITO EN ESPAÑA, ITALIA Y BRASIL

Ludmila Albuquerque Douettes Araújo

Notas:

Valores en millones de Reales (R\$)

Cambio: 1 € - 2,227 R\$ en Jul. 2010

Fuente: Banco Central do Brasil. [www.bacen.org.br](http://www.bacen.org.br)

De forma que no resulta demasiado afirmar que los conocidos ficheros de morosos, actualmente ya forman parte del mercado de crédito. Como bien apunta Plana<sup>391</sup>, “no cabe duda de la importancia socio-económica de cualesquiera de los datos sobre solvencia patrimonial y crédito susceptibles de ser incluidos en estos ficheros. Lo cierto es que la actividad económica y el comercio actual exigen, por parte de las empresas, lo que podríamos denominar un «control de riesgos»: para contratar con determinada persona se ha impuesto la exigencia de saber cuál es la situación económica y patrimonial del contratante, especialmente se la operación económica conlleva algún tipo de financiación. A esta finalidad responden los ficheros de solvencia patrimonial y crédito”.

En efecto, Rudelli<sup>392</sup>, igualmente resalta la importancia de la recogida de los datos referentes a solvencia del consumidor y a la exigencia de proteger la entidad financiera de los riesgos de una excesiva exposición crediticia con respecto a los sujetos no fiables. El autor en cita aún acrecienta que son dos intereses de gran relevancia social que se confrontan:

---

<sup>391</sup> PLANA, María del Carmen. “Ficheros sobre Solvencia Patrimonial y Crédito”. En: *Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/199, de 13 de diciembre, de Protección de Datos de Carácter Personal (Aprobado por RD 1720, de 21 de diciembre)*. PALOMAR OLMEDA, Alberto y GONZALEZ-ESPEJO, Pablo (Dir.). Cizur Menor: Thomson Civitas, 2008, p. 369.

<sup>392</sup> RUDELLI, Andrea. “Sistema Bancario, Finanziario ed Assicurativo”. En: *AA.VV. Codice della privacy : commento al Decreto legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative*. Milano: Giuffrè, 2004, Vol 1, p. 1479.

de un lado, la tutela del sistema crediticio que es indispensable para un correcto equilibrio de los flujos financieros dentro del mercado, con ventaja para el sistema económico como un todo, considerado el efecto del incentivo al consumo que se obtiene de las financiaciones. Por otra parte, la protección del derecho del consumidor a ser reconocido como leal participante del mercado, respetando la esfera privada (que incluye su capacidad de gasto).

En el mismo sentido, Mormile<sup>393</sup>, para quién la problemática no es encontrar un fundamento que justifique la legitimidad del funcionamiento de tales ficheros, pero sobre todo la identificación de las normas de equilibrio entre los intereses a menudo conflictivos: la protección del crédito y de las razones de las empresas crediticias y de otro lado la tutela de la *privacy*, en su acepción amplia de autodeterminación informativa.

Badin, Carazza y Ribeiro<sup>394</sup> señalan tres razones por las cuales los bancos de datos de protección al crédito ejercen un papel fundamental para el mercado de crédito: primero, el recabo, la diseminación y el análisis de las informaciones sobre los hábitos de pago de los agentes económicos facilitan la evaluación del riesgo de los potenciales clientes, permitiendo a los acreedores establecer precios, tasas de interés y condiciones de pagos diferenciadas para buenos y malos pagadores; segundo, la transmisión de los datos aumenta el estímulo para que los consumidores no se tornen incumplidores, ya que saben que un registro

---

<sup>393</sup> MORMILE, Lalage. *Il Sistema... op. cit.*, p. 1849.

<sup>394</sup> BADIN Arthur; CARAZZA DOS SANTOS, Bruno; RIBEIRO DAMASO, Otávio. "Os Bancos de Dados de Proteção ao Crédito, o CDC e o PL 5.870/2005: comentários sobre Direito e Economia" [en línea]. Disponible en

<<http://www.fazenda.gov.br/spe//publicacoes/reformasinstitucionais/estudos/ArtigoRevistaDireitoConsumido-BancosDados.pdf>> , Agosto de 2007. [Consulta en 14 fev 2010].

negativo puede representar un obstáculo a su acceso al crédito; y, finalmente, cuanto mayor el flujo de informaciones sobre clientes, mayor la competencia entre instituciones financieras y vendedores por buenos clientes, lo que se refleja en beneficios para los consumidores que habitualmente pagan en día sus obligaciones.

En efecto, no se puede prescindir de este servicio porque ya está más que comprobado que es esencial para el buen funcionamiento del sistema financiero. Opinamos que esta es precisamente la conclusión que imaginamos se pueda llegar, sobre todo después de un análisis aunque superficial de las razones de la gran crisis financiera mundial de 2008.

### 1.1. Los ficheros de solvencia patrimonial y crédito y la crisis económica mundial de 2008.

Entendemos conveniente hacer un somero repaso sobre algunas de los motivos que fueron determinantes para este colapso del sistema financiero mundial y la posición de los banco de datos de protección al crédito sobre esa problemática.

Su origen viene fundamentalmente del mercado inmobiliario estadounidense. Después de la crisis generada por las empresas “punto.com”, hubo una gran expansión de aquél mercado, creciendo la demanda por inmuebles y consecuentemente la búsqueda por hipotecas, éstas fomentadas también por las bajas tasas de juros aplicadas al crédito



inmobiliario. Señala Recalde Castells<sup>395</sup>, que “las causas de la crisis financiera parecen identificarse con facilidad en un período sin precedentes de concesión de créditos extremadamente laxa a favor de personas que no disponían siempre de la solvencia y cobertura suficientes. Así sucedió en el mercado hipotecario (donde las –ahora– vilipendiadas hipotecas subprimes no son más que la manifestación más grosera)” aunque añade también el autor que el crédito asimismo fue concedido sin garantías adecuadas para operaciones corporativas.

De hecho, los bancos en aquél momento se mostraban con un exceso de liquidez y según observa Villar Mir<sup>396</sup> muchas entidades trataron de superar los límites al crecimiento impuestos por el tamaño de sus fondos propios y de sus depósitos, “creando títulos que agrupan créditos hipotecarios que se encuentran en el balance de una entidad financiera, y que se pueden vender a otros inversores, proporcionando de esta forma una nueva liquidez a la misma entidad financiera”. De manera que la venta de estos activos, según el autor, suponía la venta de los créditos hipotecarios a otro agente diferente y separado del banco que los concedió en su origen. Sin embargo la peculiaridad de esta situación en EE.UU. fue el “desarrollo de productos estructurados, consistentes en la separación, dentro de un mismo título, de porciones de diferentes créditos hipotecarios, muy heterogéneos entre sí y con diferentes grados de riesgos”. Para Recalde Castells<sup>397</sup> otra causa de la crisis “que suele identificarse como origen del problema se sitúa en la política de las entidades de crédito de “distribuir” los activos crediticios a través de

---

<sup>395</sup> RECALDE CASTELLS, Andrés. “El papel del “Derecho” en la crisis. Algunos aspectos de la regulación financiera y de las grandes empresas en su relación con la Economía”. Documentos de trabajo (Laboratorio de alternativas), nº. 150, 2009, p. 17.

<sup>396</sup> VILLAR MIR, Juan Miguel. *La crisis económica actual. Sus orígenes y características. Medidas para salir de la crisis* [en línea].

<http://www.copitiba.com/portal/DW/Ponencia.pdf>. [Consulta: 10 ago. 2009].

<sup>397</sup> RECALDE CASTELLS, Andrés. *El papel... Op. Cit.*, pp. 17-18.

instrumentos financieros de perfiles difusos, que ni los mercados ni los mismos supervisores entendían suficientemente (y es cuestionable que los percibieran los mismos emisores)”.

Por otro lado, para que estos activos saliesen del balance de los bancos, en este país hubo una proliferación de sociedades denominadas ‘*conduits*’ o vehículos especiales de inversión, creadas por las propias entidades financieras, aunque jurídicamente independiente de éstas, que compraban inmediatamente dichos activos y los revendían en el mercado financiero. Una vez allí, podían ser vendidos nuevamente a otros inversores creando una cadena de ventas de títulos fundada únicamente en la confianza de la compra del consumidor.

Aparte de todo ello, Villar Mir<sup>398</sup> resalta que como los bancos eliminaban tales créditos hipotecarios de su balance, estos no tenían ningún incentivo para asegurarse de la solvencia de los prestatarios, estando su interés direccionado en conceder más préstamos, ya que el beneficio de este negocio residía en el volumen de los activos que se pusiesen en el mercado, sin preocuparse por su calidad ni por la capacidad de pago de los deudores. Asimismo como ha puesto de manifiesto el mismo autor, a través de su prestigio los bancos consiguieron que las agencias de calificación crediticia otorgasen las máximas calificaciones a estos paquetes, basado en la tradición de seriedad y solvencia de estas entidades y de sus clientes, aunque la garantía de esos productos era, en realidad, muy dudosa.

Además, algunas entidades especializadas en el mercado inmobiliario aprovechando el momento que se estaba atravesando en aquella época, empezaron a atender el segmento “*subprime*”, conocido en España como hipoteca de alto riesgo o hipoteca basura, que fueron vendidos igualmente en el mercado financiero como activos. Del mismo modo,

---

<sup>398</sup> VILLAR MIR, Juan Miguel. *La crisis... Op. Cit.*

estos eran comprados por gestores de fondos que buscaban rendimientos mayores, que por su turno revendían a otros gestores. Esa operación generaba a la entidad financiera de origen una nueva cuantía de dinero que era usada para conceder una nueva hipoteca, sin asegurarse de que la primera había sido paga. Hay que añadir, asimismo, que dichos bonos también servían como aval para que las entidades financieras solicitaran préstamos unas a otras, convirtiéndose en una “moneda falsa”.

De suerte que cuando el Sistema de Reserva Federal de EE.UU. empezó a subir los tipos de interés, hubo un encarecimiento del crédito, que provocó no solamente la huida de los consumidores de las hipotecas inmobiliarias y la consiguiente desestabilización de la relación entre la oferta y la demanda, como el aumento de la morosidad. Ello generó un ciclo de impago por todos aquellos que habían adquirido tales bonos. Como existía la dificultad añadida de que los activos estaban mezclados con otros productos financieros, hubo una retracción del crédito entre las entidades financieras porque no se podía evaluar quién era solvente o no<sup>399</sup>.

En lo que concierne a las hipotecas basura, hay que hacer algunas consideraciones. La primera es que esa modalidad de crédito es dada a personas que presentan un alto riesgo, es decir, que tiene un dudoso historial de crédito, no cuentan con un ingreso estable o no pueden comprobarlo, no tiene avales, etc. De manera que sabiendo que existe una exposición mayor a la suspensión de pagos, los intereses y las comisiones de estos créditos son más elevados y las entidades aseguran su inversión a través del embargo de la propiedad implicada en la hipoteca.

Ahora bien, analizando lo que ha pasado con la economía hasta llegar a la crisis actual, en efecto se puede afirmar que todo ello nos pone ante una nueva perspectiva sobre la relación entre algunos fenómenos económicos

---

<sup>399</sup><http://www.elmundo.es/especiales/2008/10/economia/crisis2008/lascausas/index.html>

y el objeto de estudio de este trabajo. Su necesidad en la actualidad es indudable para contribuir al equilibrio del sistema financiero.

Aunque sea cierto afirmar que la utilización de las informaciones contenidas en los ficheros de solvencia patrimonial y crédito son de gran valía para las operaciones en el ámbito restringido empresa (acreedora)-consumidor(deudor), ya que si este último no satisface la deuda, ello puede ocasionar incluso la quiebra económica de dicha empresa. Sin embargo, hoy por hoy no se puede vislumbrar que su finalidad resida únicamente en tal entorno.

La reciente crisis económica nos ha demostrado que las informaciones sobre la solvencia patrimonial tiene un interés mayor de lo que anteriormente se podía suponer. Es decir, aparte de los equívocos de política financiera cometidos por los bancos en el trato de sus productos y de otras circunstancias económicas, el origen de la crisis está también directamente relacionada en la evidente ausencia de vigilancia y cuidado de los bancos con las relaciones financieras de aquellos que no tenían suficiente soporte económico para asumir la responsabilidad de un crédito. Por otro lado, la información sobre la solvencia patrimonial de los individuos era conocida con antelación por los estos, pero que a su propio albedrío asumieron el riesgo de venderles sus productos.

La importancia del control de un sistema financiero es esencial para el desarrollo de los países, sobre todo cuando se está en una economía globalizada. Podemos destacar, sucintamente, el más importante aspecto que es el económico propiamente. Un sistema financiero que funciona eficientemente genera riqueza para el país, ya que garantiza fundamentalmente que el dinero sea captado por quien lo tiene, para darlo a quien le falta, garantizando el flujo de recursos de ahorro para la inversión.

De modo que todos los países que tienen una economía mínimamente desarrollada, cuentan con un complejo de órganos responsables por la regulación, control y equilibrio del sistema financiero y consecuentemente de sus mercados. Dichas actividades deberán siempre crear las condiciones necesarias para la fluidez de los mercados que componen este sistema. La regulación es, sin lugar a duda, una de las más importantes en ese contexto. Su objetivo, según Cortes<sup>400</sup>, es potenciar la actividad financiera y también crear las “*condiciones previas* de seguridad y economía que reduzcan a límites aceptables los riesgos de los inversores y los costes de las operaciones, de manera que, contando con ello el inversor, pueda *multiplicarse* el número de operaciones realizadas o cumplirse así tanto mejor o más acabadamente la función básica que se asigna al sistema financiero”. En el mismo sentido, merece destacar la opinión de Bonet Ferrer<sup>401</sup>, que con mucho acierto observa que “hay progreso económico porque existe mercado, pero sólo hay mercado allí donde existe estabilidad en las relaciones socio-económicas y eso pasa por la existencia de un marco de seguridad que es fruto de la ley. Y ello se refiere tanto a los fundamentos del orden establecido — la propiedad, la libertad de empresa, el ordenamiento del mercado y la intervención y la regulación pública misma — como a las derivaciones normativas que desarrollan la configuración, la posición, la actuación de los operadores de los operadores y sus instrumentos en el mercado.”

Sobre el tema de la morosidad en las operaciones comerciales y sus efectos para el acreedor, Díez-Picazo<sup>402</sup>, observa que ésta crea “una

---

<sup>400</sup> CORTES, Luis Javier, “Contratos y mercados financieros”. En: MENÉNDEZ, Aurelio (dir.). *Lecciones de Derecho Mercantil*. Navarra: Thomas Reuters, 2009, p. 716.

<sup>401</sup> BONET FERRER, José Luis. “La Importancia de las Marcas para la Empresa. Criterios de Valoración”. En: Fernández López, Juan Manuel (dir.). *Propiedad Industrial*. Estudios de Derecho Judicial, nº 49, Madrid: Consejo General del Poder Judicial, 2003, p. 313.

<sup>402</sup> DIEZ-PICAZO, Luis. *Fundamentos de Derecho civil patrimonial*. Pamplona: CIVITAS, 2008, p. 687.

situación de falta de los flujos monetarios que tenía derecho a esperar y puede producir inevitables y no deseadas situaciones de falta de tesorería, de falta de liquidez que pueden arrastrar al acreedor a la necesidad de establecer convenios concursales o preconsursales con sus propios acreedores”.

Siguiendo la misma línea, Cafaro y Pagliaro<sup>403</sup> señalan que la posibilidad de acceso al crédito debe equilibrarse con la necesidad de proteger la economía pública y por tanto del ahorro público. Desde esta perspectiva, acreditamos que los ficheros de solvencia patrimonial y crédito actualmente ejercen una función que va más allá de la relación empresa-cliente. Representan una función social, en los tiempos actuales, imprescindible para ayudar el buen desarrollo del sistema financiero, como verdaderas entidades de auxilio a su equilibrio y salud.

1.2. La vinculación de la consulta a las informaciones de los ficheros de solvencia patrimonial y crédito y el reparto del riesgo de la operación de concesión del crédito.

Como se sabe, todas las entidades financieras tienen acceso al histórico de solvencia de cualquier individuo que quiera comprar uno de sus productos. Pueden dentro de un margen legal, concertar comisiones y interés distintos dependiendo del tipo de producto financiero y a quien se destina; y además son libres para tomar sus propias decisiones empresariales. Consideramos que debería haber una vinculación a la

---

<sup>403</sup> CAFARO, Rossana y PAGLIARO, Paolo. *L'accesso al Credito. Banche Dati, Centrali Rischi y Privacy*. Milano: Giuffrè, 2004, p. 21.

consulta de los datos personales a estos tipos de negocios, imponiéndose parámetros legales que fundamenten tal vinculación, creando un sistema de derechos y protección para el cliente y deberes para las entidades financieras, que sean distintos de aquellas transacciones en las que el sujeto pasivo (cliente) sea alguien que tenga poco grado de riesgo. Lo que nos parece inaceptable es que dichas entidades tengan a su disposición igualmente para las dos hipótesis el mismo conjunto normativo material y procesal para los casos de impago, ya que en el primero caso (contratar con alguien que tenga dudoso historial crediticio) amenazan la salud del sistema financiero.

El cliente que presenta un considerable riesgo, si consigue un crédito, tiene que soportar intereses mayores que los que normalmente se aplican y ahí se constituye su parte del riesgo de la operación. Del mismo modo, somos de la opinión que en caso de impago por estos individuos de muy escasos avales y que ya tenían un dudoso historial de solvencia **antes** de efectuar determinada operación financiera, la entidad que le ha concedido el crédito debe asumir igualmente su parte del aludido riesgo de la operación. Así, por poner algunos ejemplos de cómo la entidad financiera podría asumirlo su porción: si el cobro de la deuda se efectúa a través de los juzgados, que sean el cliente eximido del pago de cualquier coste judicial; la imposibilidad del cobro de todo el interés referente a la deuda total si el valor ya pagado supera la mitad de la deuda bruta, serían algunas formas de compartir el riesgo de la operación, entre otros que podrían ser también añadidos para estos casos especiales. Son garantías que en nuestra opinión merecerían un análisis más profundo de la legislación actual de las leyes en vigor que podrían ser afectadas en el caso de que se pudiera vincular la consulta de las informaciones de los ficheros de solvencia patrimonial a una norma especial de gestión, cobro y ejecución de la deuda así como de responsabilidad por la mezclas de activos financieros de alto riesgos. Para esto, como ya mencionado, creemos que se necesitaría una investigación más detallada, ya que implicaría diversos sectores de la ciencia del Derecho, como el ámbito

civil, mercantil y procesal además de las ciencias económicas, razón por la cual es impracticable hacerlo aquí, además de que huye del objetivo del presente trabajo.

Ahora bien, *a priori*, los ficheros de solvencia patrimonial y crédito deberían restringirse a las finalidades anteriormente comentadas. No obstante, lo que ocurre en la práctica, sobretudo en Brasil que todavía no posee una fuerte legislación sobre protección de datos, es su utilización como una forma extrajudicial de cobro de deudas, a través de las consecuencias que un registro negativo puede traer.

Sobre este tema en España, aunque no nos parezca tan acentuado como en Brasil, la opinión no parece divergir. El Tribunal Supremo Español<sup>404</sup> en sentencia de 5 junio 2004 advirtió, “(...) se está analizando el caso de aquellas empresas o ficheros destinados a prestar servicios de información sobre solvencia patrimonial y de crédito, a través de la cual las empresas que operan en el mercado pueden comunicar a dichos titulares de ficheros de morosos, que una persona mantiene con ella una deuda, de tal suerte que **dichos ficheros de morosos o mejor dicho la anotación en dichos ficheros de morosos opera, de una parte, como instrumento de presión frente al deudor para que abone su deuda**, y, de otra, como un aviso a terceros, para evitar riesgos (...)” (subrayamos).

En efecto, al que parece la jurisprudencia ha incorporado esa función, desde nuestra perspectiva desviada de tales ficheros, aunque en la realidad se demuestra patente. La Audiencia Nacional<sup>405</sup>, tratando del principio de la calidad de los datos en los citados bancos de datos se refiere del siguiente modo: “debe considerarse, **que aquel que utiliza un medio extraordinario de cobro como es el de la anotación de la deuda en**

---

<sup>404</sup> Tribunal Supremo. Recurso de Casación para la unificación de doctrina núm. 39/2004, en 5 junio 2004. RJ 2004\5849.

<sup>405</sup> Audiencia Nacional. Sentencia de 9 enero 2009 (RJCA 2009\217).



un registro de morosos, debe garantizar el cumplimiento de todos los requisitos materiales (exactitud del dato) y formales (requerimiento previo) que permitan el empleo de este modo accesorio para conseguir el cobro de la deuda. No aplicar esta exigencia supondría, por el contrario, utilizar este medio de presión al recurrente sin el suficiente aseguramiento de las mínimas garantías para los titulares de los datos que son anotados en los registros de morosos” (subrayamos). Igualmente la Sentencia del Tribunal Supremo<sup>406</sup> que consideró la utilidad de estos ficheros para las entidades bancarias “al incluir en el mismo las personas que a su juicio resultan no pagadoras e incluso mal pagadoras y sirve para comunicarse entre sí esta circunstancia que actúa como medida de advertencia para mantener o no relaciones bancarias con los inscritos como morosos”. En dicha Sentencia, este Tribunal pone de manifiesto que la inclusión de datos en un fichero como el RAI “**ya desde principio se presenta como una actuación sancionadora en potencia** por las consecuencias de signo negativo que pueden afectar al inscrito en cuanto a sus relaciones comerciales futuras con las entidades bancarias” (subrayamos).

En efecto, en la misma sentencia anteriormente citada, la Audiencia Nacional<sup>407</sup> reconoce la importante función que realizan los ficheros de solvencia patrimonial y crédito en su contribución a la salvaguarda del sistema financiero y de la economía en general, por cuanto permiten a las entidades financieras, principalmente, conocer la solvencia de sus presentes o futuros clientes. Sin embargo, entiende este Tribunal que “la función que cumplen estos ficheros no puede imponerse por encima de la salvaguarda de los derechos fundamentales y de las previsiones plasmadas en la Ley en forma de tipos sancionadores”.

---

<sup>406</sup> Tribunal Supremo. Sentencia núm. 660/2004 de 5 julio (RJ 2004\4941).

<sup>407</sup> Audiencia Nacional. Sentencia de 9 enero 2009 (RJCA 2009\217).

Además, como asegura Freixas Gutierrez<sup>408</sup>, “no cabe duda que hay que partir de la necesidad de que el productor de servicios financieros cuente con un sistema de información fiable que le permita evaluar la situación económica de un demandante de financiación, máxime cuando la decisión a tomar se toma en corto espacio de tiempo. El problema estriba en compaginar esta necesidad con el inexcusable respeto a los derechos reconocidos constitucionalmente a todas las personas, en especial los derechos al honor y a la intimidad”.

Sobre el mismo punto, el magistrado Rosado de Aguiar, del Superior Tribunal de Justicia de Brasil, ya había consignado en fallo<sup>409</sup> que el recabo de datos y su registro en los ficheros era una de las nuevas preocupaciones del Estado moderno, ya que el uso de la informática y la posibilidad de control unificado de las diversas actividades de la persona y las múltiples situaciones de la vida permitía el conocimiento de su conducta pública y privada, con todos sus detalles, pudiendo llegar a la invasión de actos personales, invadiendo un área que debería quedarse restringida a su intimidad. El citado magistrado aún añade que el conjunto de estas informaciones podría ser usado para fines ilícitos, públicos o privados, en la prevención o represión de delitos, o incluso habilitando un sujeto a celebrar contratos con pleno conocimiento de causa, sin embargo podría servir igualmente al Estado o al particular para alcanzar fines contrarios a la moral o al Derecho, como un instrumento de persecución política u opresión económica.

Indudablemente la decisión sobre la concesión de crédito será siempre del acreedor. No obstante, este puede ser auxiliado a través de diversos mecanismo que le ayuden a que esa operación sea lo más segura posible. Así, el registro negativo en un fichero de solvencia patrimonial y crédito aunque no vincule su decisión, en la actualidad es prácticamente

---

<sup>408</sup> FREIXAS GUTIERREZ, Gabriel. *La protección... op. cit.*, p. 183.

<sup>409</sup> STJ, REsp 22.337-8/RS, Rel. Min. Ruy Rosado de Aguiar, DJU 20.04.95.

imposible que no se tengan en cuenta los datos allí registrados para fundamentarla. En efecto, la doctrina ya había señalado, como es el caso de Cafaro y Pagliaro<sup>410</sup> que antes de proceder a concesión de créditos o de préstamos para operaciones de crédito al consumo, los bancos y las sociedades financieras instruirán tal práctica, realizando una serie de controles sobre la persona que solicita. De suerte que resaltan los autores que el fundamento de la decisión de concesión del crédito depende no sólo de razones de política comercial del banco y de las informaciones internas en su posesión sobre el solicitante, pero también y sobre todo del resultado de la indagación dirigida a las centrales de riesgos sobre la fiabilidad y la solvencia del cliente.

## IV. Objeto de los ficheros de solvencia patrimonial y crédito

### 1. Legislación Española

España ha previsto los principales rasgos legales de estos ficheros en su Ley Orgánica de Protección de Datos: la utilización, el tratamiento, la cesión, los derechos del afectado, las obligaciones de los responsables por estos registros, las infracciones, entre otras disposiciones. Y a través de esta ley, como ya comentamos, transpone a su sistema jurídico la Directiva 95/46/CE.

---

<sup>410</sup> CAFARO, Rossana y PAGLIARO, Paolo. *L'accesso al Credito. Banche Dati, Centrali Rischi y Privacy*. Milano: Giuffrè, 2004, p. 55.

Se ha de recordar que el tratamiento de la LOPD para esta clase de ficheros es especial, y por lo tanto está regulado de forma específica y apartada<sup>411</sup>, aunque se enmarque dentro del contenido general de la ley. Aparte, como comentado, el Reglamento 1720/2007 amplió de modo significativo la normativa de estos ficheros.

Es necesario resaltar que algunas posiciones de doctrina sobre el artículo 29, tocante a la creación jurídica de una tipología de fichero, aseguran la diferenciación de dos grupos a saber, los “ficheros de deudores” y el “fichero de solvencia patrimonial”. Además, la Audiencia Nacional<sup>412</sup> cuando ha tenido de oportunidad de pronunciarse sobre el tema, ha remarcado que “el artículo 29 de la Ley Orgánica 15/1999 regula de forma específica los ficheros establecidos para prestar servicios de información sobre solvencia patrimonial y crédito, y distingue dentro de ellos dos supuestos, uno de los cuales son los ficheros en los que se tratan datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés”.

En nuestra opinión, aunque pueda haber distinciones en lo que concierne al tratamiento de los datos que serían objetos de uno y otro posible fichero —imaginando la hipótesis de que existiesen dos—, es importante destacar, que para aspectos prácticos y relevantes, dicha diferenciación no tiene ninguna utilidad. Pues del espíritu de la ley se deduce que objeto y objetivo serían uno solo. Y aunque la norma especifique un permiso al responsable del fichero si quiere dedicarse

---

<sup>411</sup> Como señala Vizcaíno Calderón, “se ha dicho que la causa que legitima las excepciones o modulaciones a los derechos y garantías del afectado que puedan resultar de la regulación especial de estos ficheros, se encuentra en el interés público concretado en la protección del tráfico económico, particularmente en el que se mueven las entidades de crédito”. VIZCAINO CALDERÓN, Miguel. *Comentarios a la Ley Orgánica de protección de datos de carácter personal*. Madrid: Civitas, 2001, p. 301.

<sup>412</sup> Audiencia Nacional. Sentencia de 30 mayo 2007, (JUR 2007\19947).

**también** al tratamiento de datos “relativos al cumplimiento o incumplimiento de obligaciones dinerarias”, dichos registros, por su naturaleza, forman parte de la esfera de la apreciación de las condiciones económicas del afectado, siendo este su objeto.

Tal aspecto refuerza la idea expuesta, pues aunque pueda haber diferencias entre los dos tipos de registros de informaciones personales, sus objetivos prácticos son los mismos, razón por la cual la LOPD los trata en el mismo artículo. Para Alonso Martínez<sup>413</sup>, “el artículo 29 no establece una tipología de ficheros sino que regula los derechos y obligaciones de los sujetos activos que desarrollan la actividad prevista por la norma”. La misma opinión parece compartir Prats Albentosa<sup>414</sup> refiriéndose al orden normativo de los datos descritos en el artículo 29.1, opina que “tiene por objeto la regulación mediante de disposiciones no disponibles, de una actividad entre particulares; y afecta no solo a la delimitación de su objeto, sino también, y sobre todo, a la prestación de la actividad —servicios de información sobre solvencia patrimonial y crédito previo tratamiento de datos personales—”. En efecto, el artículo 29.1 empieza su redacción estableciendo que “quienes se dediquen a la **prestación de servicios** de información sobre la solvencia patrimonial y el crédito” deberán obedecer a la disciplina legal allí impuesta.

El Reglamento 1720/2007, en su artículo 37 dispone sobre el régimen aplicado a estos ficheros, y reitera los términos del apartado 2 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, permitiendo el tratamiento de los datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En la opinión de Prats

---

<sup>413</sup> ALONSO MARTINEZ, Carlos. *apud.* VIZCAINO CALDERÓN, Miguel. *Comentarios...* *op.cit.*, p. 302.

<sup>414</sup> PRATS ALBENTOSA, Lorenzo. *Ficheros... op.cit.*, p. 221.

Albentosa<sup>415</sup>, el cometido fundamental del reciente RPD, arts. 37 a 44, “es, antes que el objeto (el fichero), la actividad, o mejor, las actividades: en primero lugar la regulación de la conducta consistente en tratar datos relativos a la solvencia patrimonial y el crédito de las personas (art. 29.1 LOPD), y, en segundo lugar, la que consiste en tratar datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias (art. 29.2 LOPD)”.

Para Agencia Nacional de Protección de Datos<sup>416</sup> la citada norma hace claramente una diferencia de dos tipos de ficheros, quedando los regulados por el artículo 29.1 de la Ley Orgánica 15/1999 sometidos al régimen general establecido en las normas de protección de datos y siendo de aplicación las especialidades de la Sección Segunda del Capítulo I del Título IV del reglamento únicamente a los ficheros regulados por el artículo 29.2 de la Ley Orgánica.

Sin embargo, en un informe jurídico más reciente, aparentando matizar su opinión, el citado órgano<sup>417</sup> ha pronunciado que el artículo 29 de la LOPD perfila “dos posibles tipos de ficheros (**o de tratamientos dentro de un mismo fichero**) diferenciados por el origen de los datos, de los cuales los segundos son los que generalmente se conocen como “ficheros de morosos”, donde los datos incluidos no provienen del deudor ni de fuentes accesibles al público, y se distinguen de los primeros que se orientan más bien a actividades de información comercial o evaluación de la solvencia económica de personas físicas”.

Como puede apreciarse, los datos que puedan determinar la capacidad crediticia de los afectados sean ellos positivos, como también negativos, los dos, pueden ser objetos de la prestación del servicio de información

---

<sup>415</sup> PRATS ALBENTOSA, Lorenzo. *Ficheros... op.cit.*, p. 220.

<sup>416</sup> Informe Jurídico 52/2008.

<sup>417</sup> Informe Jurídico 237/2009.

sobre la solvencia patrimonial y el crédito, según dispone el texto legal. Sobre este tema, Freixas Gutiérrez<sup>418</sup>, opina que “estamos ante ficheros en los que pueden convivir datos que acrediten una situación económica real y favorable de los afectados y otros que inciden una situación económica negativa facilitada por los perjudicados de esta situación, los acreedores”.

Además, el artículo 29.2 menciona el cumplimiento o incumplimiento de obligaciones dinerarias, cuyo sentido semántico aislado nos lleva a pensar en el primero como una acción de contenido positivo y en el segundo una acción negativa o más bien omisa. Sin embargo, el análisis del significado entendemos debe ser general, o sea, la consideración de la acción concurrente de cumplir o no una obligación. Por mejor decir, en las palabras de Díez-Picazo<sup>419</sup>, “en su dinámica, la relación obligatoria puede desembocar en unos hechos reales, que coincida con el primitivo programa o que se desvíen de él”. De suerte que para el autor en cita, “cumplimiento e incumplimiento son de este modo las dos grandes alternativas en que puede desembocar el vehículo dinámico en que la obligación consiste: cumplimiento si los actos reales se ajustan al programa inicial e incumplimiento si se desvían de él”.

Es interesante observar es que ni la LOPD ni su reglamento de desarrollo en ningún momento hablan de la mora, pero de *incumplimiento* de obligación dineraria. Tampoco utiliza la expresión retraso o retardo. Ello nos hace pensar que el legislador quiso mantenerse al margen de la discusión doctrinal sobre la mora y sus efectos. Sobre este tema, según apunta Díez-Picazo<sup>420</sup>, que en lo concerniente a la relación existente entre retardo y mora, la doctrina se divide en dos corrientes de pensamiento: una primera entiende que la *mora debentis* sería la traducción del retraso a términos jurídicos, de suerte que el mero retraso por sí solo es un hecho

---

<sup>418</sup> FREIXAS GUTIERREZ, Gabriel. *La protección... op. cit.*, p. 269 y 270.

<sup>419</sup> DÍEZ-PICAZO, Luis. *Fundamentos... op. cit.*, p. 541.

<sup>420</sup> DIEZ-PICAZO, Luis. *Fundamentos..., op. cit.*, p. 657.

jurídicamente intrascendente. De forma que “sólo cuando al retraso se añaden los presupuestos necesarios para entender al deudor constituido en mora, aparecen las consecuencias jurídicas y el retraso elevado a la categoría de derecho de crédito”.

La segunda tesis defiende que todo retardo es ya de por sí una infracción de los deberes que el deudor soporta y puede, por consiguiente desencadenar una responsabilidad de manera que para esta corriente, la mora sería un retardo cualificado del cual surgen unas consecuencias jurídicas especiales y, particularmente, una especial agravación de la responsabilidad del deudor, que opera fundamentalmente en lo siguiente: la conveniencia de asegurar una sanción eficaz en materia de obligaciones pecuniarias, donde no resulta fácil establecer la existencia y el alcance de los daños con arreglo a los principios generales de la teoría de la responsabilidad civil.

Pese a ello, la elección de utilizar la expresión ‘*incumplimiento*’ en el artículo 29.2 de la LOPD suscita otras cuestiones, como por ejemplo qué tipo de incumplimiento debe ser considerado. En la opinión de Prats Albentosa<sup>421</sup>, respecto a estos datos descritos en el artículo 29.2 de la LOPD, “ha de interpretarse en sentido jurídico estricto que es ‘cumplimiento y incumplimiento’, y, en concreto, al incumplimiento al que se refiere este precepto de la LOPD es al incumplimiento definitivo”. Así para este autor el mero retardo del deudor no tiene porque suponer un caso de incumplimiento definitivo. De esta suerte, él entiende que “los datos de un deudor en una obligación dineraria, si no ha sido incumplida definitivamente, no pueden ser cedidos por el acreedor, ni tratados por un tercero, sin el consentimiento previo e inequívoco del deudor”.

---

<sup>421</sup> PRATS ALBENTOSA, Lorenzo. *Ficheros... op.cit.*, p. 223.



En lo que concierne específicamente al incumplimiento, observa Llamas Pombo<sup>422</sup>, que el ordenamiento jurídico español “cifra la fuente material del incumplimiento en la idea de ‘*contravención*’, que abarca de la forma más amplia posible toda la clase de lesión al interés del acreedor”. Ello, en su opinión, ahorra muchos esfuerzos a la doctrina y jurisprudencia a la hora de incardinar dentro del concepto de ‘*contravención*’ toda clase de supuestos de lesión al derecho de crédito. Ahora bien, para establecer cuando se da el incumplimiento definitivo el citado autor<sup>423</sup> apunta que “la clave estará en que el mismo sea todavía posible y útil – aunque tardío –, en cuyo caso existirá la mora, o que por el contrario, ya no pueda cumplirse con utilidad al acreedor, lo que conduce al incumplimiento total”.

Ésta también parece ser la opinión de Díez-Picazo<sup>424</sup>, para quien “en la mora, el comportamiento del deudor o los impedimentos transitorios, conducen a una omisión de la prestación pero el obstáculo es todavía superable. De esta suerte, la prestación puede todavía ser realizada, y, una vez realizada, aunque lo sea tardíamente, es todavía idónea para satisfacer el interés del acreedor, a cuya obtención la relación obligatoria se dirige. Una hipótesis completamente distinta se presenta en aquellos casos en que la omisión de ejecución de la prestación ha de considerarse como un fenómeno definitivo, de tal suerte que ya no cabe el cumplimiento tardío o que, aunque teóricamente posible, no es legítimo imponérselo al acreedor”. Para el Tribunal Supremo<sup>425</sup>, “la mora no es un supuesto de incumplimiento, sino un caso de cumplimiento tardío de la obligación”.

---

<sup>422</sup> LLAMAS POMBO, Eugenio. “Comentario al artículo 1.101”. En: *Jurisprudencia Civil Comentada*. PASQUAU LIAÑO, Miguel (Dir.). Granada: Comares, Tomo II, 2009, pp. 1851-1852.

<sup>423</sup> *Ibid.*, p. 1840.

<sup>424</sup> DIEZ-PICAZO, Luis. *Fundamentos...*, *op. cit.*, p. 763.

<sup>425</sup> STS. de 28 de septiembre 2000 [R 7533].

Interpretar la norma de protección de datos en lo que concierne a la expresión 'incumplimiento' en sentido estricto, es decir, como incumplimiento definitivo no nos parece la que más se compatibiliza con la función de dichos ficheros. No es nuestro objetivo profundizar en el tema de la teoría de las obligaciones, sin embargo a ella recurrimos ya que las hipótesis legales para la configuración del incumplimiento definitivo son diversas y la prueba para su tipificación no siempre es sencilla. Además, en el ámbito de los ficheros de solvencia patrimonial, solamente un tipo de obligación, en el caso las dinerarias, están sujetas a ser allí registradas. De forma que la propia característica de la citada obligación impide que ella se devenga imposible, con carácter general y absoluto, como puntualiza Díez-Picazo<sup>426</sup>. A este respecto, es interesante mencionar que la Agencia Española de Protección de Datos<sup>427</sup> ha manifestado con mucha propiedad que "la obligación cuyo incumplimiento haya generado la deuda ha de ser necesariamente de carácter dinerario, como expresamente indica el precepto citado, quedando excluida por tanto la posibilidad de incluir datos cuando la relación obligacional no tenga tal carácter (así por ejemplo, aquéllas cuyo objeto sean prestaciones personales). También se excluye la posibilidad de incluir otros datos relativos a solvencia patrimonial o crédito distintos de los atinentes a aquellas obligaciones".

En realidad, la ley no ha conferido poderes a la mera inscripción en un banco de datos de solvencia patrimonial a punto de causar algún efecto legal en lo que concierne a la tipificación normativa de la mora o del incumplimiento definitivo. De este modo, creemos que el legislador no quiso interponerse en las peculiaridades de los efectos jurídicos de la lesión al derecho al crédito. Pero aparte de la problemática en el ámbito del derecho de las obligaciones, ha establecido sus propios parámetros

---

<sup>426</sup> DIEZ-PICAZO, Luis. *Fundamentos...*, op. cit., p. 293.

<sup>427</sup> Informe Jurídico 237/2009.

para la inclusión de los datos en los registros de solvencia patrimonial y crédito.

No nos parece que a la LOPD le interese si el deudor ya ha incurrido en mora o mismo si la obligación ya se configura como definitiva. La problemática y los efectos que puede causar en el ámbito de los derechos de las obligaciones de un incumplimiento, de la mora o de un sencillo retardo no pueden inmiscuirse con la normativa específica de la LOPD. La Audiencia Nacional<sup>428</sup>, analizando un supuesto semejante, entre las especificidades del Código Civil y de la LOPD, concretamente en lo que respecta a la exigencia de requerimiento de pago para la inclusión de los datos en un registro de moroso, se ha pronunciado de la siguiente forma: “la exigencia o no de requerimiento de pago a efectos civiles y en aplicación de lo previsto por el artículo 1100 del Código Civil (que no exige dicho requerimiento cuando la obligación así lo declare) **puede tener efectos puramente civiles pero no afecta a la exigencia de cumplimiento de un requisito que tiene su origen, exclusivamente, en la normativa específica de protección de datos**” (subrayamos). Pensamos que si la LOPD no establece a que tipo de incumplimiento hace referencia, así como no se remite a las disposiciones del Código Civil en la materia, y aún establece sus propios requisitos para la inclusión de los datos en los ficheros de solvencia patrimonial, ha creado dentro de su ámbito de aplicación una exigencia específica cuyos efectos no tendrán injerencia en aquellos civiles.

Además de todo ello, creemos que la función de estos ficheros es, como hemos comentado, la protección del sistema crediticio. Si hay que esperar a un incumplimiento definitivo, en este tiempo el deudor podrá establecer nuevas relaciones crediticias con otras entidades financieras, sin que estas sepan que el interesado ya está incumpliendo una obligación anterior. De este modo, frustraría la función de tales bancos de datos. Por eso, a

---

<sup>428</sup> Audiencia Nacional. Sentencia de 9 enero 2009 (RJCA 2009\217).

nuestro sentir, la ley detalla un tipo específico de incumplimiento, válido para el ámbito de su aplicación, que se perfecciona cuando concurren las características de la deuda que será registrada.

Ahora bien, el hecho de que no exista un incumplimiento de una obligación es un factor impeditivo de registro del dato en los ficheros de solvencia patrimonial, si no hay consentimiento del interesado, porque ahí sí, sería regido por el régimen general. Una de las exigencias del artículo 38, apartado 1 del RPD, que establece los requisitos **concurrentes** de inclusión de los datos de carácter personal — que serán analizados más adelante — es la existencia de una deuda cierta, vencida, exigible. De suerte que para que la deuda exista, alguien anteriormente ha contraído una obligación, y para que esté vencida y sea exigible, deberá haberse cumplido la condición o el plazo sin que el deudor haya la satisfecho. Cuando se registra un dato sobre el incumplimiento, indirectamente se está informando sobre el cumplimiento de la obligación, siendo la única excepción si tal incumplimiento se da de toda la prestación debida.

Por todo ello, los datos únicamente sobre el cumplimiento de una obligación no pueden ser tratados obedeciendo el régimen especial del artículo 29.2 de la LOPD y por lo tanto, nos lleva a concluir que tal dispositivo se refiere a los datos negativos.

En el caso de los datos tratados por el artículo 29.1 de la LOPD, y pese a que el citado dispositivo determine que sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento entendemos que los datos procedentes de fuentes accesibles al público que tengan un contenido negativo pueden ser tratados en los ficheros de solvencia patrimonial, ya que la norma no especifica ninguna prohibición, como lo hace con los datos sobre cumplimiento y incumplimiento de obligaciones dinerarias.

De hecho, como bien apunta Freixas Gutiérrez<sup>429</sup>, es difícil imaginar que los propios interesados faciliten datos o consientan su tratamiento cuando hagan referencia al incumplimiento de obligaciones dinerarias o que acrediten una situación financiera negativa. De suerte que tales informaciones tendrán que ser recabadas de otras fuentes, pero siempre respetando los derechos de los afectados y los principios rectores de la protección de los datos de carácter personal.

De esta manera, desde nuestra perspectiva, la norma establece que hay dos tipos de datos que pueden coexistir en un mismo fichero, cuya clasificación prefiere hacerla en función de las fuentes en las cuales serán obtenidos y no de su contenido: aquellos recabados de fuentes accesibles al público, o procedentes de informaciones facilitadas por el interesado o con su consentimiento y los datos facilitados por el acreedor o por quien actúe por su cuenta o interés. En efecto, aunque para la Agencia Española de Protección de Datos<sup>430</sup> existan dos tipos de ficheros, apunta que “la prestación de servicios de información sobre solvencia patrimonial y crédito se encuentra regulada por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, **que distingue dentro de los mismos, por razón del origen de los datos incluidos en ellos**, aquéllos en que los datos proceden de fuentes accesibles al público o han sido facilitados por el propio interesado (artículo 29.1 LOPD), de aquéllos otros en que los datos han sido facilitados por el acreedor o por quien actúa por su cuenta (artículo 29. 2)”.

En nuestra opinión, la LOPD en el artículo 29 no distingue ficheros, pero dos formas de recabar los datos que sean determinantes para enjuiciar la solvencia patrimonial del afectado, de tal manera que ello por sí mismo diferencia el contenido de las informaciones en sentido estricto, ya que no todas las informaciones ofrecidas por el interesado y aquellas

---

<sup>429</sup> FREIXAS GUTIERREZ, Gabriel. *La protección... op. cit.*, p. 269.

<sup>430</sup> Informe Jurídico 0237/2009.

que se pueden acceder en una fuente accesible al público son las mismas que el acreedor puede aportar. Por lo tanto, tenemos aquellos que hacen referencia el artículo 29.1 y los regulados por el artículo 29.2, referente al cumplimiento de obligaciones dinerarias, en un fichero cuya finalidad es el tratamiento de información que permita evaluar la situación económica de los afectados.

Lo que no ha sido aclarado por la LOPD, ni por su reglamento de desarrollo es la definición de la expresión “datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado”, extraída de la primera ley en el apartado 4 del artículo 29, y repetida por la segunda en el artículo 38 apartado 1. La única diferencia entre una y otra norma es que la Ley Orgánica especifica que tanto el **registro** como la **cesión** sólo podrán ser realizados de aquellos datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados, mientras que el Reglamento limita a referirse únicamente a la **inclusión** de estos datos en el fichero.

Es cierto que la expresión anteriormente citada puede ser interpretada desde una perspectiva restricta, en el sentido de que se haga alusión nada más que a los datos referentes a la deuda y al deudor respetando el principio de la proporcionalidad. No obstante una expresión tan genérica, vaga y indeterminada suscita otros cuestionamientos sobre todo cuando es repetida por una norma posterior, como lo hace el Reglamento de desarrollo de la LOPD, en el artículo dedicado a los requisitos de inclusión de datos.

Así, nos conviene indagar ¿cuál ha sido precisamente la intención del legislador? Como se ha dicho, no consideramos suficiente plantearla únicamente dentro del margen del principio de la calidad de los datos, como una exigencia reiterada de que sean estos adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades determinadas, expresas y legítimas para las cuales fueran recabados. Aunque nunca es

demasiado insistir en el ámbito legal sobre la necesidad de respetar tal principio, en este caso concreto opinamos que es necesario plantear algunas otras cuestiones.

Desde esta perspectiva, creemos que es muy importante valorar que los datos son determinantes para enjuiciar la solvencia económica del afectado. Por estar dentro del ámbito de los que tratan sobre incumplimiento de obligaciones dinerarias, no sería necesario recalcar que son datos negativos sobre deudas. Es decir, son informaciones de impagos que por su dimensión pueden interferir en la solvencia del afectado. Hemos tenido la oportunidad de destacar que actualmente los ficheros de solvencia patrimonial y crédito tienen una finalidad que va más allá del campo de actuación particular empresa-cliente, pero que guarda una función social dentro de un interés más amplio que es ayudar al sistema financiero. Así, teniendo en cuenta que la finalidad del fichero no es sencillamente catalogar aquellos que tienen obligaciones dinerarias no cumplidas, pero evaluar la capacidad crediticia del individuo para evitar riesgos al negociar con un potencial cliente, opinamos que es dentro de este contexto que debemos interpretar también la expresión utilizada por la LOPD y por el Reglamento 1720/2007.

Ahora bien, la otra duda que surge al analizar estos dispositivos es la siguiente: ¿a partir de que importe una deuda tiene la capacidad de calificar la situación de solvencia de un individuo? La Agencia Española de Protección de Datos<sup>431</sup> ha dejado claro que “no existe, por otro lado, importe mínimo establecido en la ley para la comunicación de los datos”. Pero los cuestionamientos no se agotan ahí. Porque si cualquier impago resultado de una obligación dineraria puede figurar en un registro de solvencia patrimonial, la pregunta es: ¿una deuda de cien mil euros, de diez o de mil euros, o incluso de cien euros son todas igualmente determinantes para enjuiciar la solvencia de una persona? Y más allá del

---

<sup>431</sup> Informe Jurídico 237/2009.

planteamiento del valor en sí, ¿una factura impagada de un servicio de telefonía, agua o luz es un dato “determinante para enjuiciar la solvencia económica” de un individuo? De modo que el eje de la cuestión es conseguir solucionar una pregunta sencilla en su formulación, pero de una alto grado de complejidad práctica: ¿qué parámetros se debe seguir para valorar la cuantía aceptable que tiene la capacidad de enjuiciar la solvencia del afectado? Ninguna respuesta hemos conseguido ni en la LOPD, en el RPD, tampoco en las dos instrucciones de la Agencia de Protección de Datos nº 1/1995, de 1 de marzo, y la nº 1/1998, de 19 de enero, así como en la jurisprudencia, ni sobre la el alcance de la expresión, ni tampoco específicamente sobre los parámetro que deben ser utilizados para su interpretación.

Sobre esta cuestión Prats Albentosa<sup>432</sup> refiriéndose a los datos sobre el cumplimiento o incumplimiento de obligaciones dinerarias subraya que no todo dato relativo a la conducta obligacional del deudor es determinante para llevar a cabo la evaluación de la solvencia de su titular, ya que en su opinión, “esta interpretación equivaldría a una habilitación general para registrar, ceder y conocer cualquier dato personal por irrelevante que sea, que tenga alguna relación con la conducta obligacional de una persona”. Así, el autor citado opina que los datos que se traten deben de tener relevancia para la realización del fin previsto por la ley, de suerte que para saber “cuándo posee relevancia, parece oportuno atender a qué datos son tomados en consideración por la Ley para entender — es decir, son determinantes para enjuiciar— que una persona se encuentra en la situación económica contraria, esto es, en estado de insolvencia”. Además, entiende él<sup>433</sup> que “no cualquier incumplimiento, en sí mismo considerado, puede tener el grado de permitir evaluar la solvencia económica del deudor. Ha implicar el incumplimiento de una obligación de trascendencia para el patrimonio

---

<sup>432</sup> PRATS ALBENTOSA, Lorenzo. *Ficheros... op.cit.*, pp. 227-228.

<sup>433</sup> *Ibid.*, p. 229.



del deudor, de tanta, que sea relevante para conocer su 'solvencia económica'", opinión con la cual coincidimos.

Desde nuestro punto de vista, el tratamiento legal Español sobre este tema después de la entrada en vigor del Reglamento de desarrollo de la LOPD, ha mejorado de manera significativa la disciplina de la materia, pero no ha logrado compaginar la finalidad de la norma con el principio de la calidad de los datos. Más bien, ha contribuido para aumentar esta problemática. El RPD en el artículo 38 permite que, una vez superado los tres requisitos especificados en las líneas *a)* existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada; *b)* que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico y *c)* requerimiento previo de pago a quien corresponda el cumplimiento de la obligación; se pueda incluir los datos de una deuda en los ficheros aquí estudiados.

Delante de los cuestionamientos arriba suscitados, opinamos que habría que replantear la valoración de los datos negativos que se pueden registrar en los ficheros de solvencia patrimonial. De una parte, reevaluar y determinar cual valor específicamente puede ser considerado como un alerta, suficientemente capaz de valorar la solvencia del afectado. Dentro de este entorno, haciendo un análisis de los múltiples aspectos que envuelve la cuestión, como por ejemplo el valor total de la deuda, la cantidad ya cumplida y la está pendiente de pago, etc.

Por otro lado, hay que tenerse en cuenta a quién se destinan estas informaciones registradas en estos ficheros y qué se pretenden con ellas. Es decir, como hemos subrayado anteriormente, estos ficheros no tiene la finalidad de crear un catalogo de deudores. No conviene ser un mero registro de morosos, porque un moroso no es necesariamente un insolvente. Hay que distinguir estas dos figuras también en el ámbito de los registros de solvencia patrimonial y crédito. No conseguimos

vislumbrar ninguna utilidad social efectivamente sólida que justifique la creación de un fichero con estas características, o por mejor decir, que posee una utilidad que sea capaz de predominar sobre el derecho a la intimidad y a la autodeterminación informativa.

Además de ello, el destinatario de estas informaciones son entidades cuya principal actividad, como asegura la propia Agencia de Protección de Datos<sup>434</sup>, es la financiación de bienes y servicios o de operaciones que permitan la compra de productos a crédito, aunque no sea necesario que la sociedad pertenezca a un determinado sector de actividad.

Lo que no resulta totalmente comprensible es la razón por la cual las empresas como por ejemplo de telefonía puede utilizarse de estos servicios si no se dedican a ninguna actividad financiera como actividad principal pero sí de prestación de servicios básicos. Son establecimientos que comparten sus informaciones con el sistema financiero sin a él pertenecer. Pensamos que estos datos no deberían ser objetos de los ficheros de solvencia patrimonial. Si la intención es proteger el negocio en el ámbito de su actividad, sería causa de creación de un fichero específico con la finalidad de proteger esta actividad en particular y las informaciones cedidas solamente entre las empresas de este sector.

La importancia de determinar un valor concreto que sea suficientemente capaz de evaluar la solvencia de un individuo de un lado evitaría la banalización de los registros de solvencia patrimonial y de otro podría permitir que el acumulo de deudas de un determinado sector que no se dedicara a la actividad financiera como actividad principal pudiera comunicar los datos a este registro de solvencia patrimonial y crédito

---

<sup>434</sup> Agencia Española de Protección de Datos: “Inspección a un fichero común de información sobre solvencia patrimonial e incumplimiento de obligaciones dinerarias”. Disponible en

[https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/recom\\_fichero\\_solvencia.pdf](https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/recom_fichero_solvencia.pdf) .

siempre y cuando el valor total de una o varias deudas alcanzara el nivel de “determinante para enjuiciar la solvencia” de una persona.

## 2. Legislación Italiana.

La *Centrale dei Rischi* é un sistema informático que reúne informaciones económicas cedidas por bancos y intermediarios financieros a sobre las transacciones realizadas con sus clientes. Así, contienen una serie de datos relativos a diversos sujetos y responde a una concreta exigencia de los empresarios financieros que es evaluar anticipadamente el grado de fiabilidad de sus clientes, con el objetivo de proveerles un grado razonable de seguridad en el momento de ofrecer un crédito, contribuyendo, por otro lado, para aumentar la estabilidad del sistema bancario y financiero. En Italia, la doctrina divide dichos ficheros en dos categorías, a saber, públicos y privados. Lo más importante en la diferenciación de uno y otro es la aplicabilidad o no del Código de Buena Conducta. De modo que solamente para las centrales de riesgos privadas habrá la incidencia de dicho Código.

Petrulli<sup>435</sup> destaca entre las principales características de las centrales de riesgos privadas, la ausencia de una entidad de vigilancia como existe para las centrales de riesgos públicas; la inexistencia de un límite del importe que puede ser allí registrados en los bancos de datos privados, ausencia de norma legislativa y reglamentaria, con la presencia solamente

---

<sup>435</sup> PETRULLI, Mario. *Il nuovo Codice deontologico per le centrali rischi private e le tutele per i consumatori*. Matelica: Editora Halley, 2005, p. 15

de una norma auto impuesta y, finalmente, la ausencia de obligatoriedad legal de insertar los datos del afectado en los ficheros.

Según el mismo autor<sup>436</sup>, existen varios tipos de centrales de riesgos públicas, siendo tres las principales. La primera denominada “*Servizio per la centralizzazione dei rischi bancari*”, es gestionado por la *Banca d'Italia*, cuya disciplina se encuentra principalmente en el Decreto Legislativo n.º 385 de 1º de septiembre de 1993, además de la deliberación de 16 de mayo de 1962 del *Comitato Interministeriale per il Crédito ed il Risparmio*<sup>437</sup> (en adelante CICR) y reglamentos de la propia *Banca d'Italia*. Dichos ficheros deben comunicar mensualmente a la *Banca d'Italia* los datos relativos a los créditos acordados y su uso. Así, estas informaciones son enviadas individualizando el titular, el tipo del contrato de crédito y el importe utilizado. En este fichero solamente comportan datos de créditos concedidos con importe superior a setenta y cinco mil euros.

El segundo tipo de central de riesgo pública es el banco de datos que tratan los registros de importes inferiores a 75.000 euros y superiores a 31.245 mil euros. Este fichero fue instituido por deliberación de la CIRC

---

<sup>436</sup> *Ibid.*, p. 13. En la opinión de IMPERIALI, existen solamente dos tipos de centrales de riesgos públicas: aquella gestionada por la *Banca d'Italia* y la SIA.

<sup>437</sup> El CICR es, de acuerdo con la estructura del mercado financiero de Italia, uno de los órganos responsable por la disciplina y la supervisión de la actividad bancaria, en este caso por la vigilancia en materia de crédito y tutela del ahorro, sin perjuicio de otras funciones atribuidas por el *Testo Único Bancario (TUB)* y en otras leyes. El CICR está compuesto por el Ministro de Economía y Hacienda, que es el presidente, el Ministro de Comercio Internacional, el Ministro de las políticas agrícolas Alimentaria y Forestal, el Ministro del Desarrollo Económico, el Ministro de Infraestructura, el Ministro de Transportes y el Ministro para las políticas Comunitarias. Vid.

[http://www.bancaditalia.it/servizi\\_pubbl/conoscere/vocabolario/C/cicr.txt](http://www.bancaditalia.it/servizi_pubbl/conoscere/vocabolario/C/cicr.txt)

de 3 de mayo y es gestionado por la *Società Interbancaria per L'automazione*<sup>438</sup> (en adelante, SIA).

Finalmente, la *Centrale di allarme interbancaria* (CAI) que es un banco de datos creado por la Banca d'Italia, a través de la ley 25.6.1999, n° 205, y del Decreto legislativo de 30.12.1999, n° 507. Contiene datos relativos a aquellos individuos que han emitido cheques bancarios y postales sin autorización o presentados al pago sin provisión de fondos, así como las sanciones administrativas o judiciales impuestas derivadas de este hecho. Igualmente se registran los datos de aquellos a los cuales se hayan retirado la autorización al uso de tarjetas de crédito y débito, debido a la falta de pago de las cantidades correspondientes a las operaciones o transacciones realizadas con estas tarjetas<sup>439</sup>.

Los bancos de datos que interesan a este estudio son los denominados *centrali rischi private*. Como ya como he destacado anteriormente, dichas centrales de riesgos privadas no poseen una legislación formal específica, pero una autorregulación a través del código de buena conducta que fue firmado en 12 de noviembre de 2004, por las principales entidades

---

<sup>438</sup> La SIA es un proveedor de servicios y soluciones tecnológicas para el sistema bancario y financiero, es responsable por la realización de algunos de los sistemas y soluciones para el proceso de automatización e integración de los sistemas financieros italianos, como por ejemplo la Red Nacional Interbancaria (RNI o SIAnet), entre otros. Desde el año de 2007 la empresa se denomina SIA-SSB, cuando hubo la fusión entre la SIA (*Società Interbancaria per l'Automazione*) e SSB (*Società per i Servizi Bancari*). Vide <http://www.siassb.eu>.

<sup>439</sup> Vide PETRULLI, Mario. *Il nuovo...op. cit.*, pp. 14-15 y también la definición de la Banca d'Italia en

[http://www.bancaditalia.it/servizi\\_pubbl/conoscere/vocabolario/C/cai](http://www.bancaditalia.it/servizi_pubbl/conoscere/vocabolario/C/cai).

representativas del sector y algunas asociaciones de consumidores<sup>440</sup>, y ha entrado en vigor en 1º de enero de 2005.

Compuesto por catorce artículos, el Código de buena conducta del sistema de información crediticia disciplina todos los aspectos concernientes al tratamiento de estos datos. Inicia el texto legal con las principales definiciones pertinentes a la materia, indica la finalidad del tratamiento de los datos, sus requisitos y categoría, el tiempo de conservación y las medidas de seguridad que deben ser adoptadas, los deberes de los responsables y encargados, así como los derechos de los afectados.

Además de las definiciones de la ley general de protección de datos italiana, el Código de buena conducta añade otras relativas al ámbito de su aplicación. Entre ellas, el artículo 1, c) especifica lo que es el sistema de información crediticia y acrecienta que en ellos pueden contener en particular: a) información crediticia de tipo negativo, que sólo afectan a relaciones de crédito para los cuales se hayan producido incumplimientos; b) información crediticias de tipo positivo y negativo, que afectan a peticiones/relaciones de crédito independientemente de la subsistencia de incumplimientos registrados en el sistema en el momento de su comprobación.

---

<sup>440</sup> Son ellas: AISReC - *Associazione italiana delle società di referenza creditizia*; ABI - *Associazione bancaria italiana*; FEDERCASSE - *Federazione italiana delle banche di credito cooperativo*; ASSOFIN - *Associazione italiana del credito al consumo e immobiliare*; ASSILEA - *Associazione italiana leasing*; CTC - *Consorzio per la tutela del credito*; ADICONSUM - *Associazione difesa consumatori e ambiente*; ADOC - *Associazione per la difesa e l'orientamento dei consumatori*; ADUSBEF - *Associazione difesa utenti servizi bancari finanziari assicurativi e postali*; CODACONS - *Coordinamento delle associazioni per la difesa dell'ambiente e la tutela dei diritti di utenti e di consumatori*; FEDERCONSUMATORI - *Federazione nazionale consumatori e utenti*.

En el artículo 3 dedica 5 párrafos para regular el objeto de los citados ficheros, estableciendo los requisitos y la categoría de los datos que pueden ser registrados. De modo somero, el párrafo primero determina que el tratamiento efectuado en el ámbito de un sistema de información crediticia sólo afecte a los datos relativos a la persona que solicita o es parte de una relación crediticia con un participante<sup>441</sup>, y al sujeto codeudor, también solidario, cuya posición es claramente distinta a la del deudor principal.

Según observa Imperiali e Imperiali<sup>442</sup>, las centrales de riesgos se distinguen entre “negativas”, que tratan datos relativos al incumplimiento y mora en el pago; y las “positivas” que colectan datos respecto a al comportamiento del deudor. El Código de buena conducta no prohíbe que en el mismo fichero se traten informaciones negativas y positivas conjuntamente.

Según el *Garante*<sup>443</sup>, con el Código de buena conducta, se legitima el recabo, tratamiento, y circulación de informaciones relativas a préstamos, financiación, aplazamientos de pago, compras aplazados de bienes de consumo, otras facilidades financieras sobre consumidores y empresas.

---

<sup>441</sup> Según definición del propio Código de Buena Conducta, art. 1º, e), participante es el sujeto privado titular del tratamiento de datos personales concernientes a solicitudes/relaciones de crédito, que en virtud de contrato o acuerdo con el gestor participa en el sistema de información de crédito y puede utilizar los datos del sistema, se obligando a comunicar al gestor tales datos personales relacionados con demandas/relaciones de crédito de forma sistemática, en un marco de reciprocidad en el intercambio de datos con otros participantes. Con excepción de los sujetos que trabajan en el cobro de la deuda, el participante puede ser: 1. un banco; 2. un intermediario financiero; 3. otra entidad privada que, en el ejercicio de una actividad comercial o profesional, concede un aplazamiento de pago de la contrapartida para el suministro de bienes o servicios.

<sup>442</sup> IMPERIALI, Riccardo. *Codice... op.cit.*, p. 992.

<sup>443</sup> Garante per la Protezione dei Dati Personali. Dossier – 30 de noviembre de 2005.

De suerte que en la sistemática jurídica italiana, el objeto de los ficheros de solvencia patrimonial y crédito son objetivos y restrictos a aquellas relaciones o solicitud de crédito, los riesgos a estas relacionados así como para evaluar la situación financiera y el mérito crediticio de los interesados o, en cualquier caso, su fiabilidad y puntualidad en los pagos.

En este sentido, no es lícito el registro de facturas impagadas de teléfono en estos bancos de datos, así como no es legal el acceso de empresas de telefonía a las informaciones contenidas en el sistema de información crediticia para fundamentar la elaboración de contrato con un posible cliente. El *Garante* incluso antes de la entrada en vigor del Código de buena conducta se había pronunciado sobre la imposibilidad de tal conducta. Así, ha expresado que en los sistemas de información crediticias (SIC), que a partir del primero de enero 2005 tomarán el lugar de las "centrales riesgos privadas", podrán figurar solamente datos actualizados y relativos al verdadero y propio riesgo de crédito y no informaciones relativas a facturas telefónicas no pagadas y contratos de telefonía existentes: "el tratamiento de estos últimos tipos de información no pertinentes, no es en esta sede lícito, debe ser suspendido inmediatamente y los datos personales borrados por las grandes bases de datos"<sup>444</sup>.

---

<sup>444</sup> *Newsletter* nº 238 del 20 - 26 dicembre 2004. *Vide*, también, el *Provvedimento* del 16 settembre 2004, en *Bollettino* n. 53/settembre 2004 (doc. web n. 1068987).



### 3. Legislación Brasileña.

El caso de Brasil resulta más complicado que el de España e Italia. Este país no posee, como ya hemos comentado, una legislación general de protección de datos, pero varias normas específicas y muy criticables para cada sector. Los ficheros aquí estudiados son llamados *Banco de dados de proteção ao crédito* y están reglamentados en el Código de Defensa del Consumidor, ley 8.078/90, artículo 43.

Es importante resaltar que ninguno de los cinco párrafos que componen el artículo 43 se dedica a establecer que tipos de datos son allí tratados de suerte que la doctrina ha tenido que hacer el trabajo interpretativo para extraer de la norma cada uno de los ficheros específicos que pretende regular, así como sus respectivos objetos.

La sección en la cual está ubicado el artículo 43 del CDC se titula *Dos Bancos de Dados e Cadastros de Consumidores*. Es decir, en un mismo artículo el Código regula dos tipos de ficheros, en un intento de reglamentar los derechos del consumidor en dos situaciones completamente distintas.

Según Herman de Vasconcelos Benjamin<sup>445</sup>, archivo de consumo es un género que pertenece a dos especies de ficheros: los *banco de dados* y los *cadastros de consumidores*. Aquellos que tienen correspondencia con el Derecho español a los ficheros de solvencia patrimonial y crédito, son en Brasil especies de banco de datos de consumidores, que en la doctrina son más conocidos como servicios de protección al crédito. Ya lo que se entiende por *cadastros de consumidores* son ficheros privados comunes en España, cuyo objetivo es mantener comunicados a los proveedores con los consumidores, y su objeto es dar algunos datos personales del cliente para

---

<sup>445</sup> PELEGRINE GRINOVER, Ada; VASCONCELOS BENJAMIN, Antonio Herman; *et. al.* *Código Brasileiro... Op. Cit.*, p. 422.

facilitar esa comunicación: así, nombre, dirección, preferencias personales relativas al sector específico del proveedor, etc.

En el caso de los *Bancos de Datos*, expresión genérica de ficheros, al ubicarse en el Código del Consumidor, se entiende por banco de datos de consumo, como resalta la doctrina<sup>446</sup>, aquellos cuya información registrada es importante para el mercado de consumo. Según Roscoe Bessa<sup>447</sup>, la ley limita con la expresión banco de datos de consumidores la calidad de las informaciones que pueden ser registradas, excluyendo de su disciplina los tratamientos de datos que no digan respecto al mercado de consumo. Es decir, como subraya Herman de Vasconcelos Benjamin<sup>448</sup>, cualesquier otras informaciones sobre datos personales del consumidor como su familia, su carácter, su reputación no son aceptadas por dichos banco de datos.

La redacción del artículo 43 del CDC es un poco confusa en lo que concierne a la denominación utilizada para expresar los bancos de datos que deben observar su disciplina. En efecto, se utiliza de diversas denominaciones, como “banco de datos”, “servicio de protección al crédito”, etc. Según el autor<sup>449</sup> del anteproyecto de este dispositivo del CDC, hay un desvío intencional de técnica legislativa, con el afán de ser lo más explícito y categórico posible, al incluir lado a lado en un mismo dispositivo, género y especie.

---

<sup>446</sup> HERMAN DE VASCONCELOS BENJAMIN, Antonio; LIMA MARQUES, Claudia; ROSCOE BESSA, Leonardo. *Manual de Direito do Consumidor*. São Paulo: RT, 2008, p. 240

<sup>447</sup> ROSCOE BESSA, Leonardo. *O Consumidor... Op. Cit.*, p. 178.

<sup>448</sup> PELEGRINE GRINOVER, Ada; HERMAN DE VASCONCELOS BENJAMIN, Antonio, et. al., *Código Brasileiro... Op. Cit.*, p. 435.

<sup>449</sup> *Ibid.*, p. 422

Hay que señalar además, que aludido precepto no establece la finalidad de ficheros que reglamenta, ni, como ya comentado, cual es su objeto. Aparentemente fue un intento de crear un microsistema de protección de datos que aún que no sea criticable pues en su momento consiguió alcanzar su objetivo, pensamos que actualmente es un dispositivo ultrapasado, porque empiezan a surgir otros problemas que son procedentes no de una relación de consumo solamente, sino de un derecho autónomo a la protección de datos. Por todo ello, el trabajo de la doctrina y jurisprudencia en este tema es muy importante para imponer los límites a estos bancos de datos.

De este modo, los bancos de datos de protección al crédito, como apunta Roscoe Bessa<sup>450</sup>, tratan informaciones relativas a deudas vencidas y no pagadas, aunque empieza a observarse en los últimos años el tratamiento de informaciones positivas<sup>451</sup>. Así, por regla general, cualquier deuda ya vencida y que no haya sido pagada, independiente de qué naturaleza jurídica, de su valor y de la actividad al cual pertenece el responsable por la información puede figurar en el sistema de protección al crédito, sean relativas a personas físicas o jurídicas.

Según el Reglamento interno<sup>452</sup> de unos de los más grandes ficheros de solvencia patrimonial y crédito de Brasil, el *SPC*, en el Capítulo VI cuando trata de los procedimientos generales de los registros para su uniformización, especifica en el artículo 20 que se considera incumplimiento para la finalidad de anotación en el citado fichero, el retraso en el pagamiento derivada de las operaciones mercantiles, financieras, prestación de servicios y cualesquier otras operaciones legales, que puedan ser comprobadas a través de instrumentos propios

---

<sup>450</sup> ROSCOE BESSA, Leonardo. *O Consumidor... Op. Cit.*, p. 33.

<sup>451</sup> HERMAN DE VASCONCELOS BENJAMIN, Antonio. *Manual... Op. Cit.*, p. 243.

<sup>452</sup> Es un reglamento que vincula únicamente aquellos ficheros que son parte del *SPC*.

tales como, contratos, cheques, nota promisorio, entre otros. En el párrafo primero del mismo artículo prohíbe el registro de los datos del cónyuge del deudor principal, así como del socio o administrador de la persona jurídica cuando no son solidariamente responsables.

Además, resulta interesante subrayar la exigencia mínima de los datos que deben ser registrados con el débito. Establece el artículo 33 que son ellos para persona física: a) el nombre completo del deudor principal, fiador o avalista; b) fecha de nacimiento; c) número del *Cadastro de Pessoa Física*<sup>453</sup>; d) dirección completa del deudor; e) valor y número del documento que originó el débito; f) fecha de vencimiento de la deuda; g) nombre y código del asociado (SPC) que registró la deuda; h) si en el registro el interesado es el deudor principal, fiador o avalista; y, finalmente, la identificación del sitio donde ocurrió el incumplimiento que dio origen al registro.

Por todo ello, se puede desprender que lo que ocurre en Brasil, es que los datos del mercado de consumo se mezclan con aquellos otros que solo interesan al mercado financiero y de crédito o tributarios, ya que una ejecución fiscal también puede ser registrada en lo que se entiende por sistema de protección al crédito<sup>454</sup>.

Como se sabe, los ficheros de solvencia patrimonial fueron creados en Brasil en los años 50, donde hubo una expansión de la concesión de crédito por el comerciante directamente al consumidor. Como todo el proceso era realizado manualmente y las informaciones tenían que ser

---

<sup>453</sup> CPF es un banco de datos gerenciado por la Secretaria de la *Receita Federal do Brasil* que almacena informaciones cadastrales de los contribuyentes que están obligados a inscribirse. Por mejor decir, es la identidad financiera de una persona, aunque no obligatoria su posesión, es necesaria para identificarse al realizar cualquier operación financiera. Para más informaciones, vide la pagina web de la Hacienda <http://www.receita.fazenda.gov.br/PessoaFisica/Cpf/PerguntasRespostas/Default.htm>

<sup>454</sup> STJ. REsp nº 229.278/PR, Rel. Ministro Aldir Passarinho Junior, DJU 07.10.2002.

obtenidas en cada tienda en las cuales el consumidor ya había anteriormente comprado. Además, cada establecimiento poseía y administraba su propio banco de datos, siendo un proceso largo, demorado y muy costoso. Con la intención de tornarlo más eficaz y barato, la asociación de los comerciantes de algunas provincias crearon el *Sistema de Proteção ao Crédito* – SPC<sup>455</sup>, como una entidad que tenía (y tiene) la función exclusiva de gerenciar estos tipos de informaciones<sup>456</sup>.

Ahora bien, ya no estamos en los años cincuenta y en la actualidad ha habido una fuerte tendencia a que las actividades relacionadas con el crédito se especialicen. Por regla general, el comerciante ha dejado de ser el responsable directo para la concesión de crédito; ya no asume más estos riesgos. La realidad actual perfectamente comprobada por la práctica, aunque pueda haber excepciones, demuestra que han surgido empresas que facilitan el crédito al consumidor, y algunas veces poseen oficina dentro del establecimiento del empresario, pero este último no dispone de ningún tipo de crédito directo. Por mejor decir, esta financiación directa entre empresario-consumidor de productos es una práctica que poco a poco empieza a desaparecer, dando lugar a las empresas que sirven de intermediarios entre estos dos sujetos.

De este modo entendemos que debe haber una reevaluación no solamente del objeto de los servicios de protección al crédito de Brasil, pero también a quién y a qué se destinan, ya que muchos empresarios utilizan los datos de los servicios de protección al crédito para otras finalidades que no aquellas para las cuales fueron estos ficheros creados, como no contratar a una persona por tener el registro en los “ficheros de

---

<sup>455</sup> Vide sobre ese tema: ROSCOE BESSA, Leonardo. O Consumidor... *Op. Cit.*, p. 29 y ss.

<sup>456</sup> Parece oportuno subrayar que éste no es el único fichero dedicado a prestar éste servicio. Los principales además del SPC son *Centralização de Serviços de Bancos S.A* – SERASA y el *Serviço de Proteção ao Crédito do Brasil - Check-Check*. Vid. ROSCOE BESSA, Leonardo. O Consumidor... *Op. Cit.*, p. 30.

moroso”<sup>457</sup>, o incluso la propia Administración Pública tiene acceso a estos registros y lo utiliza como justificativa para eliminar ciudadanos del proceso de un concurso a un cargo público<sup>458</sup>.

Sobre este punto, el magistrado Ruy Rosado<sup>459</sup> consignó en fallo que “el *Serviço de Proteção ao Crédito* (SPC), instituido en diversas ciudades por las entidades de clase de comerciantes, tienen la finalidad de informar a sus asociados sobre la existencia de débitos pendientes por el comprador que pretenda obtener nuevo financiamiento. Es evidente que el beneficio que de él se deriva a favor de la agilidad y de la seguridad de las operaciones comerciales, así como no se puede negar al vendedor el derecho de informarse sobre el crédito de su cliente y de compartir con los demás los datos que dispone sobre él. Esa actividad, sin embargo, en razón de la propia importancia social y de los graves efectos de ella decurrentes – ya que incluso para inscripción en concurso público tiene sido exigida certificado negativo del SPC – debe ser ejercida dentro de los límites que, permitiendo la realización de su finalidad, no se transforme en causa y ocasión de daño social mayor de lo que el bien visado”.

En Brasil, tal y como se presenta la ley, una deuda del seguro de salud, de facturas de teléfono, de agua, de luz, del financiamiento de coche, de la

---

<sup>457</sup> Marimpietri, advierte que es práctica común de varias empresas no contratar a personas que tengan su nombre registrado en un fichero de protección al crédito, aunque esto no perjudique su futura función en dicha empresa. MARIMPIETRI Flavia. “Consumismo e Superendividamento” [en línea]. Editora Magister. <https://www.magisteronline.com.br>. [Consulta en 17 de noviembre de 2009]. También disponible en: Revista Magister de Direito Empresarial, Concorrencial e do Consumidor nº 27 - Jun/Jul de 2009.

<sup>458</sup> El Tribunal de Justicia del *Rio Grande do Sul* emitió fallo manifestando la ilegalidad de la conducta de la Administración pública en aquél caso concreto, que se oponía a los principios de la razonabilidad y proporcionalidad. TJRS. AC nº 70002436368. Rel. Augusto Otávio Stern. Fecha de juzgamiento: 03/04/2001.

<sup>459</sup> STJ, REsp 22.337-8/RS, Rel. Min. Ruy Rosado de Aguiar, DJU 20.04.95.

hipoteca, etc., de cualquier valor, que no haya sido pagada, puede ser transmitida a los bancos de datos de protección al crédito, además, en los casos de los prestadores de servicios, el ciudadano tiene dicho servicio interrumpido.

Lima Marques<sup>460</sup> consigna que en Brasil, en la práctica no resulta infrecuente que la utilización algunas veces negligente y otras dolosas de estos bancos de datos están causando grandes y reiterados daños a los consumidores. De todas maneras es necesario reforzar la importancia de esos registros, cuando bien legislada la materia, para las entidades de servicios financieros, aunque deban ser severamente fiscalizados, pues los efectos de sus informaciones, utilizadas sin límites, pueden causar un grave daño social.

En los casos de los títulos de crédito, específicamente el cheque, en Brasil hay un fichero de libradores de cheques sin fondos, mantenido por los bancos. De suerte que nada más que al intentar sacar el dinero del banco, si no tiene provisión de fondos, se devuelve el título al tenedor del cheque y automáticamente estos datos van a dicho fichero que comunica sus informaciones a los demás bancos de datos de protección al crédito. De forma que en estos casos para que la deuda figure en tales bancos de datos no es necesario el protesto del título. En los demás supuestos, los títulos protestados que están en los banco de datos del notariado responsable, igualmente se comunican con los citados ficheros.

El párrafo 2º del artículo 29 de la Ley nº 9.492<sup>461</sup>, de 10 de septiembre de 1997 establece que las informaciones relativas al crédito solo podrán ser comunicadas de aquellos protestos cuyo registro no fueron cancelados y

---

<sup>460</sup> LIMA MARQUES, Claudia. "Comentario al artículo 43". *Comentarios ao Código de defesa do Consumidor*. LIMA MARQUES, Claudia; HERMAN DE VASCONCELOS BENJAMIN, Antonio; MIRAGEM, Bruno. São Paulo: Revista dos Tribunais, 2006, p. 611.

<sup>461</sup> Define competencia, reglamenta los servicios concernientes a los protestos de títulos y otros documentos de deudas y da otras providencias.

el propio *caput* del mismo artículo determina que en el notariado que se lleva a cabo el protesto del título debe enviar, cuando solicitados, un certificado diario, en forma de lista, de los protestos quitados o cancelados<sup>462</sup>.

Lo cierto es que, como bien subraya el magistrado José Otavio de Noronha en el juzgamiento del *Recurso Especial* nº 686.203/AL/2009, el título regularmente protestado funciona solamente como uno de los muchos datos que pueden constar en los ficheros de moroso, pero ni toda información constante de estos órganos necesita estar fundada en título protestado. Además, no se puede imponer, desde su punto de vista, el protesto como condición obligatoria para alimentar datos que fundamentan la concesión de crédito en el mundo comercial, porque el dispositivo legal anteriormente mencionado no lo exige como condición necesaria para posibilitar el registro en los órganos de restricción al crédito.

En el fallo, también se dejó consignado, sobre este tema, que los ficheros de protección al crédito no usurpan la función de los notariados ya que la actuación de un y de otro es completamente distinta, es decir, los bancos de datos registran y proporcionan informaciones acerca del incumplimiento de deudas a los diversos sectores de la economía, relacionados sobretudo al crédito y al consumo, apoyando las decisiones que envuelven la concesión del crédito. Por otro lado, los notariados proceden el protesto de títulos que tienen por función constituirse en acto probatorio o aún resguardar o constituir derechos, relacionándose íntimamente, aunque no exclusivamente con el mundo cambiario.

---

<sup>462</sup> Según el *Superior Tribunal de Justiça*, la limitación contenida en el artículo 29 §2º de la ley 9.492/97 dice respecto a la información prestada por el notariado a los bancos de datos de restricción al crédito, ya que solamente puede constar de la relación suministrada los protestos regulares y cuyos registros no hayan sido cancelados. STJ. RESP 686.203/AL, Rel. João Otávio de Noronha, DJe 15/06/2009.



Desde nuestro punto de vista, la estructura del sistema de protección al crédito de Brasil es muy criticable. Aunque este hecho se debe no solamente a la ausencia de una ley de protección de datos sobre todo en el ámbito privado, pero también a una falta de cultura social ante esta problemática.

De cualquier modo, el Proyecto de Ley nº 85/2009 con el texto que se ha presentado al Senado Federal actualmente ha acertado muchísimo cuando excluye de los ficheros de solvencia patrimonial el tratamiento de datos que sean resultado de incumplimiento de un servicio de facturación periódica. Aunque es cierto que habrá de esperar a que terminen las discusiones sobre el aludido texto legislativo y aguardar los eventuales cambios que pueden ocurrir. Pero lo cierto es que si no hubiere alteración, en este punto Brasil avanzaría mucho en lo que concierne al pensamiento legislativo del derecho a la protección de datos personales.

## **V. Los destinatarios de la información de los ficheros de solvencia patrimonial y crédito.**

Nos parece importante que la problemática de los ficheros de solvencia patrimonial y crédito no sea reflejada solamente desde la perspectiva de su finalidad y su objeto, sino también de los destinatarios de los datos, es decir, a quién interesa las informaciones allí registradas.

En Italia por lo que se puede observar, los destinatarios de las informaciones allí incluidas son aquellas personas participantes del sistema de información crediticia de este país, conceptuadas en el artículo 1, letra e) del Código de buena conducta, que los define como el sujeto

privado titular del tratamiento de los datos personales recogidos en el ámbito de las solicitudes/relaciones de crédito, que en virtud de contrato o acuerdo con el responsable del fichero participa del sistema de información crediticia y podrá utilizar las informaciones allí registradas, estando obligado a comunicar a dicho responsable los citados datos personales relativos a solicitud/relaciones de crédito de modo sistemático, en el marco de reciprocidad en el intercambio de datos con otros sujetos participantes. Así, la norma especifica que exceptuando las entidades de recuperación crediticia, los participantes pueden ser un banco, un intermediario financiero, o otro sujeto privado que en el ejercicio de una actividad comercial o profesional, concede un aplazamiento del pago de la contrapartida para el suministro de bienes o servicios en virtud del texto único de las leyes en materia bancaria y crediticia (Decreto legislativo n. 385, de 1 de septiembre 1993).

De este modo, el entendimiento de la Agencia de protección de datos italiana<sup>463</sup>, no conlleva la inclusión de los proveedores de servicios de comunicación telefónica, entre los sujetos anteriormente mencionados, pues no efectúan contratos de financiación, ni siquiera en la forma del aplazamiento del pago (frente a los cuales puede hacerse lícito uso de los mencionados sistemas de información crediticias), pero contemplan contratos de ejecución continuados o periódicos (en particular, de administración de servicios telefónicos o de alquiler de terminales). Concluyendo el *Garante* que los plazos periódicos representan, en efecto, no un aplazamiento del pago de la suma debida, sino (simplemente) los términos de los cuales esta última deberá ser pagada por el usuario en contrapartida de prestaciones consumidas en el correlativo margen temporal (relacionadas, en el caso, a la concesión de servicios de telefonía o al disfrute de bienes).

---

<sup>463</sup> Garante per la Protezione dei Dati Personali. Provvedimento de 4 de mayo de 2006. *Gestori Telefonici: Informazioni sulla Solvibilità e Affidabilità dei Clienti*.

El sistema de protección al crédito en España y Brasil siguen por otro camino distinto al de Italia. De hecho, la legislación española en el reglamento 1720/2007, artículo 42, regula el acceso a las informaciones contenidas en el fichero que tratan de datos sobre cumplimiento o incumplimiento de obligaciones dinerarias. La aludida norma incluye una excepción que nos parece muy elogiada ya que determina que únicamente permite que terceros accedan los datos de estos ficheros cuando precisen enjuiciar la solvencia económica del afectado. El mismo precepto determina cuando concurre dicha circunstancia enumerando las siguientes: a) que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida; b) que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio; y c) que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica. Tal precepto será mejor analizado en el capítulo siguiente.

En el caso de Brasil, a las informaciones registradas en los sistemas de protección al crédito se pueden acceder por cualquier entidad financiera y cualquier empresario de bienes de consumo o servicio, de cualquier naturaleza, siendo suficiente para ello asociarse al citado sistema, y efectuar el pago de la cuota establecida y a partir de ahí disfrutar de las informaciones de cualquier individuo, a cualquier momento, con independencia de que estén manteniendo una relación comercial, financiera o de servicio o incluso ninguna de ellas. Lo que se quiere decir es que cualquier tipo de establecimiento, debidamente registrado en la Cámara de comercio, la inscripción en la Hacienda en el *Cadastro Nacional da Pessoa Jurídica*<sup>464</sup> (CNPJ), y en la asociación de comerciantes, esta última responsable por la gestión de uno de los principales servicios de protección al crédito, ya está habilitada a afiliarse a un fichero de

---

<sup>464</sup> El CNPJ es el registro administrado por la *Receita Federal do Brasil* que registra las informaciones de las personas jurídicas y de algunas entidades no caracterizadas como tales. Vid. <http://www.receita.fazenda.gov.br/GuiaContribuinte/CNPJ/Default.htm> .

protección al crédito y acceder a sus datos. El propio reglamento del SPC determina en su artículo 15 que pueden ser usuarios de sus servicios las empresas mercantiles, prestadoras de servicios, profesionales liberales y cualquier otro que tenga una actividad similar reglamentada por ley. Además de las empresas de cobro que no pueden registrar informaciones pero sí consultarlas, así como las comunidades de vecinos y las inmobiliarias que pueden tanto consultar como registrar informaciones.

Es cierto que en Brasil, como ya hemos comentado, es muy común en los negocios efectuados en el comercio la utilización del aplazamiento de pagos en todos los sectores, para todo tipo de bienes, sean ellos perecederos o no. Son aquellas denominadas “*transacciones económico-financieras* por operaciones concertadas previa o simultáneamente (comerciales)”<sup>465</sup>. De suerte que negocios que se dedican por poner un ejemplo, a mercancía textil, o incluso supermercados (grandes o pequeños), suelen dividir el valor total de la compra, en pequeños plazos mensuales, con independencia del tipo del producto adquirido, algunas veces solamente limitado por el valor total de la compra. En efecto, se presentan generalmente en dos modalidades: la financiación por cuenta ajena, donde el empresario no respalda a deuda, pero deja la responsabilidad a una entidad de crédito, como en los casos de las tarjetas de crédito o el crédito al consumo; y la financiación por cuenta propia, donde el empresario hace las veces de una entidad de crédito, aplazando el pago de la deuda, usando principalmente el cheque como garantía de pagamento, donde la fecha de vencimiento es aplazada en cada cheque, mes a mes y solamente cuando llega la fecha inscrita en el cheque, el comerciante va hasta la entidad bancaria cobrarlo. De hecho, en Brasil hubo una desvirtualización del uso de dicho título de crédito, patrocinada por este tipo de práctica comercial.

---

<sup>465</sup> Expresión utilizada por RIVERO ALEMÁN, Santiago. *Crédito, consumo y comercio electrónico*. Navarra: Aranzadi, 2002, p. 67.

Por todo lo expuesto anteriormente, los bancos de datos de información crediticia han surgidos, como hemos comentado, por iniciativa de la asociación de comerciantes. Sin embargo, no se puede comparar los peligros que existían para los derechos y libertades fundamentales de los individuos en 1950 y en los días actuales con el proceso de automatización de los datos. Creemos que no es posible permitir que pasados tantos años que el requisito para acceder a un banco de datos de solvencia patrimonial y crédito sea únicamente tener la categoría de persona jurídica, fundamentalmente cuando se puede apreciar los cambios en el sector tecnológico que ha influido en todos los ámbitos de la vida cotidiana, incluyéndose ahí las relaciones crediticias y el propio desarrollo de los derechos fundamentales.

Aparte del natural interés de los afectados en las informaciones incluidas en los ficheros de solvencia patrimonial implica por su peculiar finalidad, como ya se ha comentado, tanto la sociedad como los partícipes de los mercados financiero, de crédito y de consumo, todos ellos, tienen interés a que de modo general sus operaciones sean las más beneficiosa y con menos riesgo posible.

No obstante ello, nos parece interesante plantear algunos aspectos. Primero, a nuestro juicio entendemos que en los días actuales es rechazable cualquier propuesta de creación de un fichero que pueda reflejar múltiples aspectos de la vida de un individuo sin que proporcionalmente no se exija las garantías necesarias para que dichos datos solamente circulen estrictamente dentro del ámbito de sus finalidades, aparte de que se establezca los derecho y obligaciones de aquellos implicados.

En efecto, los ficheros aquí estudiados contienen con respecto al del ciudadano mucho más que una deuda impagada. Se tiene a vista para los que acceden a las informaciones registradas el histórico de la vida patrimonial del individuo y su capacidad de crédito, sobre todo cuando se

nota una cierta tendencia en compaginar los datos positivos y negativos de los afectados en los citados ficheros. Aspectos como: con quién uno contrata, cual valor, cuanto ya ha satisfecho de la deuda total, si está o no en mora, etc., solamente son algunas de las múltiples informaciones que se puede extraer de estos bancos de datos. De forma que también revelan por vía transversa el objeto comprado o el servicio que fue prestado dependiendo de la empresa que ha anotado los datos, el objeto obtenido, la evolución de la vida financiera y patrimonial del ciudadano, posibles problemas de ejecución de deudas en juicio y con ello una información aunque superficial del mérito de tal procedimiento, en fin, todas estas informaciones en un único fichero, y lo más delicado es que después de obtenerlas, aquél que las posee va a hacer un evaluación, emitiendo un juicio de valor sobre la posibilidad de efectuar una operación de crédito o no con el afectado, aunque basado en datos objetivos.

De modo que nos parece que son datos que por un lado informan más allá de su contenido objetivo, siendo a la vez muy específicos, con una finalidad muy restricta de auxilio al sistema financiero y principalmente al mercado crediticio. Ahora bien, el hecho de que contribuya con dicho mercado, no quiere decir que todos sus partícipes tengan legitimidad para consultar estas informaciones. Los aludidos datos, como hemos consignado, evalúan la capacidad patrimonial de un individuo, pero únicamente sirven en el momento en que se establece una relación bilateral entre entidad financiera-cliente, cuando este último solicita el crédito. De forma que únicamente en este preciso instante, es cuando el primero tiene un interés directo sobre dichas informaciones y consecuentemente podrá utilizar estos servicios. Después de la evaluación y del desenlace de la transacción del crédito, sea ella positiva o negativa, aquél que antes era un interesado directo, vuelve a su posición de interesado indirecto o secundario, careciendo legitimidad para acceder a los datos específicos del individuo que no sean aquellos que dicha entidad haya registrado, restando únicamente el deber de aportar a los ficheros la

información del retardo del deudor en cumplir con su obligación o incluso los datos positivos de la concesión de crédito si es el caso.

Ahora bien, esto no afecta a aquellos datos históricos y principalmente a los estadísticos que en efecto son informaciones que sirven a todos los interesados indirectos, es decir a los partícipes del sistema financiero, al gobierno, a la sociedad, etc. Aunque estas son informaciones que por su naturaleza no identifica a un individuo. El hecho de que una entidad colabore compartiendo informaciones a un determinado banco de datos, este acto no le confiere *de per se* el derecho a acceder a cualesquier informaciones de los afectados.

El Proyecto de Ley nº 85/2009 establece en su artículo 15 que aquellos que consulta las base de datos de los ficheros de solvencia patrimonial solo podrán acceder a las informaciones del afectado que con este mantuviere relación comercial o crediticia. Además, en el artículo 2º dedicado a las definiciones legales, denomina lo que sería para la legislación española el 'acrededor' y para la italiana el 'participante' como *consulente* y establece que este es la persona natural o jurídica que accede a las informaciones en los banco de datos **para fines de concesión de crédito o otras transacciones comerciales y empresariales**.

En este último dispositivo encontramos un problema. La finalidad del acceso desde nuestro punto de vista no debería estar en el artículo dedicado a las definiciones, ya que es imposible en este ámbito aclarar todos los supuestos. En este caso específico, creemos que el legislador mezcla la finalidad de acceso de los datos de personas físicas con aquellos de personas jurídicas, cuando utiliza la expresión **otras transacciones comerciales y empresariales**. Consideramos que interpretar de otro modo sería admitir un amplio abanico de posibilidades para aquellos que pueden acceder al sistema de protección al crédito.

## VI. TOMA DE POSICIÓN.

La Directiva Comunitaria 95/46, consignó en su considerando nº 53 que determinados tratamientos pueden presentar riesgos particulares desde el punto de vista de los derechos y las libertades de los interesados, ya sea por su naturaleza, su alcance o su finalidad, como los de excluir a los interesados del beneficio de un derecho, de una prestación o de un contrato, o por el uso particular de una tecnología nueva. De este modo, compete a los Estados miembros, si así lo desean, precisar tales riesgos en sus legislaciones.

Éste es, precisamente, el caso de las informaciones tratadas por los ficheros de solvencia patrimonial y crédito. Aunque no es de ningún modo un registro vinculante en la relación crediticia, la practica enseña que ello impide el acceso de los interesados a una operación de crédito. Como observa Almuzara Almaida, los límites establecidos en la legislación se justifican para garantizar los derechos de los afectados, “puesto que la inclusión en un fichero de solvencia patrimonial y crédito supone una importante restricción de sus posibilidades futuras de acceso a créditos”.

Desde nuestra perspectiva, la legislación italiana en lo que concierne a la adecuación del binomio finalidad-objeto de los banco de datos de crédito es la que sistemáticamente mejor resguarda los derechos y libertades fundamentales de los afectados, sobre todo respecto al derecho a la autodeterminación informativa.

Como hemos podido dejar consignado, opinamos que la creación de un fichero es un derecho que posee cualquier persona física o jurídica, de derecho público o privado, desde que se cumplen algunos criterios que lo



legítima, como por ejemplo la definición específica de la finalidad de dicho registro y que ésta tenga un carácter revestido en una función social. Además, para nosotros, desde un punto de vista interpretativo, su finalidad debe ser entendida siempre de modo restrictivo. De esta manera, cuando se analizan los ficheros de solvencia patrimonial y crédito en lo que respecta a su finalidad, hemos consignado nuestra opinión defendiendo su finalidad como auxiliares del sistema financiero.

A nuestro modesto juicio, consideramos que la interpretación de la finalidad de tales bancos de datos restricta al ámbito del mercado de consumo está ultrapasada. En efecto, no se puede negar que lo incluye, sin embargo no se agota en este espacio así como no sirve a todos sus aspectos. Es decir, pensamos que no todo el mercado de consumo necesita de las informaciones registradas en el citado sistema de información. De otro lado, entendemos que el objeto de dichos ficheros son aquellos datos resultantes de una operación crediticia. Y de estas relaciones, sí puede haber un interés que implique al mercado de consumo, pero las informaciones más importantes para los partícipes del citado mercado no son aquellas de solvencia patrimonial y crédito, pero a las referentes concretamente a su tipo de negocio.

Así, a nuestro sentir, la legislación italiana en comparación con la normativa española y la brasileña tuvo más sensibilidad al separar los destinatarios a los cuales realmente importan las informaciones allí registradas, de aquellos que no las necesitan, además de establecer y acotar el objeto de éstos ficheros acorde con sus finalidades. De esta manera, rechaza cualquier registro en éstos bancos de datos de información provenientes de relaciones de servicios, como la telefonía, restringiéndoles a su finalidad específica: las relaciones de crédito. Ahora bien, entendiendo por relación de crédito dentro de la definición del Código de conducta, en el artículo 1º, a), siendo cualquier petición o relación relativas a la concesión, en el ejercicio de una actividad comercial o profesional, de crédito en forma de aplazamiento de pago, de

financiación o de otra facilidad financiera en virtud del texto único de las leyes en materia bancaria y crediticia (d.lg. 1 *settembre* 1993, n. 385).

En España y sobre todo en Brasil, los ficheros de protección al crédito son verdaderos “supermercados” de datos de la vida patrimonial de los ciudadanos. Es decir, de sus relaciones de consumo de bienes y servicios, de sus relaciones mercantiles, financieras, de crédito, en fin un gran almacén de informaciones a disposición tanto de las entidades de créditos como aquellas prestadoras de bienes y servicios.

A nuestro juicio, habría que separar en los citados países la protección tocante a las relaciones de consumo principalmente las relativas a la prestación de servicios con aquellas del crédito. Por mejor decir, en lo que respecta a los destinatarios, observamos que hay una cierta confusión en dichas legislaciones así como en la jurisprudencia y, en el caso de España, en los procedimientos sancionadores de la Agencia de protección de datos.

Opinamos que el origen de todo ello en España es la propia ley que no ha sistematizado mejor la inclusión del tratamiento de informaciones relativas a contratos de prestación de servicio que tenga el pago aplazado del precio. Ello tiene que encajarse con el carácter de que sea suficiente para enjuiciar la solvencia de uno. Y creemos que en raras ocasiones el hecho de no pagar una cuota periódica de una prestación de servicio se subsume al objetivo de los ficheros de solvencia patrimonial y crédito. En efecto, cuando no se procede al pago correspondiente a la prestación de un servicio, éste se interrumpe y así es imposible que se continúe a sumar los valores subsecuentes a dicha suspensión de servicio. De manera que en nuestra opinión, este tipo de datos procedentes de supuestos así, deberían ser tratados fuera del ámbito de los ficheros de solvencia patrimonial y crédito. Es más, son datos que interesan a los prestadores de servicios dentro del ámbito de su específico negocio. La creación de ficheros específicos serviría para alcanzar el objetivo de la protección

sectorial de los prestadores de servicios dentro del mercado de consumo. De suerte que las empresas tendrían un fichero donde pudiesen registrar los datos de impago relativos a incumplimiento de obligación dineraria procedente del contrato de prestación de servicios y sus efectos serían semejantes a los del fichero de solvencia patrimonial, es decir, la imposibilidad del consumidor a contratar con otras empresas que prestasen el mismo servicio si sus datos estuviesen registrados en dicho fichero.

También hay que subrayar nuestra posición respecto al artículo 42, párrafo 1º que determina que los datos contenidos en el fichero común sólo podrán ser consultados por terceros cuando precisen enjuiciar la solvencia económica del afectado. En particular, recoge la ley, se considerará que concurre dicha circunstancia entre otras, en el supuesto que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida. A nuestro juicio tal regla debería ser matizada. Como ya hemos indicado, la manutención de un contrato que no se encuentra vencido no es razón suficiente para legitimar la consulta de los datos del individuo en el sistema de protección al crédito. Si es así, todos aquellos que tienen contratada una hipoteca podrá pasar toda su vida teniendo sus datos a disposición de un establecimiento financiero, aunque solamente haya tenido una relación contractual. Desde nuestro punto de vista lo que legitima la consulta a los ficheros no es la manutención de una relación contractual, sino la solicitud para concretarla. Al final, los ficheros de solvencia patrimonial y crédito son una protección preventiva para el mercado de crédito y sus entidades. Pasada la fase de solicitud, firmada la relación contractual, no hay más ninguna razón para que la entidad financiera acceda a estos datos hasta que, como la propia ley enfatiza, sea el caso de enjuiciar la solvencia patrimonial del afectado y este supuesto solamente ocurrirá si este vuelve a requerir un crédito. Ahora bien, para esta regla la excepción consistiría, para el cumplimiento del deber de obedecer al principio de la calidad de los datos, en el caso de que sea necesaria la inclusión de nuevos datos

sobre la misma persona, o mismo la rectificación de aquellos ya registrados lo que supondría la necesidad del acceso y consulta de dichas informaciones específicas. Ahora bien, de las aludidas informaciones y no otras relativas al mismo individuo registradas por otros participantes del sistema.

En cuanto a las empresas prestadoras de servicios creemos que estas no tienen ninguna legitimidad para acceder a los datos de los individuos en un sistema de información crediticia y desde nuestra modesta opinión, el reglamento se contradice. Si lo que pretende es enjuiciar capacidad de satisfacer las deudas, el impago de una factura telefónica no es un dato *de per se* característico para tal empeño. Quizás el conjunto de facturas impagadas, con un valor relativamente alto, no contestada ni administrativa ni judicialmente podría constituirse en un alerta e interesar al mercado de crédito. Pero por la propia naturaleza de la facturación es un dato que no importa al citado mercado, así como al revés, es decir, la información sobre el incumplimiento de una obligación por un individuo que deja, por ejemplo, de pagar su hipoteca no interesa a las compañías de telefonía. Son actividades totalmente distintas ya que estas empresas no participan, no contribuyen ni influyen en el mercado de crédito. No ofertan productos financieros en tal mercado, es más, tienen el derecho que de suspender el servicio periódico una vez comprobado el impago de una factura. Los establecimientos financieros no pueden interrumpir un crédito pues la propia naturaleza del contrato no lo permite, necesitándose una acción preventiva de valoración de riesgos.

Estos mismos planteamientos pueden ser aplicados para el caso brasileño. Aunque en este país hay un agravante en relación a España que es además de la ausencia de una ley general de protección de datos, el silencio del Código del Consumidor en lo que concierne a la finalidad de los bancos de protección al crédito, a su objeto y su acceso.

No hay otro el motivo más que en la doctrina se puedan encontrar posiciones firmemente contrarias a estos ficheros, como es el caso de Ramos Covizzi<sup>466</sup>, para quien los servicios de protección al crédito en Brasil, tal y como fueron instituidos provocan graves violaciones a los derechos fundamentales y contradicen a las garantías individuales aseguradas constitucionalmente a los ciudadanos que en dichos ficheros estuvieren incluidos. Inevitablemente, continua el autor citado, de esta actividad proviene: a) la apertura de un procedimiento de cobro que condiciona el acceso al crédito a las informaciones allí registradas; b) a privación de la libertad individual de contratar y de negociar si no satisfecho dicho proceso de cobro; y por último la humillación, la deshonra provocada por la pérdida de la confianza pública en el cumplimiento de la obligaciones. Concluye que el impedimento del acceso al crédito por el impago de las prestaciones registradas en los ficheros de protección al crédito se equipara a una sanción, legitimada solamente si aplicada por el Poder Judicial, lo que significaría deducir que impuesta de este modo es equiparable aquellas deducidas por los juicios de excepción, expresamente expugnados por el texto constitucional.

---

<sup>466</sup> RAMOS COVIZZI, Carlos Adroaldo. *Práticas Abusivas da SERASA e SPC*. São Paulo: Edipro, 2001, p. 29. En el idioma original: "os serviços de proteção ao crédito, da forma como estão implementados na sociedade brasileira, provocam graves violações aos direitos fundamentais e contradizem aos garantias individuais asseguradas constitucionalmente aos cidadãos que nele estiverem incluídos, porque, inevitavelmente, da atividade decorrem: a abertura de um procedimento de cobrança que condiciona a interdição do acesso ao crédito ao resultado; a privação da liberdade individual de contratar e de negociar senão satisfeito o procedimento de cobrança, e por último, a humilhação, a desonra provocada pela perda da confiança pública no cumprimento das obrigações. O impedimento de acesso ao crédito pelo não pagamento da prestação apontada nos serviços de proteção ao crédito, equipara-se a uma sanção, legitimada somente se aplicada pelo Poder Judiciário, o que significa deduzir que, assim imposta, é equiparável àquelas deduzidas pelos juízos de exceção, expressamente expugnados pelo texto constitucional".

En efecto también compartimos de la opinión de que los servicios de protección al crédito tal como aparecen configurados en Brasil, actualmente son utilizados de modo que violan derechos fundamentales de las personas como el de la autodeterminación informativa, la intimidad y el honor. Los ficheros tienen sus propias reglas, no hay una autoridad independiente que vigile tal actividad, y los Tribunales se encuentran abarrotados de casos que en gran parte de los supuestos se arreglarían con un procedimiento administrativo.

La ausencia de una cultura social y jurídica de protección de datos en este país ha provocado graves daños económicos y sociales. La fragilidad del sistema es tamaña que con respecto al último caso denunciado<sup>467</sup> de la pagina Web *www.twister-ss.com* que vendía a cualquier persona el acceso general y simultáneo a los principales bancos de datos del país, totalizando más de veinte ficheros de más de cien millones de brasileños. Entre ellos, *Serasa-Equifax*, *SPC*, *Check-Check*, *Credd*, *ACSP*, siendo estos citados, los principales ficheros de protección al crédito del país. Pese al peligro de tal conducta, es perfectamente comprensible que se de tal situación ya que no existe ninguna legislación que les imponga reglas de seguridad y ningún órgano que vigile estos bancos de datos, es decir, un sistema legal y administrativo de protección preventiva de los derechos de los ciudadanos en relación a estos ficheros.

De tal manera que en Brasil, el sistema de protección al crédito protege mucho a éste y muy poco a las personas. Hay una descompensación de derechos y deberes entre los responsables de los ficheros y de los afectados. Sin embargo son bancos de datos, como hemos recalado, que cuando están bien regulados contribuyen al desarrollo económico de un país, aunque éste no es en absoluto el caso brasileño. No existe una

---

<sup>467</sup> El caso fue denunciado por el canal de televisión SBT, cuyo video está disponible en internet a través de la pagina Web <http://noticias.uol.com.br/ultnot/multi/2009/10/08/0402386EC4B94366.jhtm?site-reune-dados-sigiliosos-de-cidadaos-senhas-sao-vendidas-0402386EC4B94366> .

finalidad que pueda ser atribuida a los bancos de datos de protección al crédito a no ser el asalto a la vida patrimonial de los individuos en cualquier ámbito. Son como ya hemos opinado, un gran “supermercado” de datos, de cualquier relación dineraria sea ella de naturaleza civil, mercantil, tributaria o administrativa, cuyo acceso a sus informaciones es tan difícil como formalizarse persona jurídica.

Desde nuestra perspectiva, en Brasil debe darse un replanteamiento inicialmente desde el punto de vista legislativo del sistema de protección de datos actual y en lo que concierne específicamente al sistema de protección al crédito, establecer algunos parámetros definiendo primeramente el ámbito de la finalidad de dichos ficheros. Si lo que estos persiguen es como el propio nombre sugiere es la “protección del crédito”, entonces por lógica las informaciones allí registradas son de interés de aquellos que participan del mercado crediticio. De manera que el mercado de consumo debería organizarse con independencia a éste, de forma sectorial por actividad.

En efecto, en este país según estadística del *Serviço de Proteção ao Crédito – SPC*<sup>468</sup>, gran parte de los deudores registrado en este fichero, totalizando un 74,49%, deben un valor de hasta R\$250,00, que convirtiendo<sup>469</sup> a euros serían aproximadamente €97,58 según los datos de diciembre de 2009. Son valores que no necesariamente enjuician la solvencia patrimonial de nadie, es más, muchas veces solamente expresan el retraso en el pago de una prestación de un servicio. Sin embargo, si pensamos en estos banco de datos como auxiliares en la protección del crédito, el valor registrado

---

<sup>468</sup> Los datos pueden ser encontrado en

[http://www.spcnegocios.org.br/imprensa/Releases/Release\\_Indicador\\_CNDL\\_SPCBRASIL\\_Dezembro2009.pdf](http://www.spcnegocios.org.br/imprensa/Releases/Release_Indicador_CNDL_SPCBRASIL_Dezembro2009.pdf) , consultados en 15 de diciembre de 2009.

<sup>469</sup> Fecha de la cotación utilizada: 14/12/2009. Tasa: 2,56196 Real/Brasil = 1 Euro. Información del *Banco Central do Brasil*

<http://www.bacen.gov.br> .

no es lo más significativo. Más importante es la procedencia de estas informaciones adecuándolas a sus finalidades.

La conocida y popular afirmación de que si alguien no paga una deuda de por ejemplo, una factura de teléfono no tiene la capacidad de cumplir con sus obligaciones crediticias no nos parece suficiente razón para justificar la adopción de un fichero único de registro de impuntualidad de todas las obligaciones dinerarias en todos los aspectos de la vida de una persona. Este argumento va en dirección contraria a los derechos y libertades fundamentales del ciudadano, principalmente a su derecho a la intimidad y a la autodeterminación informativa.

Cumple resaltar además que en Brasil con quince días de retraso de cualquier deuda, ya se puede registrarla en el sistema de protección al crédito. Es un plazo tan pequeño que implica asumir que la prestación de dicho servicio se desarrolla perfectamente hecho que comprobadamente no es verdadero. La superintendencia de Protección y Defensa del Consumidor (Procon)<sup>470</sup> del Estado de São Paulo publica anualmente la lista de las empresas que más han sido objeto de reclamación advenidas de la prestación de un servicio o la venta de un bien en este Estado. En el año de 2008 el resultado<sup>471</sup> demuestra que de las cinco empresas más reclamadas, tres se dedican a la prestación de servicios telefónicos y dos

---

<sup>470</sup> El Decreto nº 2.181, DE 20 DE MARÇO DE 1997, que disciplina sobre la organización del Sistema Nacional de Defensa del Consumidor, en su artículo 4º prevé la creación de un órgano que integrará dicho sistema, en el ámbito de su jurisdicción y competencia para además de otras finalidades, planear, elaborar, proponer y ejecutar la política de protección de defensa del consumidor en sus respectivas áreas de actuación. Así, el "Procon" es un órgano administrativo, de 1ª instancia, creado por cada Estado, municipio o por el Distrito Federal con competencia en materia de consumo.

<sup>471</sup> Documento fue publicado en 13 de marzo de 2009, y está disponible en:

[http://www.procon.sp.gov.br/pdf/ACS\\_Ranking\\_de\\_reclama%C3%A7%C3%B5es\\_2008.pdf](http://www.procon.sp.gov.br/pdf/ACS_Ranking_de_reclama%C3%A7%C3%B5es_2008.pdf) .



son entidades financieras, siendo Telefónica la que encabeza la lista de reclamaciones de los consumidores. De manera que si hay un fallo en el servicio y el consumidor se niega a pagar una prestación, en quince días de la fecha de vencimiento de la factura ya puede tener su nombre registrado en un fichero de moroso.

Por lo que se puede apreciar, en un único banco de datos están apuntados valores diversos, derivados de operaciones de naturaleza distintas, que al final tiene una finalidad tan amplia que cualquier tentativa de definición es inocua. Aún así, intentándolo se constituirían en un fichero de morosos, de deudores y de insolventes, sean personas físicas o jurídicas, y que pretende proteger el mercado de consumo y de crédito en la disminución del incumplimiento de deudas, y en el mismo sentido colaboradores del Poder Judicial en lo que concierne a las ejecuciones de deudas y de la Administración Pública tocante a las deudas fiscales. En fin, un “súper-fichero” jamás visto, ni siquiera comparable con aquellos mantenidos en la época de la dictadura que se nutría de informaciones de todo tipo, pues hoy tienen a su disposición toda la tecnología de informatización de datos que en aquella época no era accesible.

En verdad, en este tema no se puede ignorar el problema social que existe en Brasil tocante al incumplimiento de los pagos de la contrapartida de las prestaciones de servicios, hecho que afecta al comercio de manera muy frecuente. Ello también hay que llevarse en cuenta a la hora de proponer una reforma legislativa en la materia. A nuestro juicio, la experiencia de Italia de organización de las centrales de riesgos públicas y privadas, bien como los bancos de datos de informaciones comerciales es lo que más se acerca al modelo que pretendemos proponer para Brasil. Sin embargo el modelo italiano aunque nos parezca muy bien sistematizado, solamente podría servir de inspiración porque las realidades económicas de estos países son muy distintas.

Inicialmente, como hemos dicho, habría que en primero lugar separar los ficheros que tienen por finalidad enjuiciar la solvencia patrimonial y crediticia del afectado y consecuentemente que pretenden proteger el crédito de aquellos que se destinan a la protección comercial y a partir de este punto, determinar el objeto de uno y otro fichero.

Desde nuestra perspectiva, los datos que puedan enjuiciar la solvencia patrimonial en Brasil son aquellos positivos o negativos, que sólo o conjuntamente tengan la capacidad de definir las condiciones patrimoniales de un individuo, y que puedan ser determinantes para evaluar su riesgo crediticio. Así, el valor de una específica operación de crédito no es un dato *de per se* relevante, pero si tiene relevancia cuando al ser analizado juntamente con otros da la perspectiva de evaluar la capacidad de un individuo en asumir otras obligaciones derivadas de las relaciones de crédito.

Además, podrían figurar en estos ficheros los registros de los notarios relativos a los protestos de títulos de crédito, así como los procedimientos concursales, los datos de fuentes públicas como en España, de los procedimientos de ejecución que coincidan en estas características.

En lo que concierne al acceso a dichos banco de datos opinamos que solamente estarían autorizados como en el caso de Italia los bancos, intermediario financieros u otro sujeto privado en el ejercicio de una actividad comercial o profesional concede un aplazamiento de pago de la contrapartida por el suministro de bienes o servicios, todas ellas debidamente registradas en el Banco Central y con sus actividades relativas a concesión de crédito aprobadas por el citado órgano.

Pese todo lo dicho, es cierto que a través de la utilización de los servicios ofrecidos por el comercio, un consumidor puede llegar a un nivel de endeudamiento que efectivamente influya en su capacidad de satisfacer sus obligaciones. En tales situaciones, el valor se torna en un

referente razonable, por lo que consideramos que llegado a un determinado límite estipulado por los órganos públicos implicados en el tema como por ejemplo el *Conselho Monetário Nacional*<sup>472</sup> y el Ministerio de Justicia a través del Departamento de Protección y Defensa del Consumidor, los datos personales de las relaciones en el mercado de consumo podrían ser comunicados a los ficheros de solvencia patrimonial, pero sin que ello conlleve el derecho de acceso a sus informaciones por entidades que no tuviese el carácter de establecimientos financieros.

Los ficheros constituidos como archivos de consumo, propios del Código del Consumidor y allí regulados, consideramos que deben ser entendido como ficheros sectoriales por actividades, como hemos consignado, pudiendo así, ser tratados los datos sobre deudas vencidas y no pagadas, aunque solamente cuando se constituyesen con retraso, y en la finalidad de resguardar el desarrollo de su actividad comercial. De suerte que entendemos viable la separación de las informaciones de deudas relacionadas al comercio de aquellas derivadas de las relaciones de crédito. Pues, es lo mínimo que se puede exigir como respeto al derecho a la autodeterminación informativa en el sistema jurídico brasileño.

---

<sup>472</sup> el *Conselho Monetário Nacional* es el órgano normativo, de deliberación máxima del sistema financiero de Brasil, responsable por las principales directrices del sistema financiero y su forma de actuación, integrado por el Ministro de la Hacienda (que es el Presidente del Consejo), el Ministro del Planeamiento y el Presidente del *Banco Central do Brasil*

**CAPITULO CUARTO:**

**PARTE I: EL TRATAMIENTO DE LOS DATOS SOBRE LA  
SOLVENCIA PATRIMONIAL Y CRÉDITO DE LOS  
INDIVIDUOS EN ESPAÑA E ITALIA.**

## I. Introducción.

Aunque la regulación de los ficheros de solvencia patrimonial y crédito esté enmarcada jurídicamente en la Ley de Protección de Datos y ésta se derive de la necesidad de transponer la Directiva comunitaria 95/46 al sistema jurídico interno nacional, y pese a que los países aquí estudiados sean de semejante tradición jurídica se ha observado que hay muchos matices entre estas normas. En efecto, el texto comunitario traza los principales rasgos de las cuestiones más importantes que deben ser unificadas dentro de su ámbito de aplicación, sin embargo hay un margen importante en el cual pueden los países, sin contrariar como es evidente los preceptos establecidos a nivel comunitario, llegar más lejos que el aludido texto legal.

No sabemos con certeza que razones llevan a tratamientos legales distintos de los datos objeto de éste estudio de investigación. Además, en el ámbito de éste trabajo no es posible indagar más a fondo tal problema, pero lo cierto es que el tema envuelve muchos aspectos de diversas índoles, principalmente el económico de cada país, la capacidad financiera de la población, el grado de confianza entre las entidades financieras y sus clientes, son ejemplos de las cuestiones que podrían ser tenidas en cuenta para explicar tal fenómeno.

De todos modos, lo que resulta curioso es la expansión global de la actividad de información sobre la solvencia patrimonial y crédito de los individuos, con independencia de la estructura o del poder económico del país, asimismo de la regulación de cada uno de ellos en lo que concierne al derecho de protección de datos de los individuos, como es el caso notorio de España, Italia y Brasil.

Sin embargo, a nivel europeo, la trayectoria del derecho a la protección de datos y la fuerza jurídica a él conferida, como un derecho fundamental impide que algunos excesos sean cometidos cuando se tratan datos con las características que poseen aquellos que informan sobre la solvencia patrimonial y el crédito. Específicamente en España e Italia, a tales datos, como hemos comentado en el capítulo anterior, SE les dedicara una reglamentación especial.

En el caso español, la influencia de la experiencia de la Agencia de Protección de Datos fue determinante a la hora de ampliar y desarrollar los dispositivos de la LOPD. En Italia, la doctrina observa que antes de la primera ley de protección de datos, n<sup>o</sup> 675/1996, han proliferado los sistemas de información administrado por sujetos privados, lo que supuso, como señala Mormile<sup>473</sup>, que durante años un enorme volumen de informaciones personales de los múltiples sujetos privados – consumidores o empresarios – fuese recogida, comunicada, y tratada de diferentes maneras sin reglamentación alguna y sin que se pudiera intervenir en esos procesos.

De igual modo que en Italia, en España ha sucedido algo parecido en lo que concierne a la actuación de las agencias de protección de datos. En este sentido, en España antes de la entrada en vigor del RPD la AEPD se había publicado la Instrucción normativa n<sup>o</sup> 1/1995, específica para el sector; el *Garante*, asimismo, en Italia, antes de que entrase en vigor el Código en materia de protección de datos personales (Decreto ley n<sup>o</sup> 196/2003 de 30 de junio), había emitido un *provvedimenti*<sup>474</sup> en el cual

---

<sup>473</sup> MORMILE, Lalage. “Il Sistema di Informazioni Creditizie”. En PANETTA, Rocco (coord.). *Libera circolazione e protezione dei dati personali*. Milano: Giuffrè, Tomo II, 2006, p. 1848. *Vide*, también, MARSICANO, Giorgia. “Il nuovo codice deontologico per le centrali rischi private”, en *Magistra, Banca e Finanza*, <www.magistra.it>, 19 settembre 2005 [acceso en 9 de abril 2010].

<sup>474</sup> Provvedimenti de 31 julio 2002. En: *Bollettino* n. 30 julio 2002, pag. 47. *Vide* comentarios sobre tal documento de VOTANO, Giulio, “Sistema Bancario, Finanziario

afrontaba algunas cuestiones sobre las centrales de riesgos privadas, documento este que ha sido fuente de inspiración para el *Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti*.

Lo que nos interesa en este Capítulo, es investigar cómo cada uno de estos países han dispuesto su disciplina específica sobre los sistemas de información. Es decir, cuales son las principales reglas y los aspectos más importantes que han tenido en cuenta estos dos países a la hora de definir el tratamiento de los datos en éste determinado sector, en los cuales se alejan del régimen general de la ley de protección de datos, al margen de su sistematización legislativa y del equilibrio entre los diversos intereses implicados en la materia. En fin, los principales rasgos que puedan contribuir, desde la perspectiva del estudio comparado entre los sistemas jurídicos de éstos países y el brasileño, y de la experiencia de Italia y España en la materia, para mejorar el tratamiento legal de los datos referentes a la información crediticia en Brasil.

## **II. Los requisitos para la inclusión de los datos.**

### **1. La Legislación Española.**

---

ed Assicurativo". En BIANCA, Cesare Massimo y BUSNELLI, Francesco (Dir.). *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*. Milano: CEDAN, 2007, p. 1504 y MEZZANOTTE, Massimiliano, "Centrali Rischi Private, Diritto all'oblio e Potestà «normative» del Garante". Revista: *Il diritto dell'informazione e dell'informatica*. Ano: 2004, Volume: 20 Num. 4/5, p. 661.

### 1.1. Datos sobre solvencia patrimonial y crédito.

El artículo 29.1 de la Ley Orgánica de Protección de Datos no establece *numerus clausus* para que tales datos puedan ser considerados definitivos a efectos de registro en los ficheros de solvencia patrimonial y crédito, no obstante fija algunos requisitos que deben ser observados para que estos puedan ser incluidos en los citados ficheros.

De este modo, la norma determina que solo podrán ser tratados los datos obtenidos específicamente: *a)* a través de los registros y las fuentes accesibles al público establecidos al efecto; *b)* procedentes de informaciones facilitadas por el interesado y, finalmente, *c)* por intermedio de terceros con el consentimiento del afectado.

Los datos recogidos a través de cualquiera de estas fuentes legalmente permitidas, y que sean determinantes para enjuiciar la solvencia económica de los interesados desde nuestro modesto juicio, pueden tener un carácter positivo o negativo. La ley no establece taxativamente que los datos tengan ésta doble naturaleza, pero entendemos que se puede deducir que así es, porque la norma siempre resalta las peculiaridades que deben ser observadas cuando estos sean negativos, como es el caso del apartado 4 del artículo 29 de la LOPD que determina que “sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, **cuando sean adversos**, a más de seis años...”, estableciendo un régimen jurídico especial para aquellos relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

Cuando el dato tratado sea positivo, creemos que de la ley se desprende que, las fuentes donde estos datos son obtenidos forman parte también de los requisitos de inclusión, porque no se pueden obtener de otro modo que no sean los que están allí especificados, como por ejemplo, los del



acreedor sin el consentimiento del interesado. La fuente se torna por lo tanto en una condición esencial para su incorporación al fichero. En cambio, en los casos de los datos negativos, la fuente no nos parece que sea condición *sine qua non* de inclusión, ya que teniendo éste carácter, puede ser recabado de cualquiera de las fuentes permitidas por la ley: las públicas, el acreedor o quien actúe por su cuenta o interés, y aunque sea prácticamente imposible que pueda suceder, está legalmente admitido que el propio afectado o terceros con su consentimiento informe datos con ésta característica.

El artículo 3, letra j) de la LOPD define las fuentes accesibles al público como “aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencias que, en su caso, el abono de una contraprestación” y enumera cuales tienen éste carácter. El Reglamento 1720/2007, en el artículo 7, clarifica el concepto de fuentes accesibles al público, y dispone taxativamente que sólo tendrán éste carácter aquellos que están listados en las letras subsecuentes, entre ellas, nuevamente, los diarios y boletines oficiales.

De igual modo regula las normas citadas, Y todas las fuentes con carácter de accesibles al público allí listadas, Y las que pueden ser utilizadas para la recogida de los datos positivos sobre la solvencia patrimonial y crédito en los Diarios y Boletines Oficiales. Eso entiende la Audiencia Nacional<sup>475</sup> en función del artículo 3. j) de la LOPD, considerando que “se desprende con claridad que recoge un número clausus de las fuentes que pueden calificarse como accesibles al público, lo que se remarca con el empleo del término ‘exclusivamente’ que se cohonesto a las concretas fuentes que enumera”.

En lo que respecta a los tablones de anuncio de los juzgados, estos no pueden ser considerados como fuentes accesibles al público. En efecto, la

---

<sup>475</sup> Audiencia Nacional, Sentencia de 5 noviembre 2008 (JUR 2008\375602); Sentencia de 30 mayo 2007 (JUR 2007\199490).

publicidad de los actos judiciales no forma parte del concepto de fuentes accesibles al público. Para Aparicio Salom<sup>476</sup>, “la limitación de los supuesto que se regulan por el régimen especial de las fuentes públicas da lugar a que no puedan someterse a tratamiento los datos correspondientes a las demandas que se publican en los tablones de anuncios de los juzgado, sino sólo las que se publican en los Boletines Oficiales”. A este respecto, hay que tener en cuenta el pronunciamiento de la Audiencia Nacional<sup>477</sup>, cuando tuvo oportunidad de señalar que “la publicidad de las actuaciones judiciales no significa, como ya hemos dicho, que los datos contenidos en un procedimiento judicial que se halla en fase de ejecución, puedan ser examinados y se encuentren a disposición del público en general de forma totalmente libre e indiscriminada, por lo que los procedimientos judiciales en cuestión no pueden ser considerados como fuentes accesibles al público”.

Aún hay que añadir las conclusiones de la Agencia Española de Protección de Datos sobre este tema. En Informe Jurídico<sup>478</sup> ha manifestado que podría argumentarse que la enumeración legal no es taxativa, por cuanto, con carácter previo a la misma, el artículo 3 j) indica que son fuentes accesibles al público “aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación”. No obstante para la AEPD la generalidad del concepto no impide que “resulte de aplicación la enumeración taxativa anteriormente indicada, dado que el contenido de este primer inciso no hace sino indicar un requisito indispensable para que los ficheros enumerados por la propia norma puedan ser considerados como fuentes de acceso público”. Para este órgano, la principal característica para que

---

<sup>476</sup> APARICIO SALOM, Javier. *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Navarra: Aranzadi, 2000, p. 156.

<sup>477</sup> Audiencia Nacional, Sentencia de 6 abril 2006 (JUR 2006\147661).

<sup>478</sup> AEPD. Informe Jurídico 237/2009.

tales ficheros puedan ser considerados como fuentes de acceso público es cuando su consulta pueda ser realizada por cualquiera sin ninguna limitación salvo, en su caso, el abono de un precio, no obstante ello sólo son fuentes de acceso público aquellas enumeradas, y allí no se encuentran las resoluciones judiciales.

En lo que concierne a los registros públicos, los que poseen trascendencia para aquellos que se dedican a la actividad de prestación de informaciones sobre la solvencia patrimonial y crédito son los Registros Mercantil y de la Propiedad. Cumple resaltar que la AEPD<sup>479</sup> advirtió que el Registro Mercantil no es una fuente accesible al público de las que la LOPD enumera de forma taxativa, por ello está prohibida la incorporación de los datos personales registrados que son susceptibles de consulta individualizada a bases o ficheros de datos, informatizados o no, siempre y cuando que el tratamiento de datos no esté avalado por así disponerlo una norma.

Aparte de las fuentes en las cuales pueden los datos ser recabados, hay que tener en cuenta la exigencia del principio de la calidad de los datos. De suerte que como estos datos obedecen al régimen general de la ley, los requisitos para su inclusión son aquellos que establece el apartado 1 del artículo 4, es decir, deberán ser adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

La interpretación de la Audiencia Nacional<sup>480</sup> sobre este precepto es la de que carecería de validez la recogida de datos con finalidades indeterminadas o tan vagas o genéricas que admitieran cualquier propósito. Para este Tribunal, hay una íntima conexión entre este requisito y el que impide el uso de dichos datos para finalidades ilegítimas y no

---

<sup>479</sup> AEPD. Expediente nº: E/00858/2007.

<sup>480</sup> AN. Sentencia de 11 marzo 2009 (RJCA 2009\301).

explícitas. De suerte que ahí se consagra “el llamado principio de proporcionalidad (cuantitativa y cualitativa) en el tratamiento de los datos personales”. Además, concluye la Sala que “recoge tal artículo 4 una sutil distinción entre finalidad de la recogida y finalidad del tratamiento, pues la recogida sólo puede hacerse con fines determinados, explícitos y legítimos, y el tratamiento posterior no puede hacerse de manera incompatible con dichos fines”.

## 1.2. Datos sobre el cumplimiento e incumplimiento de obligaciones dinerarias.

Respecto a los requisitos de inclusión de los datos sobre cumplimiento e incumplimiento de obligaciones dinerarias en los ficheros de solvencia patrimonial no había en la LOPD ninguna especificación sobre la materia. De suerte que para subsanar no solamente ésta pero también otras omisiones, en el ejercicio de las funciones que le atribuía el artículo 36 de la LORTAD, la Agencia Española de Protección de Datos dictó la Instrucción 1/1995, de 1 de marzo<sup>481</sup>, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito y la Instrucción 1/1998, de 9 de enero, relativa al ejercicio de los derechos fundamentales de acceso, rectificación y cancelación en ficheros automatizados. No obstante,

---

<sup>481</sup> Sobre la validez jurídica de tal Instrucción, la Audiencia Nacional en sentencia de 9 enero 2009 (RJCA 2009\217) ha pronunciado que “evidentemente la Instrucción 1/95 no es un Reglamento en su sentido formal pues no se ha dictado siguiendo el procedimiento específicamente establecido, pero no se olvide que el artículo 44.3 .d) solo habla de Disposiciones Reglamentarias. El hecho de que la Instrucción 1/95 no esté incluida entre las mencionadas por la Disposición Transitoria Tercera entre las normas preexistentes a la Ley Orgánica 15/99 cuya vigencia se mantiene, no puede impedir su carácter de disposición reglamentaria de desarrollo”.

con la entrada en vigor de la Resolución 1720/2007, los problemas planteados por la citada Agencia en dichas instrucciones fueron saneados. En efecto, para Pascual Huerta<sup>482</sup>, el Reglamento en sus artículos 38 a 44 reemplazan por completo la Instrucción 1/1995, “ya que la parece que el ánimo del legislador reglamentario ha sido integrar en un solo cuerpo legislativo todas las diversas normas y criterios interpretativos que durante los últimos años han venido apareciendo sobre distintos aspectos materiales de la protección de datos”. Aunque el Reglamento no derogue expresamente las Instrucciones de la AEPD, para el autor en cita dicha norma sustituye en bloque la antigua y ello trae como consecuencia la desaparición del ordenamiento jurídico de la Instrucción 1/1995 incluyendo aquellas reglas que podían entenderse vigente ya que no se contradicen con la nueva reglamentación.

El RPD en el artículo 38, apartado 1, refuerza, con un texto similar a la instrucción normativa 1/1995 de la AEPD, que sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, y establece que deben concurrir algunos requisitos para su inclusión, que son:

a. Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada;

b. Que sobre dicha deuda no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero.

---

<sup>482</sup> PASCUAL HUERTA, Pablo. “Ficheros de Información Sobre Solvencia Patrimonial y Crédito (arts. 37 a 44)”. En: ZABÍA DE LA MATA, Juan. (coord.). *Protección de Datos. Comentarios al Reglamento*. Valladolid: Lex Nova, 2008, pp. 347 y 348.

c. Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

d. Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.

*1.2.1. Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada.*

La LOPD y su reglamento de desarrollo establecen que los datos que pueden ser registrados son aquellos relativos al cumplimiento o incumplimiento de obligaciones dinerarias, que sean determinantes para enjuiciar la solvencia económica del afectado, cuya deuda haya resultado impagada. Dicha deuda además, deberá ser cierta, vencida y exigible. Sobre ella no podrá haber ninguna reclamación de naturaleza judicial, arbitral o administrativa, que es un hecho impeditivo de inclusión de los datos en un fichero de moroso.

Pascual Huerta<sup>483</sup> advierte que la expresión «deuda cierta, vencida y exigible» se introdujo en el Derecho español, salvo error, por la Instrucción 1/1995 de la Agencia Española de Protección de Datos y sólo se encuentra hoy en el artículo 38 del Reglamento de desarrollo de la LOPD. Además, observa el autor que ésta expresión se parece mucho a otra locución tradicional consagrada por el Tribunal Supremo que es la «deuda líquida, vencida y exigible». Para él, “el adjetivo «cierto» referido a una deuda monetaria carece de sentido técnico en el actual Derecho civil español, por lo que creemos que en ese mismo sentido no técnico, el

---

<sup>483</sup> PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 369.

Reglamento se refiere a que la deuda deba existir realmente y no ser una mera afirmación unilateral de presunto acreedor”. Este requisito parece estar muy relacionado con la veracidad del dato.

Una deuda vencida, en su concepción, sería aquella en que hubiere transcurrido el plazo fijado para el cumplimiento o cuando no exista término. Por fin, el último adjetivo «exigible» se concreta cuando se puede reclamar judicialmente. De éste modo, concluye el autor en cita que “el Reglamento alude en su artículo 38.1.a) a deudas realmente existentes, sin términos o condiciones pendientes de finalización o cumplimiento, con la cuantía determinada y cuyo cumplimiento pueda exigirse por vía judicial”.

### *1.2.2. Inexistencia de reclamación sobre la deuda.*

La continuación del artículo 38.1, letra a) del RPD exige que sobre la deuda “no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero”. Tal precepto es una novedad, ya que la LOPD y la Instrucción 1/1995 no contemplaban la observancia de dicho requisito para la inclusión de una deuda en los ficheros de moroso. Todo el artículo dedicado a los requisitos que deberán ser obedecidos antes de que se registren datos negativos pretende, de manera preventiva, que los datos anotados revelen un perfil del deudor que se ajuste a una situación real y actual. Dentro de esta concepción, nos

parece que la exigencia referida en este apartado respalda aún más esta finalidad.

De las reclamaciones que pueden impedir la inclusión de un dato en el fichero de morosos, la que más causa controversia doctrinal en relación al dispositivo legal es indudablemente las administrativas. Para Pascual Huerta<sup>484</sup>, tocante a dichas reclamaciones de una deuda sea ante un organismo de tutela de los derechos de los consumidores, o planteada ante un comisionado de los previstos en el Real Decreto 303/2004, desde su perspectiva le parece que la redacción legal dada fue excesivamente amplia, y en su opinión “puede ser positivo que se quiera dar realce a los comisionados del Real Decreto 303/2004, pero no a costa de amenazar el funcionamiento regular de los ficheros comunes de solvencia”. No obstante, para el autor aludido es acertada, en cambio, la previsión del RPD en lo que respecta a una reclamación judicial o arbitral ya que éstas “son un auténtico desafío a la versión de la realidad que mantiene la entidad acreedora, lo que se ajusta a la finalidad que pretende la norma”. Además de ello, el citado autor plantea otra cuestión respecto al Servicio de Reclamaciones del Banco de España y la propia Agencia Española de Protección de Datos y la posibilidad de que una reclamación antes estos órganos sea motivo de no inclusión del datos en el fichero de moroso. En relación al primero, a su sentir habría de reconocer su obvio carácter de órgano administrativo y su similitud con los órganos comisionados de las entidades financieras. Respecto al segundo, “parece absurdo que una simple denuncia ante la AEPD, cuyas investigaciones se inician de siempre de oficio (...) pueda de pos sí impedir el tratamiento de datos en estos ficheros”.

Sobre la misma cuestión Plana<sup>485</sup>, apunta que las reclamaciones ante el Banco de España dada las competencias de éste, impide la inclusión de los

---

<sup>484</sup> PASCUAL HUERTA, Pablo. “Ficheros... *op. cit.*, p. 373.

<sup>485</sup> PLANA, Maria del Carmen. *Ficheros... op. cit.*, p. 383.



datos, sin embargo en lo que concierne a la AEPD lo mismo no ocurre ya que ésta no es una autoridad administrativa que tenga competencia para decidir sobre la deuda. Relativamente a las reclamaciones a los Comisionados para la defensa del cliente de servicios financieros, la autora añade que la reclamación previa que debe ser presentada antes de aquella ante el Comisionado, según estipula el artículo 8 del el RD 303/2004 también es válida para impedir la inclusión de los datos en los ficheros de morosos, así como, en su opinión, las reclamaciones de consumo previas al arbitraje.

En el caso de que la deuda haya sido registrada en un fichero de solvencia patrimonial y crédito, y posteriormente el deudor entable una reclamación contra la misma, según el entendimiento de la AEPD<sup>486</sup> el acreedor deberá, a partir del conocimiento de tal reclamación, proceder la exclusión o baja de los datos en el fichero.

En lo que concierne al requisito de la inexistencia de reclamación sobre la deuda, hay algunos aspectos controvertidos que son resaltados por la doctrina. Según advierte Plana<sup>487</sup>, cualquier reclamación, según la interpretación del artículo 38 del RPD impide la inclusión de los datos en un fichero de moroso, ya que no hay, en su opinión, un incumplimiento *stricto sensu* si no está claro a qué está obligado el deudor. Así, “la reclamación que incida sobre la certeza, vencimiento, liquidez o exigibilidad de la deuda impide la inclusión”. Para la citada autora, la actitud del deudor debe ser exteriorizada a través de alguna de las vías que el ordenamiento jurídico pone a su disposición, debiendo reflejarse en la existencia de una reclamación. A su parecer, tal reclamación “se ha de

---

<sup>486</sup> AEPD. Informe Jurídico 237/2009.

<sup>487</sup> PLANA, Maria del Carmen. “Ficheros sobre Solvencia Patrimonial y Crédito”. En: PALOMAR OLMEDA, Alberto y GONZALEZ-ESPEJO, Pablo (Dir.). *Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/199, de 13 de diciembre, de Protección de Datos de Carácter Persona (Aprobado por RD 1720, de 21 de diciembre)*. Cizur Menor: Thomson Civitas, 2008, pp. 381 y 382.

entender como la exteriorización de la discusión acerca de alguno de los requisitos esenciales ligados a la existencia de la deuda”.

Analizando los diversos planteamientos sobre la materia, creemos que el legislador ha acertado en insertar entre los requisitos para la inclusión de los datos la inexistencia de reclamación sobre la deuda, también a nivel administrativo, siempre y cuando el fundamento de tal reclamación sea alguno aspecto que incida sobre la certeza, el vencimiento, su liquidez o exigibilidad, ya que como bien apunta Plana<sup>488</sup>, “aplicando esta exigencia, los datos que proporciona el fichero responden de modo mucho más fiable a una realidad de incumplimiento”, entendido como la voluntad rebelde al cumplimiento del deudor. Además, cualquier abuso por parte del deudor respecto a la utilización de las reclamaciones podría ser considerado como fraude de ley (artigo 6.4 del CC) o abuso de derecho (artículo 7.2 del CC), con sus respectivas consecuencias.

No obstante, lo que no nos parece una decisión legislativa acertada es que se excluyan los datos del fichero porque de esta forma no se podrá tener un control de los afectados que no utilizan de buena fe las aludidas reclamaciones.

*1.2.3. Existencia de un principio de prueba que contradiga los requisitos de inclusión.*

El apartado 2 del artículo 38 del Reglamento prohíbe la inclusión de datos personales en los ficheros sobre los que exista un principio de prueba que de forma indiciaria contradiga alguno de los requisitos

---

<sup>488</sup> PLANA, Maria del Carmen. *Ficheros... op. cit.*, p. 386.

especificados en este artículo. De modo que la ley añade que tal circunstancia determinará asimismo la cancelación cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado su inclusión en el fichero.

Es cierto, que en algún procedimiento sancionador la Agencia Española de Protección de Datos<sup>489</sup> ha manifestado que “la discusión de la deuda, sin un aporte documental con suficiente entidad probatoria que pudiera contradecir lo establecido en la documentación aportada en el procedimiento, no es suficiente para evitar el acceso de los datos del deudor a un fichero de morosidad”. Sin embargo, la vinculación de un documento a la expresión *principio de prueba* venía de la Instrucción 1/1995 de esta Agencia que en su norma primera establecía específicamente que no podía incluirse en los ficheros de morosos datos personales sobre los que existiera un principio de prueba documental que aparentemente contradijera alguno de los requisitos allí definidos para la deuda.

No obstante, el Reglamento se limita en el apartado 2 del artículo 38 a determinar que “no podrán incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba que de forma indiciaria contradiga alguno de los requisitos anteriores”. La redacción bastante similar a la que contenía la citada Instrucción, pero sin determinar taxativamente la obligatoriedad de que este principio de prueba sea documental. Ello nos lleva a pensar que la omisión del legislador fue voluntaria para que se pudiera ampliar la efectividad de los derechos del acreedor. Sobre este aspecto bien observa Pascual Huerta<sup>490</sup> que hay ahí un problema relativo a las cuestiones competenciales de enjuiciamiento de la deuda ya que ni la AEPD ni la Audiencia Nacional pueden inmiscuirse en las cuestiones de orden civil, como es la afirmación de la existencia o no de una deuda. A pesar de ello, para determinar el

---

<sup>489</sup> AEPD. Expediente N.º: E/00972/2006.

<sup>490</sup> PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 386.

cumplimiento de los requisitos establecidos para la inclusión de los datos personales en los ficheros de moroso hay que entrar muchas veces, aunque de modo somero, en el análisis de varios aspectos de Derecho privado del asunto. De suerte que, como dice el autor, “la AEPD y la AN se colocan en una situación intermedia entre el acreedor y el deudor, que recuerda sospechosamente a la del juez del proceso civil y que pone a la administración en la frontera de un conflicto de jurisdicción del artículo 38 de la LOPJ”. Aunque, apunta el autor en cita que tanto uno como el otro órgano están empezando a ser reacios a examinar con demasiada profundidad estas cuestiones de Derecho privado.

En efecto, para que se averigüe un principio de prueba de la existencia de una deuda, se hace necesario un análisis de mérito civil, cuya competencia no pertenece a ninguno de los órganos citados arriba. Sin embargo, la ley determina que el mero indicio de la inexistencia de la deuda ya puede ser considerado como suficiente para que se proceda la cancelación del dato. De suerte que es un análisis muy similar aquella exigida por las medidas cautelares del *fumus boni iuris*. Constituyese en un examen somero, superficial sin que se haga necesario adentrarse en la esencia del mérito. Nos parece muy adecuado subrayar el pronunciamiento del Juzgado de lo Mercantil de Sevilla, en Auto de 6 octubre 2006<sup>491</sup>, que analiza tal requisito. Aunque considerando la dificultad de conciliarlo en la mayoría de los supuestos, manifiesta el Órgano juzgador que “el art. 728.2 LECiv preceptúa que el solicitante de las medidas cautelares habrá de presentar los datos, argumentos y justificaciones documentales que conduzcan a fundar, por parte del tribunal, sin prejuzgar el fondo del asunto, un juicio provisional e indiciario favorable al fundamento de su pretensión; pudiendo en defecto de justificación documental, ofrecerla por otros medios. **Ello no quiere decir que se exija la acreditación exacta y documental de la pretensión alegada, sino que se acredite prima facie que la pretensión no es**

---

<sup>491</sup> Juzgado de lo Mercantil núm. 1 de Sevilla. Auto de 6 octubre 2006 (AC 2007\671).

**meramente ilusoria**, sino que viene respaldada por datos objetivos y pruebas, que al menos en el momento inicial permitan augurar un futuro éxito procesal, sin prejuzgar el fondo del asunto” (subrayamos).

Ahora bien, pese a que sea suficiente cualquier indicio o elemento probatorio que pueda objetar la existencia de la deuda, o mismo de la situación de incumplimiento, el principal indicio que podremos encontrar en la práctica, conforme destaca Plana<sup>492</sup>, es el documental, representado por el recibo u otro justificante de pago. Además de ello, el principio de prueba debe ser conocido por el acreedor para que se le pueda exigir la obligación, o bien previamente y así no pueda efectuar la inclusión de los datos, o en el caso de que estos ya hubiesen sido incluidos, que sean cancelados de forma cautelar conforme el párrafo segundo del artículo 38.2 del RPD. En efecto, según se desprende de la doctrina, ésta carga debe recaer sobre el titular del dato, que deberá en su caso actuar, oponiéndose a la inclusión, aportando las pruebas que crea necesarias que respalden dicha oposición<sup>493</sup>.

Respecto a la cancelación cautelar, que es la medida que el RPD pone a disposición del afectado para que se cancele los datos por indicios de inclusión indebida, deberá ser utilizada según Prats Albentosa<sup>494</sup>, “ante la falta de resultados de sus gestiones ante el acreedor o el responsable del fichero”, y solicitada a la AEPD. Hay que tenerse en cuenta, como bien apunta Pascual Huerta<sup>495</sup>, que ésta implica en la obligación de volver a

---

<sup>492</sup> PLANA, Maria del Carmen. *Ficheros... op. cit.*, p. 389. En el mismo sentido PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 388.

<sup>493</sup> En éste sentido, PRATS ALBENTOSA, Lorenzo. *Ficheros... op.cit.*, p. 233; PLANA, Maria del Carmen. *Ficheros... op. cit.*, p. 389 y PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 389.

<sup>494</sup> PRATS ALBENTOSA, Lorenzo. *Ficheros... op.cit.*, p. 234.

<sup>495</sup> PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 389.

notificar el afectado la nueva inclusión de los datos en el fichero si se vuelven a darles de alta.

#### 1.2.4. Límite temporal de tratamiento de los datos.

El reglamento de desarrollo de la LOPD, artículo 38 establece un plazo máximo de 6 años para registrar y ceder los datos adversos en materia de solvencia económica, y fija que su computo empieza a contarse desde la fecha en que hubo de procederse al pago de la deuda, o del vencimiento de la obligación, o del plazo concreto si aquélla fuera de vencimiento periódico. Éste mismo límite temporal ya estaba previsto en la LOPD, artículo 29 apartado 4, — con una redacción muy parecida a la anterior norma derogada, la LORTAD, artículo 28.3— estableciendo que sólo se podrán registrar y ceder los datos de carácter personal que no se refieran a más de seis años.

Antes de la entrada en vigor del RPD, la Instrucción normativa 1/1995 intentó determinar el día en el cual se daba el comienzo del cómputo del citado plazo. Decía tal norma que se iniciaría a partir del momento de la inclusión del dato personal desfavorable en el fichero y, en todo caso, desde el cuarto mes, contado a partir del vencimiento de la obligación incumplida o del plazo en concreto de la misma si fuera de cumplimiento periódico.

El artículo 38 del Reglamento parece haber resuelto el problema. En efecto, el precepto, como bien apunta Plana<sup>496</sup>, hace referencia a dos

---

<sup>496</sup> PLANA, Maria del Carmen. *Ficheros... op. cit.*, p. 388.

supuestos: las deudas con vencimientos periódicos y aquellas de vencimiento único. Para ésta, el día de inicio del cómputo del plazo es el de vencimiento de la deuda. En el caso de que sean de vencimiento periódico, tal plazo empezará a contarse a partir del vencimiento del plazo de cada prestación. De tal manera, deudas que hayan ultrapasado éste límite, deberán ser canceladas de los ficheros de solvencia patrimonial y crédito, constituyéndose su inobservancia en una infracción, conforme el artículo 44 de la LOPD.

La finalidad de establecer un límite temporal para la inclusión y tratamiento de los datos en los ficheros de morosos, según se desprende de la jurisprudencia, es la protección de los derechos del afectado con el pasar del tiempo. La Audiencia Nacional<sup>497</sup>, en Sentencia de 8 de Junio de 2001, consideró que: "...ha de decirse que la inclusión de una persona en el registro de morosos, es un hecho de gran trascendencia de la que se pueden derivar consecuencias muy negativas para el afectado, en su vida profesional, comercial e incluso personal, que no es necesario detallar. En razón a ello, ha de extremarse la diligencia para que los datos sobre solvencia económica no puedan perpetuarse en esos registros, en perjuicio de los derechos de los afectados, en contra de lo establecido en la Ley".

En efecto, los ficheros de solvencia patrimonial sirven para que las entidades financieras puedan tener un perfil actualizado del historial del individuo. Seis años nos parece un plazo más que razonable para tratar dichos datos, ya que éste tiempo permite que el acreedor pueda actuar en el sentido de ejercer sus derechos a través de todos los medios permitidos en derecho, puestos a su disposición para satisfacer la deuda. Sobre el referido límite temporal la Audiencia Nacional<sup>498</sup> consignó que "el acceso y permanencia en los ficheros de titularidad privada que se refieren a la solvencia patrimonial del afectado, conteniendo datos adversos, no puede

---

<sup>497</sup> Audiencia Nacional. Sentencia de 8 junio 2001 (JUR 2001\293619).

<sup>498</sup> Audiencia Nacional. Sentencia de 14 junio 2002 (JUR 2003\49774).

tener un carácter indefinido, proporcionándonos un perfil sobre la vida y evolución de dicha solvencia a través de los años, sino que el legislador ha pretendido que la finalidad a la que sirve el fichero se cumple informando sobre la reciente historia de la solvencia patrimonial del afectado, estableciendo que ese reflejo histórico no puede superar los seis años". De otra parte, no se puede permitir que una información de naturaleza negativa esté registrada *ad perpetuam* como si fuera una condena al afectado.

#### 1.2.5. *Requerimiento de pago.*

Otro requisito exigido por el RPD es que antes de que se registren las informaciones, el acreedor debe requerir el pago a quien corresponda el cumplimiento de la obligación. La LOPD no hace en su texto ninguna mención sobre este requisito. De hecho, es un precepto que proviene de la Instrucción 1/1995 de la AEPD, que exigía en su norma primera el requerimiento previo de pago a quien corresponda, en su caso, el cumplimiento de la obligación.

La finalidad de tal requisito de inclusión, según doctrina de la Audiencia Nacional, es que su ausencia privaría a los interesados del conocimiento y, en su caso, de la posibilidad de formular reparos a la exactitud, o no, del dato<sup>499</sup>. Para el aludido Tribunal, la inclusión de un dato en los ficheros de solvencia patrimonial y crédito tiene relevancia de diversa índole (económica, social y práctica) motivo por el cual se exige a quien promueve una anotación se cerciore previamente de la calidad y

---

<sup>499</sup> Audiencia Nacional. Sentencia de 23 mayo 2007 (JUR 2007\142140).



exactitud del dato, de modo que insertar una información sobre una deuda sin que se compruebe tales aspectos y sin el requerimiento de pago resulta inconciliable con el grado de diligencia exigible cuando se trata de la protección de un derecho fundamental<sup>500</sup>. Por lo tanto, se entiende que la finalidad principal del requerimiento de pago es garantizar la calidad de los datos, ofreciendo también la oportunidad al deudor de que conozca la deuda que será insertada en un fichero de moroso y pueda actuar previamente en lo que entienda necesario dentro de los derechos que le son garantizados por la ley. En definitiva, el referido requisito es “exigido a aquellos que utilizan medios extraordinarios de pago como son los ficheros de morosos, quienes deben tener una especial diligencia en el uso que realizan de los datos personales de terceros<sup>501</sup>”.

El Reglamento únicamente se restringe a incluir dicha obligación de modo general, sin especificar cualquier otra formalidad que se deba observar. Ello trae dos consecuencias: la primera, y a nuestro sentir positiva, es que para tornar tal requisito efectivo, el acreedor no tiene cualquier tipo de impedimento legal para la utilización de cualquier medio físico disponible teniendo en cuenta, eso sí, la posibilidad de acreditar la prueba de que el referido requisito se ha cumplido. Ahora bien, la segunda consecuencia es que esa generalidad legal siembra dudas respecto al contenido del requerimiento. Tocante a este tema, la Audiencia Nacional<sup>502</sup> ha considerado que “ha de realizarse el requerimiento expresando el concepto y el importe de la deuda determinante de la remisión de los datos al fichero de solvencia patrimonial, sin que pueda aceptarse, como señala la parte recurrente en su escrito de demanda, que hubiera bastado con que el titular de los datos hubiera realizado unas operaciones aritméticas para conocer el importe de la deuda que daría lugar a la inclusión de sus datos en el fichero ‘Asnef’”. Algunas

---

<sup>500</sup> Audiencia Nacional. Sentencia de 8 junio 2005 (JUR 2005\245068).

<sup>501</sup> Audiencia Nacional. Sentencia de 15 octubre 2009 (JUR 2009\468479).

<sup>502</sup> Audiencia Nacional. Sentencia de 23 mayo 2007 (JUR 2007\142140).

resoluciones de la AEDP<sup>503</sup> han decidido sancionar empresas por no constar que estas hubiesen acreditado el envío de los requerimientos de pago por el importe de las deudas por las que figuraba incluida en los ficheros de solvencia patrimonial y de crédito.

Además, hay que tener en cuenta que el requerimiento previo de pago no se confunde con el envío de una mera factura. Éste parece ser el entendimiento de la AEPD<sup>504</sup>: “no es posible atribuir la misma naturaleza a las facturas que a un requerimiento de pago previo a la inclusión en un fichero de solvencia patrimonial y crédito”. En el mismo sentido, la Audiencia Nacional<sup>505</sup> ha decidido que “la previa recepción de dichas anteriores facturas no constituye indicio suficiente para desvirtuar tal falta de prueba del requerimiento previo, requisito de obligado cumplimiento”. Coincidimos con la opinión de Pascual Huerta, para quién este criterio le parece acertado ya que solamente después de emitidas las facturas y transcurrido el plazo para efectuar el pago si éstas no se pagan es cuando surgen la situación de impago y debe verificarse a través del requerimiento de pago si los importes de las facturas son correctos.

Por lo tanto, analizando la jurisprudencia y las resoluciones de la AEPD, se puede concluir que el requerimiento de pago debe ser un documento independiente de las facturas, que conste todos los conceptos y importes relativos a la deuda que se quiere registrarla en el fichero de moroso, de manera clara y objetiva que no deje lugar a cualquier injerencia externa para su comprensión. Por otra parte, a nuestro juicio, también es requisito material del requerimiento de pago la información previa que se ordena en el artículo 39, cuyo comentario nos dedicaremos más adelante.

---

<sup>503</sup> AEPD. Resolución: R/00657/2005.

<sup>504</sup> AEPD. Resolución: R/00675/2008.

<sup>505</sup> Audiencia Nacional. Sentencia de 18 abril 2007 (JUR 2007\132034).

Es necesario añadir, aún, que el aludido requisito de requerimiento previo de pago es autónomo y, además, como considera la Audiencia Nacional<sup>506</sup>, es formal. Por mejor decir, este Tribunal<sup>507</sup>, en la Sentencia de 9 de enero de 2009, señala que “debe considerarse, que aquel que utiliza un medio extraordinario de cobro como es el de la anotación de la deuda en un registro de morosos, debe garantizar el cumplimiento de todos los requisitos materiales (exactitud del dato) y formales (requerimiento previo) que permitan el empleo de este modo accesorio para conseguir el cobro de la deuda”. Por lo que se desprende de la jurisprudencia, existe la posibilidad de sanción solamente por incumplimiento del requisito formal, aunque todos los requisitos materiales hubieran sido cumplidos. En efecto, en otra Sentencia de 19 junio 2009 emitida por el mismo Órgano juzgador citado<sup>508</sup>, deja claro que a efectos de la existencia de infracción, es indiferente que la deuda cumpla con los requisitos de certeza, vencimiento y exigibilidad y que los datos del afectado incluidos en el fichero de morosos fueran exactos, actuales y respondieran realmente a su situación. En éste fallo, tal infracción “ha consistido en no respetar una garantía vinculada al principio de calidad del dato pero que opera con independencia de dicho principio. Esto es, puede darse el caso, como aquí ocurre, que los datos que se incorporan a un fichero de morosos sean exactos y actuales sin que por ello pueda prescindirse de la garantía que supone para el afectado el hecho de que previamente se le requiera de pago, dándole así opción de evitar su inclusión en el fichero de solvencia patrimonial, bien porque se le permite de esta manera satisfacer una

---

<sup>506</sup> “De los antecedentes de hecho de esta resolución resulta claramente acreditado como el alta en el registro de morosos se produjo sin que se llegara a reclamar el pago de la minuta del procurador a los denunciados por lo que se incumplió un requisito formal cuya exigencia era previa a la anotación de la incidencia en el registro correspondiente”. Audiencia Nacional. Sentencia de 4 octubre 2006 (JUR 2006\251350).

<sup>507</sup> Audiencia Nacional. Sentencia de 9 enero 2009 (RJCA 2009\217).

<sup>508</sup> Audiencia Nacional. Sentencia de 19 junio 2009 (JUR 2009\309588)

deuda impagada, bien porque le permite poner de manifiesto al acreedor la inexactitud o inexistencia de la deuda”

Además, cumple señalar que recae sobre el acreedor el onus de la comprobación de la realización del requisito citado. En efecto, ya había dejado consignado la AEPD<sup>509</sup> que no basta con la afirmación de tal cumplimiento por parte del obligado, pues resultaría en la práctica privada de toda efectividad dicha obligación legal. Así, resulta interesante subrayar la posición de la Audiencia Nacional en la ya citada Sentencia de 18 abril 2007<sup>510</sup>, cuando advierte que “lo que viene a sostenerse reiteradamente por la Sala es que, cuando se niega la recepción de la comunicación, corresponde la carga de su prueba a quien tiene la obligación de realizarla, sin que sea suficiente acreditación la mera afirmación, aunque lo sean mediante certificación, de parte interesada, doctrina que nuevamente ha de ser ahora reiterada”.

La razón por la cual tal obligación es atribuida al acreedor, es que éste es quién conoce la situación de incumplimiento del titular de los datos. Asimismo, de lo que se desprende del propio apartado 3 del artículo 38, el aludido acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos establecidos en este artículo y del requerimiento previo al que se refiere el artículo 39.

Finalmente, otro problema que se plantea, pero de solución prácticamente unánime tanto por la doctrina, como la jurisprudencia y la propia AEPD, es la independencia del requerimiento de pago del Reglamento de desarrollo de la LOPD y aquél ubicado en las normas relativas a la mora. En efecto, existe una norma específica que exige el

---

<sup>509</sup> Vide Resolución: R/00315/2007 y R/00739/2007 de la AEPD.

<sup>510</sup> Audiencia Nacional. Sentencia de 18 abril 2007 (JUR 2007\132034)

cumplimiento del requerimiento previo de pago de la deuda expresamente y con carácter imperativo<sup>511</sup>, y esta no tiene como objeto denunciar la mora del deudor<sup>512</sup>. En efecto, la AEPD<sup>513</sup> puso de manifiesto que “hay que delimitar la obligación de requerimiento de pago para que exista mora en las obligaciones civiles, con la obligación de requerimiento de pago antes de comunicar la información a un fichero que presta a terceros la información sobre solvencia patrimonial y crédito de una persona”. Así, no se puede aceptar como justificación del cumplimiento del requerimiento de pago del RPD que el responsable de dicho pago conozca su obligación de abonar mensualmente las cuotas del préstamo concedido<sup>514</sup>. De igual modo, la Audiencia Nacional<sup>515</sup> se pronunció a respecto del tema, en diversas sentencias, afirmando con rotunda firmeza que “la exigencia o no de requerimiento de pago a efectos civiles y en aplicación de lo previsto por el artículo 1100 del Código Civil (que no exige dicho requerimiento cuando la obligación así lo declare) puede tener efectos puramente civiles pero no afecta a la exigencia de cumplimiento de un requisito que tiene su origen, exclusivamente, en la normativa específica de protección de datos”.

#### 1.2.6. Conservación de documentación.

---

<sup>511</sup> PLANA, Maria del Carmen. *Ficheros... op. cit.*, p.380.

<sup>512</sup> PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 380.

<sup>513</sup> AEPD. Resolución: R/00123/2005 y en el mismo sentido, Resolución: R/00130/2008.

<sup>514</sup> *Ibid.*

<sup>515</sup> Audiencia Nacional. 20 de Abril de 2006 (JUR 2006\152433).

El apartado 3 del artículo 38 del RPD determina que el acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos establecidos en este artículo.

Sobre éste artículo hay dos cuestiones planteadas por Pascual Huerta<sup>516</sup> que entendemos que son de interesante estudio. La primera, para el autor citado, resulta algo oscuro que el artículo preceptúe que la documentación debe de estar a disposición del responsable del fichero común. Así, se manifiesta aclarando su posición alegando que el cumplimiento de las obligaciones del responsable del fichero no depende de que el acreedor cumpla a su vez las suyas. Sugiere, aún, “que una explicación plausible de esta referencia podría ser que el responsable del fichero común podrá excluir de la participación en el fichero a las entidades que sistemáticamente incumplen los requisitos de inclusión establecidos en la norma, y por ello puede necesitar examinar la citada documentación”, aunque el mismo autor añade que este argumento no es demasiado convincente.

De nuestra parte, entendemos que fue acertada la inclusión de tal referencia en la ley. En efecto, nos parece razonable el planteamiento del autor cuando a la independencia de las obligaciones del acreedor y del responsable del fichero. Ahora bien, la Audiencia Nacional<sup>517</sup>, se ha manifestado en diversas ocasiones que “es el acreedor el único que puede incluir los datos del deudor en el fichero y de instar la cancelación de los mismos, toda vez que es él el que conoce si la deuda realmente existe o si

---

<sup>516</sup> PASCUAL HUERTA, Pablo. “Ficheros de Información Sobre Solvencia Patrimonial y Crédito (arts. 37 a 44)”. En: ZABÍA DE LA MATA, Juan. (coord.). *Protección de Datos. Comentarios al Reglamento*. Valladolid: Lex Nova, 2008, p. 390

<sup>517</sup> Audiencia Nacional. Sentencia de 29 mayo 2009 (JUR 2009\311922).

ha sido saldada o no". De suerte que toda la información relativa a los aspectos materiales y formales de la deuda están en pose del acreedor.

Sin embargo, hay ciertas obligaciones que una vez incumplidas, pueden constituirse en infracción, como tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos legalmente; impedir o obstaculizar el ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada o incluso mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan, son algunos de los problemas que pueden enfrentarse el responsable del fichero que en los casos específicos de los ficheros de solvencia patrimonial y crédito está en una situación de intermediario de las informaciones. No por otra razón que el Reglamento ha establecido algunas de las responsabilidades que recaen directamente sobre el acreedor en el artículo 43.

De todas las maneras, es necesario que el responsable del fichero conozca o por lo menos tenga el respaldo legal de la posibilidad de conocer toda la documentación que posee el acreedor fundamentalmente para los casos en que sea necesario actuar en su propia defensa. Además de ello, para ejercer bien y con eficacia la prestación de servicio a cual se dedica en lo que concierne al tratamiento (que conlleva entre otros procedimientos mantener los datos actualizados) y a la cesión de los datos, requiere que responsable del fichero y acreedor estén funcionalmente en armonía. Es decir, la actuación de uno y otro se complementan, ya que si comparamos la sistemática de los ficheros de morosos con un fichero que se dedica a otro tipo de datos, el acreedor tiene parte de la función que originariamente cabe al responsable del fichero, que es la recogida de los datos (en este caso sin consentimiento del afectado) y la verificación de la calidad de los mismos.

La segunda crítica que hace el aludido autor<sup>518</sup> es que, en su opinión, el artículo 38 apartado 3 también se refiere a la obligación de que el acreedor conserve el documento que sirva de prueba de que no existe una disputa sobre la deuda lo que en su opinión es “sencillamente imposible”. En efecto, coincidimos de este entendimiento ya que en éste punto específico es complicado que para cada deuda sea necesario conservar un documento que acredite la ausencia de cualquier tipo de reclamación. Tal responsabilidad puede existir sin que sea necesario obligarle al acreedor poseer tal documentación correspondiente. De este modo, pensamos que lo que quiso la ley en el caso de la segunda parte de la letra *a*) del apartado 1 del artículo 38, no fue imponer dicha carga al acreedor pero sí para los casos de requerimiento de previo pago y de las informaciones previas a la inclusión, así como la comprobación de los plazos ínsitos en la letra *b*) del mismo artículo. Esta parece ser la posición de Plana<sup>519</sup>, para quién “este requisito habrá que entenderlo aplicable sólo en aquellos aspectos en los que sea compatible: en especial, no parece que se pueda conservar documentación que acredite que no hay reclamación (prueba de un hecho negativo por definición, imposible)”.

---

<sup>518</sup> PASCUAL HUERTA, Pablo. “Ficheros de Información Sobre Solvencia Patrimonial y Crédito (arts. 37 a 44)”. En: ZABÍA DE LA MATA, Juan. (coord.). *Protección de Datos. Comentarios al Reglamento*. Valladolid: Lex Nova, 2008, p. 371.

<sup>519</sup> PLANA, Maria del Carmen. “Ficheros sobre Solvencia Patrimonial y Crédito”. En: PALOMAR OLMEDA, Alberto y GONZALEZ-ESPEJO, Pablo (Dir.). *Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/199, de 13 de diciembre, de Protección de Datos de Carácter Persona (Aprobado por RD 1720, de 21 de diciembre)*. Cizur Menor: Thomson Civitas, 2008, p. 390.



### 1.2.7. Información previa a la inclusión de datos.

Además de todos los requisitos que hemos comentado hasta el momento, el Reglamento de la LOPD exige al acreedor que para que se incluyan datos en los ficheros de solvencia patrimonial se proceda a la llamada información previa a la inclusión, cuya regulación se encuentra en el artículo 39 de dicha ley. Así, es de responsabilidad del acreedor informar al deudor tanto en el momento en que se celebre el contrato como al tiempo de efectuar el requerimiento previo de pago exigido por la letra *c*) del apartado 1 del artículo 38. Así que en el caso de no haberse satisfecho la obligación en el termino previsto para ello, y una vez cumplidos los aludidos requisitos del citado artículo, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

De lo que se recoge de la doctrina<sup>520</sup>, tal obligación no constaba ni en la LOPD, ni en la Instrucción 1/1995, así como tampoco en la práctica jurisprudencial o de la AEPD, ni en las recomendaciones de esta Agencia. Además, se entiende que la citada obligación “se trata de un reforzamiento del deber de información del artículo 5 de la LOPD<sup>521</sup>”.

A este respecto, creemos que la determinación de la naturaleza jurídica de ésta obligación es un reto bastante complicado. Desde nuestro punto de vista, vislumbrarla como una derivación del deber de información del artículo 5 de la LOPD trae algunos problemas de difícil solución. El primero consiste en la propia esencia del derecho a ser informado. Tal derecho está íntimamente ligado al principio del consentimiento que a su vez representa una de las más importantes formas de concreción jurídica

---

<sup>520</sup> PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 389. PLANA, Maria del Carmen. *Ficheros... op. cit.*, p. 388.

<sup>521</sup> PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 391.

del derecho fundamental a la protección de datos, como se puede desprender de la STC 292/2000 de 30 de noviembre, por mejor decir, la información a lo afectado torna eficaz su derecho a consentir. De este modo, el artículo 5 de la LOPD establece las características de un deber de información en la recogida de los datos en cuyo momento se perfeccionará un consentimiento libre e informado, como regla general.

En el caso concreto aquí analizado, los datos que serán tratados tienen una disciplina legal especial que encuentra uno de sus reflejos justamente en la ausencia del consentimiento del interesado, en cualquier fase del tratamiento. La Sentencia de 29 mayo 2009, emitida por la Audiencia Nacional<sup>522</sup>, respecto a este tema ha manifestado que “los ficheros de solvencia patrimonial de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias se encuentran regulados en el art. 29.2 de la LOPD y **no necesitan para la obtención y tratamiento de los datos el consentimiento del afectado. No obstante, frente a esta excepción, la propia norma articula una serie de contrapesos**, como es su limitación a un caso concreto (cumplimiento o incumplimiento de obligaciones dinerarias) y la obligación de notificar a los afectados el hecho de que se han registrado sus datos de carácter personal, notificación cuyos requisitos quedan reseñados en el precepto” (subrayamos). De manera que en el fallo, el Tribunal sentenciador aduce como consecuencia lógica de su dictamen que la no necesidad del consentimiento exime también de la obligación de la información del art. 5 LOPD respecto al momento de la recogida de datos.

Ahora bien, el resultado de los ‘contrapesos’ elaborado por las normas de protección de datos, de cuya alusión hace la Audiencia Nacional es que el referido derecho de información se transfiere a otro momento posterior, “pues la norma obliga a que se notifique la inclusión al afectado en el plazo de 30 días desde la incorporación al registro de la entidad”. No

---

<sup>522</sup> Audiencia Nacional. Sentencia de 29 mayo 2009 (JUR 2009\311922).

obstante, desde nuestro punto de vista, tal información deja de ser aquella que es la condición esencial para convertir el consentimiento en “eficaz”. Ahora estaríamos ante el deber de notificación, que a su turno es uno de los requisitos fundamentales que confiere la posibilidad de concreción práctica del principio de la calidad de los datos. La Audiencia Nacional en la aludida Sentencia manifiesta que “esta información frente a la prevista por el art. 5 es restringida, pues se circunscribe a una referencia de los datos que hubiesen sido incluidos y del derecho de su titular a recabar información de la totalidad de ellos en los términos establecidos en la LOPD”.

La información previa a la inclusión del dato en los ficheros de solvencia patrimonial no es derivada de aquella, igualmente información previa pero operada en el momento de la recogida de los datos, disciplinada por el artículo 5 de la LOPD, porque le falta un elemento esencial, que es la razón principal de su realización, o sea, el consentimiento.

Asimismo, es difícil aceptar que la información del artículo 39 del RPD se derive de una notificación posterior. Como se desprende del propio nombre, es una información **previa a la inclusión de los datos** y el hecho de que la ley haya elegido un momento específico para hacerse válida resultaría ilógica tal deducción.

Sin embargo, la referida información contiene, a nuestro juicio, una de las finalidades de la notificación posterior que es servir al principio de la calidad de los datos. Es decir, cuando se informa previamente que un dato podrá ser incluido en un fichero de moroso, se está dando la oportunidad a que el titular de los mismos ejerza un control previo, aunque indirecto sobre estos datos, en lo que respecta a la calidad de los mismos, como forma de una vez más compensar la ausencia del consentimiento. De otra parte, permite que el deudor conozca el posible destino que tendrán los datos de la deuda en el caso de que se mantenga el incumplimiento

Asimismo, la información previa a la inclusión de los datos sobre el cumplimiento e incumplimiento de obligaciones dinerarias es una obligación que tiene como finalidad equilibrar la excepción legal de la falta de consentimiento para el tratamiento de estos datos personales. Resáltese que no es el único medio disponible para conseguir tales finalidades, pero se ubica dentro de este contexto con los demás mecanismos puesto a disposición por las leyes de protección de datos.

Otra cuestión que se plantea con relación a la nueva información previa a la inclusión de los datos es la de que si ésta es un requisito de contenido del requerimiento previo de pago, recogido en el artículo 38, apartado 1, letra c). Al que parece, algunas voces doctrinales considera indefendible que la previsión del artículo 39 sea entendida como tal<sup>523</sup>.

El artículo 39 establece dos momentos para que sea avisado al interesado que sus datos podrán ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias: a) en el momento en que se celebre el contrato; b) en todo caso, al tiempo de efectuar el requerimiento al que se refiere la letra c) del apartado 1.

Sobre el primer momento, aunque la norma establezca que el acreedor deberá insertar tal información, si éste deja de satisfacer tal obligación no habría a nuestro sentir, ninguna sanción ya que el mismo precepto establece que se puede proceder al tiempo de efectuar el requerimiento. Ahora bien, nos parece que la ley ha impuesto una franja temporal que se iniciaría en el momento del contrato y terminaría en el momento que se efectuará el requerimiento previo de pago. Sin embargo, a nuestro juicio, la ley establece que independientemente de que se haya o no informado durante el tiempo establecido, siempre deberá hacerlo (*“en todo caso”*) en el momento en que se realice el requerimiento previo de pago, *“al tiempo*

---

<sup>523</sup> Vide PLANA, Maria del Carmen. *Ficheros... op. cit.*, p. 392.

*de efectuar el requerimiento al que se refiere la letra c) del apartado 1 del artículo anterior”.*

Desde la perspectiva sostenida en este trabajo, y a la vista de todo LO expuesto sobre la finalidad del requerimiento previo de pago (art. 38.1.c del RPD) y de la información previa a la inclusión (art. 39 del RPD) nos parece evidente que esta última es un requisito legal de contenido del primero. A este hilo, creemos conveniente subrayar la Sentencia de 22 abril 2009 de la Audiencia Nacional<sup>524</sup>, cuando establece que “la exigencia de requerimiento previo de pago para proceder a la inclusión de los datos del acreedor moroso en los ficheros correspondientes, tiene como objeto que el ‘deudor’ o la persona obligada, conozca la existencia de la deuda vencida y exigible”. Esta sería, por lo tanto, su finalidad.

Pero continua el fallo manifestando que igualmente es parte del objeto del referido requerimiento que el interesado conozca “la posibilidad de ser incluido en un fichero de morosos en el supuesto de no hacerla efectiva (*la deuda*), ya que como se ha dicho, no se necesita el consentimiento del afectado para su inclusión en esta clase de ficheros, tratando así de salvaguardar la veracidad y exactitud de los datos que se van a incluir en dichos ficheros”. Así, antes de que apareciera la información previa a la inclusión, se entendía que era el requerimiento previo que comunicaba al deudor los datos relativos al impago que podrían ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias. De manera que creemos que la ley ha tratado uno y otro en artículos distintos para reforzar los momentos en que se debe realizar la información previa (artículo 39 del RPD).

---

<sup>524</sup> Audiencia Nacional. Sentencia de 22 abril 2009 (JUR 2009\245632).

*1.2.8. Consecuencias de la no observancia de los requisitos de inclusión de los datos.*

La LOPD y su Reglamento así como la Directiva establece los principios de protección de datos que deberán ser observados en cualquier fase de tratamiento de datos personales, como ya se ha comentado, entre los cuales está el principio de la calidad de los datos. Son exigencias que se añaden y refuerzan aquellas contenidas en el artículo 38 del RPD. En este sentido, conviene destacar que el apartado 3 del artículo 4 de la LOPD establece que los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado, y según entendimiento de la Audiencia Nacional<sup>525</sup>, tal principio tiene “gran relevancia en cuanto no solo resulta necesario que los datos se recojan para su tratamiento de acuerdo con una serie de criterios (principio de proporcionalidad) y que los mismos se empleen para finalidades compatibles a las que motivaron la recogida (principio de finalidad), sino también que sean exactos y puestos al día, pues lo contrario supondría de forma implícita el incumplimiento de los citados principios, con las importantes consecuencias que puede tener para de afectado, especialmente cuando se remiten datos inexactos a un fichero de solvencia patrimonial”.

En lo que concierne al incumplimiento por parte del acreedor de la observancia de los requisitos para dar de alta en una incidencia en un fichero de morosidad, es importante señalar que tal acto se constituye en una sanción. A este hilo, la Audiencia Nacional<sup>526</sup> en sentencia de 9 enero 2009 ha desestimado el recurso del Banco Santander S.A., frente a la resolución de fecha 30 de enero de 2008 dictada por el Director de la

---

<sup>525</sup> Audiencia Nacional. Sentencia de 28 mayo 2009 (JUR 2009\268420).

<sup>526</sup> Audiencia Nacional. Sentencia de 9 enero 2009 (RJCA 2009\217).

Agencia Española de Protección de Datos por la que se imponía a dicha entidad bancaria una multa por infracción de lo previsto en el artículo 44.3.d) de la LOPD, a raíz de la violación del requisito de requerimiento previo de pago. Así como la Sentencia de 10 septiembre 2009 emitida por el mismo Tribunal<sup>527</sup>, que confirmó la resolución que sancionaba a Telefónica Móviles España S.A., en una multa por la comisión de una infracción del artículo 4.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, tipificada como grave en el artículo 44.3.d) de la misma ley, por mantener indebidamente datos correspondientes a una deuda que no era cierta, vencida ni exigible relativos al cumplimiento o incumplimiento de obligaciones dinerarias y que no respondía con veracidad y certeza a la situación del afectado en aquella fecha.

Hay que añadir, igualmente el fallo de la Audiencia Nacional<sup>528</sup>, que confirmó la resolución de la AEPD que sancionaba a una empresa por incluir datos personales sobre los que exista un principio de prueba documental que aparentemente contradecía alguno de los requisitos, en aquella época, determinados por la Instrucción 1/1995 de la AEPD: existencia de una deuda cierta, vencida y exigible, que ha resultado impagada.

En efecto, lo que entienden los Tribunales es que la Instrucción de la AEPD y en el caso el Reglamento de desarrollo de la LOPD que sigue el texto de ésta norma, establecen una presunción de no inclusión de la deuda cuando exista un principio de prueba que ponga en duda la concurrencia de los requisitos necesarios para su inclusión. Se hace eco el fallo de la Audiencia Nacional<sup>529</sup>, de 8 marzo 2006, en el cual una sentencia de divorcio establecía que la entonces esposa del reclamante

---

<sup>527</sup> Audiencia Nacional. Sentencia de 10 septiembre 2009 (JUR 2009\416499).

<sup>528</sup> Audiencia Nacional. Sentencia de 24 septiembre 2009 (JUR 2009\424380).

<sup>529</sup> Audiencia Nacional. Sentencia de 8 marzo 2006 (JUR 2006\118267).

asumiría la integridad del préstamo hipotecario suscrito en su momento por la sociedad de gananciales que formó con el reclamante, así como la propiedad de la vivienda cuya hipoteca constituye una garantía de aquel crédito concedido, consideró que “ello es lo que ocurre en el presente caso, con independencia de las discusiones jurídicas sobre la naturaleza y efectos del referido contrato de préstamo, pues la mencionada normativa de protección de datos de carácter personal tiene como finalidad proteger un derecho fundamental como es el de la intimidad, de ahí que en un caso de inclusión en un fichero de estas especiales características, que afecta gravemente al incluido en sus relaciones económicas con terceros, pues se da publicidad a una insolvencia motivada por incumplimiento de pago de una deuda, se establezca de forma muy tajante que para tal inclusión la información que de el informante y causante de la misma sea veraz, prevaleciendo ante la duda ese derecho fundamental”.

En éste caso concreto, el nudo gordiano no residía en si hubo o no una novación en ese contrato de préstamo hipotecario conforme a la normativa civil. Pero que había que tenerse en cuenta el hecho acreditativo de una sentencia firme que establecía que solamente una de las partes deudoras asumiría la totalidad de la deuda. De suerte que frente a ello la entidad bancaria podría ejercitar todas las acciones que estimase pertinente para la defensa de sus derechos, no obstante el Tribunal entiende que “lo cierto y relevante para lo que se está enjuiciando es que, efectivamente, existen dudas más que razonables para concluir que dicho reclamante pueda seguir estando incluido en un fichero de esas características, dado que es dudoso que siga siendo deudor por la deuda que motivó tal inclusión”.

Así cómo las sentencias citadas aquí, hay muchas otras<sup>530</sup> que en el mismo sentido confirman las resoluciones de los procedimientos

---

<sup>530</sup>Audiencia Nacional, Sentencia de 29 abril 2009 (JUR 2009\244875), confirma resolución de la AEPD que sancionó con multa empresa por haber incluido datos de una deuda que resultó no ser cierta por inexistente. En el mismo sentido, la Audiencia



sancionadores de la Agencia Española de Protección de Datos, cuando vulneran los requisitos para la inclusión de los datos en el fichero de solvencia patrimonial.

## 2. La Legislación Italiana.

### 2.1. Cuestiones preliminares.

En Italia, en los sistemas de información crediticia aquí estudiados pueden confluir datos positivos y negativos, como se ha indicado en el capítulo anterior. En lo que concierne al consentimiento, el *Garante* señaló a través de *Deliberazione*<sup>531</sup> que las entidades privadas que operan estos sistemas para tratar los datos de carácter positivos deben adquirir, para eventual difusión a las organizaciones participantes, el consentimiento libre e informado de los interesados. Las excepciones a esta regla son los casos en que el propio Código en materia de protección de datos en el artículo 24 resalta, que son: a) para el cumplimiento de las obligaciones derivadas de un contrato en la que el interesado sea parte, o bien con el fin de atender las peticiones concretas formuladas por el mismo

---

Nacional, Sentencia de 19 noviembre 2008 (JUR 2009\3381); Audiencia Nacional, Sentencia de 25 junio 2009 (JUR 2009\308686) igualmente confirma resolución de la AEPD de un procedimiento sancionador por la inclusión de datos, cuando existía la duda sobre la existencia de una deuda cierta, vencida y exigible y, además, se realizó sin el previo requerimiento de pago. En el mismo sentido, AN. Sentencia de 4 octubre 2006 (JUR 2006\251327).

<sup>531</sup> *Deliberazione* n. 9, de 16 novembre 2004. “Sistemi di informazioni creditizie e bilanciamento degli interessi”. GU n. 300 del 23-12-2004.

interesado, previas a la celebración de un contrato; b) para datos relativos al desarrollo de actividades económicas por parte de la sociedad, empresarios individuales y profesionales libres, respetando los límites extraídos del Código (artículo 24, párrafo 1, letra *d*); c) en los casos que sean necesarios para dar cumplimiento a una obligación impuesta por una ley, reglamento o la legislación comunitaria; d) sean necesarios para defensa ante los órganos judiciales, asimismo en relación a las solicitudes de las autoridades públicas interesadas o competentes, conforme a lo dispuesto por la ley.

De otra parte, los datos negativos no necesitan del consentimiento, según se extrae de la aludida *Deliberazione*. Ello porque, como señala Frau<sup>532</sup>, dentro de una comparación de los intereses —la tutela de los valores de la persona, contra la necesidad de contener los riesgos de crédito— el *Garante* ha considerado que, en el caso del tratamiento pertinente y no excedentes prevalezca el interés del titular, para que puedan procesar la información relativa a los retrasos en el pago.

Importa resaltar que el *Garante* ha afirmado en *Dossier*<sup>533</sup> que los datos en poder de los sistemas de información de crédito no pueden ser utilizados para la comercialización, estudios de mercado, publicidad y venta directa de productos.

La información que puede ser tratada en los ficheros italianos son aquellas relativas al deudor principal, o sea aquél que solicita o es parte de una relación crediticia (un consumidor, una empresa o un profesional liberal), asimismo, si es el caso, referentes a los deudores solidarios y

---

<sup>532</sup> FRAU, Riccardo. “Attività bancaria e trattamento dei dati personali”. En: CUFFARO, Vincenzo. *Il Codice... op. cit.* p. 785 y ss.; CASUCCI, Felice. *Tutela della privacy e misure di sicurezza dei dati personali*. Napoli: Edizioni Scientifiche Italiane, 2006, p. 543.

<sup>533</sup> *Garante per le protezione dei Dati Personali*. Dossier - 30 novembre 2005 “Le Nuove Regole sui Sistemi di Informazioni Creditizie”.

fiadores, pero nunca a personas que no tiene una relación jurídica con deudor y con su deuda.

## 2.2 Requisitos y categorías de datos.

La opción legislativa italiana fue distinta aquella española, en lo que concierne a especificación de los requisitos de inclusión de los datos. De hecho, en el código deontológico no hay un único artículo que establezca tales condiciones de inclusión tan pormenorizadamente cómo lo ha estructurado el legislador español.

Sistemáticamente el artículo 3 del citado código sería el que más se acercaría al artículo 38 del RPD de España, pero elige el legislador italiano por un lado un texto más genérico y por otro, centrarse sobre todo en aspectos referentes al dato en si, es decir a su naturaleza o mismo al tipo de información que contiene.

Para especificar aún más su objeto, el apartado 2 del aludido artículo prohíbe el tratamiento de datos sensible o judiciales en estos ficheros, conceptos estos ubicados en el artículo 4, apartado 1, letras *c)* y *d)* del Código en materia de Protección de Datos ya estudiados aquí en los capítulos anteriores. Asimismo, los datos personales registrados en las centrales de riesgos deben ser objetivos, estrictamente pertinentes y no excesivos con relación a los fines perseguidos, relativos a una solicitud o una relación de crédito, en este ámbito referirse a hechos hasta la regularización de los incumplimientos, respetando los tiempos de conservación establecidos. Resulta oportuno señalar lo que consignó el

Tribunal de Napoli<sup>534</sup> tocante a la responsabilidad del *gestore*, manifestando que éste debe efectuar una atenta verificación de los criterios utilizados y del control utilizado a garantizar la exactitud y actualización de la información.

Aparte de las consideraciones generales, el apartado 3 del artículo 3 del código de buena conducta establece una lista que para Petrulli<sup>535</sup>, es taxativa y no meramente ejemplificativa de las categorías de los datos concernientes a cada solicitud o relación de crédito señaladas en un sistema de información crediticias. Tales categorías deberán estar disponibles en el sitio de comunicación de la red de información del fichero, y transmitido analíticamente a los interesados a su petición. Son ellas: a) datos personales, número y código de Identificación Fiscal; b) la información relativa a la solicitud o relación de crédito, en particular, las que describen el tipo de contrato, el importe del crédito, la amortización y el estado de la solicitud o de la ejecución del contrato; c) la utilización de datos contables, relativos a los pagos y a su andamiento, el endeudamiento, incluyendo las deudas restante y el resumen del estado de contabilidad; d) información relativa a las actividades de recuperación de crédito o litigios, la cesión de crédito, acontecimientos excepcionales que afecten a la situación personal o bienes de empresas, personas jurídicas u otras entidades.

Según señala Mormile<sup>536</sup>, son objetos de tratamiento todos los datos relativos al contrato de financiación, a la fase precontractual, así como a los referentes a la ejecución del contrato o eventual incumplimiento,

---

<sup>534</sup> Sentencia de 12 de junio de 2003.

<sup>535</sup> PETRULLI, Mario. *Il nuovo Codice deontologico per le centrali rischi private e le tutele per i consumatore*. Matelica: Editora Halley, 2005, p. 26.

<sup>536</sup> MORMILE, Lalage. "Il Sistema di Informazioni Creditizie". En PANETTA, Rocco (coord.). *Libera circolazione e protezione dei dati personali*. Milano: Giuffré, Tomo II, 2006, p. 1847.

asimismo aquellos que conciernen a los acontecimientos sucesivos al incumplimiento, como las informaciones sobre actividad de recuperación de los créditos o evolución del contencioso. En su opinión, por un lado, se pretendía tipificar las categorías de datos que pueden ser recogidos, a fin de limitar el tratamiento únicamente a la información necesaria para la consecución de los fines señalados por el principio de finalidad. Y de otra parte, sin embargo, se ha optado por una "tipificación" muy amplia ya que pueden ser objeto de tratamiento no únicamente las informaciones crediticias de tipo negativo, sino también de tipo positivo y negativo.

El párrafo 4º del mismo artículo, determina que los códigos y los criterios eventualmente utilizados para registrar los datos en el sistema de información de crédito y para facilitar su tratamiento, se destinarán únicamente a proporcionar una representación correcta y objetiva de dichos datos, así como cualquier ocurrencia sobre la relación de crédito señalada. Ahora bien, los aludidos códigos y criterios deberán ser acompañados por indicaciones claras en cuanto a su significado, suministrada por el gestor y observados por los participantes, fácilmente accesibles por ambos y también a petición del interesado. Cuanto a esta cuestión, el *Garante*<sup>537</sup> dejó consignado que no se puede utilizar códigos o codificación ocultos para clasificar los clientes: si se utilizan, el interesado debe ser capaz de entender su significado. También nos parece interesante añadir que es ilícito cualquier dato evaluativo o que exprese juicio de valor sobre el interesado como "mal pagador"<sup>538</sup>.

El *Codice Deontologico* prevé aún que las informaciones relativas al participante que ha comunicado los datos personales relacionados a una solicitud o relación de crédito también serán registradas en el fichero. Sin embargo, tales datos de identificación solo podrán ser accedido por el

---

<sup>537</sup> Garante per la Protezione dei Dati Personali. Dossier – 30 de noviembre de 2005.

<sup>538</sup> IMPERIALI, Riccardo. *Codice... op.cit.*, p. 993; Garante per la Protezione dei Dati Personali. Dossier – 30 de noviembre de 2005;

responsable o por el interesado titular de los datos. Los demás participantes del sistema no pueden conocer tal información. Según Petrulli<sup>539</sup>, se trata de una medida de tutela del sistema y de la competencia.

Tal precepto nos parece muy acertado. A los participantes del sistema no les interesa para la finalidad de los fichero saber quién ha informado los datos, de suerte que ésta información es completamente irrelevante y desde nuestro punto de vista no solamente protege la competencia, pero también el afectado. No existe ninguna razón para que otros participantes sepan con quien éste contrata o quiere contratar un crédito. Por otro lado, de esto tipo de informaciones, se puede sacar algunas informaciones de otras entidades crediticias, como por poner un ejemplo el nivel de créditos como la cantidad de créditos concedidos y no satisfechos que detiene un determinado banco y desde esta perspectiva sí hay una gran protección de la competencia.

### *2.2.1. Tratamiento de datos provenientes de fuentes públicas.*

En Italia, también se pueden incluir las informaciones provenientes de fuentes públicas, y el código de buena conducta establece algunas particularidades. La primera, es respecto a la ubicación de tales informaciones en el fichero. El artículo 10, apartado 1, letra *a*) determina que estos deberán estar colocados en un banco de datos separado del sistema de información crediticia y no conectados con tal sistema.

Por lo tanto, la norma establece que es obligación del *gestore* adoptar las medidas técnicas y organizativas necesarias para garantizar la separación

---

<sup>539</sup> PETRULLI, Mario. *Il nuovo... op. cit*, p. 27.

y distinción de los datos del sistema de información de crédito de otras bases de datos, incluso mediante la inclusión de información adecuada, eliminando cualquier ambigüedad sobre la diferente naturaleza y origen del los datos objeto de acceso.

Para Petrulli<sup>540</sup>, se trata de una medida destinada a prevenir la mezcla de datos y que, probablemente protege al solicitante más de lo que parece: porque, en realidad, especialmente para operaciones menores, la consulta de estos datos de fuentes públicas son sólo ocasionales y no suele ser la regla.

Cuando la solicitud de crédito no haya sido aceptada, el participante deberá informar al interesado si, para fundamentar su decisión, ha consultado asimismo datos personales de tipo negativo originario de fuentes públicas y a petición del interesado deberá informar la fuente específica de donde procede tales datos.

Es oportuno señalar que el tratamiento de los datos provenientes de fuentes públicas no necesita del consentimiento, como dispone el artículo 24, letra c) del Código en materia de protección de datos italiano.

### III. Modalidad de recogida y registro de los datos.

---

<sup>540</sup> PETRULLI, Mario. *Il nuovo... op. cit.*, p. 42. Comparte la misma opinión GOBBATO, Monica. *La tutela del consumatore: clausole vessatorie, commercio elettronico e codice del consumo*. Matelica : Halley, 2007, p. 76.

## 1. Legislación Española.

El Reglamento 1720/2007 pormenoriza en el artículo 43 dos responsabilidades que recaen exclusivamente sobre el acreedor o quien actúe por su cuenta. Tales reglas derivan de la Instrucción 1/1995 de la AEPD, que en su norma primera previa que era responsabilidad de las citadas personas asegurarse que concurrían todos los requisitos exigidos por la referida norma, en el momento de notificar los datos adversos al responsable del fichero común.

El apartado 1 del artículo 43 sigue prácticamente el mismo texto, de la Instrucción, dispone que el acreedor o quien actúe por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 38 y 39 en el momento de notificar los datos adversos al responsable del fichero común. La novedad se observa en lo que respecta al apartado 2, que determina que el acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero

En nuestra opinión, la redacción dada por el reglamento ha mejorado de manera significativa en lo que concierne al ámbito de la obligación del acreedor. Ello porque ahora se resalta cual es el su deber de modo más directo, mientras que en la aludida Instrucción, el relieve estaba en la comunicación de dichos datos al responsable del fichero.

En efecto, Pascual Huerta señala que la Instrucción 1/1995 no había conseguido distribuir bien las obligaciones de los que intervienen en él, trabajo éste que se encargó la AEPD y la jurisprudencia. De hecho, en diversos fallos de la Audiencia Nacional<sup>541</sup> podemos encontrar supuestos

---

<sup>541</sup> *Vide*, por todos, Audiencia Nacional. Sentencia de 18 de enero de 2006 (RJCA 2006\601).



en los cuales especifica la responsabilidad de los intervinientes de la actividad de prestación de servicio de solvencia patrimonial. En la ocasión de la Sentencia de 18 de enero de 2006 el Tribunal ha consignado de la siguiente manera: “Y que duda cabe que la LOPD comprende bajo su régimen sancionador, **al que suministra los datos al responsable del fichero, que es quien en realidad sabe la situación en que se encuentra el crédito, si ha sido o no satisfecho, en que condiciones y en que momento ha tenido lugar.** En definitiva es el concededor de la situación de solvencia en que se encuentra el afectado. Y en caso de que se produzca una modificación de dicha situación, debe informar al responsable del fichero para que este refleje con veracidad la situación actual del afectado” (subrayamos).

Lo cierto es que solamente se podrá evaluar si verdaderamente el Reglamento ha conseguido cumplir con el objetivo de individualizar las obligaciones con el tiempo y los supuestos que sean analizados por la AEPD y por los Tribunales.

## 1.1. Notificación de inclusión.

### 1.1.1. *Datos sobre solvencia patrimonial y crédito*

Merece destacar de manera apartada, aún en el ámbito de la modalidad de colecta y registro de los datos, la notificación del afectado. Así, respecto al derecho de información del afectado, cuando los datos sean recabados de las fuentes accesibles al público, la regla general, como dispone el artículo 5, apartado 4 de la LOPD, es que el interesado deberá ser notificado cuando los datos no hayan sido facilitados por el mismo, dentro de los tres meses siguientes al momento del registro de los datos,

de forma expresa, precisa e inequívoca por el responsable del fichero o su representante. Apreciando esta norma, la Audiencia Nacional<sup>542</sup> considera que tal derecho a ser informado es “importantísimo porque es el que permite llevar a cabo el ejercicio de otros derechos, y así lo valora el texto positivo al pormenorizar su contenido, y establecer la exigencia de que el mismo sea expreso, preciso e inequívoco”.

De suerte que, salvo que el afectado ya hubiera sido informado con anterioridad, el responsable del fichero deberá informarlo del contenido del tratamiento, de la procedencia de los datos, así como: a) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y c) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Ahora bien, la excepción a la regla general está establecida en el mismo artículo 5, apartado 5 cuyo tenor dispone que cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

El Reglamento de la LOPD ha aportado a la disciplina de estos tipos de datos dos artículos (el 18 “Acreditación del cumplimiento del deber de información” y el 19 “Supuestos especiales”) que solventan algunas cuestiones que serán más adelante analizadas. A parte de ello, el artículo

---

<sup>542</sup>Audiencia Nacional. Sentencia de 15 junio 2001 (JUR 2001\293673). En la misma línea, la Sentencia de 11 diciembre 2008 (JUR 2009\3155) del mismo Tribunal señala que “La exigencia de dicha información constituye un derecho del afectado que es objeto de protección por sí mismo, aunque también es, lógicamente, un complemento previo de la prestación del consentimiento. El derecho a la información constituye el pilar necesario para el ejercicio de otros derechos que la Ley reconoce”.

37 de ésta norma aclara que el tratamiento de los datos sobre solvencia patrimonial y crédito obedecerá a la disciplina del régimen general de la LOPD y del mismo reglamento.

De suerte que en lo que concierne al deber de información, no vislumbramos ninguna excepción para que no se cumpla el comando del apartado 4 del artículo 5 de la LOPD, cuando los datos son recabados de fuentes accesibles al público. En efecto, la Agencia Española de Protección de Datos<sup>543</sup> ha alertado sobre éste aspecto manifestando que “la aplicación del régimen general de protección de datos al fichero exige extremar las cautelas en relación con el cumplimiento de los deberes establecidos en la misma y en particular la aplicación de los principios de calidad de los datos y el cumplimiento del deber de información”.

Así, relativamente a los datos recabados de fuentes accesibles al público sobre la solvencia patrimonial de los individuos, creemos que la notificación debe existir y además ser personal. Éste fue el entendimiento señalado en la Sentencia de 18 septiembre 2003, del Tribunal Superior de Justicia de Andalucía<sup>544</sup>, cuando aún vigente la LOTARD, en la cual la empresa recurrente entendía que la obligación de notificar personalmente no existía cuando el dato se había obtenido de publicaciones oficiales. El Órgano sentenciador consideró que el artículo 28 de aquella ley no distinguía diferencia entre el tratamiento legal de la notificación en situaciones en que fuesen recabados datos directamente del afectado, o del acreedor, o de fuentes publicas. Para este Tribunal, “el conocimiento de la inclusión de un dato personal en el fichero permite al ciudadano conocer la veracidad del dato y, en su caso, exigir la rectificación. Y en el caso presente hubiera permitido a la sociedad recurrente rectificar, posiblemente a instancia del ciudadano afectado, con el efecto, beneficioso

---

<sup>543</sup> AEPD. Informe Jurídico 0052/2008.

<sup>544</sup> Tribunal Superior de Justicia de Andalucía. Sentencia núm. 2711/2003, de 18 septiembre (JUR 2003\243204).

para la recurrente, de impedir la comisión de la infracción grave. Puesto que al conocer su inclusión en el fichero el particular afectado hubiera instado de la sociedad sancionada la rectificación del dato”, y a su parecer, así lo había entendido la nueva ley hoy en vigor LO 15/1999.

En efecto, la lógica argumentativa que se recoge del fallo del Tribunal era la de que sería difícil solicitar evaluaciones sobre el dato si el interesado desconoce que se ha introducido informaciones suyas en un fichero. De suerte que tanto la ley anterior como la vigente, para estos casos puntuales de ficheros sobre solvencia patrimonial, exige el conocimiento del interesado para que su dato integre el fichero. Concluye el fallo en cita que la ley “no exige el consentimiento para que un dato publicado oficialmente se utilice, pero si es razonable exigir legalmente que se notifique el hecho de que el dato publicado oficialmente pasa a integrarse en un fichero sobre solvencia patrimonial. Esa es la interpretación que ahora posibilita el juego interpretativo de los arts. 5.4 y 6 de la Ley Orgánica 15/1999”. En el mismo sentido, la Sentencia de 29 octubre de 2003, del mismo Tribunal Superior de Justicia de Andalucía<sup>545</sup>, manifiesta que “no puede confundirse la falta de consentimiento expreso para tratar un dato obtenido de una publicación oficial con la falta de conocimiento de que dicho dato, publicado oficialmente para un determinado fin de satisfacción de intereses generales, acabe siendo tratado y cedido para otros fines comerciales. La Ley Orgánica protege el dato personal y su tratamiento y no puede mantenerse esta finalidad si el afectado por el dato desconoce su utilización. Entre otras cosas no puede solicitar la rectificación o actualización del dato”.

No obstante, esta no es una posición pacífica en la jurisprudencia. En efecto, la Audiencia Nacional parece no compartir de esta interpretación.

---

<sup>545</sup> Sentencia núm. 3128/2003 de 29 octubre (JUR 2003\265306)

Así como ya había dejado consignado en varios fallos<sup>546</sup>, nos parece que merece destacar la Sentencia más reciente, de 27 febrero 2008<sup>547</sup>, en la cual el este Tribunal expresa de modo taxativo que “en definitiva, ha de concluirse que la notificación de la inclusión solo es exigible en el supuesto en el que concurren dos notas: que los datos se refieran al cumplimiento o incumplimiento de obligaciones dinerarias; y que los mismos sean facilitados por el acreedor o quién actúe por su cuenta o interés. De lo que se infiere que habiéndose tomado los datos personales, en el supuesto ahora enjuiciado, del Boletín Oficial de la Comunidad de Madrid, no existía obligación ninguna de notificar su inclusión en el Fichero de Incidencias Judiciales al titular de los mismos”.

Ahora bien, la citada Sentencia nos ha llamado la atención no tanto por la ratificación de una postura jurisprudencial como por el articulado argumentativo que abarca la interpretación, o mejor, señal interpretativa del nuevo Reglamento 1720/2000. De manera que este fallo aduce que en la vigencia de la LOTARD, por la redacción dada al apartado 1 del art. 28 que trataba de forma conjunta los ficheros de solvencia patrimonial (los formados por datos procedentes de fuentes accesibles al público o de informaciones facilitadas por el interesado o con su consentimiento), dio lugar en su día a una controversia jurídica sobre la obligatoriedad de notificación cuando los datos sean recabado de fuentes accesibles al público. En cambio, con la entrada en vigor de la LOPD, el artículo 29 desgaja aquél único apartado de la LOTARD en dos: el primer en el cual se ubican los ficheros de solvencia patrimonial, y en el segundo apartado que se sitúan los ficheros de solvencia patrimonial formados con los datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias, facilitados por el acreedor. Para la Audiencia

---

<sup>546</sup> Véase, por todas, las SSAN de 29 junio 2001 (JUR 2001\293759) y de 26 octubre 2005 (JUR 2005\261117).

<sup>547</sup> Audiencia Nacional. Sentencia de 27 febrero 2008 (JUR 2008\97931).

Nacional, tal desdoblamiento supuso una aclaración de la LOPD respecto a la obligación de notificar.

Así, señala la Sentencia que el criterio adoptado por la Sala de lo Contencioso-Administrativo es que “la exigencia de notificación a los interesados sólo opera cuando se trata de datos que versen sobre el cumplimiento o incumplimiento de obligaciones dinerarias y que hayan sido facilitados por el acreedor o quien actúe por su cuenta o interés; y que, por tanto la notificación no resulta exigible cuando se trate de datos provenientes de una fuente accesible al público”. El Órgano sentenciador añade aún en su fallo que tal posición también está avalada por el RD 1720/2007, de 21 diciembre, que aprueba el Reglamento de desarrollo de la LOPD, ya que el Capítulo I del Título IV de ésta Ley contempla tanto el tratamiento de datos del apartado 1 del artículo 29 de la LO 15/1999 (en su sección 1ª, artículo 37 ) y se refiere en su sección 2ª (artículos 38 a 44), del apartado 2 del artículo 29 LOPD y dentro de estos últimos (y no de los del artículo 29.1) se contiene la regulación de la notificación de la inclusión en el plazo de treinta días, en el artículo 40.

A pesar de nuestro respeto al Tribunal que emitió esta Sentencia, no compartimos de ningún modo su posición. En efecto la LOTARD y incluso la LOPD tal y como redactadas podrían dejar un margen muy amplio a interpretaciones sobre las especificidades de los tratamientos de los datos que son objetos de éste estudio de investigación. Sin embargo, nos parece difícil aceptar que el Reglamento tenga ratificado una posición que siquiera estaba clara en la LOPD. Ello porque si de alguna manera pudiera ser vista de este modo, el RPD, ya que no ha aclarado nada respecto al tema, habría ratificado la misma duda. Además, esta norma establece en el artículo 37 que el tratamiento de datos de carácter personal sobre solvencia patrimonial y crédito, previsto en el apartado 1 del artículo 29 de la Ley Orgánica 15/1999 se someterá a lo establecido, con carácter general, en dicha ley orgánica y en el propio reglamento. Así, si estos datos se someten al Régimen General y el deber de notificación que

conlleva un derecho de ser informado están perfectamente determinados tanto en la LOPD como en algunos puntos aclarados por el RPD, opinamos que la única conclusión que podemos llegar es la de que deberá ser respetado, a falta de una clara excepción legal, aquello que determina el artículo 5 de la LOPD, que es la regla general.

En lo tocante a este deber de información en la recogida de datos, opinamos que el afectado deberá ser informado sobre cada deuda registrada de procedencias distintas. Ni el Reglamento, ni la LOPD establecen para los datos recabados en fuentes accesibles al público registrados en los ficheros de solvencia patrimonial ninguna especificidad relativa al deber general de información. De modo que el artículo 5 apartado 4 solamente exceptúa la no observancia de éste precepto cuando el afectado ya hubiera sido informado con anterioridad sobre el contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras *a)*, *d)* y *e)* del apartado 1 del mismo artículo.

Lo que parece desprenderse de la interpretación legislativa es que la procedencia de la deuda es el aspecto diferenciador y relevante a ser llevado en consideración a la hora de realizar la información al afectado. Así, a nuestro juicio, aunque ocurra el caso de que sea la segunda deuda registrada que hubiera sido recabada de fuentes accesibles al público, y supuestamente el interesado ya haya sido informado de todo lo que se ordena en la ley, ésta nueva inclusión es una información distinta de aquellas primeras que supuestamente ya están en el fichero. De este modo, en todos los caso que el origen de la deuda —y no de la fuente— sea diverso de todos los registro que están en el fichero sobre aquella persona, consideramos que el interesado debe ser informado de tal inclusión. Por tanto, si es necesario que se le informe la procedencia de los datos registrados, deberá serlo también de todos los demás requisitos impuestos por el apartado 4 del artículo 5 de la LOPD. La excepción de éste precepto es la de que el afectado ya hubiera recibido todas las informaciones allí especificadas (contenido del tratamiento, la

procedencia de los datos, etc.) y no una de estas separadamente, razón por la cual si se sobreviene un nuevo dato, nuestro sentir el interesado deberá ser informado nuevamente de todo lo que impone dicha norma.

El reglamento ha hecho un esfuerzo para solucionar un problema muy común que es la prueba que acredite la notificación al afectado. De este modo, el apartado 1 del artículo 18 determina que la referida notificación deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado. En efecto, la ley no exige ningún mecanismo específico para que el responsable del fichero o del tratamiento proceda la notificación. Sin embargo, exige que éste conserve el soporte en el que conste el cumplimiento del deber de informar, pudiendo utilizar para ello medios informáticos o telemáticos. De esta suerte, nos parece que con ello la ley ha dejado muy claro también la cuestión de la carga probatoria que en éste caso siempre será del responsable del fichero.

El apartado 2 del artículo en comentario añade aún que en particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales. Según Prats Albentosa<sup>548</sup>, la mención particularizada de la última parte del referido apartado podría llevar a la conclusión de que esta disposición “tasa la prueba de cumplimiento a la prueba documental”. Sin embargo, señala el mismo autor que en su opinión “la disposición ha de entenderse en el sentido de que el Reglamento expresa la preferencia por la prueba

---

<sup>548</sup> PRATS ALBENTOSA, Lorenzo. “Principios de Protección de Datos: Calidad de los Datos, Consentimiento para el Tratamiento de los Datos y Deber de Información”. En: PALOMAR OLMEDA, Alberto y GONZALEZ-ESPEJO, Pablo (Dir.). *Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/199, de 13 de diciembre, de Protección de Datos de Carácter Persona (Aprobado por RD 1720, de 21 de diciembre)*. Cizur Menor: Thomson Civitas, 2008, p. 212.



documental del cumplimiento de este deber dada su posición de almacenamiento, y la mayor facilidad de su descargo en el futuro”.

Por fin, hay que añadir que el artículo 44, apartado 3, letra I) de la LOPD tipifica como infracción muy grave el incumplimiento del deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado. De suerte que pensamos que éste dispositivo refuerza aún más la importancia que ha conferido la ley a que se informe al afectado sobre la recogida de los datos. Igualmente hay que añadir que éste precepto no especifica que la notificación a que puede ser sancionada es aquella del apartado 2 del artículo 29. Ello también nos lleva a pensar que la *ratio* de la ley es evidente no sentido de que al informar sobre la inclusión de unos datos, confiere al afectado un mecanismo a través del cual pueda tornar efectivos otros derechos de éste derivado.

#### 1.1.2. Datos sobre el cumplimiento e incumplimiento de obligaciones dinerarias.

El Derecho a la protección de datos personales envuelve una serie de principios que sirven para tornar efectivo la tutela de los afectados en lo que corresponde a éste derecho, sobre todo definiendo algunos mecanismos para dotar tales principios de operatividad. Entre ellos, la información al afectado de la inclusión de sus datos en un fichero.

La LOPD en el artículo 29, apartado 2, ya había determinado la obligación de la referida notificación, específicamente en los casos de tratamiento de los datos sobre el cumplimiento y el incumplimiento de obligaciones dinerarias, estableciendo que *en estos casos se notificará a los*

*interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley. Como hemos comentado, el hecho de que para el tratamiento de datos de ésta naturaleza no se exija el consentimiento, aumenta la necesidad de establecer algunos requisitos que fortalezcan el ejercicio de los derecho del afectado, incluso como ya hemos dicho, como modo de compensar y equilibrar la balanza de derecho y deberes de aquellos que intervienen en estos ficheros y el interesado. Ésta parece ser la matización de Plana<sup>549</sup> sobre el tema, cuando afirma que “más allá de una derivación del deber de informar, ex artículo 5 de la LOPD, la doctrina ha visto en el requisito de la notificación una contrapartida a la ausencia de consentimiento y, tal planteamiento parece razonable, ya que los efectos para el afectado son similares (tratamiento lícito y posibilidad de ejercicio de sus derecho)”. No obstante, es cierto que la obligación de notificación no nace de la necesidad de nivelar derechos y deberes dentro del sistema de protección de datos. Es un principio autónomo y fundamentalmente se inserta en el articulado legal para tornar eficaz el derecho a consentir del afectado (éste sí, nudo gordiano de la protección de datos), en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales, como consignado por el Tribunal Constitucional.*

Sobre este aspecto en la opinión de Pascual Huerta<sup>550</sup>, “a diferencia quizá de lo que ocurría bajo la vigencia de la LOTARD, no puede entenderse que la notificación de inclusión del artículo 29.2 de la LOPD sea una especie de «compensación» al tratamiento de los datos sin consentimiento del afectado. En la LOPD, que sigue la tendencia de la Directiva 95/46/CE, el deber de información es un principio autónomo que debe respetar con independencia de cuál sea la legitimación del

---

<sup>549</sup> PLANA, Maria del Carmen. *Ficheros... op. cit.*, p. 394.

<sup>550</sup> PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 369.

tratamiento". Ahora bien, de otra parte, igualmente es verdad que el derecho a ser notificado de la inclusión de los datos personales sobre cumplimiento e incumplimiento de obligaciones dinerarias ha cobrado creciente importancia en la normativa actual. Y entendemos que no se puede olvidar que el tratamiento de estos datos se hace sin el consentimiento del afectado. Ante tal excepción, es lógico que el poder de control conferido por el Derecho a la protección de datos no puede tornarse efectivo a través de la obligatoriedad de tal consentimiento y por lo tanto es natural que dentro de la sistemática legislativa la notificación al afectado de la inclusión de sus datos sea tratado de manera especial, con matices diferenciados de aquellos ubicados en las reglas generales.

De este modo, el Reglamento de desarrollo de la LOPD ha ampliado de modo significativo la disciplina de la notificación especial de inclusión de los datos sobre cumplimiento e incumplimiento de obligaciones dinerarias, aclarando cuestiones como por ejemplo a quién corresponde tal obligación y especialmente sobre la acreditación de la notificación.

En lo que concierne al plazo de notificación, tanto la LOPD como el Reglamento 1720/2007 (apartado 1 del artículo 40), establecen que se debe proceder en treinta días desde dicho registro. Dado esto por sentado, hay que añadir asimismo que el artículo 6 del Reglamento fija que en los supuestos en que el reglamento señale un plazo por sea por meses, se computarán de fecha a fecha. Sobre éste punto merece subrayar las dos consideraciones de Fatás<sup>551</sup>: primero, que si no hay día equivalente en el mes de vencimiento no hubiera día equivalente a aquel en que comienza el cómputo, se entenderá que el plazo expira el último día del mes (artículo 48.2 de la Ley 30/1992); y segundo, en los casos en que el último

---

<sup>551</sup> FATÁS. José Miguel. "Título Primero. Disposiciones Generales". En: PALOMAR OLMEDA, Alberto y GONZALEZ-ESPEJO, Pablo (Dir.). *Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/199, de 13 de diciembre, de Protección de Datos de Carácter Persona (Aprobado por RD 1720, de 21 de diciembre)*. Cizur Menor: Thomson Civitas, 2008, p.p. 145-146.

día del plazo sea inhábil, será prorrogado al día siguiente (artículo 48.3 de la Ley 30/1992).

El mismo apartado determina que la obligación de tal notificación es el responsable del fichero común, aclarando de éste modo la omisión del artículo 29.2 de la LOPD que no hacía mención a quién correspondía tal deber. En lo que concierne al contenido, la notificación deberá hacer una referencia de los datos que hubiesen sido incluidos y también de la posibilidad del afectado de ejercitar sus derechos de acceso, rectificación, cancelación y oposición. Además, determina la norma que se deberá efectuar una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.

El artículo 40 del Reglamento no impone una forma concreta de cómo se debe proceder la notificación, pero exige que sea a través de un medio fiable, auditable e independiente de la entidad notificante, que se la permita acreditar su efectiva realización. En este punto, la norma empieza a volcarse a la acreditación de la notificación. Ésta era una cuestión que ya preocupaba tanto la AEPD como la Audiencia Nacional y fue razón de varias resoluciones y fallos divergentes como señala la doctrina<sup>552</sup>.

En diversas ocasiones la cuestión de la responsabilidad de notificar, su forma y su acreditación fueron analizadas por la Audiencia Nacional<sup>553</sup>, que ha señalado que no existe ningún precepto que exija que la comunicación dirigida a los interesados sobre la inclusión de sus datos personales en el fichero deba cursarse por correo certificado con acuse de recibo o por cualquier otro medio que deje constancia documental de la recepción. No obstante, el aludido Órgano sentenciador manifiesta que cuando el destinatario niega la recepción recae sobre el responsable del

---

<sup>552</sup> Vide PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 398.

<sup>553</sup> Audiencia Nacional. Sentencia de 24 enero 2003 (JUR 2005\190526)

fichero la carga de acreditar la comunicación. La justificativa residiría en que “si para considerar cumplida la obligación bastase con la afirmación de tal cumplimiento por parte del obligado, resultaría en la práctica ilusoria y privada de toda efectividad aquella obligación legal de informar a los interesados”. Por otra parte, la doctrina también ha elogiado el nuevo dispositivo fundamentalmente en lo que concierne la acreditación, dado que “se introduce en ésta materia una buena dosis de seguridad jurídica, ya que no se deja al arbitrio del intérprete la consideración de los diversos indicios que permitirían acreditar el cumplimiento del deber<sup>554</sup>”.

Cuando exige el Reglamento que la notificación se haga a través de un medio independiente de la entidad notificante, creemos que la norma refuerza aún más las exigencias de la notificación siempre confiriendo importancia a la acreditación. Según se desprende de la ley, nos parece que todas las exigencias deben ser observadas, es decir, medio fiable, auditable e independencia de la entidad que va a realizar materialmente la notificación. Así, en este sentido, la Audiencia Provincial de Granada<sup>555</sup> ha emitido fallo donde consideraba que el sistema de notificaciones por correo ordinario “no es respetuoso con el derecho del presunto moroso que está en juego, que no ha de olvidarse tiene el carácter de derecho fundamental, pues aunque, efectivamente, esta efectuado por personal independiente, no garantiza ni la recepción por el interesado, ni menos aun la devolución por el servicio de correos de las notificación a los efectos de desactivar la originaria inclusión en el fichero, por lo que no puede darse por válida tal notificación”.

Tal orientación jurisprudencial se conecta con el apartado 4 del artículo 40 del Reglamento, que exige que en todo caso, será necesario que el responsable del fichero pueda conocer si la notificación ha sido objeto de

---

<sup>554</sup> PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 398.

<sup>555</sup> Audiencia Provincial de Granada. Sentencia núm. 421/2009 de 25 septiembre (JUR 2010\5101).

devolución por cualquier causa, en cuya hipótesis no podrá proceder al tratamiento de los datos referidos a ese interesado, exceptuándose aquellos casos en que el destinatario haya rehusado recibir el envío. Para Pascual Huerta<sup>556</sup>, se ha establecido una ficción legal según la cual las notificaciones no devueltas se considera que han sido entregadas. De igual modo, la ley exige independencia entre la entidad notificante y aquella que irá promoverla, no exime la responsabilidad del responsable del fichero en estar pendiente de la notificación, es decir, la ley no hizo un traspaso de responsabilidad.

Sobre la acreditación de la notificación, la Audiencia Nacional<sup>557</sup>, aduce que la prueba exigida en estos casos, no alcanza hasta la recepción por parte del deudor, pues lo que ha de probarse es que la notificación ha sido efectivamente enviada y que la misma ha sido notificada, o al menos intentada la notificación.

En el caso de que se haya devuelto la notificación, el responsable deberá comprobar con la entidad acreedora la dirección utilizada para efectuar esta notificación se corresponde con la contractualmente pactada con el cliente a efectos de comunicaciones. Hasta que la referida entidad no confirme la exactitud de esta información, el responsable del fichero no procederá al tratamiento de los datos.

## 1.2. Información en el recabo de los datos.

---

<sup>556</sup> PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 399.

<sup>557</sup> Audiencia Nacional. Sentencia de 16 enero 2008 (JUR 2008\44422)

Resulta oportuno añadir que a parte de la notificación de inclusión, el RPD en el artículo 42 apartado 2 establece que los terceros deberán informar por escrito de su derecho a consultar el fichero común a las personas en los supuestos en que estas pretenda celebrar un contrato que implique el pago aplazado del precio o contratar la prestación de un servicio de facturación periódica. Es una información formal y previa que debe ser comunicada al afectado en una situación en que la relación contractual no esté perfeccionada, con a finalidad de evaluar el riesgo crediticio.

Sobre la forma, Pascual Huerta<sup>558</sup> señala la dificultad de interpretar la expresión “por escrito” que no sea el documento tradicional firmado. El mencionado autor manifiesta que “no se alcanza a comprender el significado que pueda tener el que la información deba ser «por escrito», lo que parece ser un requisito *ad solemnitatem*.”

La excepción a esta regla se da en el caso de que la contratación sea efectuada por teléfono. Ahora bien, la carga de la prueba de acreditación del cumplimiento del deber de informar cabrá al tercero.

## 2. La Legislación Italiana

Por regla general, el responsable del fichero solo podrá recabar los datos directamente de los participantes del sistema. Estos, en su turno, deberán tomar las medidas oportunas para la verificación y la garantía de que los datos comunicados al responsable pueden ser lícitamente utilizados en tal sistema y además que son exactos y correctos. Para

---

<sup>558</sup> PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 415.

Imperiali<sup>559</sup>, la delicadeza de las actividades desempeñadas por las centrales de riesgos impone la aplicación de un procedimiento riguroso de calidad, tanto por parte de la entidad financiera, que son las fuentes de información del sistema, como de la citada central.

En efecto, como bien resalta Mormile<sup>560</sup>, los mayores riesgos relacionados con la difusión en este sector de noticia de naturaleza económica, afectan a los posibles daños que pueden derivarse a la reputación y a la imagen del individuo y de la empresa. Dado, entonces, que estos riesgos están relacionados con la circulación de informaciones falsas o incorrectas, la predisposición de medidas para garantizar la entrada en el sistema de datos veraces y actualizados es el mejor instrumento preventivo de tutela de las personas.

En lo que respecta al responsable, cuando reciba las informaciones del participante este deberá verificar su congruencia a través de controles de carácter formal y lógico. De ahí pueden ocurrir dos supuestos: el primero en el caso de que los datos tenga el visto bueno del responsable, serán registrado en el sistema de información crediticia, estando disponibles a todos los participantes. En el supuesto de que los datos no pase por el control del responsable, por ser incompletos o incongruentes, los retransmite al participante que se los haya suministrado para que proceda con las correcciones que sean necesarias.

De suerte que Petrulli<sup>561</sup> identifica dos obligaciones del participante, extraídas del apartado 4 del artículo 4 del *Codice Deontologico*: comprobar atentamente los datos que maneja; y responder tempestivamente a los requerimientos de verificación por parte del responsable, así como aquellos derivados del ejercicio de un derecho por parte del interesado.

---

<sup>559</sup> IMPERIALI, Riccardo. *Codice... op.cit.*, p. 994.

<sup>560</sup> MORMILE, Lalage. *Il Sistema... op. cit.*, p. 1861.

<sup>561</sup> PETRULLI, Mario. *Il nuovo... op. cit.*, p. 28



El procedimiento de supresión, modificación o complementación de los datos siempre que sea técnicamente posible, por regla general deberá ser realizado directamente por el participante que haya suministrado los datos. El responsable solamente podrá hacerlo en los casos en que sea: a) a petición del participante o si no de acuerdo con éste; b) como consecuencia del ejercicio de un derecho por el interesado o c) en cumplimiento a una orden emitida por una autoridad judicial o por la Agencia de Protección de datos. Éstas son las únicas excepciones que confiere la ley al responsable la posibilidad de modificar por si mismo los datos registrado.

El apartado 6 del artículo 4 del código deontológico regula de modo específico algunas particularidades que se debe tener en cuenta a la hora de comunicar las informaciones registradas a los otros participantes del sistema crediticio. En este punto, la ley diferencia los supuesto en que los datos registrados en los ficheros que tratan informaciones negativas de aquellos que tratan tanto los datos negativos como los positivos, estableciendo los plazos para que puedan ser utilizados y puesto a disposición de los demás participantes del sistema. Según Imperiali<sup>562</sup>, el objetivo del apartado 6 del artículo 4 del *Codice deontologico* es impedir los registros precipitados que no lleven en consideración hechos sobrevinientes. Ésta es la misma opinión de Mormile<sup>563</sup>, para quien el simple retardo en el cumplimiento no es un elemento capaz de deducir, de modo inequívoco, la incapacidad de cumplir con la obligación de pago o el estado de insolvencia de una empresa, representando más bien un simple indicio de una eventual dificultad de naturaleza económica. Para la autora citada la introducción en el sistema de datos referentes a retardos no relevantes podría conllevar la previsión y difusión de un perfil distorsionado – y por lo tanto no verdadero – del sujeto que recurre al crédito.

---

<sup>562</sup> IMPERIALI, Riccardo. *Codice... op.cit.*, p. 994.

<sup>563</sup> MORMILE, Lalage. *Il Sistema... op. cit.*, p. 1863.

Así, para el fichero que tratan datos negativos, solamente se podrán revelar los datos adversos cuando hayan pasado al menos ciento veinte días a partir de la fecha límite de pago correspondiente o en caso o, en caso de falta de pago en plazos, al menos cuatro cuotas mensuales no regularizadas.

Para aquellos bancos de datos en los cuales confluyen datos positivos y negativos, la ley establece dos supuestos: si la persona a quién se refiere estos datos es un consumidor deberá ser observado lo siguiente: a) solo podrán ser revelados y utilizados los datos tras sesenta días de la actualización mensual prevista en el párrafo 8, del artículo 4. Este precepto establece que los datos registrados en un sistema de información de crédito se actualiza periódicamente sobre una base mensual, por el participante que haya suministrado los datos; b) en caso de falta de pago de por lo menos dos cuotas mensuales consecutivas; c) bien cuando la demora se refiere a uno de los dos últimos plazos de pago. En tal hipótesis, los datos estarán disponibles después de la actualización mensual sobre las cuotas no pagadas por segunda vez consecutiva.

Para los demás casos apenas podrán poner los datos a disposición de los participantes del sistema después al menos treinta días de la actualización mensual contemplado en el párrafo 8 del art. 4, o en caso de falta de pago de una cuota. Nos parece muy interesante que la ley establezca la obligatoriedad de una actualización mensual de los datos del participante al sistema de información crediticia. Sin embargo, ello trae algunos problemas que desde nuestro punto de vista reflejan en la calidad de los datos. Los datos, por ejemplo aquellos referentes a solicitudes de créditos no aceptadas, que hayan sufrido cambios en los primeros días después de la última actualización, solamente serán modificados en el sistema en la siguiente actualización mensual. De suerte que no consideramos un plazo razonable para que permanezcan en el sistema los datos de una solicitud que ya ha sido rechazada o desistida. No estamos ante ficheros manuales que conllevaban la dificultad natural de la forma

de operar, pero de sistemas automatizados que pueden ser fácilmente manejables, y por lo tanto desde nuestra opinión no nos ha parecido una buena elección legislativa.

### 2.1. La información en la recogida de los datos.

El artículo 5 del Código de deontología establece las normas a ser seguida en lo que concierne a la información prestada al afectado en el momento de la recogida de los datos personales relativos a las solicitudes o relaciones de crédito. Para Imperiali<sup>564</sup>, el objetivo de lograr la transparencia de la relación triangular (deudor-financiadora-central) ha sido confiado como era previsible, a éste instrumento de información.

El participante tiene la obligación de informar al interesado además de todo aquello que se le exige en el artículo 13 del *Codice in materia di protezione dei dati personali*<sup>565</sup>, las disposiciones que contiene específicamente en el código deontológico. De suerte que el apartado 2 del artículo comentado añade que deberá constar: a) la identificación de los

---

<sup>564</sup> IMPERIALI, Riccardo. *Codice... op.cit.*, p. 994.

<sup>565</sup> El artículo 13 establece que el interesado o la persona de quién se recoge los datos de carácter personal serán informados oralmente o por escrito sobre: a) la finalidad y modalidad de tratamiento de los datos; b) el carácter voluntario u obligatorio de proporcionarlos; c) las consecuencias de cualquier negativa a responder; d) las personas o categorías de personas a las que los datos puedan ser comunicados o que puedan tener conocimiento de ellos como responsables o encargados, así como el alcance de la difusión de datos; e) los derechos del afectado; f) la identificación del *titolare* de los datos y, si es nombrado, del representante de éste en el Estado y del responsable.

sistemas de información de crédito que proporcionan datos personales y sus gestores<sup>566</sup>; b) categorías de participantes que acceden a él, es decir, si es una entidad financiera, un banco, etc.); c) tiempo de conservación de datos en los sistemas de información de crédito que se comuniquen; d) régimen aplicable a la organización, la comparación y el tratamiento de los datos y el uso, en su caso, de técnicas o sistema automatizado de *credit scoring*<sup>567</sup>; e) los procedimientos para el ejercicio por los interesados de los derechos garantizados por el artículo. 7 del Código en materia de protección de datos.

Diferentemente del artículo 13 del Código de Protección de Datos que da la opción a que la información en el momento de la recogida de los datos pueda ser dada oralmente o por escrito, el Código deontológico exige que tal información sea realizada únicamente por escrito. Además, proporciona en anexo a su texto, un modelo del documento informativo que representa, según Petrulli<sup>568</sup>, una base mínima, inderogable para la información y debe ser suministrada por el participante. Tal iniciativa del *Garante* de elaborar un modelo de información, en nuestra opinión nos parece muy elogiable. Primero, porque la ley desde nuestro punto de vista

---

<sup>566</sup> Según definición del código de deontología, *gestore* es el sujeto privado, titular del tratamiento de datos personales registrados en un sistema de información de crédito y que administra este sistema y establece su modo de funcionamiento y de utilización;

<sup>567</sup> La definición de técnica o sistema automatizado de *crediti scoring* se encuentra en la letra *h*) del artículo 1 del código de deontología, siendo el modo de organización, agregación, comparación o tratamiento de datos personales relativos a las solicitudes o relaciones de crédito, consistente en el uso de sistemas automáticos basados en la aplicación de métodos o modelos estadísticos para evaluar el riesgo de crédito, y cuyos resultados se expresan en forma de juicios sintéticos, indicadores numéricos o puntuación, asociados al interesado, con el objetivo de proporcionar una representación en términos de predicción o probabilidad, su perfil de riesgo, la fiabilidad, o la puntualidad de pago.

<sup>568</sup> PETRULLI, Mario. *Il nuovo... op. cit*, p. 31.

hace muchísimas exigencias materiales de contenido lo que de cierta manera puede dificultar su interpretación por los participantes. Por otro lado se debe suponer que un documento que pasa por la aprobación de una Autoridad de protección de datos, tendrá sido llevados en cuenta todos los aspectos legales, observados de forma conjunta, y particularmente a los derechos del afectado.

En la hipótesis de que el participante incluya tal modelo en un formulario, deberá, en este caso, estar debidamente destacado, puesto de modo autónomo y unificado, en partes o cuadros distintos de aquellas referentes a cualesquier otras eventuales finalidades de tratamiento realizadas por el participante.

Ahora bien, el apartado 5 del artículo 5 establece que el responsable del fichero para complementar la información dada por los participantes individualmente a cada individuo, el operador proporcionará una más detallada a través de otros métodos de difusión de información al público, incluso a través de la telemática. Imperiali<sup>569</sup>, comentando éste apartado, señala que si vamos a hacer las compras de Navidad y nos adherimos a una iniciativa “comprar ahora y pagar en el futuro”, nos encontraremos en esta situación y debemos recibir una información sobre cómo funciona el flujo de nuestros datos personales entre proveedor, central y el directo interesado.

Cuando la solicitud de crédito no sea aceptada, el participante informará al interesado si para evaluar tal solicitud consultó los datos personales relativos a la información crediticia de tipo negativo en un o más sistemas de crédito, debiendo de éste modo, proporcionar los datos de éste, con los detalles necesarios para identificar tanto el sistema utilizado como fuente de la información y el respectivo titular del tratamiento.

---

<sup>569</sup> IMPERIALI, Riccardo. *Codice... op.cit.*, p. 994.

Aparte de esta notificación previa a la hora de recabar los datos personales, el Código de buena conducta determina en el párrafo 7 del artículo 4 que se deberá proceder a la comunicación previa a la inclusión del registro en el sistema de información crediticia. Tal mandato obliga a que el participante, al producirse los retrasos en los pagos, advierta al interesado sobre el inminente registro de los datos negativos. La ley permite que el participante pueda cumplir con tal obligación de informar también en el momento del envío de solicitud de pago o de otras comunicaciones. Como bien apunta Ninno<sup>570</sup>, no debe ser un acto formal distinto y específico. Los datos relativos al primer retraso en el pago, señalados en el apartado 7 del art. 4, solo serán puestos a disposición de los participantes después de al menos quince días a partir del envío de la aludida información al interesado. Su contenido debe observar la regla general del artículo 13 del Código en Materia de Protección de Datos.

Mormile<sup>571</sup> señala que la información previa se trata en general de una noticia relativa al sistema de información de crédito en la cual serán introducidos los datos de la persona en cuestión, como la identificación del operador, las categorías de participantes que acceden al sistema – y que, a su vez, pueden conocer los datos – el tiempo de conservación de la información y la forma de organización del sistema. La información, para la referida autora, asegura la máxima transparencia del tratamiento de los datos en el ámbito del sector crediticio, garantizando al interesado el concreto ejercicio de sus derechos.

La norma italiana el caso de la información previa a la inclusión difiere de la española en lo que concierne al momento en que se debe procederla. El legislador italiano opta por un sistema informativo preventivo, obligando a que el interesado sea notificado antes de cualquier registro.

---

<sup>570</sup> NINNO, Alessandro del. *La tutela dei dati personali: guida pratica al Codice della privacy (D. lgs. 30.6.2003, n. 196)*, Padova: CEDAM, 2006, p. 513.

<sup>571</sup> MORMILE, Lalage. *Il Sistema... op. cit.*, pp. 1865 y 1866.

No obstante, en España la norma divide en dos los momentos de la información: aquella previa que deberá ser efectuada tanto en el momento de la solicitud de crédito o del requerimiento de pago y otra, solamente después de los datos ya registrados. No nos parece la elección más adecuada el momento en que ésta última información debe ser realizada. Aunque, sea cierto, que el afectado ya haya recibido la alerta del propio acreedor. Sin embargo, cuando éste realiza la información previa, los datos aún no están incluidos en los ficheros. De suerte que cuando son comunicados y registrados es el responsable del fichero el que informa al afectado que ya están allí. Pese a ello, creemos que la opción de la legislación española en compartir los deberes de información entre el acreedor y el responsable del fichero es muy elogiada. Pues a partir de esto, el afectado podrá saber cuándo efectivamente los datos ya están a disposición del sistema de protección al crédito.

Por otra parte, la norma italiana tiene un procedimiento más sencillo, que no comparte la obligación del deber de informar por el gestor, sin embargo compensa con las disposiciones como el tiempo de espera hasta que un dato pueda ser incluido en el sistema.

#### **IV. Acceso a la información contenida en el fichero**

##### **1. Legislación Española.**

El artículo 42 del RPD establece tres situaciones en las cuales puede un tercero acceder a los datos contenidos en un fichero común. La regla general es que estos tengan la necesidad de enjuiciar la solvencia

económica del afectado. Tal circunstancia como prevé la ley concurre en los supuestos en que: a) el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida; b) el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio; c) el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

De manera que, según el reglamento hay dos situaciones anteriores al negocio que se pretende realizar, dándose la segunda en los casos en que ya exista la relación contractual pero ésta aún no esté vencida. Según opina Pascual Huerta y Plana<sup>572</sup>, este dispositivo no establece una lista con carácter de *numerus clausus*.

En estos casos expuestos por el Reglamento, resulta interesante detenerse en la matización realizada por Pascual Huerta<sup>573</sup> sobre éste aspecto y el problema del uso de las informaciones de ficheros de solvencia en relación con actividades de marketing. En su opinión, “no hay obstáculo legal alguno para consultar los datos de una persona en un fichero común de solvencia, siempre que, efectivamente se precise enjuiciar la solvencia económica del afectado”. Justifica tal afirmación aduciendo que “puede ser que el producto o servicio que vaya a ser ofrecido sólo sea adecuado o interesante para personas de un determinado nivel de solvencia”. Con el debido respeto, tomamos una opción diametralmente opuesta a esta postura. Ya hemos tenido la

---

<sup>572</sup> PASCUAL HUERTA, Pablo. “Ficheros de Información Sobre Solvencia Patrimonial y Crédito (arts. 37 a 44)”. En: ZABÍA DE LA MATA, Juan. (coord.). *Protección de Datos. Comentarios al Reglamento*. Valladolid: Lex Nova, 2008, p. 412; PLANA, Maria del Carmen. “Ficheros sobre Solvencia Patrimonial y Crédito”. En: PALOMAR OLMEDA, Alberto y GONZALEZ-ESPEJO, Pablo (Dir.). *Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/199, de 13 de diciembre, de Protección de Datos de Carácter Persona (Aprobado por RD 1720, de 21 de diciembre)*. Cizur Menor: Thomson Civitas, 2008, p. 404.

<sup>573</sup> PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 413.



oportunidad de señalar nuestra posición, de que los ficheros de morosos no son supermercados de datos, en los cuales se puede seleccionar clientes a partir de un perfil de su solvencia económica, lo que desvirtúa completamente su finalidad. Por otro lado, conforme la redacción del artículo 42.1 letras *a)*, *b)* y *c)*, pone en relieve el afectado como la persona central que ejerce la acción principal que se recoge de la norma, es decir, que **mantiene** (letra *a)*), **pretende celebrar con** (letra *b)*) o **pretende contratar con** (letra *c)*). El tercero puede consultar los ficheros de solvencia cuando precise enjuiciar la solvencia económica del afectado, pero cuando derive de éste la iniciativa de un supuesto que en el cual concurra dicha circunstancia. Aparte de ello, el apartado 2 del artículo 42 exige a los terceros que informen por escrito a las personas en las que confluyan los supuestos contemplados en las letras *b)* y *c)* del mismo artículo de su derecho a consultar el fichero, solo exceptuando los casos de contratación telefónica de los productos o servicios, que la información podrá realizarse de forma no escrita, pero correspondiendo siempre al tercero la prueba del cumplimiento del deber de informar.

De este modo, consideramos que la ley no permite que un tercero pueda consultar a espaldas del afectado sus datos en un fichero, ya que deberá comunicarle con anterioridad de su derecho a hacerlo. A nuestro sentir, tolerar tal hecho, a parte de generar un ambiente de inseguridad jurídica, es invertir los bienes jurídicos protegidos no solo por las normas específicas de los ficheros aquí en estudio pero de la propia esencia de la ley de protección de datos, que resguarda primeramente la persona y no los datos.

El único aspecto de la ley española y especialmente del artículo mencionado anteriormente, que a nuestro modesto juicio entendemos que no se inserta dentro de los objetivos de los ficheros de solvencia patrimonial y crédito es la aceptación tanto de la inclusión de datos de prestación de servicios de facturación periódica como la posibilidad de que terceros que se dediquen a tales servicios puedan acceder a las

informaciones constantes allí. Hoy por hoy son innumerables las sentencias y los procedimientos sancionadores de la Agencia de Protección de Datos<sup>574</sup> que tienen actuado contra los abusos de las entidades que se dedican a la prestación del servicio de informaciones sobre la solvencia patrimonial y crédito de los individuos. Es en verdad un sector extremadamente problemático no solo desde el punto de vista de la prestación del servicio en sí, pero también del tratamiento de los datos, sobre todo de aquellos que pueden ser registrados en estos ficheros. Aunque desde nuestro modesto entendimiento, como ya hemos consignado nuestra opinión en el Capítulo anterior, el equívoco legislativo es de raíz, o sea, es considerar el contrato con tercero que presta un servicio de facturación periódica como un dato que pueda enjuiciar la solvencia patrimonial de un individuo.

## 2. Legislación Italiana

La legislación establece que los participantes podrán acceder al sistema de información de crédito desde que tales informaciones tengan para el mismo un justificado interés y establecen tres supuesto en los cuales pueden referirse: a) a los consumidores que soliciten y/o sean partes de una relación crediticia con dicho participante, así como los co-obligados, también solidarios; b) a las entidades que actúen en el contexto de su negocio y / o actividades profesionales, para los que se han iniciado investigaciones con el fin de establecer una relación de crédito o en cualquier caso para efectuar un riesgo de crédito, o bien si ya son parte de una relación crediticia con dicho participante, c) a las entidades que tiene

---

<sup>574</sup> *Vide*, por ejemplo, los procedimientos sancionadores: Expediente nº: E/00586/2004; Procedimiento nº PS/00261/2007; y Expediente nº: E/00613/2007.

una relación jurídica con los mencionados en la letra b) anterior, en particular, porque actúan como obligados solidarios o bien pertenecen a grupos empresariales, siempre que los datos personales que el participante desee acceder sean realmente necesarios a fin de evaluar la situación financiera y solvencia de las entidades mencionadas en dicha letra b). Está prohibido el acceso a las entidades de cobro de deudas<sup>575</sup>.

El apartado 2 del artículo 7 determina que el acceso al sistema de protección al crédito solo podrá ser realizado por el participante o por el *gestore*, exclusivamente a través de un número limitado de responsables y encargados del tratamiento que deberán especificarse por escrito, y sólo con respecto a los datos estrictamente necesarios, pertinentes y no excesivos con relación a las finalidades de aquellos ficheros, enunciadas en el artículo 2. Además, con los mismos límites y la misma modalidad, también pueden acceder al sistema de información crediticia los bancos y entidades financieras que pertenezcan al grupo bancario del participante.

Hay que tener en cuenta también lo que fija el apartado 4 del artículo 7 que permite el acceso de terceros cuando sean provenientes de las peticiones de los tribunales y de la policía judicial, por razones de justicia, o por otras instituciones, las autoridades, administración o entes públicos únicamente en los casos previstos por ley, reglamentos o normativa comunitaria, y de conformidad con las normas que regulan la materia.

En lo que concierne concretamente a la modalidad de funcionamiento de cómo el participante accederá al sistema de información de crédito, la ley determina que será a través de los mecanismos y herramientas, incluidos los electrónicos, que hayan sido establecidos por escrito conjuntamente con el gestor en el cumplimiento de la legislación de protección de datos. Es una reglamentación que no encuentra una similar en los preceptos específicos dedicados a los ficheros de solvencia

---

<sup>575</sup> *Garante per le protezioni dei Dati Personali*. Dossier - 30 novembre 2005 “Le Nuove Regole sui Sistemi di Informazioni Creditizie”.

patrimonial de la norma de España, porque ha preferido el legislador de este país dejar que siguiera, en éste punto, el régimen general de las Medidas de Seguridad, ubicadas en el Título VIII del RPD. Allí, tal ley hace una detallada codificación del llamado documento de seguridad (Art. 88 del RPD).

Además, los datos personales relativos a las solicitudes o relaciones de crédito registrados en el fichero deben ser consultados a través de etapas, graduales y sucesivas, a través de uno o varios niveles de consulta de las informaciones sintéticas de los datos referentes al interesado, antes de permitir el acceso a la información detallada.

En los sistemas de protección al crédito están vetadas, incluso técnicamente, modalidad de consulta que permita obtener información en masa o lista de datos referentes a solicitudes o relación de créditos de sujetos distintos de los que han solicitado establecer o formar parte de una relación de crédito con el participante.

## **V. Conservación y actualización de los datos.**

### **1. Legislación Española.**

El articulado legal de la ley de protección de datos fija, así como para la inclusión de los datos, los requisitos para su conservación y tratamiento. De suerte que a parte de la obligatoriedad impuesta de obediencia a otros principios legales sobre la materia, tanto la LOPD como su Reglamento de desarrollo establecen que los datos deben responder con veracidad a la situación de la deuda en cada momento concreto, o por mejor decir, tienen

el deber de “reflejar en el tratamiento todos los cambios que sucedan respecto de los hechos a que se refieren los datos, y la de rectificar los inexactos...”<sup>576</sup>.

Fundamentalmente para los datos recogidos de las fuentes accesibles al público, desde nuestro punto de vista, el respecto por el principio de la calidad de los datos, sobre todo en lo que concierne a su actualización es una condición importantísima para garantizar la licitud del tratamiento y los derechos de los afectados. Es cierto que cuando se recaba datos de una fuente pública las dificultades para el responsable del fichero en seguir la evolución de la información son más grandes que aquellas facilitadas por el acreedor, a quién cumple la obligación de comunicar las actualizaciones necesarias para que el dato revele la real situación de la deuda. No obstante, no se puede olvidar que la naturaleza de la actividad lucrativa que prestan aquellos que se dedican a la información sobre la solvencia patrimonial y crédito de los individuos envuelve derechos fundamentales, constitucionalmente protegidos, razón que nos parece suficiente para que estos asuman los riesgos provenientes tal actividad.

De este modo, el titular del fichero tiene el deber de velar por los datos que son registrados, para que sean veraces y que correspondan con la situación actual, es decir respeten el principio de la calidad de los datos. El RPD en el artículo 43.2 determina como responsabilidad de acreedor o quien actúe por su cuenta o interés de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero. Trataremos de tal precepto más adelante.

Sobre la veracidad y exactitud de los datos provenientes de fuentes accesibles al público, el Tribunal Superior de Justicia de Madrid<sup>577</sup>, señaló

---

<sup>576</sup> APARICIO SALOM, Javier. *Op.Cit.*, p. 98

<sup>577</sup> Tribunal Superior de Justicia de Madrid, Sentencia núm. 565/2003 de 22 mayo (JUR 2004\143830).

que las empresas que se dedican a la explotación comercial de archivos sobre solvencia patrimonial y crédito, han de ser extraordinariamente cuidadosas con la veracidad de los datos que publican por las consecuencias lesivas, cuando no irreparables, que dicha publicación conlleva ya que los datos que manejan pertenecen a uno de los círculos más reservados de las personas. Por lo tanto, advierte que “cuando no puedan contrastar la veracidad del dato, la actualidad del mismo o su mantenimiento a lo largo del tiempo, deberán optar por no utilizarlo antes que arriesgarse a dar publicidad a datos inexactos”. Concluye el fallo que lo que es inadmisibile es acoger un dato publicado por un Boletín y presumir que el mismo se mantiene veraz *sine die*.

Igual no resulta inoportuno traer a colación la Sentencia de 15 febrero 2006, de la Audiencia Nacional<sup>578</sup>, que entiende que “la LOPD establece sin lugar a dudas la necesidad de salvaguardar el derecho fundamental de proteger los datos personales de la persona, que en el principio de calidad de datos se traduce en que, **tanto quien es responsable del fichero en donde esos datos de carácter personal están incluidos, en cuanto que decide sobre su uso, como quien los trata de forma automatizada, han de tomar las diligencias adecuadas para garantizar que esos datos sean ciertos, es decir, se ajustan a la realidad, más cuando se decide por ese responsable su destino a un fichero de los denominados de morosos que, como luego se expondrá, su inclusión sí afecta a la fama de las personas, especialmente en una realidad tan importante actualmente como son las de relaciones económicas**” (subrayamos).

Una gran evolución desde la entrada en vigor de la antigua LOTARD a los días actuales con la LOPD y el Reglamento 1720/2007 no sólo desde una perspectiva legislativa pero también de orientación interpretativa es la superación de la problemática de las practicas de los prestadores de servicio de información de datos de solvencia patrimonial relativas al

---

<sup>578</sup> Audiencia Nacional. Sentencia de 15 febrero 2006 (JUR 2006\119487).

“saldo 0”<sup>579</sup>. No pretendemos de ningún modo profundizar la discusión sobre este tema, no obstante nos ha parecido muy elogiable el cambio tanto de la AEPD como jurisprudencial de prohibir la información del “saldo cero” en los ficheros<sup>580</sup>. En nuestra opinión, tal información no corresponde con la veracidad de la situación de la deuda, porque ésta ha dejado de existir en el momento en que fue satisfecha. De otra parte, creemos que si aún había alguna duda sobre la prohibición legal de éste tipo de registro, el RPD es rotundamente claro en lo que concierne a los datos sobre cumplimiento e incumplimiento de obligaciones dinerarias cuando en el apartado 1 del artículo 41 ordena que *el pago o cumplimiento de la deuda determinará la cancelación inmediata de todo dato relativo a la misma*.

Ahora bien, en el caso de que el pago o el cumplimiento de la deuda no suceda, el tiempo máximo permitido para el tratamiento de estos datos son seis años, contados a partir del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico. El aludido plazo ya venía determinado por la LOPD en su artículo 29, apartado 4. De suerte que también debe ser considerado en los casos en que sean los datos adversos y recogidos de fuentes accesibles al público.

En cuanto a la finalidad e importancia de establecerse un período máximo para el tratamiento de los datos Vizcaíno Calderón<sup>581</sup>, opina que “lo que pretende el artículo 29.4 es que los datos adversos sean olvidados a los seis años de tal manera que el afectado pueda recuperar su privacidad que quedó limitada por la necesidad, en defensa de los

---

<sup>579</sup> Para un análisis más detenido sobre el tema, por todos, GARCÍA IZQUIERDO, Santiago. “El ‘saldo cero’ y los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito”. Revista de derecho bancario y bursátil, nº 87, 2002, pp. 297-304.

<sup>580</sup> Vide comentario de PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, pp. 401 y ss.

<sup>581</sup> VIZCAÍNO CALDERÓN, M. *Op.Cit.*, p 327.

intereses generales de que se hacía mérito más atrás, de registrar esos datos sin su consentimiento". A este hilo, la Audiencia Nacional<sup>582</sup> señala que tanto el acceso como la permanencia en los ficheros de solvencia patrimonial que contienen datos adversos del afectado, "no puede tener un carácter indefinido, proporcionándonos un perfil sobre la vida y evolución de dicha solvencia a través de los años, sino que el legislador ha pretendido que la finalidad a la que sirve el fichero se cumple informando sobre la reciente historia de la solvencia patrimonial del afectado, estableciendo que ese reflejo histórico no puede superar los seis años".

De hecho, dichos registros no pueden ser utilizados indefinidamente, necesitando de un plazo razonable y adecuado para que permanezcan en estos ficheros. Así, en el caso de España, *la memoria del fichero tiene un límite temporal infranqueable: seis años*<sup>583</sup>. Para Plana<sup>584</sup>, tratase de un límite temporal absoluto. En nuestra opinión, el afectado no puede estar susceptible a que un registro de incumplimiento de una obligación dineraria sea una penalización eterna que macule su vida privada ante la sociedad, aparte de todas las demás consecuencias derivadas de un registro de ésta naturaleza en los aspectos referentes a sus relaciones económicas y financieras, mientras subsista la información.

Resulta oportuno señalar que según doctrina la Audiencia Nacional, en la misma sentencia anteriormente citada, en lo tocante al computo del plazo de seis años, éste no se puede ser confundido con el computo propio de los plazos prescriptivos, susceptibles de ser interrumpidos cuando se produce una alteración, "se trata, por el contrario, que el fichero de solvencia patrimonial no pueda recordar datos o hechos que acaecieron hace más de seis años".

---

<sup>582</sup> Audiencia Nacional. Sentencia de 21 septiembre 2001 (JUR 2002\9279).

<sup>583</sup> Audiencia Nacional. Sentencia de 3 octubre 2007 (JUR 2007\316038)

<sup>584</sup> PLANA, Maria del Carmen. *Ficheros... op. cit.*, p. 401.



## 2. Legislación Italiana.

El Código de buena conducta ha preferido tratar en un único artículo las reglas de conservación y actualización de los datos. Tanto una como otra acción es de vital importancia para el buen funcionamiento del sistema, ya que cuando bien desarrolladas, aseguran la fiabilidad y la calidad de las informaciones protegiendo de ésta manera los derechos del afectado. En efecto, según observa Votano<sup>585</sup>, la eficacia del sistema en la persecución de la tutela del sujeto solicitante del crédito en el confronto de la “avidez de información” del concedente pasa a través de la atención a la calidad de la información y de que su gestión no esté necesariamente en conflicto con una permanencia más prolongada de la información en el banco de datos.

Es interesante observar que mientras en España el legislador ha determinado un plazo único de conservación de los datos, Italia sigue otra regla en la cual contempla algunas situaciones fácticas y a partir de ellas fija el período de conservación correspondiente que deberá ser observado.

De modo que el código de deontológica, en su artículo 6, establece tres situaciones distintas y determina para cada una de ellas un tiempo de conservación. La norma divide tales hipótesis en: a) los datos registrados se refieran únicamente a solicitudes de crédito; b) los datos negativos; y, finalmente, c) los datos positivos.

---

<sup>585</sup> VOTANO, Giulio, “Sistema Bancario, Finanziario ed Assicurativo”. En BIANCA, Cesare Massimo y BUSNELLI, Francesco (Dir.). *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 (“Codice della privacy”)*. Milano: CEDAN, 2007, p. 1507.

El apartado 1 de la norma comentada trata del supuesto de los datos relativos a la solicitud de crédito y empieza su texto manifestando de modo general que estos pueden ser almacenados en un sistema de información de crédito durante el tiempo necesario para su investigación. Sin embargo, en cualquier caso, no más que ciento ochenta días de la fecha de presentación de tal solicitud. Ahora bien, asimismo el precepto regula otra situación en la cual fija un plazo distinto, que es aquella en la cuales la solicitud de crédito no haya sido aceptada o el interesado cambia de idea y renuncia el préstamo. En estos supuestos, el participante deberá notificar al operador en el momento de la actualización mensual de los datos contemplada en el artículo 4, apartado 8. Así, en tales hipótesis, los datos que indican la renuncia o el rechazo de tal solicitud no podrá ser conservado en el sistema más que treinta días de la fecha de su comunicación al sistema.

En el caso de información negativa, los supuestos se dividen en aquellos en los cuales el deudor ya haya sanado la morosidad y aquél en que permanece el impago, fijando de éste modo dos períodos diferentes.

En la primera hipótesis, el código fija dos tiempos de conservación dependiendo de la importancia del retraso en el pago. Si tal retraso es inferior a dos meses o a dos plazos, el tiempo de conservación será de doce meses, contados a partir de la fecha de registro su regularización. Cuando el retardo en el pago sea superior a dos meses o dos plazos, podrán conservarse hasta un periodo de veinte cuatro meses a contar igualmente de la fecha en que fue registrado el cumplimiento.

Al término de los citados plazos, los datos deberán retirarse del sistema de información de crédito si durante los mismos intervalos de tiempo no se registraran informaciones relativas a nuevos retrasos o incumplimientos.

El participante y el gestor actualizarán sin retraso los datos relativos a la regularización del incumplimiento de los que tienen conocimiento, que se ha realizado después de la cesión del crédito por parte del participante a un sujeto que no participa al sistema, o en el caso de requerimiento del interesado provisto con la declaración del sujeto que ha cedido el crédito u otra documentación idónea.

Para los incumplimientos o falta de pago que no fueron sanados, el Código establece el tiempo de conservación en treinta y seis meses. El cómputo de tal período empieza a contarse a partir la expiración del acuerdo contractual a que se refieren. Ahora bien, en el caso de que ocurran otros eventos que son significativos para el pago, como por ejemplo un acuerdo de pago, el plazo se contará a partir de la fecha en que la información había sido actualizada o, en cualquier caso, de la fecha que puso término a la citada relación.

Los datos positivos referentes a una relación en la cual se puso término por extinción de todas las obligaciones monetarias pueden mantenerse en un sistema de información crediticia por un período que no excederá veinticuatro meses a partir de la fecha del término o de la expiración del acuerdo contractuales pertinentes, o bien a partir de la primera actualización realizada en el mes siguiente a éstas fechas mencionadas.

El aludido tiempo puede ser mayor si con tales informaciones positivas estén presentes otros informes de crédito referentes al mismo interesado, con datos negativos sobre retrasos o incumplimientos no sanados. De suerte que el plazo será de los 36 meses fijados por el apartado 5 del artículo 6.

En el caso de que el consumidor interesado comunique al participante de la revocación de su consentimiento para el tratamiento de datos positivos, éste deberá en la actualización mensual informar al *gestore*. En este caso y en aquellos en que la revocación del consentimiento haya sido

dada directamente al responsable del tratamiento de los datos, éste deberá eliminar tales informaciones positivas antes de 90 días contados a partir del instante en que fue comunicada la citada revocación, o que el participante la haya actualizado.

El apartado 8 del artículo 6 aún añade que antes de retirar los datos de un sistema de información de crédito de conformidad con las especificaciones establecidas, el *gestore* puede transferirlos a otro soporte, a fin de conservar exclusivamente durante el tiempo que sea necesario con el fin de defenderse a una reclamación legal, o bien con el fin de procesarlos en forma anónima para fines estadísticos.

Para Imperiali<sup>586</sup>, el sistema ha perseguido el justo equilibrio a través de una articulada gradación del tiempo en relación a la naturaleza del hecho objeto de registro y de la gravedad crediticia del mismo. O sea, para éste autor, la mora é evaluada diversamente según los plazos implicados, o su duración y menos gravemente que el incumplimiento *tout court*.

Algunas voces doctrinales defienden que el tiempo de permanencia del dato en el sistema de información crediticia es más garantista al derecho de la *riservatezza* ya que el límite temporal para que los datos estén en el fichero comparativamente con otros países es muy pequeño<sup>587</sup>. De suerte que creemos que aunque los plazos de conservación de los datos en la legislación italiana sean menores que el caso español, tal y como está redactada la norma, ésta provoca un injusto desequilibrio entre las informaciones registradas y la correspondiente situación actual del afectado deudor.

En efecto, los periodos son menores si comparados con otras legislación, como la española. Sin embargo, nos parece que su

---

<sup>586</sup> IMPERIALI, Riccardo. *Codice... op.cit.*, p. 995.

<sup>587</sup> *Vide* la comparación y comentarios de VOTANO, G., *Sistema Bancario... op.cit.*, p. 1508 y PETRULLI, Mario. *Il nuovo... op. cit.*, p. 36.

actualización es tardía. Los datos que informan una deuda posteriormente regularizada continúan constanding en el fichero. Es decir, lo que aparenta es que el legislador italiano ha beneficiado quien no paga, ya que cada vez en que se intente renegociar la deuda o pasa cualquier evento de ésta naturaleza, o mismo otro retraso, el tiempo vuelve a contarse. No obstante, aquél que no paga tendrá un plazo único que esperar hasta que los datos sean retirados del sistema.

## **VI. Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.**

### **1. Legislación Española**

La Ley Orgánica de Protección de Datos establece en el artículo 29.3 que en cualquier caso de tratamiento de datos de carácter personal de solvencia patrimonial y crédito o los datos sobre el cumplimiento o incumplimiento de obligaciones dinerarias, siempre que sea solicitado por el interesado, deberá el responsable del tratamiento comunicarle tales datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

Para lo que nos interesa en este capítulo, solamente nos vamos a detener en la regulación específica de los datos sobre cumplimiento o incumplimiento de obligaciones dinerarias, ubicada en el artículo 44 del Reglamento 1720/200, ya que aquellos referentes a la solvencia patrimonial y crédito se somete integralmente a lo establecido con carácter

general en la LOPD y en el propio RPD, y ya ha sido objeto de apreciación por nuestra parte en los capítulos anteriores.

Claramente inspirado en la Instrucción 1/1998 de la Agencia Española de Protección de Datos, el citado precepto establece en su apartado primero que sin perjuicio de lo señalado en éste artículo, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición se rige por lo dispuesto en los capítulos I a IV del título III del Reglamento. De hecho, el artículo 44 solamente define las reglas que deben ser llevadas en consideración por aquellos intervinientes en la actividad de prestación de informaciones sobre solvencia patrimonial y crédito cuando son instados por el interesado que desea ejercer unos de sus derechos.

De este modo, en lo que concierne al derecho de acceso, según se desprende del apartado 2 del artículo 44 establece el interesado podrá ejercer su derecho frente al titular del fichero común o a cualquier otra entidad participante en el sistema. Para Plana<sup>588</sup>, la fórmula utilizada en el Reglamento resulta muy útil, ya que antes solo se hacía referencia al acreedor y de este modo se amplía el ámbito y también porque en ocasiones se desconoce el titular del fichero común “e incluso no se sabe la deuda que ha motivado la inclusión en el fichero”.

Cuando la solicitud se dirija al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero, facilitando las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios. El precepto deja muy claro que todas las informaciones deben ser dadas al interesado.

En el caso de que el afectado ejerza su derecho de acceso a cualquier otra entidad participante en el sistema, tales entidades están obligadas a comunicarlo todos los datos relativos al mismo a los que ella pueda

---

<sup>588</sup> PLANA, Maria del Carmen. *Ficheros... op. cit.*, p. 411.

acceder, así como la identidad y dirección del titular del fichero común para que pueda completar, si así lo desea, el ejercicio de su derecho de acceso

El Reglamento de Desarrollo de la LOPD no fija un plazo especial para que las solicitudes de acceso en el ámbito de los ficheros de morosos sean resueltas. De suerte que deberá ser observado el tiempo determinado en el artículo 29 de esta ley, que establece que el responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud.

En lo que concierne a los derechos de rectificación o cancelación, el Reglamento prevé tres supuestos en los cuales puede el afectado ejercer su derecho, siendo ellos: a) dirigir la solicitud al titular del fichero común; b) a quien haya facilitado los datos al fichero común y c) a otra entidad participante en el sistema, que no hubiera facilitado al fichero común los datos.

En el primero caso, el titular del fichero deberá tomar las medidas necesarias para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. Si tal entidad no contesta, éste deberá proceder por su cuenta la rectificación necesaria o la cancelación cautelar del dato en un plazo de siete días. Ahora bien, para Pascual Huerta<sup>589</sup>, son dos los plazos que gozan el titular del fichero: uno de siete días para proceder la rectificación o la cancelación, establecido en el citado artículo 44, y otro para la contestación al afectado del procedimiento adoptado, que serían de diez días, según el artículo 16.1 de la LOPD y 32.2 del RPD. Compartimos la opinión del autor.

Desde nuestro modesto juicio, la redacción de éste precepto no fue muy afortunada. No es muy clara en determinar cuándo se empieza a contar el plazo de los siete días, si de la solicitud del afectado o del acuse de

---

<sup>589</sup> PASCUAL HUERTA, Pablo. *Ficheros... op. cit.*, p. 428.

recibimiento de la entidad del traslado efectuado por el titular del fichero. Si es la primera opción, concordamos con Pascual Huerta en que habría que utilizarse de los dos períodos: el de siete días para el traslado y espera de contestación de la entidad; y el otro, del régimen general, de 10 días para resolver la solicitud y comunicarla al interesado. Esta tal vez sea la mejor interpretación ya que de otro modo, siete días no sería suficiente para esperar la respuesta de la entidad, proceder la rectificación y comunicar los datos al interesado.

Aunque nos parezca muy elogiable que la ley haya facilitado de manera significativa el acercamiento del afectado con los intervinientes de los ficheros de solvencia patrimonial, creemos que no fue acertada la opción del legislador en exigir que el titular del fichero rectifique un dato, basado únicamente en la solicitud del interesado, que es lo que pasa cuando no recibe respuesta de la entidad. Ello desde nuestro punto de vista genera una inseguridad jurídica ya que los datos allí insertado son especiales, teniendo en cuenta que no necesitan del consentimiento del afectado para que se proceda a su tratamiento. Mejor hubiera sido exigir antes de la rectificación, una medida como el bloqueo de los datos o su cancelación cautelar.

En el supuesto de que quien reciba una solicitud de rectificación o cancelación de los datos sea una entidad participante que no ha sido la responsable por facilitar los datos al fichero, ésta deberá informar al afectado tal hecho, en un plazo máximo de diez días debiendo además, proporcionarle la identidad y dirección del titular del fichero común para que en su caso, puedan ejercitar sus derechos ante el mismo.

Cuando la solicitud sea dirigida directamente a quien haya facilitado los datos al fichero común deberá, en un plazo también de diez días, si así procede, para rectificar o cancelar los datos de su propio fichero y notificarlo al titular del fichero común los cambios que hubiere producido



dando asimismo respuesta al interesado en los términos previstos en el artículo 33 del RPD.

Sin lugar a duda, el reglamento ha hecho un gran esfuerzo en facilitar el ejercicio de los derechos del afectado, fundamentalmente cuando obliga a todas las entidades participantes del sistema, aunque no sea la responsable por suministrar la información al fichero común, a colaborar con el interesado.

## 2. Legislación Italiana

El código de deontología, en el artículo 8, manifiesta expresamente que el interesado podrá ejercer sus derecho tanto ante el *gestore* como al participante que haya comunicado los datos personales. Tales entidades deberán encargarse de resolver oportuna y tempestivamente las solicitudes a través de la adopción de adecuadas medidas organizativas y técnicas.

En la solicitud formulada para ejercer sus derechos, el afectado titular de los datos deberá especificar, si es posible, su N.I.F. y/o C.I.F. con el fin de facilitar la búsqueda de los datos que le conciernen en el sistema de información de crédito.

La legislación italiana también permite que un tercero ejerza en nombre del afectado sus derechos, cuando éste último haya dado poderes para tal función. Ahora bien, el tercero podrá tratar los datos personales recibidos de un sistema de información de crédito exclusivamente para la tutela de los derechos del interesado, no siendo permitida ninguna otra finalidad perseguida por dicha tercera persona u otra a ésta ligada.

Si la solicitud se dirige al participante, éste deberá contestar directamente al afectado, decidir sobre las modificaciones y proceder las que se hicieren necesarias, y en el caso de que sea técnicamente imposible, deberá hacerlo a través del titular del tratamiento. Cuando la petición de ejercicio de un derecho se dirija al *gestore*, éste procederá de la misma manera que el participante, siempre consultando a éste último cuando sea necesario. En este caso, el *gestore* deberá informar al interesado, como prevé el *Codice* de protección de datos, en el plazo de quince días que será necesario verificar con el participante algunas informaciones, y indicará un nuevo plazo para la respuesta que no podrá ser superior a quince días.

Para Imperiali<sup>590</sup>, la consulta al participante, por lo menos para las informaciones de tipo negativo, es siempre preferible para garantizar exactitud y completitud de la respuesta, incluso cuando no necesaria.

Durante el periodo de verificación entre *gestore* y participante, el código deontológico, establece que los primeros quince días, el *gestore* deberá mantener en el sistema una indicación referente al desarrollo de una inspección de la información de crédito, con codificación específica o un mensaje *ad-hoc* a ser publicadas con los datos que son objeto de la solicitud presentada por el interesado. Tal medida, según opinión de Petrulli<sup>591</sup> pretende evitar perjuicio al afectado por la mora de la inspección.

Siendo necesario un tiempo superior a estos quince días, el *gestore* deberá suspender la visualización en el sistema de los datos objetos de la verificación<sup>592</sup>. Ésta medida en la opinión de Mormile<sup>593</sup>, está destinada a

---

<sup>590</sup> IMPERIALI, Riccardo. *Codice... op.cit.*, p. 996.

<sup>591</sup> PETRULLI, Mario. *Il nuovo... op. cit*, p. 39.

<sup>592</sup> De cualquier modo, el *gestore* debe proteger tales informaciones. Como ha señalado el Tribunal de Napoli, el bloqueo de los datos solo suspenden temporalmente su visualización, no supone que alejará el interesado del peligro del perjuicio derivado de su difusión. Sentencia de 15 de octubre de 2003.

<sup>593</sup> MORMILE, Lalage. *Il Sistema... op. cit.*, p. 1866.

garantizar la presencia, dentro del sistema de informaciones crediticias, de datos completos. Desde su punto de vista, se elimina así una potencial situación de peligro para el interesado. En realidad, en caso de duda sobre el resultado de un proceso de verificación, que también podría dar lugar a la presencia dentro del sistema de datos incorrectos, se evita el riesgo de que puedan ponerse en circulación como datos verídicos. De suerte que la autora cree que se evita que posibles retrasos de un procedimiento de verificación se transforme en una situación de peligro para el interesado.

Parece interesante remarcar la observación de Cecamore<sup>594</sup>, comentando el derecho general de acceso de los interesados a las informaciones personales disponibles en un banco. En opinión de la autora, éste no puede limitarse a una simple devolución de los extractos de cuenta proporcionados mensualmente, sino que debe ofrecer una respuesta completa de las informaciones en su poder, aun cuando estos ya hayan sido en todo o en parte comunicados. De tal modo, creemos que ésta sea la intención del legislador: que la información dada al interesado sea la más amplia posible, tanto que prevé un plazo mayor para cuando sea necesaria alguna comunicación entre el *gestore* y el participante del sistema.

En el caso de que la solicitud de ejercicio de derecho verse sobre controversias relativas a incumplimiento del vendedor/proveedor de bienes o servicio objeto del contrato que se basa la relación de crédito, el *gestore* a pedido del interesado o del participante, o informando a éste último, deberá apuntar prontamente en el sistema de información crediticia la noticia de la existencia de tales controversias, a través de un código específico a ser publicado con los datos relativos a la relación de crédito en cuestión.

---

<sup>594</sup> CECAMORE, Francesca. "Il sistema bancario, finanziario ed assicurativo". En *Il Diritto alla protezione dei Dati Personali: La disciplina sulla privacy alla luce del nuovo Codice*. ACCIAI, Riccardo (Dir.), Santarcangelo di Romagna: Maggioli, 2004, p. 680.

El Garante<sup>595</sup> ha manifestado sobre éste precepto que al interesado se le debe la máxima transparencia. Éste tiene el derecho de acceso y la respuesta a su petición debe ser tempestiva y completa. Además, los solicitantes podrán completar, modificar o borrar los datos almacenados en un sistema de información de crédito. Para este órgano, la que pretende la norma es que haya más claridad y menos burocracia manera en que los derechos pueden ser ejercidos, ya sea en el banco o agente financiero o por el sistema.

Sobre la gratuidad del ejercicio del derecho de acceso del afectado frente a un fichero de solvencia patrimonial y crédito, el *Garante* se ha pronunciado en *Deliberazione*<sup>596</sup> sobre la necesidad de compaginar de un lado los intereses a la determinación de una contribución de gastos, en el caso al fichero Crif, debido a un incremento sustancial de solicitudes de acceso a datos personales, dando como resultando un aumento significativo en el costo para hacer frente al mismo; y de otro, la exigencia de no tornar demasiado difícil y costoso ejercicio de los derechos del afectado.

En este sentido, la Autoridad de Protección de Datos italiana ha decidido fijar que siempre será gratuito el derecho al acceso cuando: el interesado lo solicita expresamente la respuesta mediante el envío por e-mail y una sola vez durante el periodo de cada año, independientemente de la forma elegida para obtener el contestación requerida, tendrá el derecho de ejercer a título gratuito.

Los supuestos en los cuales el afectado tendrá que arcar con alguna carga serán: a) para las solicitudes posteriores a la primera gratuita durante el periodo de cada año, el Crif puede requerir una contribución

---

<sup>595</sup> *Garante per le protezioni dei Dati Personali*. Dossier - 30 novembre 2005 “Le Nuove Regole sui Sistemi di Informazioni Creditizie”.

<sup>596</sup> *Deliberazione* n. 18 del 18 marzo 2010. En: *Bollettino* del n. 114/marzo 2010.

de gastos proporcionales a los costes efectivamente soportados y, de todos los modos, hasta un máximo de euros siete (incluidos los gastos postales); b) cuando sea presentada una solicitud incompleta por parte de un sujeto que, sin embargo, sea identificado y legitimado, y se haga indispensable establecer un contacto con el mismo para adquirir las informaciones necesarias para proporcionar una adecuada respuesta, la contribución de gastos no deberá exceder los costes efectivamente soportados y, en cualquier caso, no deberá superar la suma de euros tres.

## VII. Particularidades de la legislación italiana.

El código de deontología regula algunos aspectos que o no fueron observados por la legislación española, como es el caso del *credit scoring*, o no son objeto de tratamiento específico en el ámbito de los ficheros de solvencia patrimonial y crédito, debiendo observarse, en estos casos, el régimen general como en los casos de algunas medidas de seguridad y algunas sanciones que ha entendido el legislador italiano incluirlas y reforzarlas en el código deontológico.

### 1. Uso de técnicas o sistema automatizado de credit scoring

El artículo 9 del Código deontológico establece algunos principios que deben ser observados por aquellos sistemas de información crediticia que se utilizan de la técnica del *credit scoring*.

El artículo 1, letra *h*) del código deontológico le define como el modo de organización, agrupación, comparación y tratamiento de datos personales referente a solicitudes o relaciones de crédito, que consiste en el uso de sistemas automatizados basados en métodos estadísticos o modelos con el objetivo de evaluar el riesgo de crédito, cuyos resultados son expresados en forma de juicios sintéticos, indicadores numéricos o puntos asociados al interesado y tienen por finalidad suministrar una representación predictiva o probabilista de su perfil de riesgo, fiabilidad y puntualidad de pago. O, por mejor decir, según la breve y lucida concepción de Meo y Ciccía<sup>597</sup>, es la expresión numérica de la solvencia del cliente.

Así, la norma solo permite que la técnica o el programa de *credit scoring* se utilice para la investigación de una solicitud de crédito o para la gestión de las relaciones de crédito iniciadas. Además, el acceso a los datos relativos a los juicios, indicadores y puntos referentes a un interesado serán tratados y comunicados por el *gestore* solamente al participante que ha recibido la solicitud de crédito por el interesado o que ha previamente comunicado datos concerniente a la relativa relación de crédito, de suerte que no pueden tales informaciones estar a disposición de otros participantes del sistema.

Los modelos o los factores de análisis estadísticos y algoritmos para el cálculo de las evaluaciones, indicadores o puntos son auditados periódicamente por lo menos una vez al año y actualizado en función de los resultados de dichas auditorías.

En el caso de que una solicitud de crédito no sea aceptada, el código establece que el participante deberá comunicar al afectado se ha consultado datos relativos a juicios, indicadores o puntos de tipo negativo obtenidos mediante el uso de técnicas de sistema automatizado de *credit scoring*. Si el interesado lo solicita, el participante deberá presentarle los

---

<sup>597</sup> MEO, Baldo y CICCIA, Antonio. *Privacy e Consumatori*. Roma: Istituto poligrafico e Zecca dello Stato, Libreria dello Stato, 2006, p. 98.

datos en cuestión y explicar la lógica de funcionamiento de los sistemas utilizados y los principales factores que se han tomado en cuenta en la tramitación de la solicitud.

## 2. Medidas de seguridad de los datos

El artículo 11 del código deontológico trata en el ámbito del sistema de información crediticia de algunas medidas de seguridad que deben ser llevadas en cuenta por aquellos implicados en dicha actividad.

En primer lugar, la norma establece que los datos que son tratados en estos tipos de ficheros tienen carácter confidencial y no puede ser revelados a terceros fuera de los casos previstos en el Código de Protección de Datos Personales y en el Código deontológico. Así como, todos aquellos que en calidad de responsableS o encargadoS del tratamiento de los datos designados por el *gestore*. En segundo, los participantes que tienen acceso al sistema tienen el deber de mantener el secreto de los datos personales recogidos y responden por la violación de la obligación de confidencialidad derivados de la utilización de información o divulgación a terceros para otros fines o incompatible con los fines especificados en el artículo 2 del Código de buena conducta.

Es interesante resaltar que el citado Código involucra tanto al *gestore* como al participante en la responsabilidad de adoptar las medidas que garanticen la seguridad. De manera que el apartado 3 determina claramente que ellos deberán patrocinar las medidas técnicas, lógicas, informáticas, de procedimiento, físicas y organizativas aptas para garantizar la seguridad, la integridad, y la confidencialidad de los datos

personales y de las comunicaciones electrónicas en conformidad con la disciplina en materia de protección de datos personales. Establece en el apartado 5 que el *gestore* y el participante deberán dar instrucciones específicas por escrito a los respectivos responsables y encargados del tratamiento y se aseguraran de que dichas instrucciones con plenamente respetadas también por medio de las verificaciones llevadas a cabo por los órganos de control adecuados.

Particularmente en lo que corresponde al *gestore*, el Código determina que a éste incumbe realizar las medidas adecuadas de seguridad a fin de asegurar el correcto y buen funcionamiento del sistema de información crediticia, así como el control de los accesos. Estos últimos deberán ser registrados y almacenados en el sistema informativo del aludido *gestore* así como por todos los participantes que poseen una copia de la base de datos.

### 3. Sanciones

Cumple señalar ahora, el modo como ha tratado el Código de buena conducta las medidas sancionadoras. El artículo 12 determina que el *gestore* y a los participantes conjuntamente o a través de las asociaciones que subscriben el código establecieran mecanismos adecuados para la aplicación de sanciones, en particular por las aludidas asociaciones o por el organismo a que se refiere el artículo 13, apartado 7<sup>598</sup>, clasificadas según el grado de violación.

---

<sup>598</sup> El organismo creado por el artículo 13, apartado 7 tiene por objetivo controlar las revisiones periódicas que deben ser realizadas por el *gestore*, por lo menos una vez al



Las aludidas sanciones son fijadas sin perjuicio de aquellas de naturaleza administrativas, civiles y penales previstas por la ley y deberán ser previamente informadas al Garante. Las medidas especificadas por el código de buena conducta son la reclamación formal, la suspensión o revocación del acceso al sistema de información de crédito y, en casos más graves, la publicación del aviso de la violación en uno o más periódicos o revistas nacionales a costa del infractor.

---

año, sobre la legalidad, exactitud del tratamiento, el control de la exactitud e integridad de los datos comunicados a través de una muestra de solicitudes y relaciones de crédito. El citado organismo se compone de al menos un representante del *gestore*, un representante de los participantes que serán nombrados designados por rotación, y un representante de las asociaciones de consumidores que serán nombrados por el Nacional de Consumidores y del Consejo de Usuarios.

**PARTE II: EL TRATAMIENTO DE LOS DATOS SOBRE LA  
SOLVENCIA PATRIMONIAL Y CRÉDITO DE LOS  
INDIVIDUOS Y LA LEGISLACIÓN BRASILEÑA.**

## I. Introducción

La legislación brasileña, como ya hemos comentado, ha elegido ubicar la disciplina de los ficheros de solvencia patrimonial y crédito en el Código de Defensa del Consumidor, dedicando a tal efecto el artículo nº 43 y sus respectivos párrafos.

Uno de los autores del anteproyecto<sup>599</sup> del aludido código ha señalado que los principales hechos que le llevaron a redactar el citado artículo fueron los notorios abusos de estos ficheros, donde las informaciones eran llevadas al conocimiento público, divulgadas por medios de comunicación causando la insatisfacción generalizada derivada de la natural gravedad y frecuencia de tales abusos.

En este sentido, afirma Vasconcelos Benjamin<sup>600</sup>, que la inspiración para el texto brasileño fue obtenida del derecho Norte Americano, llevándose en consideración el *National Consumer Act* y el *Fair Credit Report*. La influencia del derecho europeo, como recoge el mencionado autor, fue mínima, ya que solo en 1995 fue aprobada una Directiva Comunitaria sobre la materia. El Código del Consumidor brasileño fue publicado en 11 de septiembre de 1990.

Es verdad que en aquella época, y comparándola con otros países de su entorno, era una legislación muy avanzada y que efectivamente hacía frente a la protección de los consumidores en un tema socialmente muy

---

<sup>599</sup> PELEGRINI GRINOVER, Ada; HERMAN DE VASCONCELOS BENJAMIN, Antonio, et al. *Código Brasileiro de Defesa do Consumidor: comentado pelos autores do anteprojeto*. Rio de Janeiro: RT, 2004, p. 399.

<sup>600</sup> *Ibid.*, p. 400.

problemático y sin disciplina legal. Sin embargo, desde 1990 a los días actuales, Brasil no ha evolucionado en materia de protección de datos. Pasamos de una legislación que en su momento respondía a las necesidades de protección de algunos de los derechos de los ciudadanos, a estar entre los últimos, incluso de Latino America, en lo que concierne no sólo a las discusiones sobre el derecho a la autodeterminación informativa, como propiamente a su efectiva disciplina legal. Tal afirmación no sorprende si tenemos en cuenta todo lo que se ha trabajado en Europa desde la Directiva 95/46, e incluso antes de ella, y el esfuerzo de los países de éste continente en ajustar sus leyes a una mejor protección de sus ciudadanos en lo tocante a la protección de datos de carácter personal; de igual modo, lo mismo está pasando en Latino America<sup>601</sup> y desde

---

<sup>601</sup> Se puede citar, por poner algunos ejemplos de cómo varios países de Latino América ya han impulsado sus legislaciones hacia una mejor protección de los ciudadanos en lo que concierne a la protección de datos personales, como Chile y su Ley 19.812 de 13 de Junio de 2002 cuyo ámbito de aplicación es explicitada por el artículo 1º que determina: el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley”; en Uruguay, la Ley nº 18.331 de 11 de agosto de 2008, estableció que el derecho a la protección de los datos personales es inherente a la personalidad humana. El objetivo de ésta ley es regular la totalidad de los bancos de datos personales existentes en poder de personas físicas y jurídicas, públicas o privadas; En Argentina, la Ley 25.326 de Protección de Datos (Habeas Data) de 2 noviembre de 2000, que tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre; y, finalmente, Colombia que ha publicado la reciente Ley Estatutaria 1.266 de 31 diciembre 2008, que tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales. Además, se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada.

nuestro punto de vista, Brasil está completamente adormecido en ésta materia.

Como ya hemos indicado, incluir la disciplina del derecho a la protección de datos en el Código de Defensa del Consumidor en su época fue un hecho extremadamente importante, sin embargo actualmente no responde a las nuevas exigencias. Este mismo aspecto fue destacado por Badin, Carazza y Ribeiro<sup>602</sup>, que apuntan que, no obstante el Código del Consumidor establezca las principales directrices para la protección del consumidor en relación al eventual carácter invasivo de los bancos de datos, el tratamiento de tal materia tan relevante en solamente un artículo, torna poco efectivos los derechos del interesado, además de no proteger con efectividad al consumidor contra los posibles daños a su reputación. Concluyen que la ausencia de una legislación general provoca inseguridad jurídica que obstaculiza el desarrollo del sector.

El Derecho a la Protección de Datos desde nuestro punto de vista no puede estar vinculado al derecho del consumidor en ningún de sus aspectos y modalidades de protección. Es un derecho autónomo que tiene sus correspondientes principios y contornos, cuya tutela para que se torne efectiva necesita que esté integrada dentro de una sistemática legislativa propia, para que pueda enfrentar los avances de la tecnología y con ella sus posibles violaciones a los derechos más fundamentales de los ciudadanos. Además, consideramos que las relaciones jurídicas que se establecen entre todos los sujetos que forman parte de un sistema de informaciones crediticias, en lo que concierne a los problemas que conllevan el tratamiento de los datos personales no son de consumo. Es

---

<sup>602</sup> BADIN Arthur; CARAZZA DOS SANTOS, Bruno; RIBEIRO DAMASO, Otávio. “Os Bancos de Dados de Proteção ao Crédito, o CDC e o PL 5.870/2005: comentários sobre Direito e Economia” [en línea]. Disponible en

<<http://www.fazenda.gov.br/spe//publicacoes/reformasinstitucionais/estudos/ArtigoRevistaDireitoConsumido-BancosDados.pdf>> , Agosto de 2007. [Consulta en 14 fev 2010].

decir, entre el responsable del fichero y el acreedor, hay una relación empresarial; Y entre el acreedor y el deudor, en un primer momento hubo una relación de consumo, pero que, desde el instante de la decisión del registro de los datos en el fichero, la esencia de la aludida relación deja de ser determinante por la inclusión de las informaciones; y, finalmente, entre el titular de los datos y el responsable del fichero existe una relación jurídica proveniente del derecho a la protección de datos.

Así, hoy por hoy los sistemas de protección al crédito están incluidos dentro de este entorno legislativo protector del derecho a la autodeterminación informativa. A este tenor, no resulta extemporáneo resaltar la observación de Herman de Vasconcelos Benjamin<sup>603</sup> al defender que en el mundo en que vivimos es posible identificar cuatro tipos básicos de poder: el económico, el militar, el tecnológico y el de la información. De todos estos, puntualiza el autor, los sistemas de protección al crédito ostentan tres, es decir, el económico, el tecnológico y el de la información. Una razón más, desde nuestra perspectiva, para que sea una actividad que deba poseer una normativa especial.

La elección europea de crear una estructura general de ley de protección de datos y que sobre ella graviten los casos más especiales y fundamentalmente la creación de agencias especializadas en el tema nos parece que fue muy acertada y que viene dando buenos resultados.

Brasil por lo que se puede inferir, ha elegido hasta el momento presente centrarse en normas fragmentadas, referentes a cada sector. Tanto que ya tramita en el Senado, como se ha comentado, el Proyecto de Ley nº 85/2009 que pretende disciplinar en particular a los ficheros de solvencia patrimonial y crédito. Tal y como está redactado el texto del aludido proyecto, pensamos que solucionará algunos de los problemas actuales en el tema de los sistemas de protección de datos, sin embargo no es ni la

---

<sup>603</sup> PELEGRINE GRINOVER, Ada; HERMAN DE VASCONCELOS BENJAMIN, Antonio; *et. al. Código Brasileiro... Op. Cit.*, p. 405.

sombra del avance que representó a su tiempo el artículo 43 del Código de Defensa del Consumidor brasileño.

En todo el análisis que pretendemos hacer en este apartado, se tendrá en consideración por supuesto el CDC, además de la ley del *Habeas Data* n. 9.507/97 y también para las omisiones y los problemas que las normas en vigor no pueden solucionar, nos referiremos cuando sea posible al Proyecto de Ley nº 85/2009, ya que en el presente momento es la más importante referencia sobre cómo piensa actualmente el legislador brasileño en esta materia.

## II. Requisitos y categorías de datos.

El Código de Defensa del Consumidor no dedica como lo hacen las legislaciones italiana y española un precepto especial donde se determine los requisitos o las categorías de datos que pueden ser incluidos en un fichero de solvencia patrimonial. Sin embargo, de la lectura del artículo 43 del CDC se puede extraer algunas condiciones que son necesarias para el registro de los datos, así como de las categorías de informaciones que se pueden inserirlas.

Primeramente, el aludido precepto no prohíbe el tratamiento de datos positivos, aunque es cierto que todo el texto legislativo se vuelca de modo muy especial a aquellos negativos. El *caput* del artículo 43 hace una declaración general del derecho que tiene el consumidor de conocer sus informaciones, declarando que: *el consumidor tendrá acceso a las informaciones existentes en catastros, fichas, registros y datos personales e de consumo archivados sobre él, así como sobre sus respectivas fuentes.*

De hecho, es una manifestación infraconstitucional de parte de un derecho garantizado en la Ley Fundamental brasileña, como hemos defendido en este trabajo, que es el derecho a la autodeterminación informativa. Todos los demás párrafos sucesivos continúan tratando de la disciplina de estos ficheros y siempre se refiere a las excepciones de los datos negativos, cuando necesarias. Para Roscoe Bessa<sup>604</sup>, el precepto que cuida de la calidad de la información no excluye o limita directamente el tratamiento de los datos adversos, es decir, cuando instituye el régimen temporal diferenciado para el que denomina informaciones negativas, se admite implícitamente el tratamiento de otras especies de informaciones, o sea, las positivas. Estamos de acuerdo con ésta posición, de suerte que, aunque la ley no haya manifestado de modo claro sobre la posibilidad o no del tratamiento de datos positivos, estos pueden ser tratados en los banco de datos de protección al crédito.

Los ficheros de solvencia patrimonial y crédito en los países aquí estudiados tratan datos positivos y negativos, y estos primeros poco a poco empiezan a cobrar importancia dentro del contexto en el cual se encuentran dichos banco de datos. Para Badin, Carazza y Ribeiro<sup>605</sup>, si las entidades que ofrecen crédito solamente poseen informaciones negativas de un potencial cliente, no conseguirán clasificarlo como un buen o malo cliente. Únicamente conseguirán catalogarlo a partir del conocimiento del pasado crediticio, dependiendo por lo tanto, también, de las informaciones sobre sus hábitos de pago, lo que el mercado llama de informaciones positivas. Para los autores, estas informaciones estimulan la competencia entre los bancos ya que estas entidades pueden identificar

---

<sup>604</sup> ROSCOE BESSA, Leonardo. “Bancos de dados de proteção ao crédito e os limites jurídicos do tratamento de informações positivas”. Director: Gustavo Tepedino. Universidad del Estado de Rio de Janeiro. Facultad de Derecho, 2008.

<sup>605</sup> BADIN Arthur; CARAZZA DOS SANTOS, Bruno; RIBEIRO DAMASO, Otávio. *Os Bancos... op. cit.*



con facilidad los buenos clientes y pueden competir más agresivamente por su preferencia, ofreciendo mejores precios y condiciones por sus servicios.

Hay que tener en cuenta a la hora de proteger la esfera de la privacidad de los ciudadanos, que indudablemente aquellos datos negativos son los que más interfieren en los derechos fundamentales en especial a la autodeterminación informativa, al honor y a la intimidad, sobre todo porque gozan de una disciplina marcada por la excepción a las reglas generales de protección de datos. En efecto, los derechos de las personas ante tales registros son más estrictos, y aunque los deberes de los responsables también se impongan de manera más dura, creemos que es más difícil conseguir el equilibrio o compensación de uno en relación al otro cuando el límite que se impone es a un derecho fundamental.

En Italia su legislación establece la posibilidad de que las centrales de riesgos puedan tratar los mencionados datos positivos y negativos. De hecho, la norma hace referencia clara y directa a los dos tipos de datos, permitiendo el Código de Buena Conducta en el artículo 1º, letra c, apartado 2, el tratamiento en sistemas de protección al crédito de ambas informaciones.

En España, a su vez, hay que matizar lo que se entiende por datos positivos. En efecto, ni la LOPD ni su Reglamento de desarrollo utiliza esta expresión, pero esta primera norma, así como el Código de Defensa del Consumidor de Brasil, siempre que necesario resalta cuando quiere referirse a “datos adversos”, como en el apartado 4 del artículo 29: *sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años*. De suerte que la LOPD no excluye su tratamiento pero sí lo limita en los términos establecidos por el RPD que hace referencia al régimen general.

Ahora bien, en el derecho brasileño a pesar del hecho de que la ley no disponga claramente de estos datos y por lo tanto no haya ningún precepto que exija su consentimiento, no ha dejado de considerarse por la doctrina como necesario. Sacco Neto<sup>606</sup> fundamenta la exigencia del consentimiento en estos tipos de datos en el principio de la igualdad y del equilibrio de los intereses implicados, ya que según su opinión, la eventual obligatoriedad de la divulgación de hechos que no perjudicarían la colectividad desentonaría el equilibrio razonable y proporcional de los derechos en debate, imponiéndose al consumidor algo que no se justifica desde la óptica de los derechos colectivos y que, si fuese adoptado, vendría a desmerecer incluso el argumento que sirve de fundamento a autorizar tratamiento diverso para los registros negativos.

De otra parte, para Roscoe Bessa<sup>607</sup>, en un ambiente propicio de información adecuada, el consumidor debe tener pleno derecho de elección de decidir lo que es más conveniente y adecuado. Por lo tanto, para el aludido autor, la solución pasa por la idea de que el consentimiento legitima el tratamiento puntual y específico de datos positivos. Es decir, la información completa y adecuada sobre las razones de la colecta de estos datos, sus peligros y ventajas entre otros fundamentos en su opinión deriva del principio de la buena fe objetiva, y de la idea de transparencia y lealtad en las relaciones.

A nuestro sentir, aparte de todo ello, la necesidad del consentimiento en el sistema jurídico brasileño puede ser también argumentada desde la perspectiva del derecho a la autodeterminación informativa. Es derivación del poder de control que tiene el individuo sobre sus datos, de suerte que consentir, es el eje de este derecho, la regla general es que solamente puede ser inexigible en los caso que la ley así lo disponga, sopesando a

---

<sup>606</sup> SACCO NETO, Fernando. *Cadastros de Proteção ao Crédito*. São Paulo: Método. Vol. 1. Parte Geral. 2009, p. 77

<sup>607</sup> ROSCOE BESSA, Leonardo. *Bancos de dados... op. cit.* p. 216.

través del principio de la proporcionalidad los intereses implicados, pero siempre respetando los límites impuestos por la libertad informática.

Como ha manifestado Murillo de la Cueva<sup>608</sup>, el derecho a la autodeterminación informativa “tiene por objeto principal poner en mano de los individuos todos los medios jurídicos para controlar el uso por terceros de sus datos personales. Del mismo modo que uno de los sentidos de la palabra autodeterminación es el que apunta al ejercicio por cada uno de la propia libertad, ese término con el calificativo «informativa» indica definición o control por el afectado de la información que le concierne”. Este control, continua el autor, descansa en dos elementos principales que son condiciones de licitud de las actividades de captación y utilización de datos personales por terceros. El primero es el del consentimiento “inequívoco, libre e informado que permite a la persona a la que se refieren autodeterminarse informativamente. No obstante, es claro que en ciertas ocasiones ha de ser posible tratar información personal sin que medie la autorización del afectado. Por eso, y aquí viene el segundo elemento, la ley puede autorizarlo expresamente, bien de forma general, al darse las circunstancias por ella previstas, o caso por caso”.

Por lo tanto, no hay en ningún dispositivo la excepción al consentimiento para los datos positivos en el ordenamiento jurídico brasileño. Si los ficheros de protección al crédito pretenden tratar estos tipos de datos, habrá que hacerlo con previo consentimiento de su titular.

En lo que concierne a los datos negativos, Rizzato Nunes<sup>609</sup> señala algunos requisitos que deben confluír para su registro que son: a) la

---

<sup>608</sup> MURILLO DE LA CUEVA, Pablo Lucas. *Perspectivas... op. cit.*

<sup>609</sup> RIZZATTO NUNES, Luiz Antônio. *Comentários ao Código de Defesa do Consumidor*. São Paulo: Saraiva, 2009, p. 533.

existencia de una deuda: b) que tal deuda esté vencida; c) que su valor sea líquido y cierto; d) que no haya oposición del consumidor.

Para Herman de Vasconcelos Benjamin<sup>610</sup>, hay cuatro características principales que deben ser observadas para que se legitime el registro del dato: a) teleológicos (= de finalidad) que dicen respecto a los objetivos a la hora de la colecta, almacenamiento y circulación de los datos recabados; b) substantivos (= de contenido) se refieren a la naturaleza y al tipo de información, es decir, la ausencia de cuestionamiento sobre la deuda, la exactitud de la información y el tipo de dato registrado<sup>611</sup>; c) procedimentales (= de forma) que están relacionados con ciertas formalidades impuestas a los responsables del fichero; y d) temporales (= vida útil o termo inicial y final) que comandan en el tiempo la validez del registro.

Aunque la ley no establezca de modo detallado todas las características exigidas para el registro de los datos como lo hace la legislación española, no obstante, se puede recoger en los párrafos del artículo 43 las siguientes: a) notificación previa de inclusión, dispuesto en el párrafo 2º del Art. 43; y b) que no haya transcurrido 5 años desde la fecha de la deuda (Art. 43 párrafo 1º) o cuando consumada la prescripción relativa al cobro de la deuda (Art. 43 párrafo 5º). Tales requisitos serán analizados detenidamente más adelante.

De todas las condiciones que resultan de la interpretación doctrinal exigidas para el registro de una deuda, la más controvertida, indudablemente, es aquella que determina que no haya oposición del consumidor, o por mejor decir, que no haya reclamación de ninguna naturaleza sobre la deuda. No nos parece que la mera oposición del

---

<sup>610</sup> PELEGRINE GRINOVER, Ada; HERMAN DE VASCONCELOS BENJAMIN, Antonio; *et. al. Código Brasileiro... Op. Cit.*, p. 425.

<sup>611</sup> *Ibid.*, p. 429

consumidor al responsable del fichero sea suficiente para evitar el registro del dato. En verdad, como comentaremos en el apartado dedicado a los derechos del interesado, el aludido derecho a la oposición en el ámbito administrativo (ante el responsable del fichero), no está legalmente configurado aunque podrá ser ejercido fundándose en los principios generales del Derecho Administrativo. Sin embargo no existirá vinculación jurídica entre el ejercicio de tal derecho y el no registro del dato.

Rizzatto Nunes<sup>612</sup>, que tiene una opinión distinta a la nuestra, señala que si el consumidor recibe el aviso previo de notificación del dato del acreedor o del responsable del fichero y les remite una contestación en la cual se opone a la inclusión del dato fundamentando su escrito en que, por ejemplo, el valor cobrado de la deuda es excesivo. A su sentir, el servicio de protección al crédito no podrá anotarlo ya que se ha instaurado una disputa entre el acreedor y el consumidor. Para el mencionado autor, como el órgano de protección al crédito no ejerce función jurisdiccional no podrá decidir la disputa y por lo tanto no deberá incluir el dato en el sistema. Concluye que ante la oposición del consumidor solamente restaría al acreedor requerir a través del Poder Judicial que se insertara la información.

Una vez más recalamos que el derecho a oposición no tiene esa capacidad en el sistema jurídico brasileño, hoy por hoy, de impedir el registro del dato, si la información dada por el acreedor es de una deuda cierta, vencible, exigible y que además cumpla los otros requisitos: el límite temporal y la notificación previa

Para Herman de Vasconcelos Benjamin<sup>613</sup>, el carácter incuestionable del dato es la esencia de los ficheros de morosos y esta característica es vista

---

<sup>612</sup> RIZZATTO NUNES, Luiz Antônio. *Comentários... op. cit.*, p. 534.

<sup>613</sup> PELEGRINE GRINOVER, Ada; HERMAN DE VASCONCELOS BENJAMIN, Antonio; *et. al. Código Brasileiro... Op. Cit.*, p. 429.

en una doble perspectiva: a) certeza sobre la deuda y b) convicción sobre la información en si. De suerte que desde su punto de vista, el acreedor solamente podrá informar el dato cuando la obligación restar incontestada, tanto por conformismo del deudor, como por un pronunciamiento judicial. A su sentir, no es ejercicio regular de derecho práctica que contraríe tales exigencias, al revés, sería abuso de derecho.

Estamos de acuerdo con la opinión de que cuando hay una reclamación ante un órgano del Poder Judicial es indebida la inclusión de los datos. La jurisprudencia, sin embargo, ha cambiado de entendimiento en lo que concierne a este tema. Como bien observa Roscoe Bessa<sup>614</sup>, hasta el final de 2003 los fallos del Superior Tribunal de Justicia eran favorable a que las deudas que estuviesen siendo discutidas judicialmente, no podrían ser registradas por los bancos de datos de protección al crédito. Hubo, no obstante, un cambio en el entendimiento de este Tribunal, a partir del juzgamiento del recurso nº 527.618<sup>615</sup> y desde entonces se infiere que no tiene respaldo legal obstaculizar el acreedor del registro en los bancos de datos de protección al crédito apenas y únicamente por el hecho de que haya discusión de la deuda en juicio.

Así que, según la mencionada Sentencia, deben concurrir tres requisitos para que el dato no sea registrado en el fichero por el motivo de la reclamación sobre la deuda: a) que haya acción propuesta por el deudor contestando la inexistencia total o parcial de la deuda; b) que haya efectiva demostración de que la contestación del cobro indebido se funda en la apariencia de buen derecho y en la jurisprudencia consolidada de aquél Tribunal; c) que cuando la disputa sea por parte de la deuda, haya el depósito del valor referente a la parte que no hay controversia o preste caución idónea.

---

<sup>614</sup> ROSCOE BESSA, Leonardo. *Bancos de dados... op. cit.* p. 193, nota al pie de página.

<sup>615</sup> STJ. Resp nº 527.618-RS. Rel. Min. Cesar Asfor Rocha, juzgado en 22 de octubre 2003.

Nos parece oportuno destacar la sentencia de la *Primeira Turma Recursal dos Juizados Especiais Cíveis e Criminais* del Distrito Federal<sup>616</sup> que ha señalado que no obstante la colecta de datos sea una actividad pública, tácitamente permitida por el ordenamiento jurídico, incluso con la tolerancia del Estado, por intermedio de sus órganos judiciales, ella soporta un componente injusto. Se dice eso porque se deja al arbitrio del responsable por la base de datos la inserción de informaciones sobre los ciudadanos que aún no fueron pronunciados por el Estado, a través de un juez competente. Dichos datos serán *a posteriori* colocados onerosamente a disposición de – y compartida con – sus clientes actuales y futuros. De esta manera, entiende el Órgano juzgador que cuando se divulga que un procedimiento judicial se ha iniciado, este hecho es únicamente un apelo al Estado para que se pronuncie sobre una relación jurídica. Lo que se pretende es una declaración judicial de la cual depende el crédito para subsistir como tal y que sea oponible contra el presunto deudor.

La Sentencia continua argumentando que la actividad de recogida de informaciones para la formación de un banco de datos no es por sí ilícita. Sin embargo, sus efectos pueden serlo si dicha actividad no es ejercida con cautela y responsabilidad. Ello exige que se proceda a filtraje de los datos que se recaban. Toda esa cautela debe acompañar tal actividad y de ser necesario, suspender la recogida de no existir, por lo menos, una sentencia definitiva que genere un crédito para el hasta entonces supuesto acreedor.

Para Herman de Vasconcelos Benjamin<sup>617</sup>, solamente las deudas incuestionables pueden ser objeto de registro. Cuando hay duda judicial y razonablemente materializada sobre su valor o sobre la propia existencia

---

<sup>616</sup> Primeira Turma Recursal dos Juizados Especiais Cíveis e Criminais del Distrito Federal. Registro do Acórdão nº 276513, relatora Editte Patricion, juzgado en 03/04/2007.

<sup>617</sup> PELEGRINE GRINOVER, Ada; HERMAN DE VASCONCELOS BENJAMIN, Antonio; *et. al. Código Brasileiro... Op. Cit.*, p. 430.

de la obligación, no se puede mantener el registro de ningún modo, aunque sea como mera anotación. De suerte que a su sentir, mientras haya litigio judicial, no existe seguridad y certeza suficiente para legitimar el juzgamiento público y masificado que los archivos de consumo propician. De no ser así, continúa el autor, estaríamos en la mano inversa de la historia, transformando los archivos de consumo en verdaderos tribunales de excepción.

Desde nuestra perspectiva, como hemos indicado, cuando la reclamación de naturaleza judicial o administrativa incide sobre la certeza, el vencimiento, la liquidez o exigibilidad de la deuda, los datos no deberían ser incluidos en un fichero, ya que mientras ésta es discutida, no reflejará una situación que corresponda fielmente la realidad. En efecto, a pesar de lo indicado de Herman de Vasconcelos Benjamin<sup>618</sup>, este matiza que no toda impugnación judicial puede llevar a obstaculizar el registro de una información, “la regla de oro del ordenamiento es siempre la razonabilidad”.

Ahora bien, creemos que no se debería excluir del fichero la información, pero sí bloquearla temporalmente hasta que se termine la controversia. De esta manera, el gestor del fichero puede ejercer un control a través de un sistema de alerta sobre el deudor en el sentido de que se evite el abuso del derecho de contestar a deuda para que así no se tenga registro suyo de incumplimiento y de este modo tener la posibilidad de solicitar otros créditos. Tal sistema de alerta que proponemos no podría ser visualizado por los participantes del sistema de protección al crédito. Serían informaciones solicitadas siempre por la autoridad judicial o Administrativa para que se evitaran múltiples demandas de un determinado deudor y sus respectivos bloqueos de datos, con la finalidad de “limpiar su nombre” y estar apto a solicitar nuevos créditos, burlándose del sistema.

---

<sup>618</sup> *Ibid.*, p. 431.



De otra parte, el plazo de los cinco años para la inclusión de la deuda se contaría a partir de la fecha de la publicación de la sentencia o en su caso de la decisión administrativa que es cuando se constituye en un dato real y fiable. De otro modo, la lentitud de una demanda de esta naturaleza siempre beneficiaría al deudor fuese cual fuese la decisión final. Es decir, o porque efectivamente tenía razón de ser su petición o porque el tiempo del inicio del cómputo del mencionado plazo ya habría disminuido considerablemente.

Además de todo ello, hay algunas exigencias que el Código de Defensa del Consumidor hace que se asemejen mucho al principio de la calidad de los datos que establece la propia Directiva 95/46. De modo que el párrafo primero del artículo 43 del CDC determina que las informaciones que serán incluidas deben ser objetivas, claras, verdaderas y en lenguaje de fácil comprensión.

En el artículo 4º del Proyecto de Ley nº 85/2009 SE repiten las mismas exigencias del CDC, pero se conceptúa cada uno de estos requisitos en el párrafo primero del mencionado precepto. De suerte que las informaciones objetivas son aquellas descriptivas de los hechos y no envuelve juicio de valor. Para Roscoe Bessa<sup>619</sup>, no se permite el análisis subjetivo de la situación financiera del consumidor. La valoración de las informaciones es tarea a ser realizada por el destinatario de las aludidas informaciones. Ello se asemeja a la misma prohibición consignada por la Agencia Italiana de Protección de Datos<sup>620</sup> sobre dato evaluativo o que exprese juicio de valor sobre el interesado.

Respecto al requisito de informaciones claras, el PL nº 85/2009 consigna que son las que posibilitan el inmediato entendimiento del interesado

---

<sup>619</sup> ROSCOE BESSA, Leonardo. *O Consumidor e os Limites dos Bancos de Dados de Proteção ao Crédito*. São Paulo: Revista dos Tribunais, 2003, p. 186.

<sup>620</sup> *Garante per la Protezione dei Dati Personali*. Dossier – 30 de noviembre de 2005.

independientemente de la remisión a anexos, formulas, siglas, símbolos, términos técnicos o nomenclatura específica.

Las informaciones verdaderas son aquellas exactas, completas y sujetas a comprobación. Para Roscoe Bessa<sup>621</sup>, “información verdadera es información actualizada”. En efecto, la información tiene que reflejar una situación real y para que se pueda ser así, los datos incluidos en un fichero tiene que ser no solamente verdaderos desde el origen, pero siempre actualizados. En efecto, son innumerables las sentencias que condenan al acreedor al pago de daños morales derivados o del registro y manutención de información sobre deuda inexistente. A este hilo, la sentencia del TJDF<sup>622</sup> que manifiesta que comete daño moral, posibilitando la debida compensación pecuniaria la empresa prestadora de servicio que incluye indebidamente datos del afectado en un sistema de protección al crédito por deuda inexistente. En efecto, según entendimiento del TJRS<sup>623</sup>, configurada la irregularidad de la introducción de los datos del afectado en los órganos de protección al crédito por deuda inexistente, es evidente el daño moral *in re ipsa*. La indebida inclusión es suficiente por si solo para la concesión de indemnización, ya que mancha el nombre del consumidor y impide la obtención de crédito, que desde el punto de vista señalado en la sentencia son situaciones que van más allá que la mera molestia.

Por fin, el lenguaje de fácil comprensión es el último requisito que trata el CDC. El PL nº 85/2009 conceptúa como aquellas informaciones que garantizan al afectado el pleno conocimiento del contenido, del sentido y

---

<sup>621</sup> ROSCOE BESSA, Leonardo. *O Consumidor... op. cit.*, p. 187.

<sup>622</sup> TJDF. Apelação Cível no Juizado Especial. nº 2008.03.1.019128-9. Rel. José Guilherme. Juzgado en 08 de septiembre 2009.

<sup>623</sup> TJRS. Recurso Inominado, nº 71002071314. Rel. Leila Vani Pandolfo Machado. Juzgado en 24 de marzo de 2010.

del alcance de los datos incluidos sobre su persona. Para Roscoe Bessa<sup>624</sup>, tal condición objetiva que el interesado al ejercer su derecho de acceso pueda comprender exactamente el contenido y el significado del registro. Así, según el aludido autor, no se admiten informaciones codificadas, lenguaje técnica o mismo utilización de idioma extranjero.

Aparte de estos requisitos, el Proyecto de Ley también añade en su texto que están prohibidas informaciones excesivas, no proporcionales o que no estén vinculadas al análisis de riesgo de crédito; igualmente, informaciones sensibles las cuales establece que son aquellas pertinentes al origen social y étnico, a la salud, orientación sexual y a las condiciones políticas, religiosas y personales del interesado. Además, prohíbe incluir informaciones de incumplimiento de servicios de prestación continuada como agua, luz y teléfono.

Es natural que comparativamente tales prohibiciones no se encuentren en la legislación específica sobre los ficheros de solvencia patrimonial de Italia y de España porque los principios que están consagrados en la ley general de protección de datos de estos países ya prevén que todos los datos tratados obedezcan a determinadas exigencias sobre todo referentes a la calidad de los datos, que protege los datos en todas las fases de su vida física: la recogida, el registro y la conservación. De suerte que a nuestro sentir, ya que en Brasil no es posible recurrir a una ley general de protección de datos, cuanto más completa la norma específica, mejor tutelado estará el derecho a la autodeterminación informativa. En este punto, creemos que el aludido Proyecto de Ley ha hecho un esfuerzo en el intento de compensar la omisión legislativa en materia de protección de datos. Tanto es así, que ha necesitado definir lo que son datos sensibles, algo que a nuestro parecer no es el ámbito legal adecuado para que se aclare este concepto en una norma que trata sobre sistemas de protección al crédito. Sin embargo, también tenemos que admitir que es mejor que

---

<sup>624</sup> ROSCOE BESSA, Leonardo. *O Consumidor... op. cit.*, pp. 184-185.

haya preceptos que empiecen a insertar y esclarecer en el ordenamiento jurídico brasileño algunos conceptos imprescindibles a la protección de datos.

Hay otros dos requisitos que también están contemplados en el texto del mencionado proyecto de ley que igualmente pueden entenderse como requisitos de inclusión. El artículo 7 permite la inclusión de informaciones de incumplimiento de cualquier obligación derivada de ley o contrato, pero exige que haya sido emitido el título o el documento fiscal correspondiente, debidamente contabilizado. Aparte, el párrafo 1º del mismo artículo prevé que las obligaciones que proviene de decisión judicial, solamente podrán ser incluidas si ésta es no es recurrible. Ya el siguiente párrafo prohíbe la inclusión de información advenida de contratación efectuada por teléfono o por cualquier otro medio que genere dudas acerca de la identidad del deudor, salvo si se pueda ser confirmada su identificación por cualquier medio.

Por fin, la que nos parece más importante, aunque no concordando con el valor fijado, es el requisito ubicado en el párrafo 4º del artículo 7 que prohíbe el registro de datos de incumplimiento de obligación cuyo valor no ultrapase sesenta reales. Igualmente, consideramos muy acertado que en esta posible nueva ley los datos de servicios de prestación continuada no sean objetos de un fichero de solvencia patrimonial y crédito. Creemos que todo ello significa un notable cambio de pensamiento del legislador brasileño como hemos comentado en el capítulo anterior.

### **III. Modalidad de recogida y registro de los datos**

Como hemos venido incidiendo, el hecho de que la disciplina de los ficheros de protección al crédito se ubique en el Código de Defensa del Consumidor, ello hace con que haya un cambio de foco en la tutela de los intereses implicados. Es decir, la protección que se quiere alcanzar es del ciudadano como consumidor y no desde la perspectiva de un autónomo derecho a la protección de datos.

De suerte que de ello se derivan dos situaciones: primero una legislación extremadamente protectora al consumidor y por otro lado, el natural olvido de la disciplina de las otras partes implicadas en la prestación del servicio de información crediticia. Una vez más queremos recalcar que en nuestra opinión el artículo 43 del CDC tuvo a su tiempo una importancia fundamental para imponer los límites a estos ficheros, sin embargo hoy por hoy no es un instrumento que pueda comportar todas las exigencias para una tutela efectiva del derecho a la autodeterminación informativa en este ámbito.

El mencionado precepto por tratar, como ya se ha indicado, de un derecho desde la perspectiva del consumidor no ha establecido algunas reglas como las que hacen las legislaciones italiana y española. Se puede citar, por ejemplo, la determinación de la responsabilidad del acreedor y del responsable del fichero en el momento de la colecta y registro de los datos, la información en la recogida de las informaciones, la notificación de inclusión, el tiempo que un dato puede estar disponible en el sistema, en fin estas normas disciplinan algunos de los aspectos prácticos necesarios para el justo equilibrio de los intereses implicados.

En efecto, son preceptos que en nuestra opinión podrían servir de inspiración al legislador brasileño. Desde nuestro punto de vista la solución dada por la legislación italiana sobre algunas cuestiones referentes a la individualización de la responsabilidad de los acreedores y de las entidades de protección al crédito podrían ayudar a disminuir la carga transferida al Poder Judicial para resolver algunos conflictos

derivados de la omisión legal brasileña. Citemos, por ejemplo, la regla que determina que el gestor solo podrá obtener los datos que serán registrado en el sistema de protección al crédito del participante (art. 4 apartado 1 del Código de deontología) y también aquél que establece que cada participante deberá adoptar las medidas necesarias para comprobar y garantizar que los datos comunicados al gestor puedan utilizarse legalmente en el sistema y además que son exactos y correctos (art. 4, apartado 2 del Código de deontología). Estos dos artículos se constituyen en una individualización de obligaciones y si a ello añadimos la responsabilidad del gestor de verificar la congruencia de los datos a través de un control formal y lógico, la posibilidad de que se incluya un información incorrecta disminuye considerablemente ya que lo que hace la ley italiana es imponer una dupla verificación, implicando tanto el acreedor como el responsable del fichero en la comprobación de los datos que serán registrados en el sistema. Aunque es cierto que al gestor se le impone una obligación menor que la del acreedor, ya que la verificación que tiene que realizar es solamente desde un punto de vista “formal y lógico”. En efecto, no hay en la legislación española una mayor preocupación en este sentido si comparamos con la legislación de Italia, aunque no se puede olvidar que el artículo 43 del RPD enmarca la responsabilidad del acreedor, fijando que este debe asegurarse de la concurrencia de todos los requisitos de inclusión antes de notificar los datos al responsable del fichero así como igualmente debe encargarse de la inexactitud y de la inexistencia de los datos que hubiera facilitado para su inclusión en el fichero. Otro precepto que nos parece muy interesante también de la ley italiana es la obligación impuesta al participante de informar al interesado en el momento de recabar sus datos sobre la posibilidad de incluirlo en un fichero de solvencia patrimonial.

Aparte, también nos ha parecido acertado que el legislador italiano, como se ha indicado, haya fijado un plazo para que se pueda informar los datos de un primero retraso en el pago a un sistema de protección al crédito (artículo 4, apartado 7). En la ley española, aún podríamos citar la

notificación de inclusión de los datos que deberá ser realizada por el responsable del fichero, a través de un medio fiable, auditable e independiente de la entidad notificante, que se la permita acreditar su efectiva realización, y la información previa a la consulta ubicado en el artículo 42.2 del RPD.

Todas estas normas citadas podrían ser perfectamente adaptadas al derecho brasileño, sobre todo en el presente momento en que se discute un proyecto de ley para disciplinar el funcionamiento de los bancos de datos de protección al crédito. Pero mejor que una sencilla adaptación normativa es intentar entender la lógica legislativa de estos países.

De modo que a nuestro sentir y después del estudio de las legislaciones italiana y española, para una mejor tutela del derecho a la protección de datos el primero planteamiento que debería hacer el legislador brasileño es sobre la definición de las responsabilidades de los acreedores y del banco de datos, respectivamente en el momento de la colecta y del registro de las informaciones.

Para el primero caso, se puede notar la importancia conferida por las legislaciones de los mencionados países en que el afectado esté a todo momento informado sobre el destino de sus datos. Como se ha dicho, cuando se trata de datos que no necesitan el consentimiento del afectado el conocimiento de éste sobre el destino de sus informaciones personales cobra una importancia aún mayor, ya que solamente a partir de esta notificación podrá ejercer el poder de control que le es asegurado por el derecho a la autodeterminación informativa.

De un lado, España exige una información previa que es de responsabilidad del acreedor que es la del artículo 39; y una notificación posterior de inclusión que deberá ser realizada por el responsable del fichero, donde acentúa siempre que ésta deberá ser efectuada de modo que pueda ser comprobada la acreditación de su cumplimiento. En el caso

de Italia se exige solamente una información previa de pago efectuada por el acreedor. Desde nuestro punto de vista no es la sencilla declaración del deber de informar que nos ha llamado la atención, pero todos los requisitos impuestos al texto del documento informativo que va desde lo que ordena el régimen general, hasta el tiempo de conservación de los datos en el sistema. Como debe haber tal comunicación a partir del instante en que se solicita un crédito, el afectado ya está informado de todo lo que puede pasar con sus datos en cualquier fase del contrato crediticio.

De cualquier modo, consideramos que la comunicación previa a la inclusión que prevé la reforma legislativa brasileña (PL nº 85/2009) que deberá ser cumplida en el caso por el responsable del fichero, tal y como se plantea alcanza el objetivo pretendido que es por un lado que el deudor tenga conocimiento de donde sus datos serán registrados y asimismo que pueda ejercer sus derechos. Sin embargo, aún no hay disposición sobre la información en el momento de la colecta de los datos hecho que pensamos que debería ser reconsiderado por el legislador brasileño.

De igual manera el aludido proyecto dedica un capítulo al recabo, a la inclusión y a la cesión de las informaciones. Sin embargo, en lo que concierne a la recogida, la norma confiere una atención especial a los datos positivos y a la cuestión del consentimiento y además la comunicación de estas informaciones y de aquellas negativas. No nos parece de todo mal que así lo haga, ya que todo lo que se incluya efectivamente hace falta en el ordenamiento jurídico brasileño en materia de protección de datos. No obstante creemos que hay algunos problemas, u omisiones legales, con relación a los datos negativos que podrían ser solventados ya en este proyecto de ley.

En lo que respecta a las responsabilidades del gestor y del acreedor en el momento de registro de los datos, en ambos países —Italia y España— como ya consignado, están fijadas las obligaciones legales de uno y otro.



Es cierto que hay un matiz que diferencia la legislación española e italiana respecto a este tema que es el deber impuesto por esta última a que el responsable del fichero también ejerza una verificación de los datos aunque formal y lógica. De hecho, la legislación italiana describe exactamente cuáles datos podrán ser registrados en el fichero en el artículo 3 apartado 3 del Código de deontológica. De manera que la verificación del gestor es meramente objetiva y este siempre deberá consultar al acreedor cuando los datos no pasen por el mencionado control formal. Lo que más nos llama la atención en esta sutil, pero importante diferencia entre una y otra norma es que ello evita que los datos estén incompletos o que se registre más información de la que se deberían.

Consideramos que comprometer a los dos intervinientes como lo ha hecho Italia fue una opción bastante interesante y acertada. La reforma legislativa brasileña no contempla la especificación de las obligaciones resultantes del registro de los datos. Es cierto que el texto del proyecto mejora bastante el problema de la comunicación de inclusión (que será tratada más adelante), y también como hemos dicho la cuestión del consentimiento para cada uno de los datos — positivos y negativos — y el registro de datos de fuentes accesibles al público. Lo que no creemos que sea la mejor manera de abordar el problema es, como actualmente prevé la legislación brasileña, dejar a cargo de la labor interpretativa de los preceptos sancionadores para de allí extraer cuáles son las obligaciones de las partes en los sistemas de protección al crédito.

En efecto, la jurisprudencia ya se tiene manifestado entendiendo que el control de la calidad de los datos es de responsabilidad del acreedor, como será analizado más adelante. Justamente por el hecho de que ya haya tenido tantas sentencias a este respecto, es una razón más para que el legislador ya hubiera definido cada una de las responsabilidades.

#### IV. Acceso a la información

El tema que ahora nos proponemos analizar no aparece previsto en ningún precepto de la legislación brasileña que regula el tratamiento de los datos de solvencia patrimonial y crédito.

Ello conlleva a un problema que consideramos extremadamente serio: dejar que los propios bancos de datos se auto regulen en éste sentido. De suerte que no parece que sea la elección más apropiada que los ficheros además de decidir quién puede o no participar del sistema de información al crédito, fijen a su criterio — o bien de manera conjunta con las entidades acreedoras participantes del sistema — la determinación de los casos en que se puede realizar una consulta a su base de datos.

Herman de Vasconcelos Benjamin<sup>625</sup>, tratando sobre este tema señala que los ficheros de solvencia patrimonial se destinan a auxiliar el funcionamiento del mercado de consumo, facilitando las operaciones contractuales entre consumidores y proveedores y consecuentemente no es cualquier persona que puede tener acceso a las informaciones allí archivadas. Así, en su opinión, el acceso depende de que concurren dos condiciones: a) solicitud individual decurrente de b) una necesidad de consumo.

En efecto, aunque los ficheros puedan en sus reglamentos internos preconizar las hipótesis en las cuales se debe proceder a una consulta, no tendrán como fiscalizar si los acreedores están cumpliendo sus recomendaciones así como creemos que no existe ningún interés por parte

---

<sup>625</sup> PELEGRINE GRINOVER, Ada; HERMAN DE VASCONCELOS BENJAMIN, Antonio; *et. al. Código Brasileiro... Op. Cit.*, p. 430.

del responsable del banco de datos ni de disciplinar estos casos ni de inspeccionarlos, ya que su actividad es remunerada y algunas veces se exige el pago de una tasa al acreedor por cada vez que éste accede al sistema.

Analizando las legislaciones española e italiana, hemos podido observar que el acceso a las informaciones por los participantes está absolutamente restringido a situaciones que impliquen efectuar una evaluación de riesgo en una relación de crédito, como es de esperarse, ya que todos los intervinientes tienen el deber de atenerse a la finalidad del fichero. Como ya tuvimos oportunidad de señalar en los capítulos anteriores, la legislación española, en efecto, establece en el artículo dedicado al acceso y consulta de los datos que la consulta por terceros solo podrá ser realizada cuando necesite enjuiciar la solvencia económica del afectado (Art. 42 del RPD). Ya la legislación italiana por su parte declara que el participante puede acceder los datos de un sistema de información para los cuales tenga un interés justificado (Art. 7 del Código deontológico). Tanto una como otra norma establecen en seguida algunos supuestos en los cuales se justifica el acceso a los datos. Uno de ellos que se encuentra en ambos textos legislativo es que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida o que pretenda celebrar un contrato que implique el pago aplazado del precio. La norma española añade también el caso en que se pretenda celebrar un contrato de facturación periódica que no hay similar en la ley italiana ya que en este país no se puede insertar datos derivados de tal supuesto.

El PL nº 85/2009 contiene algunos artículos que parecen poder solucionar algunas cuestiones respecto a la cesión de las informaciones. Además, existen dos artículos en especial en este texto que nos han llamado mucho la atención. El primero es el artículo 8º que prohíbe la cesión al acreedor de información que no sea necesaria para la evaluación del riesgo crediticio del interesado y en el caso de persona jurídica

también de sus relaciones comerciales. Tal precepto debe ser leído conjuntamente con el artículo 15 que establece que el acreedor solamente podrá acceder a informaciones constantes en los bancos de datos del afectado con los que mantenga una relación comercial o crediticia.

Indudablemente consideramos que estos dos artículos fijan un antes y un después en el tema del acceso a las informaciones dentro de la sistemática legislativa brasileña. No obstante pensamos que hubiera sido mejor fijar algunos supuestos como lo hacen la legislación italiana y española, principalmente para que se pudiera diferenciar los supuestos especiales de las personas jurídicas. Además, el texto del artículo 15 no nos parece muy afortunado si consideramos que la consulta podrá ser realizada —y con más frecuencia— cuando los interesados todavía no tienen perfeccionada la relación crediticia, es decir, en los casos en que se solicitan un crédito. Sin embargo, la declaración legal sobre que el acceso solamente se justifica cuando haya relación comercial o crediticia ya confiere una mejora significativa para que se eviten abusos en la consulta a las informaciones registradas en estos ficheros.

Por otro lado, no serán estos todos los datos a los que los participantes podrán tener acceso, lo que nos hace creer que los responsables del fichero tendrán que tomar las medidas técnicas y organizativas necesarias para impedir la cesión de los datos que no sean necesarios para enjuiciar el riesgo crediticio del afectado. Así, consideramos que entre ellos estará el dato del participante que ha comunicado las informaciones al fichero. De suerte que si en efecto no hay ningún cambio en el proyecto de ley, aunque sean los mencionados preceptos declaratorios, es decir, sin que conste ninguna hipótesis específica se asemejará mucho a la legislación italiana.

Aparte de los mencionados dispositivos, el PL nº 85/2009 también incluye en el texto la posibilidad de cesión de información a otros bancos de datos. De hecho, prohíbe que los responsables del fichero exijan de los

participantes exclusividad de las informaciones. Tal dispositivo no encuentra uno similar ni en el apartado de regulación específica de los ficheros de morosos en España ni en el Código de Deontología de Italia. Desde nuestro punto de vista, esta regla tiene la finalidad de proteger la competencia. En efecto, no tiene ningún sentido que se exija exclusividad de las fuentes, ya que la finalidad de la actividad es la protección del mercado de crédito y también como consecuencia del tráfico mercantil y mismo realizada por entidades privadas (aunque en caso de Brasil con carácter público), no se podría conseguir que ejerciera su función social si la competencia no fuese libre.

Resulta oportuno señalar sobre este tema, la decisión del Tribunal de la Competencia<sup>626</sup>, el caso del fichero RAI en España. Examinando la cuestión específica del intercambio de información, el aludido Órgano juzgador entendió que los acuerdos restrictivos de la competencia solo se pueden autorizar en virtud de ley si contribuyen con la mejora de la producción o la comercialización de bienes y servicios, o a promover el progreso técnico o económico, *siempre que permitan a los consumidores o usuarios participar de forma adecuada de sus ventajas, no impongan a las empresas interesadas restricciones que no sean indispensables y no consientan a las empresas partícipes la posibilidad de eliminar la competencia respecto de una parte sustancial de los productos o servicios concernidos*. De modo que el fichero RAI, según el Tribunal “al estar reservado su acceso a las entidades partícipes con exclusión, incluso, de los acreedores, no proporciona suficiente participación en las ventajas del acuerdo a los consumidores y usuarios; que las condiciones impuestas a los partícipes del acuerdo son innecesariamente restrictivas y que existe la posibilidad de una eliminación de la competencia en el mercado de informes patrimoniales y de solvencia económica, si se discrimina en el acceso al RAI entre las empresas del sector”.

---

<sup>626</sup> Tribunal de Defensa de la Competencia. Caso RAI. Resolución de 9 septiembre 2002 (JUR 2002\230127).

De este modo, nos parece que las mismas razones que inspiraron la decisión del Tribunal nos pueden servir como fundamento del dispositivo en análisis. Es decir, la imposibilidad de imponer a las empresas participantes restricciones que no sea estrictamente necesarias para cumplir con la finalidad de mejorar la prestación del servicio a cual se dedica.

Ahora bien, según el PL, hay algunos casos en los que otro responsable del fichero, cuando ha recibido de otro banco de datos informaciones a través de intercambio, puede equipararse al gestor que originariamente anotó la información a todos los efectos de la ley, incluso en lo que respecta a la responsabilidad solidarias por eventuales perjuicios causados, así como al deber de observancia de los derechos de los interesados constantes tanto en el texto del aludido proyecto, como aquellos dispuestos en el Código de Defensa del Consumidor. En lo tocante a la actualización de los datos, es de responsabilidad del gestor originario informar a los ficheros con quienes intercambia información de sus respectivas alteraciones.

## **V. Conservación y actualización de los datos**

El Código de Defensa del Consumidor dedica el párrafo 1º y el 5º del artículo 43 para fijar el tiempo de conservación de los datos personales en un fichero de solvencia patrimonial y crédito.

De modo que hay dos plazos que conviven en el dispositivo legal: a) uno de cinco años ubicado en el aludido párrafo 1º; y b) cuando se consume en la prescripción relativa al cobro de la deuda.

Consideramos que la solución dada por el legislador brasileño, a vista de lo estudiado anteriormente del derecho español e italiano, es la más equitativa tanto desde el punto de vista del derecho del afectado, como del acreedor.

Ya hemos señalado, en España el plazo de conservación es único, de seis años contados a partir del vencimiento de la obligación o del plazo concreto si aquella fuera de vencimiento periódico. En Italia, la solución apuntada parte de supuestos fácticos, y a partir de ellos se fijan diversos plazos que varían de seis meses a treinta e seis meses dependiendo si respecta a una solicitud de crédito o a un incumplimiento considerado grave.

De suerte que por un lado, consideramos que seis años es un plazo demasiado largo si tenemos en cuenta que la eficiencia de un fichero de protección al crédito reside también en mantener los datos correctos y actualizados. Por otra parte, el sistema italiano fija plazos menores, sin embargo creemos que el sistema de actualización acaba por penalizar el interesado.

Así, la elección brasileña nos parece la más sencilla y acertada. Son fijados dos plazos, debiendo observar el responsable del fichero aquél que primero ocurra. Según señala Herman de Vasconcelos Benjamin<sup>627</sup>, ningún dato negativo puede superar los cinco años, siendo este la vida útil máxima y genérica de cualquier información incluida. Cinco años nos parece tiempo suficiente para que un dato se conserve en un sistema de protección al crédito. Además, la elección de incluir el plazo prescripcional entre las opciones normativas es muy elogiable. Si el acreedor no ha hecho ninguna gestión para obtener su crédito, y se ha consumada la prescripción, no hay motivo relevante algún para que la

---

<sup>627</sup> PELEGRINI GRINOVER, Ada; HERMAN DE VASCONCELOS BENJAMIN, Antonio, et al. *Código Brasileiro de Defesa do Consumidor: comentado pelos autores do anteprojeto*. Rio de Janeiro: RT, 2004, p. 443.

información registrada continúe a generar efectos negativos al afectado, cuando aquél que tiene el derecho y el interés en que la deuda sea satisfecha se ha quedado inerte.

Sobre este tema, el texto del PL n° 85/2009 mantiene el plazo de los cinco años, fijando la fecha en que se inicia su computo, en el caso cuando vence la obligación. Ahora bien, el PL no incluye el plazo de la prescripción como opción del tiempo de conservación de los datos. Sin embargo, creemos que si el texto tal y como se encuentra ahora fuese aprobado y publicado, la regla del CDC continuaría en vigor, ya que el propio PL en el artículo 1º señala que: *esta ley disciplina la actuación de los bancos de datos de protección al crédito y de relaciones comerciales, así como su relación con los interesados, fuentes de informaciones y participantes, sin perjuicio de lo dispuesto en la Ley n° 8.078, de 11 de septiembre de 1990 – Código de Defensa del Consumidor.*

Resulta oportuno señalar algunas consideraciones sobre el inicio del cómputo del plazo. La ley silencia sobre este aspecto. Para Herman de Vaconcelos Benjamin<sup>628</sup>, empieza a contarse de la data de vencimiento de la deuda. Del mismo modo Roscoe Bessa<sup>629</sup> señala que el termo inicial del plazo debe coincidir con el momento en que es posible efectuar la inscripción de la información en los bancos de datos de protección al crédito: un día después del vencimiento de la deuda.

La jurisprudencia, sin embargo, tiene una interpretación distinta. El *Superior Tribunal de Justiça*<sup>630</sup>, en Sentencia de 16 de mayo 2003 ha consignado que el registro deberá ser mantenido en el fichero por un periodo máximo de cinco años a contar de la data de su inclusión. En el

---

<sup>628</sup> *Ibid.*, p. 450.

<sup>629</sup> ROSCOE BESSA, Leonardo. *O consumidor... op. cit.* pp. 211-212.

<sup>630</sup> STJ. REsp 473873. Rel. Min. Nancy Andrighi. Publicado en 16 de mayo 2003.



mismo sentido la Sentencia de 23 de junio 2004<sup>631</sup> del mismo Tribunal, que ha manifestado que las informaciones adversas deben ser excluidas después del quinto año de su registro. Los fallos más recientes señalan el mismo entendimiento, como la de 23 de junio 2009<sup>632</sup>, en que se ha determinado que el cómputo del plazo prescripcional debe observar la efectiva inclusión en el fichero restrictivo de crédito, no el vencimiento de la deuda.

No compartimos la posición adoptada por el aludido Órgano juzgador. En el sistema jurídico brasileño, el único requisito exigido que tiene la capacidad de interferir en el tiempo del cómputo del plazo de conservación del registro es la comunicación previa que puede ser realizada a cualquier momento después del incumplimiento de la obligación. De este modo, una vez cumplida ésta obligación, el acreedor puede en un plazo muy corto ejercer su derecho a incluir los datos del deudor en un fichero de moroso. Si no lo hace, ello tendrá sus consecuencias, como así lo es para los plazos prescripcionales de las acciones de cobranza de la deuda. Consideramos que la posición del STJ permite premiar el acreedor por su inercia en ejercer un derecho legalmente reconocido alargando el tiempo de conservación de la información. Por lo tanto, no nos parece que el registro del dato deba ser el punto de partida del tiempo de manutención de la información, pero sí el día del vencimiento de la deuda.

El Proyecto de Ley nº 85/2009 pretende resolver este problema, ya que establece en el artículo 13 que el plazo de cinco años empieza a ser contado de la fecha de vencimiento de la obligación.

En lo que concierne a la actualización de los datos, el CDC no fija ninguna regla especial. Lo que sí establece en el párrafo 3º del artículo 43

---

<sup>631</sup> STJ. REsp 472203/RS. Rel. Min. Humberto Gomes, juzgado en 23 de junio 2004.

<sup>632</sup> STJ. AgRg en el Ag 713.629/ES. Rel. Min. Paulo Furtado, juzgado en 23/06/2009.

es que el consumidor siempre que encontrar inexactitud en sus datos podrá exigir su inmediata corrección. No consideramos que éste sea un precepto que determine la responsabilidad por la actualización de los datos al propio consumidor, sino que establece un derecho de control de la calidad de los datos a su titular, que consiste en rectificarlos.

Según opina Herman de Vasconcelos Benjamin<sup>633</sup>, se responsabiliza al acreedor cuando suministra datos falsos, incompletos, inexactos, imprecisos o engañosos. El responsable del fichero responde por el incumplimiento de los deberes relacionados a los derechos básicos del interesado. Por fin, es de responsabilidad tanto del acreedor como del gestor velar sobre los requisitos de inclusión de los datos. No obstante, señala el autor que en cualquier modalidad de responsabilidad, el régimen adoptado es el de solidaridad, como determina la regla del artículo 7º del CDC.

En el mismo sentido Roscoe Bessa<sup>634</sup> manifiesta que todos los presupuestos que legitiman el registro son dirigidos a todos los que participan del tratamiento de la información. De suerte que a su sentir, todos contribuyen por acción u omisión para la difusión del registro y se aplica la regla de la solidaridad prevista en el Código Civil en su artículo 942 y el artículo 7º del Código de Defensa del Consumidor.

Así, se puede inferir de este pensamiento que la actualización de los datos es de responsabilidad de aquél que suministra, es decir, el acreedor pero que en el momento de requerir la responsabilidad, podrá el banco de datos responder solidariamente.

---

<sup>633</sup> PELEGRINI GRINOVER, Ada; HERMAN DE VASCONCELOS BENJAMIN, Antonio; et al. *Código Brasileiro de Defesa do Consumidor: comentado pelos autores do anteprojeto*. Rio de Janeiro: RT, 2004, p. 471.

<sup>634</sup> ROSCOE BESSA, Leonardo. *O Consumidor... op. cit.*, p. 250.

En efecto, desde la perspectiva del derecho del consumidor ésta interpretación es perfectamente válida y hoy por hoy es la que mejor tutela los derechos implicados en la sistemática jurídica brasileña. Sin embargo, si analizamos la problemática desde la óptica del derecho a la protección de los datos, es de fundamental importancia la determinación de responsabilidades por la ley, como hemos matizado anteriormente al analizar los requisitos de inclusión de los datos.

El servicio de prestación de informaciones crediticia es una actividad extremadamente delicada y compleja, que implica muchos intereses, derechos y deberes por todos aquellos que de modo directo o no, participan del sistema. Además, tal actividad se organiza de manera muy particular, como un engranaje donde todas sus piezas tienen que funcionar a perfección.

Así, a cada uno de los implicados en el sistema de protección al crédito debe ser detallada su función y sus responsabilidades. Y, en este caso preciso de actualización de los datos, entendemos que debe corresponder a aquél que los suministra. Primero, porque es el acreedor quien tiene más interés y beneficios derivados de la inclusión de una información en el fichero; de otra parte, es él quién puede controlar la evolución de la deuda. No es posible transmitir tal obligación al responsable del fichero cuando legalmente éste no puede acceder al banco de datos del acreedor y sus clientes y acompañar el progreso del cumplimiento del contrato.

La reciente Sentencia de 19 de mayo 2009<sup>635</sup> del *Superior Tribunal de Justiça*, ha señalado que la responsabilidad por la cancelación de los datos en el fichero es del acreedor. Su inercia en proceder a la actualización de las informaciones genera el deber de indemnizar. De igual modo, el mismo Órgano Juzgador, y la Sentencia de 21 de febrero 2008<sup>636</sup>, han

---

<sup>635</sup> STJ. AgRg em Ag 1094459/SP, Rel. Min. Sidnei Beneti, juzgado en 19/05/2009.

<sup>636</sup> STJ. RESP 994.638/AM, Rel. Min. Aldir Passarinho Junior, juzgado en 21.2.08.

consignado que cabe a las entidades acreedoras que hacen uso de los servicios de información de protección al crédito mantenerlos actualizados, de suerte que una vez recibido el pago de la deuda, deben providenciar en un breve espacio de tiempo, la cancelación del registro.

Resulta oportuno señalar que los dos sistemas legislativos estudiados han establecido con claridad tal responsabilidad. En España, el RPD (Art. 43.2) ha fijado la responsabilidad del acreedor o quien actúe por su cuenta o interés por la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero. En Italia, el participante debe actualizar una vez al mes los datos informados a un fichero (Art. 4.8 del Código de Buena Conducta).

Ahora bien, la regla sería que aquél que comunica los datos debe también responsabilizarse por su actualización. En el caso de las informaciones recabadas en las fuentes públicas, no puede haber excepción. Ningún dato puede estar en un fichero desactualizado. Hay que tenerse en cuenta que al inserir una información negativa de determinado ciudadano en los ficheros de moroso de Brasil, ello equivaldrá inmediatamente a la imposibilidad de solicitar cualquier tipo de crédito, en cualquier parte del país. Significando de este modo una total exclusión del afectado en el mercado de consumo.

De suerte que al proceder la recogida de datos de los boletines oficiales o directamente en la notaría, en nuestra opinión, el responsable por el fichero no podrá excusarse de cumplir sus deberes, escudado en el origen público de la fuente. Consideramos que si éste desea que su banco de datos contenga informaciones sobre los procesos judiciales de cobro de deuda existentes, habrá de tener la cautela mínima de actualizar estos datos, informar previamente al afectado y permitir que este ejerza todos los derechos que entienda necesarios.

En lo que concierne a los datos recabados en las fuentes accesibles al público, el PL nº 85/2009 no dedica ningún precepto que discipline la obligatoriedad de su actualización. A nuestro sentir, éste es un supuesto que debería merecer una atención especial por el legislador. Son diversos los problemas de interpretación que conlleva la recogida de datos de tales fuentes: ausencia de consentimiento, necesidad de comunicación al afectado, actualización de las informaciones, reglas para su cesión, en fin, planteamientos que no pueden estar al margen de la preocupación del legislador.

No obstante ello, hay que resaltar que el aludido proyecto solventa algunas otras cuestiones relativas a los datos suministrados por el acreedor y su procedimiento de actualización. Pero no fija con precisión legislativa las responsabilidades de cada uno —acreedor y responsable del fichero— pero por el conjunto normativo se puede inferir que el pensamiento del legislador es involucrar estas dos partes en el deber de poner los datos al día. En el procedimiento establecido en el citado texto, los participantes tendrán 5 días laborales para informar a los gestores la regularización de la obligación por parte del deudor. A su vez, el responsable del fichero deberá proceder la inmediata actualización en su sistema.

Al deudor se le faculta para dirigirse directamente al banco de datos y mediante documento probatorio de cumplimiento de la obligación, deberá el responsable proceder la inmediata actualización.

A nuestro sentir, es criticable que el legislador no fije claramente las responsabilidades de todos los implicados en el sistema de información de crédito y termine con cualquier tipo de dudas que notadamente surgieran tanto expresadas por la doctrina como materializadas concretamente cuando se analiza las sentencias de los Tribunales. Es un punto que creemos que debería ser reconsiderado en el proyecto de ley.

## VI. Los derechos del afectado

### 1. El derecho al acceso

El *caput* del artículo 43 del Código de Defensa del Consumidor establece como primero derecho del afectado el de acceso y pretende conferirle la mayor amplitud posible, cuando establece que el consumidor tendrá acceso a cualquier tipo de informaciones que existan en catastros, fichas, registros y datos personales y de consumo guardados sobre él, así como sus respectivas fuentes.

Ya hemos consignado repetidas veces que el Código brasileño del consumidor ha intentado crear un microsistema de protección de datos, dentro de su ámbito, y que a su momento tuvo una gran importancia para definir límites de la prestación del servicio de datos personales crediticios.

Sin embargo, diferentemente de la ley española que trata del tema, no hay en la norma brasileña la conceptualización de este derecho, ni los límites que deben ser observados al respecto. De suerte que no existe en el Código del Consumidor nada más que una declaración del derecho al acceso, sin que se pormenore los detalles de cómo deberá proceder el interesado en el caso de que quiera ejercerlo.

Ello trae un problema ya que, como se verá más adelante, el procedimiento general establecido por la ley del *Habeas Data* no es suficiente para sanar todas las cuestiones que pueden surgir en el intento del interesado en ejercer su derecho de acceso. Uno de ellos es con

relación al plazo máximo que deberá ser contestada la solicitud del afectado.

Resulta oportuno señalar que el derecho de acceso está íntimamente relacionado con el procedimiento administrativo y la acción del *Habeas Data*. De suerte que es común encontrar en la doctrina brasileña referencias directas a éste instituto cuando se habla del derecho de acceso. De modo que es un derecho que está constitucionalmente garantizado y así lo ha entendido el *Tribunal Regional Federal da 2ª Região*<sup>637</sup> que ha manifestado que el acceso a las informaciones sobre hechos relativos a la persona del afectado es garantía constitucional fundamental que tiene la misma amplitud del bien jurídico de la libertad, asegurado como derecho inherente al hombre desde del principio del desarrollo de las doctrinas jurídicas. Además, el fallo consigna que una vez no se respeten los principios constitucionales se estaría negando vigencia al propio Estado Democrático de Derecho.

Con relación específicamente al precepto del Código de Defensa del Consumidor Roscoe Bessa<sup>638</sup>, señala que cualquier persona puede dirigirse a las entidades responsables por la administración de los bancos de datos de protección al crédito y exigir que sean informadas sobre la existencia o no de los registros concernientes a sí mismo. Si los hay, continua el autor, el consumidor tiene derecho a saber el contenido de los datos así como en la indicación de la respectiva fuente.

Desde nuestro punto de vista, lo que necesita el ordenamiento jurídico brasileño es más que la mera declaración de un derecho ya asegurado en

---

<sup>637</sup> TRF 2ª Região. Processo nº: 2000.02.01.055404-6. Rel. Des. Frederico Gueiros. J. 17 de junio de 2009.

<sup>638</sup> ROSCOE BESSA, Leonardo. "Banco de Dados de Consumo". En: HERMAN DE VASCONCELOS BENJAMIN, Antonio; LIMA MARQUES, Claudia; ROSCOE BESSA, Leonardo. *Manual De Direito do Consumidor*. São Paulo: Revista dos Tribunais, 2008, p. 262.

la esfera constitucional, pero en el ámbito de una ley infraconstitucional establecer los matices específicos que requiere la actividad de información de datos sobre la solvencia patrimonial y crédito de los interesados que, incluso, pueden o no ser considerados consumidores. Es decir, para que se tenga acceso a las informaciones registradas en un fichero de esta especie, no es necesario que el interesado esté dentro de la concepción de lo que se entiende por consumidor. Esta es una limitación inaceptable porque la Constitución no la hace, y además los datos de cualquiera pueden ser usados de modo fraudulento sin que el afectado nunca haya estado en la condición de consumidor.

Sobre este último punto, parece que el legislador pretende solventarlo con el texto del Proyecto de Ley nº 85/2009. Sin embargo, el artículo 16 de tal proyecto no hace ninguna mención sobre el procedimiento de los derechos del afectado. Así que una vez aprobado el texto, se continuará con los mismos problemas derivados de esta omisión.

Sobre el aludido proyecto de ley, hay que resaltar lo que puede venir a ser una importante novedad en el sistema legislativo brasileño tocante al derecho de acceso del ciudadano que es determinar específicamente de qué el gestor tiene obligación de informar al interesado cuando acuda a éste para ejercer su derecho. De suerte que el párrafo 2º del artículo 16 texto le obliga a suministrar: a) informaciones constante sobre el afectado en el momento de la solicitud; b) indicación de las fuentes relativas a las citadas informaciones incluyendo la dirección y el teléfono para contacto; c) la indicación de los banco de datos con los cuales las informaciones fueron comunicadas; d) la indicación de todos los participantes del sistema que tuvieron acceso a cualquier información sobre el interesado en los últimos seis meses anteriores a la solicitud; e) una copia del texto que contenga resumidamente sus derechos con relación a los banco de datos, así como la lista de los órganos de la Administración a los cuales puede acudir en el caso de que considere que sus derechos fueron violados.



A nuestro sentir, hay dos obligaciones que fueron aquí ya indicadas que nos parecen muy elogiables, fundamentalmente si tenemos en cuenta el uso abusivo de las cesiones de datos de los sistemas de información crediticia en Brasil y que deben ser leídas conjuntamente con lo que prevé el artículo 8 del mismo PL, que prohíbe la cesión de datos cuando no sea necesaria para la evaluación del riesgo de crédito. La primera, informar al afectado tanto los ficheros como los participantes que accedieron a sus datos. Pensamos que este precepto podrá evitar o por lo menos ayudará a que disminuya el acceso de datos registrados en los ficheros de morosos con quienes el interesado nunca mantuvo cualquier relación de crédito o incluso de prestación de servicio. Es decir, para finalidades distintas para los cuales fueron estos ficheros creados. Por citar un ejemplo, en Brasil es práctica común (y desde nuestro punto de vista abusiva) el uso de la consulta a un fichero de solvencia patrimonial de informaciones sobre los candidatos de a un puesto de trabajo en una empresa privada asimismo de aquellos que se presentan a oposiciones de cargos públicos. O incluso para cualquier otra finalidad, ya que hay muchos servicios a través de Internet que ofrecen el servicio de consulta de datos a cualquier persona, siendo suficiente tener el número del NIF (CPF, en Brasil) de la persona que se quiere tener las informaciones<sup>639</sup>.

La segunda, el suministro de la lista de los órganos de la Administración en los cuales puede acudir en caso de violación del

---

<sup>639</sup> Como por ejemplo, la pagina *web* [www.consultaja.com.br](http://www.consultaja.com.br). Tal sitio ofrece el servicio de consulta a los principales banco de datos de protección al crédito de Brasil, cobrando un valor de R\$25,00 (veinte y cinco Reales). Según la propia página, “una vez elegida la opción (*de consulta*) deseada, basta con informarnos a través del correo electrónico el número del documento (CPF o CNPJ) a ser consultado, enviándonos junto el comprobante de pago”. Exactamente así de sencillo es hoy en Brasil acceder a las informaciones en un sistema de protección al crédito. Lo más curioso, sin embargo, es que según la propia página *web*, “este sitio pertenece al IBRADDIC - *Instituto Brasileiro em Defesa dos Direitos do Cidadão*. Entidad sin fines lucrativos, reconocida por el Ministerio de Justicia - Brasilia - DF.”

derecho, que igualmente nos parece que tiene una gran utilidad si tenemos en cuenta que la ausencia de una Agencia de protección de datos a estilo de España o Italia, de cierto modo dificulta para el ciudadano saber donde debe dirigirse para presentar su denuncia por la violación de sus derechos.

## 2. El derecho de rectificación

El párrafo 3 del artículo 43 del Código de Defensa del Consumidor establece que siempre que un consumidor encuentre alguna inexactitud en sus datos podrá exigir su inmediata corrección, y establece un plazo de cinco días para que el responsable del fichero informe a todos los participantes a los cuales se les hayan cedidos tales datos sobre su alteración.

Ésta es la única mención del dispositivo de la ley brasileña específica de los ficheros de moroso tocante al derecho de rectificación. De otra parte, de la misma manera que el derecho de acceso, la Constitución Federal también prevé el derecho a la rectificación de los datos (Art. 5º, inciso LXXII, letra *b*) y por lo tanto los afectados deberán someterse a lo que esté dispuesto en la ley del *Habeas Data*, procedimiento que analizaremos más adelante.

De cualquier modo, de nuevo nos encontramos ante declaraciones de derechos que poseen el interesado. Es incluso difícil intentar establecer cualquier comparación con el sistema italiano y español, porque el cuerpo legislativo de las leyes de protección de datos de estos países conllevan un gran aparato normativo que se pone a disposición del interesado para el

ejercicio de sus derechos, como la posibilidad de ejercerlo no solamente frente al acreedor, pero también al titular del fichero o, en el caso de España, a cualquier otro participante del sistema. Así, la doctrina y la jurisprudencia, y sobre todo esta última, poseen una gran carga de responsabilidad por la omisión legislativa en determinados puntos.

Para Sacco Neto<sup>640</sup>, la rectificación debe ser comprendida en sentido amplio, abarcando medidas como la sustitución de los datos, cancelación de informes, inclusión de registros adicionales o complementación de la información, etc.

La ley brasileña no fija otros derechos como lo hace la norma española que distingue el citado derecho de rectificación, del derecho de cancelación. Así, mejor que la interpretación que se recoga en el texto legal de Brasil sea la más amplia posible, como modo de compensar la ausencia de una mejor técnica legal. Y en este sentido, aunque sea elogiada esa actitud de la doctrina, no nos parece que el derecho a la rectificación sea suficiente para englobar todos los derechos que a él se quiere atribuir.

En España, como ya hemos visto, el derecho de rectificación es aquél que comprende la modificación de los datos que resulten inexactos o incompletos y el derecho de cancelación es aquél en que se suprimen los datos que resulten inadecuados. El RPD en su artículo 5 establece que la cancelación es el procedimiento en virtud del cual el responsable cesa en el uso de los datos. Ésta implicará en el bloqueo de los datos, “consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de

---

<sup>640</sup> SACCO NETO, Fernando. *Cadastrós... op. cit.*, p. 113.

prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos”.

A su vez, Italia garantiza al interesado el derecho a la cancelación, o a la transformación de la información en forma anónima o el bloqueo de los datos tratados ilegalmente, incluidos los que no son necesarios su conservación en relación a los fines para los que fueron recogidos o sucesivamente tratados.

De suerte que no nos parece que el derecho a la rectificación tenga fuerza conceptual para asumir, por ejemplo, el deber de bloqueo de los datos, o el anonimato de estos. El propio procedimiento brasileño de rectificación, como se verá más adelante, es muy sencillo, de modo que no tiene como extenderse para ayudar a una mejor sistematización de cuales derechos realmente estarían dentro de su órbita.

Si a todo ello añadimos el derecho de oposición, muy bien conceptuado por el RPD como el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese el mismo, dejamos la legislación brasileña en una situación aún más complicada.

En la opinión de Sacco Neto<sup>641</sup>, el derecho a la oposición (especie) es una de las formas de ejercicio del derecho a la rectificación (genero). No estamos de acuerdo con esta posición. La esencia del derecho a la rectificación es la modificación de los datos para que estos reflejen con veracidad la situación actual del interesado. El fundamento del derecho de oposición, según se extrae de la norma española (art. 34 del RPD) y de la norma italiana (art. 7, apartado 4, letras *a* y *b* del *Codice in materia de protezione dei dati personali*) no reside en el cambio de información. Está mucho más vinculado al consentimiento, es decir, al derecho que tiene el interesado a no permitir que sus datos sean tratados si se encuentran dentro de algunos supuestos previamente fijados por la ley. La

---

<sup>641</sup> SACCO NETO, Fernando. *Cadastrós... op. cit.*, p. 110.

rectificación, desde nuestro punto de vista, estaría relacionada a la calidad de los datos, o sea, al derecho que tiene el interesado de que sus informaciones reflejen la veracidad de su situación, que sean exactos y puestos al día. De ésta manera, no nos parece que sea posible extender la interpretación de uno y de otro derecho a punto de que se tornen especie y género sin que exista alguna característica común que se les pueda atribuir.

En lo que concierne al PL nº 85/2009, no se habla de un derecho a la rectificación, pero un derecho a “impugnación” de los datos. El texto no explica que es este derecho de impugnación, pero todo el artículo 17 y 18 gira en torno a cambios o alteraciones de los datos, lo que supone que se trate del mismo derecho a la rectificación. Es difícil inferir la razón por la cual el legislador no pretende continuar a utilizar esta última acepción. Quizás esté intentando extender lo máximo posible el alcance del derecho a la rectificación, a través de un “procedimiento de impugnación”. En nuestra opinión si ésta es la razón, nos parece que no tendrá ningún resultado práctico relevante el sencillo cambio de nombre. Es decir, manteniendo como procedimiento de rectificación, no habrá ninguna modificación en el alcance de tal derecho si se analiza el texto de los aludidos artículos. Lo que sí habría sido más útil era incluir en este procedimiento de impugnación tanto el derecho a la cancelación de los datos como el derecho a la oposición, y así entenderíamos justificable el cambio de nombre que pretende el texto del proyecto. De cualquier manera, el hueco legislativo del procedimiento de rectificación sería solventado.

Creemos que para compensar las obligaciones impuestas que indudablemente supondrán un incremento en el coste del banco de datos, el proyecto de ley faculta al gestor la implantación de sistema electrónico, por teléfono o por otros medios que permitan al interesado consultar y actualizar sus informaciones a través de claves.

### 3. El derecho de información.

El Código de Defensa del Consumidor establece como derecho del afectado la comunicación del registro de datos que le concierne, siempre que no sea solicitada por el propio afectado (art. 43 §2º). Para Sacco Neto<sup>642</sup>, hay varias razones que justifican ese derecho del consumidor de ser comunicado sobre las informaciones personales registradas en un fichero, entre ellas, la protección de derechos de la personalidad y la posibilidad de que el interesado ejerza sus derechos. En la opinión de Rizzato Nunes<sup>643</sup>, esta garantía se deriva directamente del texto constitucional de preservación de la privacidad del consumidor (art. 5º X).

Desde nuestro punto de vista, el derecho a la comunicación (o información) procede de un derecho fundamental que se encuentra perfectamente asegurado en la Constitución Federal, que hemos defendido en este trabajo de investigación en el capítulo 1, que es el derecho a la autodeterminación informativa. Así, para que el interesado pueda controlar sus datos necesita o bien consentir su tratamiento, o bien, como en el caso de los datos aquí estudiados, en la ausencia de la exigencia legal del consentimiento, debe ser informado de que sus informaciones serán registradas, tratadas y cedidas en un fichero.

El Código de Defensa del Consumidor solamente ha dedicado, así como con los otros derechos, un precepto que poco aporta más allá de su

---

<sup>642</sup> SACCO NETO, Fernando. *Cadastrados... op. cit.*, p. 84.

<sup>643</sup> RIZZATTO NUNES, Luiz Antonio. *Curso de Direito do Consumidor*. São Paulo: Saraiva, 2007, p. 562.

reconocimiento como un derecho del interesado. La consecuencia de la escasa normativa sobre el tema, resulta en la aparición de algunos problemas de orden práctico. Uno de ellos es el momento en el cual debe procederse la comunicación. Con la omisión legal, la jurisprudencia de forma mayoritaria tiene entendido que la información al deudor deberá ser realizada antes de que sean los datos registrados.

En efecto, el Superior Tribunal de Justicia<sup>644</sup> ha manifestado que en la sistemática del Código de Defensa del Consumidor es imprescindible la comunicación al consumidor del registro en el fichero de protección al crédito. Con independencia de la condición que el deudor ostente idóneo o no, fiador o avalista— tiene el derecho a ser informado a respecto de los datos negativos registrados a su nombre. Para que la comunicación sea garantista y ultime el fin a que se destina deberá ser efectuada antes del registro de la deuda en retraso. En el mismo sentido, la otra Sala<sup>645</sup> del mismo Tribunal ha decidido que la inscripción del nombre del deudor en el fichero SERASA deberá ser precedida de la comunicación exigida en el art. 43, §2º do Código de Defensa del Consumidor. Según Rizzato Nunes<sup>646</sup>, tal aviso deberá ser remitido al afectado con una antelación mínima de cinco días. No obstante, ésta es una interpretación que hace el autor por analogía al precepto que viene justo después, relativo al derecho de rectificación que fija un plazo de cinco días para que el responsable del fichero comunique eventual alteración de los datos rectificadas a aquellos a los que hayan sido cedidos. Sacco Neto<sup>647</sup> asimismo señala que tal argumento es pertinente y añade que el plazo debe ser contado a partir de la fecha en que el consumidor reciba tal comunicación.

---

<sup>644</sup> STJ. REsp 402.958/DF, 3ª Turma, Rel. Min. Nancy Andrighi, DJ 30/09/2002.

<sup>645</sup> STJ. REsp 373.219/RJ, 4ª Turma, Rel. Min. Sálvio de Figueiredo, DJ 12/08/2002.

<sup>646</sup> RIZZATTO NUNES, Luiz Antonio. *Curso ... op. cit.*, p. 563.

<sup>647</sup> SACCO NETO, Fernando. *Cadastro... op. cit.*, p. 86.

Otro punto que nos parece oportuno comentar es la atribución de la responsabilidad de la comunicación al afectado. En sentencia de 19 de abril de 2001<sup>648</sup>, el STJ había consignado que era responsabilidad de la entidad administradora del fichero informar al afectado el registro de sus datos. En efecto, el Tribunal manifestó en aquella oportunidad que: *la existencia del protesto es un hecho que se atribuye a quien ha llevado el título al notario; la irregularidad de su lanzamiento debe ser atribuida al notario; la creación de un título sin causa, a su emisor; pero la responsabilidad por el registro indebido de los datos en un fichero es de aquél que inserta las informaciones.* Continúa el fallo añadiendo que si la información es colectada de una publicación oficial, por iniciativa del administrador del banco de datos, se acentúa aún más su obligación de comunicación.

Algunas voces doctrinales<sup>649</sup>, sin embargo, defienden que el precepto del Código de Defensa del Consumidor no establece el destinatario de tal obligación, porque lo importante es que el consumidor sea efectivamente comunicado. En nuestra opinión, actualmente tal y como está redactada la ley, no se puede atribuir la responsabilidad exclusiva al responsable del fichero. De suerte que también entendemos que hay, ahí, una obligación solidaria entre el acreedor y el gestor del banco de datos.

No obstante, ésta no es una posición pacífica. Según Passarinho Junior<sup>650</sup>, por la naturaleza de los bancos de datos y en consonancia con el art. 43, parágrafo 5º, del CDC, estas son entidades de carácter público, teniendo ellas la responsabilidad específica y exclusiva por actos que

---

<sup>648</sup> STJ. Resp 285401/SP. Rel. Min. RUY ROSADO DE AGUIAR, J. 19/04/2001.

<sup>649</sup> Vide ROSCOE BESSA, Leonardo. *O consumidor... op. cit.* p. 199 y SACCO NETO, Fernando. *Cadastrros... op. cit.* p. 87.

<sup>650</sup> PASSARINHO JUNIOR, Aldir Guimarães. “Cadastrros de consumidores: questões controvertidas sob a ótica do Superior Tribunal de Justiça”. Jus Navigandi, Teresina, ano 11, n. 1258, 11 dez. 2006. Disponible en:

<http://jus2.uol.com.br/doutrina/texto.asp?id=9177> [Consulta en 22 abr. 2010].



únicamente es de su competencia y no a los acreedores que hacen uso de sus servicios. Para el autor, quién registra el dato es la el responsable del fichero, de suerte que si es este el acto que tiene que ser informado al consumidor, la obligación debe estar con quién concretamente promueve dicho acto y no el acreedor que solamente requiere el registro.

Pese a que el Código de Defensa del Consumidor solamente se refiera a una comunicación que es aquella que se realizará cuando se vaya a proceder el registro de los datos, la interpretación de la norma brasileña se asemeja más a la sistemática legislativa italiana. No obstante, hay algunas consideraciones que entendemos que deben ser señaladas. La primera, es que Italia y España aunque de modo distinto fijan dos tipos de informaciones que deben ser realizadas, es decir aquella previa en que se debe comunicar al interesado que sus datos podrán someterse a tratamiento por un sistema de protección al crédito, siendo que en Italia, hay que acordarse de que incluso los datos de las solicitudes de crédito son registrados y en España solamente en caso de incumplimiento de la obligación; y aquella información que debe ser realizada cuando es inminente el registro de los datos (Italia) o cuando los datos ya hayan sido registrados (España).

Nos parece muy acertada la línea jurisprudencial brasileña que entiende que la notificación tiene que ser enviada antes del registro de los datos. Sin embargo, hay algunas cuestiones que nos parece importante que sean replanteadas en la ley brasileña, a la vista del estudio comparado. La primera es la necesidad de insertar en la norma la obligación del acreedor en proceder la notificación previa de que los datos suministrados por el interesado podrán ser comunicados a un sistema de protección al crédito; la segunda, la necesidad de fijar el momento en el cual se debe proceder la comunicación de la inminente inclusión de los datos en el registro y cuantos días se debe esperar entre tal comunicación y el efectivo registro de los datos en el fichero y, finalmente, determinar

específicamente a quién compete el deber de notificación previa al consumidor.

El Proyecto de ley nº 85/2009 en el artículo 6º, tal y como se encuentra su redacción hoy, parece que solucionará algunas de las cuestiones planteadas. El precepto determina que en los casos en que la deuda no haya sido protestada, deberá ser comunicada antes de su inclusión por escrito al deudor. Soluciona, así, la cuestión de la obligatoriedad del gestor del fichero en informar previamente del registro. De otra parte, el inciso VI del mismo artículo determina que en el propio escrito de la comunicación se indique al afectado el plazo a partir del cual la información será introducida en el banco de datos. Desde nuestro punto de vista, el proyecto ya podría haber establecido tal plazo y no dejarlo en las manos del gestor la decisión de fijarlo. La solución italiana en este punto nos parece muy elogiable, como anteriormente nos hemos referido, ya que determina que los datos solamente estarán disponibles después de por lo menos 15 días de la comunicación previa a la inclusión (art. 4, apartado 7 de la LOPD).

El texto del referido proyecto no fija con claridad quién tiene el deber de proceder la notificación previa, aunque el párrafo 4º del artículo 6 obliga a que tanto el acreedor como el gestor del fichero guarden la comprobación de que tal notificación fue efectuada, lo que nos lleva a pensar que quiere el legislador que tanto uno como otro puedan realizar la comunicación. Ahora bien, nos resulta curioso que con independencia de que sea esa la intención del legislador, no está claro en el texto a quien incumbe tal responsabilidad.

Además no menciona ninguna obligación por parte del acreedor en informar al deudor sea en el momento de la recogida de los datos, sea en cualquier otro tiempo, que sus datos podrán ser comunicados a un sistema de protección al crédito. Si es el acreedor quién recoge los datos y que se los envía a un fichero, pensamos que el interesado debería ser

informado por éste sobre los posibles destinos de sus informaciones. La ley española, a nuestro sentir, es la que mejor comparte las responsabilidades de la información, ya que tanto el acreedor como los responsables del fichero deberán informar, cada uno dentro de su ámbito de responsabilidad, lo que sucederá con sus datos o donde están registrados. Ya hemos señalado que no nos ha convencido la elección legislativa de España en cuanto a que, el responsable del fichero comunique al afectado con posterioridad al registro de sus datos. No obstante ello, desde nuestro punto de vista, la mejor solución sería compartir responsabilidad, como la ley española, pero todas las informaciones tienen que ser realizadas antes de que se registren los datos. De otra parte, debería ya fijarse legalmente cuanto tiempo pueden estar disponibles los datos después de tal comunicación, como lo hace la ley italiana.

### 3.1. Forma, contenido y acreditación de la notificación.

Una de las pocas aportaciones procedimentales que hace la ley brasileña, aparte de como hemos consignado de la proclamación de tal derecho, es la exigencia de que la información sea por escrito.

Es importante recordar sobre este aspecto que la legislación italiana no hace ninguna mención sobre la forma que se debe adoptar la información previa a la inclusión, preocupándose mucho más con la advertencia en si, tanto que permite que se haga bien en el momento del requerimiento de pago, o bien cuando se efectúe otras comunicaciones. Aunque, como ya hemos señalado anteriormente, la información en el momento de la recogida de los datos debe obedecer a una forma concreta.

La norma española tampoco exige un modo específico de cómo deberá ser procedida ni en la información previa a la inclusión (art. 39 del RPD) ni en la notificación de inclusión (art. 40 del RPD). Sin embargo, exige para esta última comunicación, que sea realizada a través de un medio fiable, auditable e independiente de la entidad notificante, que la permita acreditar la efectiva realización de los envíos. Lo que se puede recoger de la ley española es la preocupación en que se pueda acreditar el cumplimiento del deber de informar.

Ahora bien, como hemos visto, en lo que concierne al contenido, examinando el conjunto de la norma española, ésta fija algunas exigencias comunes que deberán ser incluidas en todas las informaciones al afectado: a) los datos de la deuda, ya que la información previa deberá, en todo caso, efectuarse al momento del requerimiento previo de pago y en la notificación de inclusión, la ley habla de una referencia de los datos que hubiesen sido incluidos; y b) la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición. De igual modo entre otras informaciones que deberán constar en el escrito al afectado, la legislación italiana (Art. 5 del Código de Buena Conducta) también requiere la mención al dato que será registrado y a los derechos del interesado.

Pensamos que la legislación española ha acertado al no exigir una forma puntual con la cual debe seguir el responsable del fichero a la hora de comunicar la inclusión de los datos personales al interesado. El hecho de que fije el foco de la ley en la exigencia de la acreditación desde nuestro punto de vista es mucho más eficaz, ya que deja al quien corresponda cumplir tal deber un margen muy grande para actuar que compensa la aludida exigencia.

La legislación brasileña ha elegido, sin embargo, establecer la forma escrita como la hábil a proceder tal comunicación. Creemos que así lo hizo para que fuera más seguro que tal información llegara al consumidor

además de facilitar a la hora de comprobar si tal obligación fue cumplida, en el caso, por el responsable del fichero.

No obstante, la jurisprudencia tiene consolidado un entendimiento que nos parece muy criticable, ya que genera una inseguridad jurídica muy grande. El Supremo Tribunal de Justicia<sup>651</sup> (STJ), en 24 de noviembre de 2009, ha publicado un acuerdo que uniformiza el entendimiento del citado órgano juzgador, en el sentido de que para la notificación previa es dispensable el acuse de recibimiento del afectado. Para éste Tribunal<sup>652</sup>, es suficiente con que se compruebe el envío al consumidor en la dirección suministrada por el acreedor. Del mismo Órgano juzgador<sup>653</sup>, la Sentencia de 03 de diciembre 2007, que del igual modo interpreta que el dispositivo legal exige solamente que la notificación se dé por escrito, no siendo necesario que el responsable del fichero verifique si el notificado aún reside en la dirección suministrada por el acreedor, siendo solamente necesaria la comprobación de la emisión de la notificación

Para Roscoe Bessa<sup>654</sup>, aunque el Código de Defensa del Consumidor no haya establecido que la comunicación sea realizada con documento comprobatorio, como el acuse de recibo, tal providencia es recomendable, ya que si hay discusión judicial cabe al responsable del fichero demostrar que la comunicación fue efectuada.

A pesar de nuestro respeto por el *Superior Tribunal de Justiça* de Brasil, discrepamos rotundamente de su posicionamiento. Es cierto que la ley no

---

<sup>651</sup> *Sumula 404:* "É dispensável o aviso de recebimento (AR) na carta de comunicação ao consumidor sobre a negativação de seu nome em bancos de dados e cadastros".

<sup>652</sup> STJ. Recurso Especial nº 1.083.291 – RS. Rel. Min. Nancy Andrighi. Juzgado en 09 de septiembre de 2009.

<sup>653</sup> STJ. Agravo de Instrumento nº 833.769 – RS. Rel. Min. Humberto Gomes de Barros. Juzgado en 03 de diciembre 2007.

<sup>654</sup> ROSCOE BESSA, Leonardo. *O consumidor... op. cit.*, p. 195.

obliga a una forma específica en la cual deba el responsable del fichero someterse, solamente determinando que sea por escrito. Sin embargo, el simple envío de una comunicación no comprueba ni que el afectado haya recibido ni que no lo haya hecho. Si por un lado a efecto de análisis del conjunto probatorio es relativizada la declaración del afectado de la ausencia de recibimiento de la notificación, desde nuestro punto de vista, hay que tener algunos indicios que comprueben que esta fue realizada y a la así equilibre la posición de las dos partes ante las pruebas.

De suerte que si el medio que ha elegido el responsable del fichero no acredita ni la recepción ni su devolución, no puede ser considerado un modo fiable. Porque si es verdad que el responsable no necesita comprobar que el interesado sigue en la misma dirección, y ahí estamos de acuerdo con el Tribunal, de otra parte sí es su responsabilidad verificar si la causa de la devolución puede ser atribuida al acreedor. Porque en este caso, deberá repetir tal notificación. Si no es así, entonces el fundamento de la notificación previa es meramente una ficción jurídica sin ningún efecto práctico. Nos parece oportuno remarcar nuestra postura sobre la importancia de tal comunicación, principalmente cuando para tratar los datos no es necesario recabar el consentimiento del consumidor, de modo que la información previa al registro le permite garantizar la calidad de los datos y darle oportunidad para ejercer sus derechos. Lo que no nos parece que sea necesario es que el interesado reciba la comunicación personalmente. Creemos que es suficiente con que se pueda atestar que ésta ha llegado a la dirección dada por él al acreedor. En el momento de la celebración del contrato

Ahora bien, el PL nº 85/2009 mantiene la forma como escrita, y además que pueda ser comprobada su envío a la dirección indicada por el deudor a través de acuse de recibimiento o servicio similar poniendo, de este modo, fin al problema de la comprobación de envío. Asimismo, el proyecto exige tanto al gestor como al acreedor que se guarden los comprobantes de envío durante un plazo de cinco años.

Para nosotros, en este punto de la reforma, el legislador ha ponderado los problemas de orden práctico que estaban ocurriendo cuando no ha exigencia de la comprobación de envío y recibimiento de la información al afectado además de poner en relieve la importancia de tal comunicación.

A pesar de ello, creemos que habría que ponderar el coste para los ficheros de cumplir tal obligación, ya que la norma solamente prevé que sea por escrito. Además, lo más importante es que la comunicación llegue al afectado y que su contenido sea comprensible y contenga aquellas informaciones que en cada país se considera más importantes. De suerte que el modo de realizarla no es el factor fundamental. Así, consideramos que la legislación española ha tenido esa sensibilidad orientando la norma para la acreditación de la comunicación.

En lo que concierne al contenido, señala Roscoe Bessa<sup>655</sup> que se debe indicar los datos de quién ha solicitado la inclusión de la información, todos los detalles relativos a la deuda, la dirección del fichero que están registrados los datos, así como la posibilidad y el modo de ejercicio del derecho de acceso, requisito este que el autor ha trasladado de la experiencia europea, conforme previsto en la Directiva 46/95. De otra parte, para Herman de Vasconcelos Benjamin<sup>656</sup> el derecho a la comunicación conlleva un triple deber de notificar: a) el registro; b) las fuentes de los datos; y c) el contenido de las informaciones que serán incluidas.

El PL nº 85 en el artículo 6º enumera lo que debe incluir la comunicación, y desde nuestro punto de vista se asemeja a la norma italiana. De esta manera, exige que se especifique: a) la especie, número y valor del título o en su ausencia, del documento fiscal contabilizado que

---

<sup>655</sup> ROSCOE BESSA, Leonardo. *O consumidor... op. cit.*, p. 198.

<sup>656</sup> PELEGRINI GRINOVER, Ada; HERMAN DE VASCONCELOS BENJAMIN, Antonio, et al. *Código Brasileiro de Defesa do Consumidor: comentado pelos autores do anteprojeto*. Rio de Janeiro: RT, 2004, p. 459.

dio origen a la deuda; b) naturaleza de la obligación; identificación completa de la persona natural o jurídica que solicitó la inclusión conteniendo: Nombre, NIF o CIF, dirección, teléfono y medio electrónico para contacto; c) plazo a partir del cual la información de incumplimiento será registrada en el fichero; d) identificación de los banco de datos en que la información de incumplimiento será incluida, así como la dirección y teléfono del responsable del fichero; e) hacer mención al derecho a la rectificación de la información identificando los medios de contacto y la forma para solicitar la rectificación y, finalmente, deberá señalar el valor principal de la deuda, los plazos vencidos y los que aún no han vencido.

Tal y como se encuentra el texto del proyecto, nos ha parecido que ha acertado el legislador brasileño ya que cubrirá una omisión que consideramos muy grave en el sistema legislativo de Brasil para la tutela del derecho a la autodeterminación informativa en relación a los datos tratados por el sistema de información crediticia.

3.2. La comunicación y los datos recabados de fuentes accesibles al público.

Sopesando todo aquello ya expuesto sobre las peculiaridades del derecho brasileño en lo que concierne al derecho de comunicación, hacer referencia a los datos que provienen de fuentes accesibles al público es un reto bastante complicado.

Si es notable que la legislación no es suficiente para abarcar y solucionar los problemas con los datos que son suministrados directamente por el acreedor y a ello se suma la ausencia de una norma general de protección



de datos a la cual se podría recurrir en los supuestos que a normativa específica no fuese suficiente, los interesados en lo que concierne a sus datos expuestos en fuentes públicas se quedan en una posición muy vulnerable.

Distintamente de España, que establece que tales datos obedecerán al régimen general de la ley, y de esto surgen, como ya comentado, algunas dudas con relación a la necesidad de comunicación del registro de estos datos; en Brasil el párrafo 2º del artículo 43 del CDC es claro al disponer que cualquier registro deberá ser comunicado por escrito al consumidor cuando no solicitada por él. Es decir, si los datos no fueran recabados directamente del consumidor, la regla es la información de la inclusión.

Este punto ha originado divergencias entre los jueces de los órganos judiciales colegiados. En sentencia de 2006<sup>657</sup>, el *Tribunal de Justiça do Distrito Federal*, entendió que cuando recogido datos de una fuente accesible al público como los registros judiciales oficiales, la información previa exigida por el artículo 43, párrafo 2º del Código de Defensa del Consumidor es desnecesaria y legalmente inexigible. Ello porque, en su comprensión, efectivamente no se crea cualquier banco de datos referente a la persona del consumidor, sino se registra una información de naturaleza pública obtenida a través de un servicio judicial. Por lo tanto, en el caso concreto analizado, se había procedido solamente la anotación de que existía un procedimiento ejecutivo que era promovido en disfavor del afectado.

El Magistrado del Superior Tribunal de Justicia, Jorge Scartezzini<sup>658</sup>, reconoció en sentencia que no existe diferencia de donde fue recogido el

---

<sup>657</sup> TJDF, número del proceso: 2002.01.1.036295-2. Rel. Benito Augusto Tiezzi, juzgado en 18/12/2002.

<sup>658</sup> STJ. Recurso Especial nº 720.493 - SP (2005/0014086-4). Rel. Min. Jorge Scartezzini. J. 16 de junio 2005. Señala El magistrado: “conquanto inexistia diferenciação acerca da necessidade de prévia comunicação de cadastramento com

dato (si de fuente pública o no) para que se exija la información previa al consumidor, pero su rigor es atenuado cuando se recoge de fuente pública, como los boletines oficiales, que era el caso que se sometía a examen por el Órgano sentenciador. Así, continúa el fallo, no obstante el artículo 43, párrafo 2º, la finalidad del dispositivo es conferir la oportunidad de los consumidores sobre la circulación de informaciones negativas sobre si, para que pueda posibilitarles el acceso a las mismas, y, en caso de inexactitud de los datos, ejercer su derecho a rectificación.

Sin embargo, pese estas consideraciones, el supuesto descrito en la sentencia tenía como causa de pedir indemnización por daño moral, fundada en la ausencia de comunicación previa al consumidor de la inclusión de registro. Fue decidido que, no obstante la falta de información, ello no ocasionaba efectivo daño moral, ya que constaba en el fichero un dato verídico. Por lo tanto, el recurso fue desestimado.

Éste, así como otros innumerables casos llevados a los tribunales<sup>659</sup>, siempre tienen como causa pedir el resarcimiento del daño moral y algunas veces del daño material. Ello deriva de la ausencia de una ley de protección de datos que asegure otras posibilidades como la cancelación del registro y sanciones de naturaleza administrativas que serían más eficaces en el sentido de que los bancos de datos adecuasen su actividad a la tutela del derecho a la autodeterminación informativa del ciudadano, como hemos venido recalando en este trabajo de investigación. En la Sentencia citada, el Tribunal no ha vislumbrado el daño moral a ser indemnizado; de otra parte, el responsable por el fichero no llevó a efecto

---

base na origem dos dados, seu rigor resta atenuado em se cuidando de informações coligidas de fontes públicas”.

<sup>659</sup> Vide, por ejemplo, reciente sentencia del TJRS, Apelação Cível nº 70033790841, Rel. Des. Paulo Antônio Kretzmann, juzgado en 11 de febrero de 2010. Señala que “não colore a figura do ato ilícito o fato de a SERASA colher informação de assento cartorário, que é de domínio público, sendo totalmente despicienda a prévia comunicação”.

lo dispuesto en el precepto y no fue ni será penalizado por dejar de cumplirlo. A nuestro sentir éste es un equívoco muy grande del sistema legislativo brasileño, que se analizará más adelante.

Otro fallo que nos parece oportuno traer a colación también ES EL del *Superior Tribunal de Justiça*<sup>660</sup>, que analizaba un caso en que igualmente el demandante requería daños morales por registro de datos sobre la ejecución fiscal de una deuda en un fichero de solvencia patrimonial, recabados de un Tribunal en el marco de un convenio de cesión de datos entre éste y el citado fichero. En el supuesto, el interesado no había sido comunicado de tal registro. Según el fallo, el responsable del fichero no tenía obligación de realizar tal comunicación por tratarse de información de carácter público. Además el afectado realizó el pago de la deuda y, curiosamente la sentencia manifiesta que éste no había comunicado al fichero de que tal deuda había sido sanada, “como podría y debería haberlo hecho, a tenor del artículo 4º de la ley 9.507/97 (*Ley del Habeas Data*)”.

Una vez más, no compartimos la misma opinión del STJ. Es más, creemos que tal fallo va en dirección opuesta a los fundamentos más básicos del derecho a la autodeterminación informativa del ciudadano. En una primera vertiente de consideración, nos parece absurdo que se pueda permitir un convenio entre un Tribunal y un fichero de protección al crédito. Cuando alguien se dirige al juzgado, sea como parte autora o re, en ningún momento se les son comunicados de que sus datos podrán ser cedidos a ningún tipo de fichero. De este modo, consideramos que ello viola uno de los pilares fundamentales del derecho a la autodeterminación informativa que es lo de ser informado sobre el destino de sus datos; además vulnera del derecho del titular de los datos

---

<sup>660</sup> STJ. Agravo de Instrumento nº 1.036.057-SP. Rel. Min. Aldir Passarinho Junior. J. 03 de marzo de 2009.

de que estos sean tratados dentro del ámbito y finalidades para los cuales fueron recogidos. De manera que no vislumbramos ninguna relación que justifique la cesión de los datos de un Tribunal a un fichero como los de solvencia patrimonial.

Si comparamos la legislación española en estos casos, la regla general es que la cesión y tratamiento de los datos sólo pueden ser realizados con el consentimiento del afectado. No obstante, hay supuestos que los legitiman sin la necesidad de tal consentimiento. Entre ellos, el RPD (art. 10, apartado 2, aline a b), lo permite cuando *los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado*. Ahora bien, cuando en estos casos esté como responsable la Administración pública, *sólo podrán comunicar al amparo de este apartado los datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley*. En la misma línea el sistema italiano, en el artículo 19.3 del Código en Materia de Protección de Datos, establece que solamente está permitido que sujetos públicos comuniquen datos a sujetos privados cuando existe una ley o un reglamento que así lo prevea.

La cuestión se centra en el siguiente planteamiento: es cierto que parte de los datos que están en un Tribunal interesan a los ficheros de morosos. Sin embargo, ¿cuál es el interés de un juzgado en enviar directamente a un sistema de información crediticia tales datos, que al fin y al cabo serán públicos? Dentro de las funciones institucionales de un Tribunal no está la de ayudar al mercado crediticio, ni el de consumo. La comunicación de tales informaciones no forma parte de la función esencial y directa ni indirecta de este órgano. La sentencia tampoco se ha inmiscuido en este punto.

De cualquier modo, no nos parece que un Tribunal, como órgano público, sin que haya una ley que permita la transferencia de datos, pueda hacerlo a través de un convenio. Por mejor decir, como se trata de un derecho fundamental de las personas, solamente una ley podría permitir y establecer los límites de la cesión de datos personales entre un ente privado y un público. Así, no encontramos ninguna razón que legitime tal conducta incluso porque el interés público tampoco se vislumbra.

La segunda consideración es sobre la ausencia de obligatoriedad de que se informe al afectado de los datos recabados de fuentes públicas y el ejercicio de los derechos del interesado. Es cierto que en el caso concreto el afectado ya había sido citado para el proceso y antes de esto, había pasado por un procedimiento administrativo de cobro de la deuda, en el cual ha sido igualmente notificado. El problema está en saber si tales actos sustituyen el deber de información del artículo 43, párrafo 2º. A nuestro sentir, pensamos que esto no es posible. Si en la citación judicial hubiese alguna alusión a la posibilidad de que los datos fuesen comunicados a ficheros de moroso, una información previa de donde puede ir los datos, podríamos entender que el responsable del fichero no tendría la obligación de repetir tal comunicación. Ahora bien, ¿cómo se puede garantizar la tutela del derecho a la autodeterminación informativa, si el afectado por la naturaleza de los datos no tiene el poder de consentir su tratamiento, como es el caso, y además de ello no es informado sobre la posible cesión de los mismos?

Lo que nos parece aún peor, es que por un lado el fichero de solvencia no haya actualizado los datos del interesado, cuando se ha terminado el procedimiento de ejecución. De otra parte, el Órgano juzgador en la aludida Sentencia entiende que esta actualización cabe al afectado que “**podría y debería** haberlo hecho a tenor del artículo 4º de la ley 9.507/97 (*Ley del Habeas Data*)” (subrayamos). Ahora bien, ¿cómo **podría y debería** ejercer sus derechos si no tenía información de que sus datos estaban siendo tratados por un fichero de moroso? ¿Cómo **podría y debería**

hacerlo si no sabe en cual fichero están tratando sus datos? Por fin, ¿cómo **podría** y **debería** hacerlo si no sabe de la existencia, ni tiene por qué saberlo, de un convenio de cesión de datos entre el Tribunal cedente y el fichero de protección al crédito? Sencillamente, no se puede.

En efecto los datos que están en fuentes de acceso público, por su naturaleza pueden ser conocidos por cualquiera. Sin embargo, no se puede comparar la organización de un fichero de solvencia patrimonial y de un Boletín Oficial. El almacenamiento, su tratamiento automatizado, enlazamiento y la circulación de datos en uno y otro soporte no son los mismos. No se pretende en aquí indagar si hubo configuración del daño moral. No obstante, nos parece inaceptable que desde la perspectiva de esta reciente Sentencia el responsable del fichero no tenga ninguna obligación con el derecho a la protección de datos del ciudadano.

Según Neder Meneghelli<sup>661</sup>, aunque con una opinión distinta de la nuestra, señala que en el momento del registro de las informaciones, nombres de terceros son vinculados —con independencia de que tales datos puedan o no ser conocidos por otros medios, como los procedimientos judiciales, informaciones sobre protestos, etc.— objetivando la prestación de los servicios auxiliares en general y concibiendo, organizando y ejecutando un sistema central de archivo con los datos registrados. Para el autor, la inclusión de tales informaciones, la cesión a terceros, la organización del banco de datos solamente pueden ser imputadas a los responsables del fichero, que se dedican a este tipo de actividad, y su conducta atañe la esfera jurídica de terceros.

---

<sup>661</sup> NEDER MENEGHELLI, José Eduardo. "Temas sobre a anotação do Nome do Consumidor em Cadastro de Entidades Prestadoras de Serviços e Concedentes de Crédito" [en línea]., Vol. 47, nº 264. São Paulo: Revista Jurídica, out./1999, p. 84/86. Disponible en

<http://www.prr5.mpf.gov.br/nid/Onid0551.htm> [consultado en 22 de enero 2010]

Ahora bien, a su sentir, no es obligatoria la comunicación cuando los datos recogidos proceden de fuentes accesible al público, ya que la publicidad del acto objeto del registro es “inmanente”, incluso para el afectado.

El planteamiento del autor, desde nuestro punto de vista, invierte algunas situaciones jurídicas. Es decir, parte del principio que el interesado y cualquier otra persona conoce el dato porque es público. Pero si el argumento es éste, no sería necesario nunca comunicar al titular de los datos que estos serán registrados en ningún fichero porque si son datos personales, el interesado ya lo conoce previamente y muchos de ellos también son conocidos públicamente. La cuestión no se centra en el conocimiento mayor o menor de los datos en sí, sobre todo cuando se trata de datos tan especiales como los de solvencia patrimonial y crédito. Por mejor decir, el derecho a la autodeterminación informativa está planteado sobre el fundamento de control de los datos y no en su conocimiento previo. De otra parte, el hecho de que sean datos que son recabados en fuentes que son públicas, y cualquiera pueda acceder a ellos no consideramos que la naturaleza de las aludidas fuentes tiene la idoneidad por si solas de crear un perfil desde la perspectiva de la solvencia patrimonial y crédito del afectado, como lo hace cuando están en un fichero de moroso. Es más, seguramente no sería viable para un acreedor buscar informaciones en fuentes públicas de cada cliente que solicite sus servicios crediticio. Esta función organizativa es otro punto que hace con que comparativamente, la publicidad de los datos de una fuente publica no tenga tanta capacidad de difusión con consecuencias que interfieren muchísimo en la vida del afectado como un fichero con las características de aquellos de protección al crédito.

#### 4. El *Habeas Data* y los derechos del afectado

El Código de Defensa de Consumidor previa en su artículo 86 la posibilidad de la utilización del *habeas data* para la tutela de los derechos e intereses de los consumidores. Sin embargo, tal precepto fue vetado<sup>662</sup> con la justificativa de que tanto el *Mandado de Segurança* como el *Habeas Data* eran acciones que se destinaban, por su naturaleza, a la defensa de derechos subjetivos públicos y tenían, por lo tanto, como objetivo precipuo los actos de los agentes del poder público y así su extensión o aplicación a otras situaciones o relaciones jurídicas sería incompatible con su índole constitucional. Ello causó mucha polémica en la doctrina jurídica a su tiempo<sup>663</sup>.

No obstante el veto, el párrafo 4º del artículo 43 del CDC eleva a la categoría de entidades de carácter público los ficheros de moroso. Así, ello no consiguió impedir, dentro de la sistemática legal, el uso del *Habeas Data* por los interesados para obtener informaciones suyas de los ficheros de moroso, tesis esa reforzada más adelante con la entrada en vigor de la ley 9.057/97 que regula el derecho de acceso a las informaciones y disciplina el rito procesal del *Habeas Data*. En esta norma el párrafo único del artículo primero considera de carácter público todos los banco de datos que contengan informaciones que sean o puedan ser transmitidas a terceros y que no sean de uso privativo de la propia entidad depositaria de tales informaciones. Superada, por lo tanto, la discusión de la

---

<sup>662</sup> Mensaje nº. 664 de 11 de septiembre de 1990. El contenido del veto está disponible en:

[http://www.planalto.gov.br/ccivil\\_03/LEIS/Mensagem\\_Veto/anterior\\_98/vep664-L8078-90.htm#art85](http://www.planalto.gov.br/ccivil_03/LEIS/Mensagem_Veto/anterior_98/vep664-L8078-90.htm#art85) .

<sup>663</sup> Vide sobre el tema SACCO NETO, Fernando. *Cadastros de Proteção ao Crédito*. São Paulo: Método. Vol. 1. Parte Geral. 2009, p. 107.



posibilidad o no de los bancos de datos figurar en el polo pasivo del *Habeas Data*.

En efecto, la jurisprudencia parece tener el mismo entendimiento de la doctrina. El Tribunal de Justicia del Distrito Federal<sup>664</sup> ha decidido que los bancos de datos relativos a consumidores, los servicios de solvencia patrimonial y crédito (servicios de protección al crédito) y congéneres son considerados de carácter público, no habiendo cualquier impedimento a la utilización del *habeas data* para el conocimiento de los datos en ellos existentes. En el mismo sentido, la Sentencia de 29 de noviembre 2005, del *Tribunal de Justiça de Rondonia*<sup>665</sup>, señala que el *Habeas Data* es el instrumento adecuado de utilización por el consumidor que pretende solicitar informaciones en los bancos de datos de protección al crédito.

Como ya hemos comentado en el capítulo 1, la ley del *Habeas Data* tiene una triple función: a) garantizar el conocimiento de las informaciones (acceso); b) rectificación de los datos; y c) complementación de las informaciones. Además, prevé dos tipos de procedimientos, uno administrativo y otro judicial. De éste modo, como el Código de Defensa del Consumidor no prevé ningún procedimiento ni plazos para el ejercicio de los derechos de los afectados, la norma del *Habeas Data* deberá ser observada a tal efecto.

Hay que señalar, por fin, que el CDC no hace ninguna mención a la gratuidad de los derechos allí preceptuados, sin embargo la ley del *Habeas Data* en su artículo 21 dice que tanto el procedimiento del derecho de acceso como el de rectificación, son gratuitos. En el Proyecto de Ley nº 85/2009 prevé en el artículo 16 que el afectado tendrá a cualquier tiempo garantizado el acceso gratuito a las informaciones que a él se refiera

---

<sup>664</sup> TJDF. Número del proceso: 19980110248160, relatora VERA ANDRIGHI, juzgado en 17/05/1999.

<sup>665</sup> TJRO. AC 200.000.2003.009620-0; Primeira Câmara Cível; Relator Gabriel Marques de Carvalho; juzgado en 29/11/2005

existentes en un fichero. Para Roscoe Bessa<sup>666</sup>, en Brasil, un país de población pobre, la mejor interpretación de la ley conduce a la conclusión de que no es lícito el cobro de cualquier valor por el ejercicio de los derechos de acceso, aunque solicite por escrito.

Así, diferentemente de lo que ha pasado recientemente con Italia, donde el *Garante* ha fijado algunas tasas para el ejercicio de acceso a por los afectados en los servicios de protección al crédito, el legislador brasileño parece querer continuar garantizando la gratuidad y nos parece que así debe ser, ya que el afectado no solicita nada más que obtener informaciones sobre datos que son suyos.

#### 4.1. El ejercicio de los derechos del interesado.

Según la Ley nº 9.507, de 12 de noviembre de 1997, el afectado deberá dirigirse directamente al fichero presentando su solicitud. En efecto, el artículo 2º establece que “el requerimiento será presentado al órgano o entidad depositaria del registro o banco de datos y será deferido o no en el plazo de cuarenta y ocho horas”. El interesado deberá ser comunicado de la decisión del responsable del fichero en un plazo de veinte y cuatro horas.

La ley determina aún que en el caso de que el responsable acepte el pedido, deberá marcar día y hora para que el interesado tome conocimiento de las informaciones. En la hipótesis de que sea constatada alguna inexactitud de cualquier dato, el afectado podrá solicitar su rectificación, añadiendo los documentos comprobatorios de su pedido.

---

<sup>666</sup> ROSCOE BESSA, Leonardo. *O consumidor... op. cit.* p. 191.

Según la norma del *Habeas Data*, específicamente para la rectificación, ésta deberá ser efectuada en un plazo máximo de diez días a contar del recibimiento de la solicitud y el afectado deberá ser notificado de la aludida rectificación, aunque la citada ley no establece plazo para ello. Sin embargo, para los sistemas de protección al crédito, el Código de Defensa del Consumidor la complementa, ya que en el párrafo 3 del artículo 43 del CDC determina que siempre que el consumidor encontrar inexactitud en sus datos podrá exigir su inmediata corrección, debiendo el responsable del fichero en un plazo de cinco días comunicar la alteración a los eventuales destinatarios de las informaciones incorrectas.

Aunque no haya inexactitud del dato, la ley 9.507/1997 ordena que si el interesado presenta alguna explicación o contestación sobre las informaciones, justificando una posible pendencia sobre el hecho objeto del dato, tal explicación deberá ser anotada junto a los datos en cuestión.

En el caso de que el responsable del fichero se niegue a dar conocimiento al interesado de sus datos o, en su caso, a rectificarlos, el último podrá solicitarlo a través de la vía judicial, con el procedimiento descrito para ello en la ley, si así lo desea.

Resulta oportuno puntualizar que no hay previsión legal del plazo para que el responsable del fichero conteste el pedido del derecho de acceso, o que informe al afectado sus datos cuando solicitado. Para Herman de Vasconcelos Benjamin<sup>667</sup>, el acceso tiene que ser ofrecido inmediatamente, en tiempo no superior a aquél que el responsable del fichero llevaría para informar a un participante sobre los datos de algún afectado. Consideramos ésta una solución muy ecuaníme sobre todo cuando el afectado se dirige directamente a la entidad responsable del fichero. No obstante ello, entendemos que el PL nº 85/2009 ya podría disciplinar no

---

<sup>667</sup> PELEGRINI GRINOVER, Ada; HERMAN DE VASCONCELOS BENJAMIN, Antonio, et al. *Código Brasileiro de Defesa do Consumidor: comentado pelos autores do anteprojeto*. Rio de Janeiro: RT, 2004, p. 464.

solamente ésta situación como también aquellas en que el afectado la ejerza por escrito.

El PL nº 85/2009 que prevé como ya mencionado el “derecho a la impugnación” disciplinando un procedimiento a ser utilizado por el interesado cuando tiene algún motivo para oponerse al registro de los datos. De este modo, se garantiza la comprobación de las informaciones y su contenido, asimismo podrá fundarse en la imposibilidad de localizar el acreedor para efectuar el pago de la deuda.

El texto fija un plazo de diez días para que el responsable del fichero se manifieste rechazando o no la solicitud. En el caso de que la información registrada no sea veraz, el plazo también es el mismo para excluirla. Si el gestor no acepta la impugnación deberá presentar al interesado un escrito justificando la manutención de la información. En el supuesto de que acepte total o parcialmente la impugnación, el texto obliga que se presente una comprobación y justificativa de la regularización de la información al aludido interesado. Además, cuando solicitado por el afectado, deberá comunicar la alteración de los datos tanto a aquellos que han accedido a ellos como a los bancos de datos a los cuales fueron cedidas las informaciones. El PL pretende establecer un procedimiento más detallado para el derecho de rectificación, y aunque no es de todo criticable, consideramos que lo mejor hubiera sido separar un procedimiento específico para cada derecho, ya que siempre habrá que remitirse a este cuando hubiere alguna omisión en el modo de ejercitar los demás.

El *Habeas Data* es un instrumento que sirve al ciudadano para ejercer sus derechos frente a cualquier fichero público. Ahora bien, tales derechos según la ley se restringen a asegurar el conocimiento de las informaciones del interesado; su rectificación de los datos; o, en su caso, añadir contestación o explicación sobre el dato verdadero, sin embargo justificable y que esté pendiente de resolución judicial o amigable. De este modo, quedan excluidos los derechos de oposición y cancelación.

A partir del estudio realizado anteriormente sobre la legislación española e italiana, hemos observado que tales países cuentan con matices legales específicos para los ficheros de solvencia patrimonial, respecto al ejercicio de los derechos del afecto, aparte de lo que dispone el régimen general.

Comparativamente, desde nuestro punto de vista, la legislación brasileña se encuentra en una posición muy rezagada. En la primera vertiente de consideración, podemos señalar la imposibilidad de que el afectado pueda hacer frente a sus derechos a través de las entidades que participan del sistema de protección al crédito. Desde nuestro punto de vista, no hay ningún argumento que pueda convencernos de la imposibilidad de que aquellos que se benefician de las informaciones de un sistema de información no puedan tener la carga de dividir la obligación con el responsable del fichero en recibir las solicitudes de ejercicio de derechos de los afectados. Por otra parte, esta obligación se funda en el deber de los que participan en un sistema de protección al crédito de mantener la calidad de los datos allí registrados.

El Código deontológico italiano (Art. 8 apartado 1), por un lado, establece rotundamente que los derechos de los afectados podrán ser ejercidos tanto ante el responsable del fichero como ante al participante que haya comunicado los datos. La ley española, en el RPD (Art. 37 apartado 2, letras *a*) y *b*) y Art. 44, apartado 2) a su vez, determina que la petición de ejercicio de los derechos puede dirigirse al responsable del fichero, que estará obligado a satisfacer en cualquier caso dichos derechos, así como vislumbra la posibilidad de que la solicitud se dirija a cualquier otra entidad participante en el sistema. Aunque no impone como es lógico una carga muy grande a estos últimos, ya que tocante al derecho de acceso deberán únicamente comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad y dirección del titular del fichero común para que pueda completar el ejercicio de su derecho.

Lo que se quiere demostrar aquí es que los participantes del sistema deben tener una parcela de responsabilidad en lo que concierna a la facilitación del ejercicio de los derechos del interesado, aunque no sea comparable con la del responsable del fichero como es el caso de la legislación española. No nos parece aceptable y no encontramos ningún argumento que pueda sostener el hecho de que las entidades participantes permanezcan intocables en lo que respecta a tal situación en la ley brasileña.

Además, lo que sí se puede observar es que la intención legislativa de España e Italia es la de que los datos que figuren en el sistema sean siempre correctos y puestos al día y que se evite cualquier perjuicio para el afectado cuando éste pretende ejercer sus derechos, aunque regulados de manera distintas, o incluso de modo más o menos acertado desde nuestro punto de vista. Sin embargo, por poner un ejemplo, para el derecho de rectificación tanto uno como otro país crearan mecanismos para que la comunicación entre la entidad participante del sistema y el titular del fichero de solvencia patrimonial sea la más rápida posible para que se verifique el posible error de los datos y si así no sucede, transfiere al último la responsabilidad de actuar e interferir directamente para satisfacer tal finalidad.

Este punto nos parece de fundamental importancia. Las informaciones una vez registradas en el fichero pueden ser rápidamente comunicadas. Así, igualmente deben ser rectificadas cuando se proceda. El sistema adoptado por Brasil restringe mucho la actuación del sistema de protección al crédito, considerado como todo, sobrecargando únicamente el acreedor. De forma que creemos que no sea la opción más acertada si lo que si quiere es mejorar la calidad de las informaciones y facilitar el ejercicio de los derechos del afectado.

Aparte de ello, si el fichero está informatizado, no necesariamente habrá en todas las ciudades brasileñas una oficina del responsable del fichero.

Por poner un ejemplo, el fichero SERASA EXPERIAN, aunque esté presente en todos los Estados brasileños, en algunos de estos solamente hay oficina en la Capital<sup>668</sup>.

De este modo, nos parece como mínimo absurda la dificultad impuesta al afectado, sea de desplazamiento, sea de medios técnicos para ejercer sus derechos cuando cualquier participante del sistema podría intermediarlo. De hecho, la legislación española en apartado 2 del artículo 24 determina que deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Y no solamente eso, pero también prohíbe que el ejercicio por el afectado de sus derechos suponga un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

El caso brasileño se torna aún más serio si pensamos que la ley del *Habeas Data* no es una norma específica para los sistemas de protección al crédito, y que el Código de Defensa del Consumidor a su vez no ha establecido prácticamente ninguna regla sobre el procedimiento que debe ser observado por el responsable del fichero, el participante y el afectado para que este último pueda ejercer sus derechos. De hecho, el sistema propuesto por Italia y España para el aludido procedimiento cuando no pormenoriza aún más las reglas a ser observadas específicamente para los sistemas de protección al crédito, el régimen general lo complementa, hecho que es imposible que ocurra en Brasil.

Analizando las legislaciones de los aludidos países europeos, a la legislación brasileña le falta mucho más que matices, pero un completo sistema de tutela de los derechos del afectado que no puede depender prácticamente en su totalidad de la interpretación jurisdiccional. Primero porque por sentido común, toda actividad desarrollada en una sociedad conlleva en sí la observancia por todos de derechos y obligaciones. De

---

<sup>668</sup> Vide [http://www.serasa.com.br/serasaexperian/agencias/agencias\\_al.htm](http://www.serasa.com.br/serasaexperian/agencias/agencias_al.htm)

otra parte, los datos tratados en estos ficheros, como hemos viniendo insistiendo en este trabajo de investigación, poseen más informaciones de lo que a primera vista se puede suponer, además de que son considerados como datos de carácter personales, y por lo tanto a quienes se refieran deben tener un mínimo de seguridad jurídica conferida previamente por el legislador, a través de una norma, y no posterior al daño causado que es lo que ocurre cuando se llega a la vía jurisdiccional.

Hoy por hoy la legislación brasileña carece de una reglamentación que estructure, organice y discipline con más claridad los derechos de los afectados, no solamente de un modo general pero también en el ámbito específico de los ficheros de morosos. Una somera observación de los sistemas de protección de datos de los países aquí estudiados muestra que tales derechos han sido notadamente con el pasar del tiempo cada vez más individualizados lo que demuestra la complejidad que implica garantizar un sistema que realmente tutele el individuo en relación a sus datos personales. Tal y como están sistematizados los derechos en Brasil, creemos que aún se está muy lejos de conseguir una efectiva tutela del derecho fundamental a la autodeterminación informativa.

## **5. Sanciones**

Como en Brasil no existe una autoridad de protección de datos y las reglas sobre el tratamiento de informaciones sobre solvencia patrimonial y crédito fueron confiadas al Código de Defensa del Consumidor y al Decreto 2.181/1997 que dispone sobre la organización del Sistema Nacional de Defensa del Consumidor.



Lo cierto es que las sanciones no están tan bien conectadas a un sistema de protección de datos, como es el caso de España e Italia. Aún así, incluso vista a través del derecho del consumidor, la legislación brasileña es muy débil. Exigir que exista un cuerpo legal de protección de datos personales en un Código del Consumidor puede que sea demasiado, sin embargo, mejor hubiera sido fijar pocas pero efectivas cláusulas sancionadoras. Uno de los puntos que nos parece criticable es que las descripciones de las infracciones administrativas son demasiado específicas, cuando se podrían haberlas dejado más abiertas ya que los preceptos que establecen los derechos de los afectados son, como hemos comentado, declaraciones de derechos.

La fiscalización de las prácticas de los ficheros de morosos fue encargada a los órganos responsables por el control de las relaciones de consumo. Así, como señala Roscoe Bessa<sup>669</sup>, la aplicación de las sanciones administrativas descritas en el Decreto 2.181/1997 y en el Código de Defensa del Consumidor es de atribución del *Procon*. El artículo 10 del citado Decreto determina que la fiscalización deberá ser efectuada por agentes fiscales, oficialmente designados, vinculados a los órganos de protección y defensa del consumidor en el ámbito federal, estatal, del Distrito Federal y de los municipios debidamente identificados.

En lo que concierne a las sanciones impuestas a la no observancia de los derechos estudiados, aquellas de naturaleza administrativa son fijadas por el aludido Decreto. Respecto al derecho de acceso, el art. 13, inciso X, establece que es considerada infracción el acto de impedir o dificultar el acceso gratuito del consumidor a las informaciones existentes en los banco de datos personales y de consumo, registrados sobre él, así como sobre las respectivas fuentes.

---

<sup>669</sup> ROSCOE BESSA, Leonardo. "Sistema Nacional de Defesa do Consumidor". En: VASCONCELOS BENJAMIN, Antonio Herman, LIMA MARQUES, Claudia, ROSCOE BESSA, Leonardo. *Manual De Direito do Consumidor*. São Paulo: Revista dos Tribunais, 2008, p. 326.

La infracción al derecho de rectificación, tipificada en el inciso XIV constituyese en dejar de corregir inmediata y gratuitamente la inexactitud de datos, cuando solicitado por el consumidor. Además, es igualmente infracción administrativa dejar de comunicar a éste, en el plazo de cinco días las correcciones de sus datos.

Finalmente, tocante al derecho de comunicación, el inciso XIII establece como infracción dejar de comunicar, por escrito, al consumidor el registro de sus datos personales y de consumo cuando no solicitada por él.

De otra parte, el Código de Defensa del Consumidor ha creado dos tipos penales en sus artículos 72 y 73. De suerte que el primero, vinculado al derecho de acceso, tipifica como crimen las conductas de impedir o dificultar el acceso del consumidor a las informaciones que sobre él consten en ficheros de cualquier especie. Prevé una pena de detención de un a seis meses o multa. Ya el otro tipo penal corresponde al derecho de rectificación, sanciona con las mismas penas las conductas de dejar de corregir inmediatamente información sobre el consumidor en banco de datos, fichas o registros que sabe o debería saber que era inexacta.

Algunas voces de la doctrina jurídica<sup>670</sup> opinan que todo ese conjunto de preceptos sobre el derecho a la rectificación, tanto en el ámbito constitucional, civil y en el penal muestra el alto grado de importancia en la prestación de informaciones exactas.

En nuestra opinión, la estructura legislativa de Brasil no puede funcionar si no hay una autoridad que se haga cargo de fiscalizar los ficheros. Establecer sanciones administrativas, exige que exista una estructura también en el ámbito administrativo para limitar, fiscalizar y corregir cuando necesario los abusos de los ficheros que se dedican a ésta actividad. De forma que desde nuestra opinión, lo más recomendable sería, a través de la creación legislativa, disciplinar todos los aspectos

---

<sup>670</sup> Vide SACCO NETO, Fernando, *Cadastro... op. cit.*, p. 86.

generales que deben seguir los bancos de datos con independencia de la actividad que desarrolle. Una ley, como la española o la italiana que incluya las principales directrices y principios a ser seguidos, y en lo que respecta a sanciones, no sean como actualmente mera declaraciones sin ningún efecto práctico.

Además, en el análisis hecho de la legislación brasileña, la creación de tipos penales no nos parece que es una forma de que el legislador exprese el grado de importancia de que se respeten determinadas conductas. Ha parecido un intento desesperado de compensar el desequilibrio entre la finalidad legal y las posibilidades reales ofrecidas por el Estado de ejercer su función fiscalizadora. No es otra la razón de que los Tribunales estén abarrotados de pedidos de indemnización por daños morales, fundados en los más diversos actos ilícitos pero que por lo general podrían ser evitados si la Administración asumiera la responsabilidad de fiscalización de tales ficheros. Asimismo, las sanciones penales no mejorarán ni impondrán límites a la actividad, ya que para que pueda ser efectiva, deberá perseguir individualmente a un sujeto (o sujetos) por una conducta específica en un momento determinado, no podrán sustituir la prevención administrativa necesaria. Así, consideramos que el sistema de sanciones de los ficheros solamente puede tornarse efectivo si se confiere no solamente en el plan normativo pero también en el práctico una estructura que pueda custodiarlos preventivamente evitando abusos.

## CONCLUSIONES (ESPAÑOL)

Aunque inevitablemente en estas páginas se repiten algunas de las afirmaciones que se han vertido en las precedentes, no nos parece que esté de más una breve recapitulación que de forma numérica nos ayude a precisar una reflexión final sobre esta investigación. En ella nos ceñimos a marcar la importancia de la informática en las relaciones sociales; y como no, al objeto y contenido de los ficheros, así como los destinatarios de las informaciones en ellos registradas. Además de ello, exponer las propuestas de cambio en la legislación brasileña tomando como referencia las directrices seguidas en el derecho español e italiano.

**PRIMERA.** El desarrollo de la informática ha modificado de manera muy marcada las relaciones sociales. Así, el cambio en el *modus vivendi* supone no solo alteraciones sino incluso el nacimiento de nuevas relaciones jurídicas y, con ellas, sus conflictos. El Derecho necesitaba y aún necesita responder adecuadamente ante el avance tecnológico a las nuevas formas de intromisiones ilícitas en las libertades y derechos individuales y también colectivos.

En esta perspectiva, en lo que concierne a los datos personales frente a las nuevas tecnologías, se ha operado una evolución en el concepto del derecho a la intimidad pero que no ha resultado del todo suficiente para tutelar a las personas en lo que respecta a esta materia. En este entorno surge el derecho a la autodeterminación informativa como un nuevo derecho autónomo capaz de hacer frente a los retos impuestos por la tecnología y los datos personales.

A nuestro juicio, el aludido derecho a la autodeterminación informativa por tratar de afrontar la evolución tecnológica, no puede ser limitado en su concepción e interpretación en función de los medios que actualmente pueden hacer efectivo su violación, dejándose ello a cargo del derecho objetivo a la protección de datos personales.

**SEGUNDA.** En cuanto al ámbito del derecho comparado, el derecho a la autodeterminación en Brasil encuentra su fundamento en la Constitución brasileña en el artículo 5º, inciso LXXII donde asegura el uso del instrumento del *habeas data* para el efectivo control de los datos personales, además de los artículos 1º, inciso III (dignidad de la persona humana como fundamento de la Republica Federativa de Brasil), y 3º, inciso I (construcción de una sociedad libre, justa y solidaria como uno de los objetivos fundamentales de la República Federativa de Brasil).

Pese a ello, un aspecto que debería ser reconsiderado por el legislador de Brasil es la aprobación de una ley general de protección de datos, que pueda además de declarar formal y específicamente este derecho de los ciudadanos, integrar las diversas normas que regulan ficheros y datos personales en el ordenamiento jurídico de este país, dando coherencia al sistema en esta materia, estableciendo los principios rectores, estructurando los derechos y obligaciones de todos los sujetos implicados.

**TERCERA.** En lo que concierne a los ficheros de solvencia patrimonial y crédito, en sus aspectos más generales hemos planteado algunas cuestiones que pueden ser aplicadas en cualquiera de los países estudiados. La primera, respecto a su finalidad. A nuestro juicio, entender estos ficheros desde la perspectiva que contribuyen para mejorar el flujo del mercado de consumo, y de este modo igualmente a la relación entre cliente-empresario es restricta y arcaica. Consideramos que estos sirven

como entidades auxiliaadoras del sistema financiero. Por ello, proponemos que el acceso a las informaciones contenidas en tales ficheros implique una imposición de deberes y responsabilidades por parte de aquellos que puedan acceder a ellas, fundamentalmente la de compartir los riesgos con quien haya establecido una relación de crédito, siempre que de tal persona se supiera —o se pudiese saber— su historial crediticio, ya que operaciones de este tipo pueden poner en peligro la salud del sistema financiero.

**CUARTA.** En relación al objeto de estos ficheros. Las informaciones tratadas en los mismos desde nuestra perspectiva, deben ser únicamente aquellas que resulten de una solicitud o una relación crediticia, excluyéndose cualquier registro de informaciones que procedan de relaciones de prestación de un servicio de facturación periódica ya que tales datos no tienen la capacidad de evaluar la solvencia patrimonial de una persona.

En cuanto a las aludidas informaciones de facturación periódica, consideramos que deberían formar parte de un fichero específico que serviría para alcanzar el objetivo de la protección sectorial de los prestadores de servicios dentro del mercado de consumo. es decir, registrar los datos de impago relativos a incumplimiento de obligación dineraria procedentes de contrato de prestación de servicios, siendo sus efectos semejantes a los del fichero de solvencia patrimonial, ante la imposibilidad del consumidor de contratar con otras empresas que prestasen el mismo servicio si sus datos estuviesen registrados en dicho fichero. A tales informaciones solamente podrían acceder las empresas del sector específico.

En lo que concierne a la cesión de tales datos, solamente serían de interés para el mercado de crédito en el caso de que una determinada

persona llegase a un específico valor de impago, debiendo ser fijado por la ley. De modo que alcanzado tal importe, sea por una deuda o la suma de varias, se podría permitir su comunicación a los ficheros de solvencia patrimonial y crédito.

**QUINTA.** En cuanto a los destinatarios de las informaciones. Opinamos que únicamente pueden acceder a las informaciones de un fichero de solvencia patrimonial y crédito los intermediarios financieros u otros sujetos privados en el ejercicio de una actividad comercial que conceden un aplazamiento de pago de la contrapartida por el suministro de bienes, pero todos ellos debidamente registrados en el Banco Central correspondiente a cada país y con sus actividades relativas a concesión de crédito aprobadas por el citado órgano.

Respecto a la legitimidad de la consulta sobre los datos registrados, sólo se debe acceder a ellos cuando se necesite enjuiciar la solvencia económica del afectado, pero especificándose dicha circunstancia. En nuestra opinión lo que legitima la consulta a los ficheros no es el mantenimiento de una relación contractual, sino la solicitud del afectado para concretarla. De este modo, aunque una entidad financiera comparta sus informaciones en el sistema de protección al crédito, ello no legitima el acceso indiscriminado a los datos sobre una persona que estén registrados en el fichero. Pasado el momento de la solicitud del crédito, las entidades solamente podrán acceder a los datos de un individuo cuando sea necesario actualizarlos.

En cuanto a legislación brasileña, después del estudio comparado con la normativa española e italiana, hemos planteados algunas cuestiones que desde nuestro punto de vista podría ser reconsideradas en el ordenamiento jurídico brasileño.

**SEXTA.** Inicialmente, la disciplina de los ficheros de solvencia patrimonial y crédito necesita salir completamente del Código de Defensa del Consumidor y tener su propia normativa, estructurada de modo a centrarse en el justo equilibrio de los intereses implicados, fundamentalmente en la tutela del ciudadano en todos sus aspectos y no solamente en la vertiente consumidor.

De esta manera, consideramos que en la ley propuesta para los ficheros de solvencia patrimonial y crédito el legislador debería incluir pormenorizadamente los requisitos de los datos que pueden ser registrados. Así, analizando comparativamente las legislaciones de España e Italia, desde nuestra perspectiva el legislador debería llevar en consideración la inserción en la ley de lo siguiente:

a) posibilidad de tratamiento de datos negativos y positivos, siempre que estos últimos solamente puedan ser registrados con el consentimiento del afectado.

b) de ser negativo, sería necesario que se tomaran determinadas medidas antes de la inclusión del mismo, como:

1) la existencia de una deuda cierta, vencida y exigible

2) la inexistencia de una reclamación de naturaleza judicial, administrativa o arbitral que necesariamente incida sobre la certeza, el vencimiento, la liquidez o exigibilidad de la deuda

3) la notificación al afectado de la existencia de una deuda y de su inminente inclusión en un fichero de solvencia patrimonial y crédito



4) la conservación del plazo de cinco años para que se pueda incluir una deuda, especificando a partir de qué momento empieza a contarse tal plazo, siendo nuestra opinión que éste se inicie a partir del vencimiento de la deuda.

En el caso de aquellas deudas en las que incide una reclamación judicial, administrativa o arbitral, el cómputo del plazo debería empezar a contarse a partir de la fecha de la publicación de la sentencia o en su caso de la decisión administrativa o arbitral que es cuando se constituye en un dato real y fiable.

**SÉPTIMA.** Aún en relación a los datos sobre los cuales hay una reclamación de naturaleza judicial o administrativa, a nuestro sentir, tales informaciones no deben ser excluidas del fichero pero si bloqueadas temporalmente hasta que se termine la controversia. De este modo, se confiere al gestor del fichero la responsabilidad de ejercer un control a través de un sistema de alerta sobre el deudor en el sentido de que se evite el abuso del derecho de contestar una deuda cada vez que ésta tuviese a punto de ser registrada en un fichero, evitando que se tenga un registro suyo de incumplimiento y así tener la posibilidad de solicitar otros créditos, es decir, la principal función sería evitar el abuso del derecho por parte del deudor con el uso múltiples demandas y reclamaciones. Los datos que estuviesen en el aludido sistema de alerta no podrían ser comunicados a ningún participante tales informaciones, excepto si se verifica abuso de derecho y por una decisión judicial o administrativa se permita su comunicación. En todo caso, tales datos deberían estar a disposición de la Administración pública, Jueces y Tribunales, durante el tiempo de la demanda. Una vez sea resuelta la disputa, o bien se procedería la supresión de los datos o bien se liberaría el acceso a los demás participantes del sistema, dependiendo del contenido de la resolución.

**OCTAVA.** Respecto a la modalidad de recogida y al registro de los datos, hemos observado que las principales preocupaciones de las legislaciones española e italiana se centran en el reparto de responsabilidades entre el acreedor y el responsable del fichero y en la notificación al interesado, aparte de lo que determina el régimen general. Para el sistema jurídico de Brasil, analizando también los problemas por varias veces discutidos en los tribunales sobre la determinación de la responsabilidad del acreedor y del responsable del fichero, asimismo de los costes que tienen que soportar esto último en su actividad, hemos observado lo siguiente:

En lo concerniente a su recogida, en Brasil, el legislador debería considerar la inclusión de un precepto que obligue al acreedor a informar desde la celebración del contrato la posibilidad que los datos puedan ser comunicados a un fichero de solvencia patrimonial. Para el registro de los datos, opinamos que habría que aclarar las responsabilidades de cada uno de los implicados. Y en lo que respecta al acreedor, exigirle como lo hace la ley italiana que éste compruebe y garantice que los datos informados al gestor puedan ser comunicados en el sistema y además que son exactos y correctos, es decir, fijarle la responsabilidad por la calidad de los datos. También comprometer al responsable del fichero a verificar de modo objetivo si los datos que van a ser registrados cumplen con los requisitos formales, y si hay más informaciones que deberían ser incluidas, o al revés, si existen algunas que faltan. Tales datos se refieren al nombre del deudor, dirección, número de documento de identidad, número de la factura no pagada, etc., en fin, informaciones objetivas que pueden ser controlarlas por el gestor, ya que es quien procede a su inclusión. De suerte que pensamos que el sistema propuesto por Italia de doble verificación es más seguro y además evitaría demandas innecesarias al Poder Judicial.

**NOVENA.** Creemos que en la notificación de inclusión se debe hacer constar un requerimiento de pago y que el legislador podría considerar fijar un plazo razonable para la inclusión de la información, contado a partir del recibimiento de tal notificación. Además, exigir, como lo hace la ley española, que su procedimiento se realice a través de un medio fiable, auditable e independiente de la entidad notificante, y que en todo caso la carga de la prueba de su cumplimiento sea del responsable del fichero. No obstante, la aludida notificación debería ser enviada a la dirección facilitada por el afectado en el momento de la celebración del contrato crediticio, de modo que no sea necesaria su recepción personal.

Igualmente, consideramos importante que se introduzca en la norma el momento en el cual se debe proceder la comunicación de la inminente inclusión de los datos y cuantos días se debe esperar entre tal comunicación y su efectivo registro en el fichero.

Para los datos obtenidos de fuentes accesibles al público, creemos que el afectado debería ser informado de la existencia de la deuda en el fichero. De modo que el responsable del fichero debe proceder una notificación para cada registro independiente de donde han sido recogidos los datos.

**DÉCIMA.** El matiz anteriormente mencionado de la definición de responsabilidad también influye en lo que concierne a la actualización de los datos contenidos en un fichero de solvencia patrimonial. Así, entendemos que la responsabilidad de actualizarlos es del acreedor ya que es el único que puede controlar la evolución de la deuda. Además, el gestor no tiene el poder de interferir en el fichero particular del acreedor que contiene las informaciones necesarias de sus clientes para proceder la mencionada actualización.

Ya en relación a las informaciones recogidas sobre las fuentes accesibles al público, pensamos que el legislador debería reconsiderar su elección en cuanto a la posible discrecionalidad sobre el proceder de la actualización. A este tenor, opinamos que el gestor es el responsable por actualizar esos datos. De suerte que no podrá excusarse de cumplir sus deberes, en base al argumento de que el origen de los datos es público. Pensamos que éste, asumiendo el riesgo propio de la actividad, habrá de tener la cautela mínima de actualizar tales datos, informar previamente al afectado de su inclusión y permitir que este ejerza todos los derechos que entienda necesarios.

Sobre la conservación de los datos entendemos que el plazo fijado de cinco años es razonable, y está de acuerdo con lo que se pretende con los registros en estos ficheros que son informaciones actuales sobre una persona. Además, igualmente es elogiable el precepto que determina que si se opera la prescripción de la deuda antes de estos cinco años deberá ser cancelada la información. No obstante, es importante que el legislador establezca a partir de cuando se empieza a contar el aludido plazo general de cinco años. En nuestra opinión, su cómputo debe comenzar a partir del vencimiento de la deuda.

**UNDÉCIMA.** Respecto a los derechos del afectado, la legislación brasileña necesita reconsiderar toda su estructura para sistematizar tales derechos. En nuestra opinión, el procedimiento general establecido por la ley del *Habeas Data* no es suficiente para sanar todas las cuestiones que pueden surgir en el intento del interesado en ejercer sus derechos. De modo que habría que además de hacer la mera declaración de derechos, establecer los matices específicos de cada uno de ellos que se pretende tutelar ante la actividad de información de datos sobre la solvencia patrimonial y crédito de los interesados, como la individualización y

conceptuación de cada uno de los derecho que posee el afectado, incluyendo además de los ya existentes, el de cancelación y oposición.

Sobre este aspecto, nos preocupa mucho que tenga que venir de la doctrina la interpretación de que el derecho a la rectificación pueda abarcar tanto el de cancelación, como el de oposición. De suerte que desde nuestra perspectiva, es imposible que estos estén conceptualmente mezclados. Principalmente respecto al derecho a oposición al tratamiento, pensamos que el legislador brasileño debería estimar su inserción urgente en el sistema jurídico, ya que rectificar y oponerse tienen naturaleza distinta. Es decir, el primero se vincula al principio de la calidad de los datos, mientras que el segundo encuentra su fundamento en el consentimiento y por lo tanto es muy difícil que pueda estar incluido dentro del concepto del derecho a la rectificación.

Fijar sus condiciones generales de ejercicio y su procedimiento y asimismo establecer la posibilidad de que el interesado pueda ejercerlos tanto a través del gestor como también de cualquiera de las entidades que participan del sistema de protección al crédito, compartiendo por lo tanto la responsabilidad entre todos los implicados en el aludido sistema.

**DUODÉCIMA.** Finalmente opinamos que en Brasil, el sistema de sanciones concernientes a los ficheros de protección de datos ha fracasado. El aparato sancionador de consumo no puede hacerse cargo de los pormenores que exige un tema como la protección de los datos personales. Hay un notorio desequilibrio entre la finalidad sancionadora y las posibilidades reales ofrecidas por el Estado de ejercer su función fiscalizadora. Aparte de ello, sin que exista una ley general de protección de datos que incluya las principales directrices y principios a ser seguidos, y en lo que respecta a sanciones, no sean como actualmente mera

declaraciones sin ningún efecto práctico, y además sin una autoridad competente para que cuide del cumplimiento de la aludida legislación y controle su aplicación, fundamentalmente de los ficheros de solvencia patrimonial y crédito, las pocas sanciones que se les puedan atribuir dentro de un Código del Consumidor no son efectivas, razón por la cual defendemos una completa reforma de la estructura legislativa brasileña en materia de protección de datos, incluyendo la creación de una autoridad de protección de datos inspirada en las que ya actúan en Europa.

## CONCLUSÕES (PORTUGUÊS)

Inevitavelmente nestas páginas se repetem algumas das afirmações que foram feitas nas precedentes, não parecendo que seja demasiado recapitular brevemente, de forma numérica de modo que nos ajude a precisar uma reflexão final sobre esta investigação. Nela nos centramos em marcar a importância da informática nas relações sociais e, como não, ao objeto e conteúdo dos bancos de dados, bem como dos destinatários das informações nestes registradas. Ademais, expor as propostas de mudança na legislação brasileira tomando como referencia as diretrizes seguidas no direito espanhol e italiano sobre a matéria.

**PRIMEIRA.** O desenvolvimento da informática modificou de modo muito significativo as relações sociais. Assim, o cambio no *modus vivendi* supõe não somente alterações mas o nascimento de novas relações jurídicas e, com elas, seus conflitos. O direito necessitava e ainda necessita responder adequadamente diante dos avanços tecnológicos às novas formas de intromissões ilícitas nas liberdades e direitos individuais e também coletivos.

Nesta perspectiva, no que concerne ao dados pessoais frente às novas tecnologias, operou-se uma evolução no conceito do direito da intimidade que sem embargo não foi suficiente para tutelar as pessoas no que respeita a esta matéria. Neste entorno surge o direito a autodeterminação informativa como um novo direito autônomo capaz de fazer frente aos retos impostos pela tecnologia e os dados pessoais

A nosso sentir, o aludido direito a autodeterminação informativa por tratar de afrontar a evolução tecnológica não pode ser limitado na sua conceituação e interpretação em função dos meios que atualmente podem efetivar sua violação, deixando isto a cargo do direito objetivo a proteção de dados.

**SEGUNDA.** Enquanto ao âmbito do direito comparado, o direito a autodeterminação informativa no Brasil encontra seu fundamento na Constituição Brasileira no artigo 5º, inciso LXXII, onde assegura o uso do instrumento do *Habeas Data* para o real controle dos dados pessoais, além dos artigos 1º, inciso III (dignidade da pessoa humana como fundamento da República Federativa do Brasil), e o 3º, inciso I (construção de uma sociedade livre, justa e solidaria como um dos objetivos fundamentais da República Federativa do Brasil).

Em que pese tudo que foi dito, um aspecto que deveria ser reconsiderado pelo legislador no Brasil é a aprovação de uma lei geral de proteção de dados, que possa além de declarar formal e especificamente este direito dos cidadãos, integrar as diversas normas que regulam os bancos de dados e os dados pessoais no ordenamento jurídico deste país, dando coerência ao sistema nesta matéria, estabelecendo os princípios reitores, estruturando os direitos e obrigações de todos os sujeitos implicados.

**TERCEIRA.** No tocante aos bancos de dados de solvência patrimonial e crédito, nos seus aspectos mais gerais, abordamos algumas questões que podem ser aplicadas a qualquer dos países estudados. A primeira, é sobre sua finalidade. Na nossa opinião, entender estes bancos de dados desde a ótica de que contribuem para melhorar o fluxo do mercado de consumo, e deste modo também a relação entre cliente-empresário é restrita e arcaica.



Consideramos que estes servem como entidades auxiliadoras do sistema financeiro. Por isso, propomos que o acesso às informações contidas em tais bancos de dados implique em uma imposição de deveres e responsabilidades por parte daqueles que podem aceder a elas, principalmente a de compartilhar os riscos com quem tenha estabelecido uma relação de crédito, sempre que de tal cliente pudesse, ou efetivamente se conhecesse, seu histórico creditício, já que comprovadamente estas operações podem colocar em perigo o sistema financeiro.

**QUARTA.** Em relação ao objeto destes bancos de dados. As informações ali tratadas, desde nosso ponto de vista, devem ser unicamente aquelas que resultem de uma solicitação ou uma relação creditícia, excluindo-se qualquer registro de informações que procedam de relações de prestação de um serviço de cobrança periódica, já que tais dados não tem a capacidade de valorar a solvência patrimonial de um indivíduo.

Enquanto as aludidas informações de cobrança periódica, consideramos que estas deveriam formar parte de um banco de dados específico que serviria para alcançar o objetivo da proteção setorial dos prestadores de serviço dentro do mercado de consumo. Ou seja, registrar os dados de dívidas relativas ao incumprimento de uma obrigação pecuniária procedentes de contrato de prestação de serviços, sendo seus efeitos semelhantes aos sistema de proteção ao crédito, impossibilitando que o consumidor contrate com outras empresas que prestem o mesmo serviço se seus dados se encontrarem registrados em tal cadastro. Estas informações somente estariam disponíveis às empresas deste setor específico.

No que concerne a cessão destes dados, apenas seriam do interesse do mercado de crédito no caso em que um determinado indivíduo alcançasse pelo seu inadimplemento um determinado valor, que deve ser fixado por lei. De forma que atingido este importe, seja por uma dívida ou pela soma de várias, poderia permitir sua comunicação aos sistemas de proteção ao crédito.

**QUINTA.** Com relação ao destinatários das informações. Opinamos que unicamente podem ter acesso as informações de um sistema de proteção ao crédito os intermediário financeiros ou outros sujeitos privados no exercício de uma atividade comercial que concedem um aprazamento do pagamento da contrapartida pelo fornecimento de bens. Contudo, todos estes devem estar devidamente registrados no Banco Central correspondente de cada país e com suas atividades relativas a concessão de crédito aprovadas pelo citado órgão.

Relativamente a legitimidade da consulta sobre os dados registrado, apenas se deve acessá-los quando seja necessária emitir um juízo sobre a situação de solvência econômica do interessado, especificando-se tal circunstância. Na nossa opinião, o que legitima a consulta a estes bancos de dados não é a manutenção de uma relação contratual, mas a solicitação do interessado para concretá-la. De este modo, mesmo que uma entidade financeira compartilhe suas informações em um sistema de proteção ao crédito, isto não legitima *de per si* o acesso indiscriminado aos dados de uma pessoa que estejam registrados nestes bancos de dados. Passado o momento de solicitação do crédito, as entidades somente poderão acessá-los quando seja necessária sua atualização.

Em relação a legislação brasileira, depois do estudo comparado com as normas espanhola e italiana, abordamos algumas questões que desde

nosso ponto de vista poderiam ser reconsideradas no ordenamento jurídico brasileiro:

**SEXTA.** Inicialmente, a disciplina dos sistemas de proteção ao crédito necessita sair completamente do Código de Defesa do Consumidor e ter sua própria normativa, estruturada de maneira que possa se centrar no justo equilíbrio dos interesses implicados, principalmente na tutela do cidadão em todos seus aspectos e não unicamente na sua vertente de consumidor.

Assim, consideramos que na proposta de lei para os sistemas de proteção ao crédito o legislador deveria incluir detalhadamente os requisitos dos dados que podem ser registrados. Dentro de uma análise comparativa das legislações da Espanha e Itália sobre este ponto, consideramos que o legislador deveria inserir na norma o seguinte:

a) possibilidade de tratamento de dados negativos e positivos, sempre que estes últimos apenas possam ser registrados com o consentimento do interessado.

b) com relação aos dados negativos, seria necessário que se tomassem algumas medidas antes da inclusão do mesmo, como:

1) a existência de uma dívida certa, vencida e exigível;

2) a inexistência de uma reclamação de natureza jurídica, administrativa ou arbitral que necessariamente incida sobre a certeza, o vencimento, a liquidez ou a exigibilidade da dívida;

3) a notificação ao interessado da existência de uma dívida e de sua iminente inclusão em um sistema de proteção ao crédito;

4) a conservação do prazo de cinco anos para que se possa incluir uma dívida, especificando a partir de que momento se começa a contar tal prazo, sendo nossa opinião que este comece a partir do vencimento da dívida.

No caso daquelas dívidas sobre as quais incide uma reclamação jurídica, administrativa ou arbitral, o início da contagem do prazo deveria ser a partir da data de publicação da sentença ou no caso da decisão administrativa ou arbitral, que é quando se constitui em um dado real e confiável.

**SÉTIMA.** Ainda em relação aos dados sobre os quais existe uma reclamação de natureza judiciária, administrativa ou arbitrariedade, a nosso sentir, tais informações não devem ser excluídas do banco de dados, mas apenas bloqueadas temporariamente até que se termine a controvérsia. De esta forma, confere-se ao gestor a responsabilidade de exercer um controle através de um sistema de alerta sobre o devedor no sentido de que se evite o abuso do direito de contestar uma dívida cada vez que esta estiver a ponto de ser registrada e assim ter a possibilidade de solicitar outros créditos. Ou seja, a principal função seria evitar o abuso do direito por parte do devedor com o uso de múltiplas demandas e reclamações. Os dados que estivessem no aludido sistema de alerta não poderiam ser comunicados a nenhum participante do sistema, exceto se se verifica o uso abusivo deste direito, e uma decisão judiciária ou administrativa permite sua comunicação. Em todo caso, tais informações deveriam estar a disposição da Administração pública e do Poder Judiciário. Uma vez que a disputa esteja resolvida, ou se suprime os dados ou se libera seu acesso, dependendo do conteúdo da resolução.

**OITAVA.** Com respeito a modalidade de coleta e registro dos dados, observamos que as principais preocupações das legislações espanhola e italiana se centram no repartido de responsabilidades entre o credor e o responsável pelo banco de dados e a notificação ao interessado, independente do que determina o regime geral das leis de proteção de dados. Para o sistema jurídico do Brasil, analisando também os problemas por varias vezes discutidos nos tribunais sobre a determinação da responsabilidade do credor e do gestor do banco de dados, assim como dos custos que tem que suportar este último por sua atividade, observamos o seguinte:

No que concerne a sua coleta, no Brasil o legislador deveria considerar a inclusão de um preceito que obrigasse ao credor a informar desde a celebração do contrato a possibilidade que os dados pudessem ser comunicados a um sistema de proteção ao crédito. Para o registro de informações, opinamos que haveria que aclarar as responsabilidades de cada um dos implicados. No tocante ao credor, exigir-lhe como faz a lei italiana que este comprove e garanta que os dados informados ao gestor possam ser comunicados no sistema e além disso que são exatos e corretos, ou seja, fixar-lhe a responsabilidade pela qualidade dos dados. Igualmente comprometer o responsável do banco de dados a verificação objetiva de que os dados que serão registrados cumprem com os requisitos formais e se há mais informações que deveriam ser inseridas ou, ao revés, se existe alguma que falta. Tais dados se referem ao nome do devedor, endereço, numero do documento de identidade, numero da fatura não paga, etc., enfim, informações objetivas que podem ser controladas pelo gestor já que é quem procede a inclusão. Desta maneira, pensamos que o sistema proposto pela Itália de dupla verificação é mais seguro e ademais evitaria demandas desnecessárias ao Poder Judiciário.

**NONA.** Cremos que na notificação de inclusão se deve fazer constar um requerimento de pagamento e que o legislador poderia considerar fixar um prazo razoável para a inclusão da informação, contado a partir

do recebimento de tal notificação. Ademais, exigir, como faz a lei espanhola, que seu procedimento se realize através de um meio confiável, auditável e independente da entidade notificante, y que em todo caso o ônus da prova do seu cumprimento seja do responsável do banco de dados. Não obstante, a aludida notificação deveria ser enviada a direção facilitada pelo afetado no momento da celebração do contrato creditício de modo que não seja necessária sua recepção pessoal.

Igualmente, consideramos que se introduza na norma o momento no qual se deve proceder a comunicação da iminente inclusão dos dados e quantos dias se deve esperar entre tal comunicação e seu efetivo registro no banco de dados.

Para os dados obtidos de fontes públicas, cremos que o interessado deveria ser informado da existência da dívida no banco de dados. Assim, o responsável pelo sistema de informação ao crédito deve notificar cada dívida registrada independente de onde foram coletadas.

**DÉCIMA.** O matiz anteriormente mencionado da definição da responsabilidade também influi na atualização dos dados contidos em um sistema de informação ao crédito. Assim, entendemos que a responsabilidade de atualizá-los é do credor já que é o único que pode controlar a evolução da dívida. Além disso, o gestor não tem o poder de interferir no banco de dados privado do credor que contém as informações necessárias de seus clientes para proceder a atualização do sistema de proteção ao crédito.

Em relação às informações coletadas nas fontes públicas, pensamos que o legislador deveria reconsiderar sua eleição no que tange a possível discricionariedade de proceder a atualização. Por tanto, opinamos que o gestor é o responsável por atualizar estes dados. De modo que não poderá

escusar-se de cumprir seus deveres, fundado no argumento de que a origem das informações é pública.

Pensamos que este haverá que ter a mínima cautela de atualizar os dados, informar previamente ao afetado da inclusão e permitir que este exerça todos os direitos que entenda necessários, assumindo o risco próprio da atividade.

Sobre a conservação dos dados, entendemos que o prazo fixado de cinco anos é razoável e está de acordo com o que se pretende com os registros nestes bancos de dados que são informações atuais sobre um indivíduo. Entendemos que é elogiável o preceito que determina que se se opera a prescrição da dívida antes destes cinco anos deverá ser cancelada a informação. Não obstante, é importante que o legislador estabeleça a partir de quando se começa a contar o aludido prazo geral de cinco anos. Em nossa opinião, seu cômputo deve iniciar-se a partir do vencimento da dívida.

**DÉCIMA PRIMERA.** Finalmente, com relação aos direitos do interessado, a legislação brasileira necessita reconsiderar toda sua estrutura para sistematizá-los. Na nossa opinião, o procedimento geral estabelecido pela lei do *Habeas Data* não é suficiente para sanar todas as questões que podem surgir no intento do interessado exercer seus direitos, estabelecer os matizes específicos de cada um deles que se pretende tutelar ante a atividade de informação de dados sobre a solvência patrimonial e crédito dos interessados, como a individualização e conceituação de cada um dos direitos que possui o afetado, incluindo ademais dos já existentes, o de cancelamento e oposição.

Sobre este aspecto, nos preocupa muito que tenha que vir da doutrina a interpretação de que o direito a retificação pode abarcar tanto o de cancelamento como o de oposição. De sorte que desde nossa ótica, é

impossível que estes estejam conceitualmente mesclados. Principalmente com relação ao direito a oposição ao tratamento, pensamos que o legislador brasileiro deveria estimar sua inclusão urgente no sistema jurídico brasileiro, já que retificar e opor-se tem naturezas distintas. Ou seja, o primeiro se vincula ao princípio da qualidade dos dados, enquanto que o segundo encontra seu fundamento no consentimento e por tanto é muito difícil que possa estar incluído dentro do conceito de direito a retificação.

Fixar suas condições gerais de exercício e seu procedimento e assim mesmo estabelecer a possibilidade de que o interessado possa exercê-los tanto através do gestor como também de qualquer das entidades que participam do sistema de proteção ao crédito, compartilhando por tanto a responsabilidade entre todos os implicados no aludido sistema.

**DÉCIMA SEGUNDA.** Opinamos que no Brasil, o sistema de sanções concernente aos bancos de dados de proteção ao crédito fracassou. O aparato sancionador de consumo não pode encarregar-se dos pormenores que exige um tema como a proteção de dados pessoais. Há um notório desequilíbrio entre a finalidade sancionadora e as possibilidades reais oferecidas pelo Estado no exercício de sua função fiscalizadora. Ademais, sem que exista uma lei geral de proteção de dados que inclua as principais diretrizes e princípios a serem seguidos e no tocante às sanções, sendo meras declarações sem nenhum efeito prático e, também, sem uma autoridade competente que vele pelo cumprimento da mencionada legislação e controle sua aplicação, fundamentalmente dos sistemas de proteção ao crédito, as poucas sanções que podem ser atribuídas dentro de um Código do Consumidor não são efetivas, razões pelas quais defendemos uma completa reforma da estrutura legislativa brasileira em matéria de proteção de dados, incluindo a criação de uma autoridade de proteção de dados inspiradas nas que já atuam na Europa.



**ESTUDIO COMPARADO DEL RÉGIMEN JURÍDICO DE LOS FICHEROS DE  
SOLVENCIA PATRIMONIAL Y CRÉDITO EN ESPAÑA, ITALIA Y BRASIL**

**Ludmila Albuquerque Douettes Araújo**

## ÍNDICE BIBLIOGRÁFICO

### **A. Fuentes legislativa, jurisprudencial y documentos de las agencias de protección de datos.**

#### A.1. Legislación.

##### *A.1.1. Internacional y Comunitaria.*

- Declaración Universal de los Derechos Humanos, de 10 de diciembre de 1948.

- Consejo de Europa. Resolución (73) 22, de 26 de septiembre de 1973, sobre la regulación jurídica de los ficheros electrónicos en el sector privado.

- Consejo de Europa. Resolución (74) 29 en el 26 de septiembre de 1974 la sobre la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector público.

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980.

- Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

- Carta de los derechos fundamentales de la unión europea, Hecho en Niza, el siete de diciembre 2000.

- Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea, *Diario Oficial n° C 115 de 09/05/2008*.

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

#### A.1.2. España

- Constitución Española de 1978.

- Ley Orgánica de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, 1/1982, de 5 de mayo

- Ley Orgánica de Tratamiento Automatizado de Datos de Carácter Personal, 5/1992, de 29 de octubre

- Ley Orgánica de Protección de Datos de Carácter Personal, 15/1999, de 13 de diciembre

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

*A.1.3. Italia.*

- Costituzione della Repubblica Italiana. Gazzetta Ufficiale della Repubblica Italiana n. 298, edizione straordinaria, del 27 dicembre 1947 .

- Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

- Legge 31 dicembre 1996, n. 676. "Delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"

- Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti. (G.U. n. 300 del 23 dicembre 2004)

- Decreto Legislativo 30 giugno 2003, n. 196. "Codice in materia di protezione dei dati personali"

- Legge 24 marzo 2001, n. 127. "Differimento del termine per l'esercizio della delega prevista dalla legge 31 dicembre 1996, n. 676, in materia di trattamento dei dati personali".

*A.1.4. Brasil.*

- Constituição da República Federativa do Brasil de 1988.

- Lei nº 8.078 de 11 de setembro de 1990, dispõe sobre a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor).

- Lei Complementar nº 105, de 10 de janeiro de 2001, dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

- Lei 9.507, de 12 de novembro de 1997, regula o direito de acesso a informações e disciplina o rito processual do habeas data.

- Decreto nº 2.181, de 20 de março de 1997, dispõe sobre a organização do Sistema Nacional de Defesa do Consumidor - SNDC, estabelece as normas gerais de aplicação das sanções administrativas previstas na Lei nº 8.078, de 11 de setembro de 1990, revoga o Decreto Nº 861, de 9 julho de 1993, e dá outras providências.

- Projeto de Lei nº 85/2009, do Senado Federal, disciplina o funcionamento de bancos de dados e serviços de proteção ao crédito e congêneres e dá outras providências

## A.2. Jurisprudencia.

### A.2.1. *España.*

Tribunal Constitucional, Sentencia 290/2000, de 30 de noviembre de 2000 (RTC 2000\290).

Tribunal Constitucional, Sentencia 292/2000, de 30 de noviembre de 2000 (RTC 2000\292).

Tribunal Supremo. Recurso de Casación para la unificación de doctrina núm. 39/2004, de 5 junio 2004. (RJ 2004\5849).

Tribunal Supremo. Sentencia de 28 de septiembre 2000 (R 7533).

Tribunal Supremo. Sentencia núm. 660, de 5 julio 2004 (RJ 2004\4941).

Audiencia Nacional. Sentencia de 8 junio 2001 (JUR 2001\293619).

Audiencia Nacional. Sentencia de 29 junio 2001 (JUR 2001\293759).

Audiencia Nacional. Sentencia de 15 junio 2001 (JUR 2001\293673).

Audiencia Nacional. Sentencia de 21 septiembre 2001 (JUR 2002\9279).

Audiencia Nacional. Sentencia de 14 junio 2002 (JUR 2003\49774).

Audiencia Nacional. Sentencia núm. 3128 de 29 octubre 2003 (JUR 2003\265306).

Audiencia Nacional. Sentencia de 24 enero 2003 (JUR 2005\190526).

Audiencia Nacional. Sentencia de 26 octubre 2005 (JUR 2005\261117).

Audiencia Nacional. Sentencia de 8 junio 2005 (JUR 2005\245068).

Audiencia Nacional. Sentencia de 4 octubre 2006 (JUR 2006\251327).

Audiencia Nacional. Sentencia de 4 octubre 2006 (JUR 2006\251350).

Audiencia Nacional. Sentencia de 8 marzo 2006 (JUR 2006\118267).

Audiencia Nacional, Sentencia de 6 abril 2006 (JUR 2006\147661).

Audiencia Nacional. Sentencia de 15 febrero 2006 (JUR 2006\119487).

Audiencia Nacional. 20 de Abril de 2006 (JUR 2006\152433).

Audiencia Nacional. Sentencia de 18 de enero de 2006 (RJCA 2006\601).

Audiencia Nacional. Sentencia de 18 abril 2007 (JUR 2007\132034)

Audiencia Nacional. Sentencia de 18 abril 2007 (JUR 2007\132034).

Audiencia Nacional. Sentencia de 3 octubre 2007 (JUR 2007\316038)

Audiencia Nacional. Sentencia de 3 septiembre 2007 (JUR 2007\276044).

Audiencia Nacional. Sentencia de 30 mayo 2007 (JUR 2007\199490).

Audiencia Nacional. Sentencia de 30 mayo 2007, (JUR 2007\19947).

Audiencia Nacional. Sentencia de 23 mayo 2007 (JUR 2007\142140).

Audiencia Nacional. Sentencia de 23 mayo 2007 (JUR 2007\142140).

Audiencia Nacional. Sentencia de 24 octubre 2007 (JUR 2007\346164).

Audiencia Nacional. Sentencia de 27 febrero 2008 (JUR 2008\97931).

Audiencia Nacional. Sentencia de 5 noviembre 2008 (JUR 2008\375602);

Audiencia Nacional. Sentencia de 10 julio 2008 (JUR 2008\291771).

Audiencia Nacional. Sentencia de 16 enero 2008 (JUR 2008\44422)

Audiencia Nacional. Sentencia de 11 diciembre 2008 (JUR 2009\3155).

Audiencia Nacional, Sentencia de 19 noviembre 2008 (JUR 2009\3381).

Audiencia Nacional en sentencia de 9 enero 2009 (RJCA 2009\217)

Audiencia Nacional, Sentencia de 25 junio 2009 (JUR 2009\308686).

Audiencia Nacional, Sentencia de 29 abril 2009 (JUR 2009\244875).

Audiencia Nacional. Sentencia de 15 octubre 2009 (JUR 2009\468479).

Audiencia Nacional. Sentencia de 11 marzo 2009 (RJCA 2009\301).

Audiencia Nacional. Sentencia de 10 septiembre 2009 (JUR 2009\416499).

Audiencia Nacional. Sentencia de 24 septiembre 2009 (JUR 2009\424380).

Audiencia Nacional. Sentencia de 9 enero 2009 (RJCA 2009\217).

Audiencia Nacional. Sentencia de 19 junio 2009 (JUR 2009\309588)

Audiencia Nacional. Sentencia de 19 noviembre 2009 (JUR 2010\18130).

Audiencia Nacional. Sentencia de 22 abril 2009 (JUR 2009\245632).

Audiencia Nacional. Sentencia de 28 mayo 2009 (JUR 2009\268420).

Audiencia Nacional. Sentencia de 29 mayo 2009 (JUR 2009\311922).

Audiencia Nacional. Sentencia de 29 mayo 2009 (JUR 2009\311922).

Audiencia Nacional. Sentencia de 9 enero 2009 (RJCA 2009\217).

Audiencia Nacional. Sentencia de 9 enero 2009 (RJCA 2009\217).

Audiencia Nacional. Sentencia de 9 enero 2009 (RJCA 2009\217).

Audiencia Nacional. Sentencia de 9 enero 2009 (RJCA 2009\217).



Tribunal de Defensa de la Competencia. Caso RAI. Resolución de 9 septiembre 2002 (JUR 2002\230127).

Tribunal Superior de Justicia de Andalucía. Sentencia núm. 2711/2003, de 18 septiembre (JUR 2003\243204).

Tribunal Superior de Justicia de Madrid, Sentencia núm. 565/2003 de 22 mayo (JUR 2004\143830).

Audiencia Provincial de Granada. Sentencia núm. 421/2009 de 25 septiembre (JUR 2010\5101).

Juzgado de lo Mercantil núm. 1 de Sevilla. Auto de 6 octubre 2006 (AC 2007\671).

#### *A.2.2. Italia.*

Tribunal de Roma, Sentencia de 14 de septiembre de 1953, en Foro Italiano, 1954, I.

Corte D'appello di Milano, Sentencia de 26 agosto 1960, en Foro Italiano, 1961, I.

Corte de Cassazione, Sentencia n.º 4487 de 22 de diciembre de 1956.

Corte de Cassazione, Sentencia n.º 990 de 20 de abril de 1963, en Foro Italiano, 1963.

Corte de Cassazione, Sentencia n.º 2.129, de 27 de mayo de 1975, en Foro Italiano, 1976,1.

Tribunal de Napoli, Sentencia de 15 de octubre de 2003.

Tribunal de Napoli, Sentencia de 12 de junio de 2003.

*A.2.3. Brasil.*

STF. MS 22801/DF, Rel. Min. Alberto Menezes Direito, 17/12/2007.

STJ, HD nº 147-DF (2006/0224991-/DF); Rel. Min. Arnaldo Esteves Lima; Julg. 12/12/2007.

STJ, REsp 22.337-8/RS, Rel. Min. Ruy Rosado de Aguiar, DJU 20.04.95.

STJ, REsp 22.337-8/RS, Rel. Min. Ruy Rosado de Aguiar, DJU 20.04.95.

STJ. Agravo de Instrumento nº 1.036.057-SP. Rel. Min. Aldir Passarinho Junior. J. 03 de marzo de 2009.

STJ. Agravo de Instrumento nº 833.769 – RS. Rel. Min. Humberto Gomes de Barros. Juzgado en 03 de diciembre 2007.

STJ. AgRg em Ag 1094459/SP, Rel. Min. Sidnei Beneti, juzgado em 19/05/2009.

STJ. AgRg en el Ag 713.629/ES. Rel. Min. Paulo Furtado, juzgado en 23/06/2009.

STJ. Recurso Especial nº 1.083.291 – RS. Rel. Min. Nancy Andrichi. Juzgado en 09 de septiembre de 2009.

STJ. Recurso Especial nº 720.493 - SP (2005/0014086-4). Rel. Min. Jorge Scartezzini. J. 16 de junio 2005.

STJ. Recurso Especial nº 781.969-RJ. Rel. Min. Luiz Fux, Juzgado en 08/05/2007.

STJ. Resp 285401/SP. Rel. Min. RUY ROSADO DE AGUIAR, J. 19/04/2001.

STJ. REsp 373.219/RJ, 4ª Turma, Rel. Min. Sálvio de Figueiredo, DJ 12/08/2002.

STJ. REsp 402.958/DF, 3ª Turma, Rel. Min. Nancy Andrighi, DJ 30/09/2002.

STJ. REsp 472203/RS. Rel. Min. Humberto Gomes, juzgado en 23 de junio 2004.

STJ. REsp 473873. Rel. Min. Nancy Andrighi. Publicado en 16 de mayo 2003.

STJ. RESP 686.203/AL, Rel. João Otávio de Noronha, DJe 15/06/2009.

STJ. RESP 994.638/AM, Rel. Min. Aldir Passarinho Junior, juzgado en 21.2.08.

STJ. REsp nº 229.278/PR, Rel. Ministro Aldir Passarinho Junior, DJU 07.10.2002.

STJ. Resp nº 527.618-RS. Rel. Min. Cesar Asfor Rocha, juzgado en 22 de octubre 2003.

TJDF, nº 20050111155592, Relator BENITO TIEZZI, juzgado en 04/10/2006.

TJDF, nº 2002.01.1.036295-2. Rel. Benito Augusto Tiezzi, juzgado en 18/12/2002.

TJDF. Apelação Cível no Juizado Especial. nº 2008.03.1.019128-9. Rel. José Guilherme. Juzgado en 08 de septiembre 2009.

TJDF. Número del proceso: 19980110248160, Rel. Min. VERA ANDRIGHI, juzgado en 17/05/1999.

TJRO. AC 200.000.2003.009620-0; Rel. Gabriel Marques de Carvalho; juzgado en 29/11/2005

TJRS, AC nº 70033790841, Rel. Des. Paulo Antônio Kretzmann, juzgado en 11 de febrero de 2010.

TJRS. AC nº 70002436368. Rel. Augusto Otávio Stern. Juzgado en 03 de abril de 2001.

TJRS. Recurso Inominado, nº 71002071314. Rel. Leila Vani Pandolfo Machado. Juzgado en 24 de marzo de 2010.

TRF 1ª R., AC 2007.38.13.004331-4/MG, Rel. Selene Maria Almeida, DJF 22/05/2009.

TRF 2ª R., RHD nº 2007.51.01.028690-5, Rel. Poul Erik Dyrlund, Juzgado en 03 de junio de 2008.

TRF 2ª R., RHD nº 762008.51.10.001149-1, Rel. Antonio Cruz Netto, DJU 06/08/2009.

TRF 2ª Região. Processo nº: 2000.02.01.055404-6. Rel. Des. Frederico Gueiros. Juzgado en 17 de junio de 2009.

TRF 4ª R., AC nº 2007.71.02.001229-8/RS, Rel. Marga Inge Barth Tessler; DEJF 02/03/2009.

TRF 4ª R., AI nº 2008.04.00.041892-3/SC, Rel. Celso Kipper, DEJF 07/04/200;

TRF 4ª R., AC nº 2007.70.06.002062-0, Rel. Celso Kipper, DEJF 18/11/2008;

TRF 5ª R., AC nº 2007.84.00.000789-1/RN, Rel. Barros Dias, DJU 09/03/2009.

TRF 5ª R., AC nº 2008.82.00.001275-8/PB, Rel. Margarida Cantarelli, DJU 09/07/2009.

TRF, 2ª R., RHD 2007.51.01.021645-9, Rel. Raldênio Bonifacio Costa, DJU 17/06/2009.

TRF, 4ª R., AC nº 2005.71.00.003081-0/RS, Rel. Victor Luiz dos Santos Laus DJU 30/11/2005.

TRF, 4ª R., AC nº 2008.72.004430-0, Rel. Romulo Pizzolatti, DEJF 25/08/2009.

Primeira Turma Recursal dos Juizados Especiais Cíveis e Criminais del Distrito Federal. Registro do Acórdão nº 276513, rel. Editte Patricion, juzgado en 03/04/2007.

#### *A.2.4. Otras Sentencias.*

Tribunal de Justicia de las Comunidades Europeas. Sentencia 6 de noviembre de 2003 (TJCE 2003\368).

Tribunal Constitucional Alemán, sentencia de 15 de diciembre de 1983, publicada en Boletín de Jurisprudencia Constitucional (BCJ), DARANAS, Manuel (trad.), núm. 33 (Enero 1984), Madrid: Publicaciones de las Cortes Generales

### A.3. Documentos de las Agencias de Protección de Datos.

#### A.3.1. España.

AEPD. Expediente nº E/00586/2004

AEPD. Expediente nº E/00613/2007.

AEPD. Expediente nº E/00858/2007

AEPD. Expediente nº E/00972/2006.

AEPD, Informe Jurídico nº 17/2009.

AEPD. Informe Jurídico nº 0052/2008.

AEPD. Informe Jurídico nº 0237/2009.

AEPD. Informe Jurídico nº 52/2008.

AEPD. Informe Jurídico nº 42/2008.

AEPD. Informe Jurídico nº 0342/2008.

AEPD. Informe Jurídico nº 234/2008.

AEPD. Procedimiento nº PS/00261/2007

AEPD. Resolución: R/00123/2005.

AEPD. Resolución: R/00130/2008.

AEPD. Resolución: R/00315/2007.

AEPD. Resolución: R/00739/2007.

AEPD. Resolución: R/00326/2004.

AEPD. Resolución: R/00657/2005.

AEPD. Resolución: R/00675/2008.

AEPD. Memoria 2007. Texto disponible en:

[http://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/memoria\\_AEPD\\_2007.pdf](http://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/memoria_AEPD_2007.pdf)

AEPD. “Inspección a un fichero común de información sobre solvencia patrimonial e incumplimiento de obligaciones dinerarias”. Disponible en:

[https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/recom\\_fichero\\_solvencia.pdf](https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/recom_fichero_solvencia.pdf)

*A.3.2. Italia.*

Garante per le protezione dei Dati Personali. Provvedimenti de 31 julio 2002. En: Bollettino n. 30 julio 2002, pag. 47.

Garante per la Protezione dei Dati Personali. Newsletter n° 238 del 20 - 26 dicembre 2004.

Garante per la Protezione dei Dati Personali. Provvedimento de 4 de mayo de 2006. Gestori Telefonici: Informazioni sulla Solvibilità e Affidabilità dei Clienti.

Garante per la Protezione dei Dati Personali. Provvedimento del 16 settembre 2004, en Bollettino n. 53/settembre 2004 (doc. web n. 1068987).

Garante per le Protezione dei Dati Personali. Bollettino n° 9, 34, de 2 de junio de 1999.

Garante per le protezione dei Dati Personali. Deliberazione n. 18 del 18 marzo 2010, en Bollettino del n. 114/marzo 2010.

Garante per le protezione dei Dati Personali. Deliberazione n. 9, de 16 novembre 2004. "Sistemi di informazioni creditizie e bilanciamento degli interessi". GU n. 300 del 23-12-2004.

Garante per le protezione dei Dati Personali. Dossier - 30 novembre 2005 "Le Nuove Regole sui Sistemi di Informazioni Creditizie".



## B. Bibliografía

AFONSO DA SILVA, José. Curso de Derecho Constitucional. São Paulo: Malheiros, 1998.

APARICIO SALOM, Javier. Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Navarra: Aranzadi, 2000.

ARRUDA ALVIM WAMBIER, Teresa (coord.). Habeas Data, São Paulo, Revista dos Tribunais, 1998.

BARDUSCO, Aldo. "Articolo 1 (Diritto alla protezione dei dati personali)". En Codice della Privacy: Commento al Decreto Legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative. Vitorio, Italia (coord.). Milano: Giuffrè, Vol. I, 2004.

BARROSO, Luis Roberto. "Viagem Redonda: Habeas Data, Direitos Constitucionais e Provas Ilícitas". En: ARRUDA ALVIM WAMBIER, Teresa (coord.). Habeas Data, São Paulo, Revista dos Tribunais, 1998.

BIANCA, Cesare Massimo. "Note Introdutive I". En BIANCA, Cesare Massimo y BUSNELLI, Francesco (Dir.). La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della privacy"). Milano: CEDAN, 2007.

BONET FERRER, José Luis. “La Importancia de las Marcas para la Empresa. Criterios de Valoración”. En: Fernández López, Juan Manuel (dir.). Propiedad Industrial. Estudios de Derecho Judicial, nº 49, Madrid: Consejo General del Poder Judicial, 2003.

BRINES ALMIÑANA, Javier. Novedades más significativas del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos. Editorial LA LEY. Diario La Ley, nº 6921, Sección Doctrina, 9 Abr. 2008, Año XXIX.

BUTTARELLI, Giovanni. Banche dati e tutela della riservatezza: la privacy nella società dell'informazione: commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale. Milano: Giuffrè Editore, 1997.

CAFARO, Rossana y PAGLIARO, Paolo. L'accesso al Credito. Banche Dati, Centrali Rischi y Privacy. Milano: Giuffrè, 2004.

CALDIROLA, Debora. Il Diritto alla Riservatezza. Milano: CEDAN, 2006.

CASSANO, Giuseppe, y FADDA, Stefano. Codice in materia di protezione dei dati personali: commento articolo per articolo al Testo unico sulla privacy D. lgs. 30 giugno 2003, n. 196. CASSANO, Giuseppe, y FADDA, Stefano (coord.), Milano: IPSOA, 2004.

CASTELLS, Manuel. La era de la información. Vol. 1, Madrid: Alianza, 2001.

CASUCCI, Felice. Tutela della privacy e misure di sicurezza dei dati personali. Napoli: Edizioni Scientifiche Italiane, 2006.

CECAMORE, Francesca. “Il sistema bancario, finanziario ed assicurativo”. En Il Diritto alla protezione dei Dati Personali: La disciplina sulla privacy alla luce del nuovo Codice. ACCIAI, Riccardo (Dir.), Santarcangelo di Romagna: Maggioli, 2004.

CHAVELI, Eduard. “El estatuto del encargado del tratamiento en el Reglamento de Desarrollo de la LOPD”. En MARÍ, Joana, VILASAU, Mònica (coord.). El Reglamento de protección de datos de carácter personal. Aspectos clave. Barcelona: UOC, 2008.

CIRILLO, Gianpiero Paolo. La Tutela della Privacy nel Sistema del Nuovo Codice sulla Protezione dei Dati Personali, Milan, CEDAM, 2004.

CLIMENT BARBERÁ, Juan. Derecho y nuevas tecnologías: lección magistral leída en la apertura del curso 2001-02. Valencia: Universidad Cardenal Herrera-CEU, 2001.

COMISIÓN EUROPEA. Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Documento de Trabajo: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. DG XV D/5025/98. WP 12. Aprobado por el Grupo de Trabajo el 24 de julio de 1998.

CORTES, Luis Javier, “Contratos y mercados financieros”. En: MENÉNDEZ, Aurelio (dir.). Lecciones de Derecho Mercantil. Navarra: Thomas Reuters, 2009.

CUFFARRO, Vincenzo. “Il Principio di Protezione dei Dati”. En Il Codice del Trattamento dei Dati personali. RICCIUTO, Vincenzo; D`ORAZIO, Roberto; CUFFARO, Vincenzo (coord.). Torino: G. Giappichelli, 2007.

CUPIS, Adriano de. “I diritto alla riservatezza esiste”. Foro Italiano, IV, 1954.

DATE, C. J. Introducción a los sistemas de bases de datos. Mexico: Pearson Educación, 2001.

DAVARA RODRIGUEZ, Miguel Angel. "Derecho y Tecnología de la Información". En BECERRIL RUIZ, Diego (coord.). TIC y sociedad en el siglo XXI. Granada: Editorial Universidad de Granada TIC y Sociedad en el Siglo XXI, 2007.

DAVARA RODRIGUEZ, Miguel Angel. "El nuevo Reglamento de Medidas de Seguridad de la ley de Protección de Datos". WESTLAW [en línea]. Actualidad Jurídica Aranzadi, núm. 690/2005.

DAVARA RODRÍGUEZ, Miguel Angel. La Protección de Datos en Europa. Madrid: Editorial Grupo Asnef Equifax, 1998.

DAVARA RODRIGUEZ, Miguel Angel. Manual de Derecho Informático. Navarra: Aranzadi, 2006.

DENNINGER, Erhard. "El Derecho a la autodeterminación informativa". En: PEREZ LUÑO, Antonio Enrique (Dir.). Problemas actuales de la documentación y la informática jurídica. Madrid: Tecnos, 1987.

DÍEZ-PICAZO, Luis Maria. Sistema de Derechos Fundamentales, Madrid: Thomson/Civitas, 2008.

DIEZ-PICAZO, Luis. Fundamentos de Derecho civil patrimonial. Pamplona: CIVITAS, 2008.

DOWNING, Douglas A.; COVINGTON, Michael A. y MAULDIN COVINGTON, Melody. Dictionary of Computer and Internet Terms. Hauppauge: Barron's, 10ª Edición, 2009.

DRUMOND, Victor. Internet, Privacidad y Datos Personales, Madrid: Reus, 2004.

ELLI, Gianmario; ZALLONE, Raffaele. Il nuovo Codice della privacy. Torino: G. Giappichelli, 2004.

ELMASRI, Ramez, NAVATHE, Shamkant B. Sistema de base de datos. Conceptos fundamentales. Mexico: Addison-Wesley Iberoamericana, 1997.

FATÁS. José Miguel. "Título Primero. Disposiciones Generales". En: PALOMAR OLMEDA, Alberto y GONZALEZ-ESPEJO, Pablo (Dir.). Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/199, de 13 de diciembre, de Protección de Datos de Carácter Persona (Aprobado por RD 1720, de 21 de diciembre). Cizur Menor: Thomson Civitas, 2008.

FERRAJOLI, Luigi. “Los Fundamentos de los Derechos Fundamentales”. En FERRAJOLI, Luigi [et. al.]. Los fundamentos de los derechos fundamentales,. Debate con Luca Baccelli et al. Madrid: Trotta. 2001.

FIORIGLIO, Gianluigi. Il Diritto alla privacy. Nuove frontiere nell’era di Internet. Bologna: Bononia University Press, 2008.

FIORIGLIO, Gianluigi. Temi di Informatica Giuridica [en línea],

[http://www.informaticagiuridica.com/temiig/fiorigliotemi\\_di\\_informatica\\_giuridica.pdf](http://www.informaticagiuridica.com/temiig/fiorigliotemi_di_informatica_giuridica.pdf)

FRANCESCHELLI, Bruno. Il diritto alla riservatezza. Napoli: casa Editrice Jovene, 1960.

FRAU, Riccardo. “Attività bancaria e trattamento dei dati personali”. En: CUFFARO, Vincenzo. Il Codice... op. cit. p. 785 y ss.; Casucci, Felice. Tutela della privacy e misure di sicurezza dei dati personali. Napoli: Edizioni Scientifiche Italiane, 2006

FREIXAS GUTIERREZ, Gabriel. La protección de los datos de Carácter Personal en el Derecho Español. Barcelona: Editorial Bosh, 2001.

FROSINI, Tommaso Edoardo. “Nuevas tecnologías y constitucionalismo”. Revista de Estudios Políticos, núm. 124, 2004.

FROSINI, Vittorio. “Banco de datos y tutela de la persona”. Revista de Estudios Políticos, núm. 30, Noviembre-Diciembre 1982.

GALETTA, Diana-Urania. “La cooperazione fra polizie e il Sistema informativo Schengen (SIS) per una sicurezza e una giustizia europee” En: LOSANO, Mario. La legge Italiana sulla privacy: un bilancio dei primi cinque anni, Laterza, 2001, Bari.

GARCÍA IZQUIERDO, Santiago. “El ‘saldo cero’ y los ficheros de prestación de servicios de información sobre solvencia patrimonial y crédito”. Revista de derecho bancario y bursátil, nº 87, 2002.

GARCÍA PÉREZ, Rosa. “Comentario al artículo 1.124”. En: Jurisprudencia Civil Comentada. PASQUAU LIAÑO, Miguel (Dir.). Granada: Comares, Tomo II, 2009.

GARCIA, Maria. “Habeas Data. O Direito à Informação. O Direito Fundamental à Intimidade, à Vida Privada, à Honra e à imagem das pessoas. Um Perfil Constitucional”. En ARRUDA ALVIM WAMBIER. Teresa (coord). Habeas Data, São Paulo, Revista dos Tribunais, 1998.



GIANNANTONIO, Ettore. Losano, Mario. Zeno- Zencovich, Vincenzo (Coord.). La tutela dei Dati Personali. Comentario alla Ley 675/1996, Padova: CEDAN, 1999.

GOBBATO, Monica. La tutela del consumatore: clausole vessatorie, commercio elettronico e codice del consumo. Matelica : Halley, 2007.

GONZALÉZ MÉNDEZ, Amelia. La Protección de Datos Tributarios y su Marco Constitucional. Valencia: Tirant lo Blanch. Consultado a través de Tirant On Line (370.005).

GONZALEZ MURÚA, Ana Rosa. El Derecho a la Intimidad, el Derecho a la Autodeterminación Informativa y la L.O. 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos Personales. Barcelona: Institut de Ciències Polítiques i Socials, 1994.

GRACIANO REGALADO, Juan Carlos. “Ficheros de información sobre solvencia patrimonial y crédito: los ficheros RAI y ASNEF”. Diario La Ley. 2005, nº 6223.

GRIMALD, Pedro. “El consentimiento y el tratamiento con fines publicitarios y prospección comercial”. En: El Reglamento de protección de datos de carácter personal. Aspectos clave. MARÍ, Joana, VILASAU, Mònica (coord.). Barcelona: UOC, 2008.

HEILBRONER, Robert L. “¿Son las maquinas el motor de la historia?”. En MARX, Leo; SMITH, Merritt Roe. Historia y determinismo tecnológico. Madrid: Alianza, 1996.

HERMAN DE VASCONCELOS BENJAMIN, Antonio; LIMA MARQUES, Claudia; ROSCOE BESSA, Leonardo. Manual de Direito do Consumidor. São Paulo: RT, 2008.

IMPERIALI, Riccardo. y IMPERIALI, Rosario. Codice della privacy. Commento alla normativa sulla protezione dei dati personali. Milano: Il sole-24 ore, 2005.

J. MITCHELL, William. E-topía. Valderrama, Fernando (trad.). Barcelona: Gustavo Gili, 2001.

KIRSCHEN, Sabina. “Il Codice della privacy, fra tradizione ed innovazione”. En: Libera circolazione e protezione dei dati personali. PANETTA, Rocco (coord.). Milano: Giuffré, Tomo I, 2006.

LAPORTA, Francisco. “Respuesta a Pérez Luño, Atienza y Ruiz Manero”. Doxa, nº 4, 1987.

LAPORTA, Francisco. "Sobre el Concepto de Derecho Humanos". *Doxa*, nº 4, 1987.

LAURIA TUCCI, Rogério. "Processo e Procedimento da Ação de Habeas Data". En:

LIMA MARQUES, Claudia. "Comentario al artículo 43". *Comentarios ao Código de defesa do Consumidor*. LIMA MARQUES, Claudia; HERMAN DE VASCONCELOS BENJAMIN, Antonio; MIRAGEM, Bruno. São Paulo: Revista dos Tribunais, 2006.

LLAMAS POMBO, Eugenio. "Comentario al artículo 1.101". En: *Jurisprudencia Civil Comentada*. PASQUAU LIAÑO, Miguel (Dir.). Granada: Comares, Tomo II, 2009.

LOSANO, Mario. *Curso de Informática Jurídica*. Madrid: Tecnos, 1987.

LUPO, Nicola. "Le fonti della privacy". CUFFARRO, Vincenzo. "Il Principio di Protezione dei Dati". En RICCIUTO, Vincenzo; D'ORAZIO, Roberto; CUFFARO, Vincenzo (coord.). *Il Codice del Trattamento dei Dati personali*. Torino: G. Giappichelli, 2007.

MALTA VIEIRA, Tatiana. *O Direito à privacidade na sociedade da informação*, Porto Alegre: Sergio Antonio Fabris Editor, 2007.

MANTOVANI, Ferrando. “La proclamación de los derechos humanos y la ineffectividad de los derechos humanos”. Trad., Peris Riera, Jaime M. (inédito). Conferencia realizada en la Facultad de Derecho de la Universidad de Granada, en 9 de abril de 2006.

MARIMPIETRI Flavia. “Consumismo e Superendividamento” [en línea]. Editora Magister. <https://www.magisteronline.com.br> . También disponible en: Revista Magister de Direito Empresarial, Concorrencial e do Consumidor nº 27 - Jun/Jul de 2009.

MARTIN PALLÍN, José Antonio. “Protección de los derechos y libertades individuales frente al uso de la informática y las telecomunicaciones”. Anuario de jornadas 1989-1990. Bilbao: Servicio de Estudios del IVAP, 1991.

MARTÍNEZ MARTÍNEZ, Ricard. “El Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Consideraciones generales”. Revista de Protección de Datos. Madrid: Agencia de Protección de Datos de la Comunidad de Madrid, 2007, nº 2.

MARTÍNEZ MARTÍNEZ, Ricard. “Las Medidas de Seguridad”. En MARTÍNEZ MARTÍNEZ, Ricard (coord.). Protección de datos Comentarios al Reglamento de Desarrollo de la LOPD. Comentarios al Reglamento de Desarrollo de la LOPD. Valencia: Tirant lo Blanch, 2009.

MARTÍNEZ MARTÍNEZ, Ricard. “Prólogo”. En MARTÍNEZ MARTÍNEZ, Ricard (coord.). Protección de datos Comentarios al Reglamento de Desarrollo de la LOPD. Comentarios al Reglamento de Desarrollo de la LOPD. Valencia: Tirant lo Blanch, 2009.

MARTÍNEZ SÁNCHEZ, M., “La notificación de ficheros para su inscripción en el Registro General de Protección de datos y la seguridad de las bases de datos”, en Protección de Datos de carácter personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos, celebrado en La Antigua-Guatemala del 2 al 6 de junio de 2003, Valencia, 2005.

MARX, Leo; SMITH, Merritt Roe. Historia y Determinismo Tecnológico. Madrid: Alianza, 1996.

MELCHIONNA, Silvia. “Principi generali”. En Il Diritto alla protezione dei Dati Personali: La disciplina sulla privacy alla luce del nuovo Codice. ACCIAI, Riccardo (Dir.), Santarcangelo di Romagna: Maggioli, 2004.

MEO, Baldo; CICCIA, Antonio. Privacy e Consumatori. Roma: Istituto poligrafico e Zecca dello Stato, Libreria dello Stato, 2006.

MESSIAS DE LA CERDA BALLESTROS, Jesus Alberto. *La Cesión o Comunicación de Datos de Carácter Personal*, Madrid: Civitas, 2003.

MORAES, Alexandre de, *Direito Constitucional*, São Paulo: Atlas, 2005.

MORENO NAVARRETE, Migual Angel. “Aspectos Jurídicos privados de las tecnologías Web 2.0 y su repercusión en el derecho de la intimidad”. En BOIX REIG, Javier (Dir.). *La protección Jurídica de la Intimidad*, Madrid: Iustel, 2010.

MORILLAS FERNÁNDEZ, Marta. “La protección jurídica del menor ante las redes sociales”. En BOIX REIG, Javier (Dir.). *La protección Jurídica de la Intimidad*, Madrid: Iustel, 2010.

MORMILE, Lalage. “Il Sistema di Informazioni Creditizie”. En *Libera circolazione e protezione dei dati personali*. PANETTA, Rocco (coord.), Milano: Giuffré, Tomo II, 2006.

MURILLO DE LA CUEVA, Pablo Lucas. “La Constitución y el Derecho a la autodeterminación informativa”, *Cuadernos de Derecho Público*, Madrid: Instituto Nacional de Administración Pública, 2003.

MURILLO DE LA CUEVA, Pablo Lucas. *El Derecho a la Autodeterminación Informativa*. Madrid: Tecnos, 1990.

MURILLO DE LA CUEVA, Pablo Lucas. *Informática y Protección de Datos Personales*. Madrid: Centro de Estudios Constitucionales, 1993.

NAVALPOTRO NAVALPOTRO, Yolanda. “Antecedentes de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (LOPD)”. En ALMUZARA ALMAIDA, Cristina (coord.). *Estudio Práctico sobre la protección de datos de carácter personal*. Lex Nova, Valladolid, 2007.

NIGER, Sergio, *La nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Milano: CEDAN, 2006.

NIGER, Sergio. “Il diritto alla protezione dei dati personali”. En MONDUCCI, Juri; SARTOR, Giovanni (coord.). *Il Codice in Materia di Protezione dei dati personali*. Milano: CEDAN, 2004.

NINNO, Alessandro del. “Nuove tecnologie e tutela del diritto alla protezione dei dati personali”,. En *I Diritto Della Persona: Tutela Civile, Penale, Amministrativa*, CEDON, Paolo (coord.). Torino: UTET, 2006.

NINNO, Alessandro del. *La tutela dei dati personali: guida pratica al Codice della privacy (D. lgs. 30.6.2003, n. 196)*, Padova: CEDAM, 2006.

NOJIRI, Sergio. “O Habeas Data e o Direito à Autodeterminação Informativa”. En En ARRUDA ALVIM WAMBIER. Teresa (coord). Habeas Data, São Paulo, Revista dos Tribunais, 1998.

OROZCO PARDO, Guillermo. “Consideraciones sobre los derechos de acceso y rectificación en el proyecto de Ley Orgánica de Regulación del tratamiento automatizado de los datos de carácter personal”. Informática y derecho: Revista iberoamericana de derecho informático, nº 4, 1994.

OROZCO PARDO, Guillermo. “Intimidad, privacidad «extimidad» y protección de datos del menor ¿Un cambio de paradigma?. En BOIX REIG, Javier (Dir.). La protección Jurídica de la Intimidad, Madrid: Iustel, 2010.

OROZCO PARDO, Guillermo. “Notas acerca del Régimen Jurídico de los Ficheros de Datos Personales de Titularidad Universitaria”. Informática y derecho: Revista iberoamericana de derecho informático, nº 23-26, 1998.

OROZCO PARDO, Guillermo. “La protección de datos en Derecho español a la luz de la reciente jurisprudencia constitucional”. Aranzadi. Actualidad civil, nº 1, 2002

OROZCO PARDO, Guillermo. “Los derechos de las personas frente al tratamiento de datos personales: un análisis crítico”. BECERRIL RUIZ,



Diego (coord.). TIC y sociedad en el siglo XXI. Granada: Editorial Universidad de Granada TIC y Sociedad en el Siglo XXI, 2007.

OROZCO PARDO, Guillermo. “Notas acerca de la L.O. 15/1999 de protección de datos de carácter personal: ¿una reformatio in peius?”. En HERRERA CAMPOS, Ramón (coord.). Homenaje al profesor Bernardo Moreno Quesada. Almería, Universidad de Almería (coeditado), Servicio de Publicaciones, Vol. 3, 2000.

ORTI VALLEJO, Antonio. “Cinco años de la Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal”, La Ley, Madrid, num. 4438, 1997.

ORTI VALLEJO, Antonio. “El nuevo derecho fundamental (y de la personalidad) a la libertad informática (a propósito de la STC 254/1993, de 20 de julio)”, Derecho privado y Constitución, nº 2, 1994.

ORTI VALLEJO, Antonio. Derecho a la intimidad e informática. Granada: Comares, 1994.

PARADISO, Massimmo. Corso di Istituzioni di Diritto Privato. Torino: Giappichelli, 2008.

PARDOLESI, Roberto. “Dalla Riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità”. En *Diritto alla riservatezza e circolazione dei dati personali*, PARDOLESI, Roberto (Dir.), Milano: Giuffrè, Vol. I, 2003.

PASCUAL HUERTA, Pablo. “Ficheros de Información Sobre Solvencia Patrimonial y Crédito (arts. 37 a 44)”. En: ZABÍA DE LA MATA, Juan. (coord.). *Protección de Datos. Comentarios al Reglamento*. Valladolid: Lex Nova, 2008.

PECORELLA, Claudia; DI PONTI, Riccardo. “Privacy y control del correo y de la navegación por la Red en el puesto de trabajo”. En: BOIX REIG, Javier (Dir.). *La protección Jurídica de la Intimidad*, Madrid: Iustel, 2010.

PELEGRINI GRINOVER, Ada; HERMAN DE VASCONCELOS BENJAMIN, Antonio; et al. *Código Brasileiro de Defesa do Consumidor: comentado pelos autores do anteprojeto*. Rio de Janeiro: RT, 2004.

PÉREZ LUÑO, Antonio Enrique. *Cibercidadani@ o ciudadaní@.com?*, Barcelona, Gedisa, 2004.

PÉREZ LUÑO, Antonio Enrique. “Concepto y Concepción de los Derechos Humanos (Acotaciones a la Ponencia de Francisco Laporta)”. *Doxa*, nº 4, 1987.

PÉREZ LUÑO, Antonio Enrique. "El Derecho a la autodeterminación informativa". En Anuario de jornadas 1989-1990: (Servicio de Estudios del IVAP). Bilbao, 1991.

PÉREZ LUÑO, Antonio Enrique. "Internet y los derechos humanos". Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento, nº. 2, Huelva, 2002.

PEREZ LUÑO, Antonio Enrique. "La protección de la intimidad frente a la informática en la Constitución Española de 1978". REP, 1979, nº. 9.

PÉREZ LUÑO, Antonio Enrique. "Las Generaciones de Derechos Humanos". Revista del Centro de Estudios Constitucionales, núm. 10 (Septiembre-Diciembre 1991).

PÉREZ LUÑO, Antonio Enrique. Derechos humanos, Estado de Derecho y Constitución, Madrid: Tecnos, 2005.

PÉREZ LUÑO, Antonio Enrique. Manual de Informática y Derecho. Barcelona: Editorial Ariel, 1996.

PERRI, Pierluigi. Privacy, Diritto e Sicurezza Informatica. Milano: Giuffrè, 2007.

PETER, Rob; CORONEL, Carlos. Sistemas de bases de datos: diseño, implementación y administración. México D.F.: Thomson Editores, 2004.

PETRULLI, Mario. Il nuovo Codice deontologico per le centrali rischi private e le tutele per i consumatore. Matelica: Editora Halley, 2005.

PETRULLI, Mario. Il nuovo Codice deontologico per le centrali rischi private e le tutele per i consumatore. Matelica: Editora Halley, 2005.

PIÑAR MAÑAS, José Luis. “El derecho fundamental a la protección de datos personales”. En PIÑAR MAÑAS, José Luis (dir.). Protección de datos de carácter personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos, La Antigua - Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch, 2006.

PIÑAR MAÑAS, José Luis. “El porqué de un Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos”. Revista de Protección de Datos. Madrid: Agencia de Protección de Datos de la Comunidad de Madrid, 2007, nº 3.

PINORI, Alessandra, “La responsabilità Civile per Trattamento Illecito dei Dati Personali”. En La Politica Economica tra Mercati e Regole: scritti

in ricordo di Luciano Stella. Barberis, Guido, et al. (Dir.), Catanzaro: Rubbettino.

PIRAINO, Fabrizio. "Il codice della privacy e la tecnica del bilanciamento di interessi". Libera circolazione e protezione dei dati personali. CEDON, Paolo (coord.) Milano: Giuffré, Vol. I, 2006.

PLANA, Maria del Carmen. "Ficheros sobre Solvencia Patrimonial y Crédito". En: Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/199, de 13 de diciembre, de Protección de Datos de Carácter Persona (Aprobado por RD 1720, de 21 de diciembre). PALOMAR OLMEDA, Alberto y GONZALEZ-ESPEJO, Pablo (Dir.). Cizur Menor: Thomson Civitas, 2008.

PRATS ALBENTOSA, Lorenzo. "Ficheros de información sobre solvencia patrimonial y crédito". En: MARTÍNEZ MARTÍNEZ, Ricard (coord.). Protección de datos Comentarios al Reglamento de Desarrollo de la LOPD. Comentarios al Reglamento de Desarrollo de la LOPD. Valencia: Tirant lo Blanch, 2009.

PRATS ALBENTOSA, Lorenzo. "Principios de Protección de Datos: Calidad de los Datos, Consentimiento para el Tratamiento de los Datos y Deber de Información". En PALOMAR OLMEDA, Alberto y GONZALEZ-ESPEJO, Pablo (Dir.). Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/199, de 13 de diciembre, de Protección de Datos de Carácter Persona (Aprobado por RD 1720, de 21 de diciembre). Cizur Menor: Thomson Civitas, 2008,

PUENTE ESCOBAR, Agustín. “Breve descripción de la evolución histórica de y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal”. PIÑAR MAÑAS, José Luis (dir.). Protección de datos de carácter personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos, La Antigua - Guatemala, 2-6 de junio de 2003. Valencia: Tirant lo Blanch, 2006.

PUENTE ESCOBAR, Agustín. “Consentimiento del afectado y deber de información”. En MARTÍNEZ MARTÍNEZ, Ricard (coord.). Protección de datos Comentarios al Reglamento de Desarrollo de la LOPD. Comentarios al Reglamento de Desarrollo de la LOPD. Valencia: Tirant lo Blanch, 2009.

PUENTE ESCOBAR, Agustín. “Legitimación para el tratamiento”. En MARTÍNEZ MARTÍNEZ, Ricard (coord.). Protección de datos Comentarios al Reglamento de Desarrollo de la LOPD. Comentarios al Reglamento de Desarrollo de la LOPD. Valencia: Tirant lo Blanch, 2009.

PUGLIESE, Giovanni. “Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche”. Foro Italiano, 1954, I.

QUADRI DI CARDANO, Gioacchino. La privacy informatica: trattamento dei dati personali e tutela dell'affidamento. Bologna: Libreria Bonomo, 2008.

RAMOS COVIZZI, Carlos Adroaldo. Práticas Abusivas da SERASA e SPC. São Paulo: Edipro, 2001.

REBOLLO DELGADO, Lucrecio. El Derecho Fundamental a la Intimidad, Madrid: Dykinson, 2005.

RECALDE CASTELLS, Andrés. “El papel del ‘Derecho’ en la crisis. Algunos aspectos de la regulación financiera y de las grandes empresas en su relación con la Economía”. Documentos de trabajo (Laboratorio de alternativas), nº. 150, 2009

RESTA, Fabio di. Protezione delle informazioni: privacy e sicurezza. Torino: G. Giappichelli, 2008.

RIBEIRO BASTOS, Celso. “Habeas Data”. En: ARRUDA ALVIM WAMBIER, Teresa. Habeas Data, São Paulo, Revista dos Tribunais, 1998.

RIVERO ALEMÁN, Santiago. Crédito, consumo y comercio eletrônico. Navarra: Aranzadi, 2002.

RIZZATTO NUNES, Luiz Antônio. Comentários ao Código de Defesa do Consumidor. São Paulo: Saraiva, 2009.

RIZZATTO NUNES, Luiz Antonio. Curso de Direito do Consumidor. São Paulo: Saraiva, 2007.

RODOTÀ, Stefano. Tecnologie e diritto. Bologna: Il Mulino, 1995.

ROSCOE BESSA, Leonardo. “Banco de Dados de Consumo”. En: HERMAN DE VASCONCELOS BENJAMIN, Antonio; LIMA MARQUES, Claudia; ROSCOE BESSA, Leonardo. Manual De Direito do Consumidor. São Paulo: Revista dos Tribunais, 2008.

ROSCOE BESSA, Leonardo. “Bancos de dados de proteção ao crédito e os limites jurídicos do tratamento de informações positivas”. Director: Gustavo Tepedino. Universidad del Estado de Rio de Janeiro. Facultad de Derecho, 2008.

ROSCOE BESSA, Leonardo. “Sistema Nacional de Defesa do Consumidor”. En VASCONCELOS BENJAMIN, Antonio Herman; LIMA MARQUES, Claudia; ROSCOE BESSA, Leonardo. Manual De Direito do Consumidor. São Paulo: Revista dos Tribunais, 2008.

ROSCOE BESSA, Leonardo. O Consumidor e os Limites dos Bancos de Dados de Proteção ao Crédito. São Paulo: RT, 2003.



ROSSI, Valentina. “Art. 117. Affidabilità e puntualità nei pagamenti”. En: CASSANO, Giuseppe, y FADDA, Stefano (coord.). Codice in materia di protezione dei dati personali: commento articolo per articolo al Testo unico sulla privacy D. lgs. 30 giugno 2003, n. 196. Milano: IPSOA, 2004

RUDELLI, Andrea. “Sistema Bancario, Finanziario ed Assicurativo”. En: AA.VV. Codice della privacy : commento al Decreto legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative. Milano: Giuffrè, Vol 1, 2004.

SACCO NETO, Fernando. Cadastros de Proteção ao Crédito. São Paulo: Método. Vol. 1. Parte Geral. 2009.

SATORETTI, Claudia. Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale. Torino: Giappichelli, 2008.

SCALISI, Antonino. Il Diritto alla Riservatezza. Milano: Giuffrè, 2002.

SERRANO PÉREZ, María Mercedes. “El derecho fundamental a la protección de datos. Su contenido esencial”. Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas, Sevilla, núm. 1, 2005.

SERRANO PÉREZ, Maria Mercedes. El Derecho Fundamental a la Protección de Datos, Derecho Español y Comparado. Madrid: Editorial Civitas, 2003.

SILEONI, Serena, SIMONCINI, Andrea. "I codici deontologici di buona condotta". En CUFFARO, Vincenzo (coord.). Il Codice del Trattamento dei Dati personali. Torino: G. Giappichelli, 2007.

STUART MILL, John. Sobre la libertad. AZCÁRATE, Pablo de (trad.). Madrid: Alianza, 2004.

TELLEZ AGUILERA, Abel. Nuevas Tecnologías. Intimidad y Protección de Datos. Madrid: Edisofer, 2001.

TONIATTI, Roberto. "Libertad Informática y Derecho a la Protección de los Datos Personales: Principios de Legislación Comparada". Anuario de jornadas 1989-1990. Bilbao: Servicio de Estudios del IVAP, 1991.

VECCHI, Paolo Maria. "Comentario al artículo 4º". En BIANCA, Cesare Massimo y BUSNELLI, Francesco (Dir.). La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della privacy"). Milano: CEDAN, 2007.

VECCHI, Paolo Maria. "Comentarios a los artículos 1º y 2º". En BIANCA, Cesare Massimo y BUSNELLI, Francesco (Dir.). La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della privacy"). Milano: CEDAN, 2007.

VITERBO, Francesco Giacomo. Protezione dei dati personali e autonomia privata: profili di interferenza e di reciproca funzionalizzazione. Napoli: Edizioni Scientifiche Italiane, 2008.

VIZCAINO CALDERÓN, Miguel. Comentarios a la Ley Orgánica de protección de datos de carácter personal. Madrid: Civitas, 2001.

VOTANO, Giulio, "Sistema Bancario, Finanziario ed Assicurativo". En BIANCA, Cesare Massimo y BUSNELLI, Francesco (Dir.). La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della privacy"). Milano: CEDAN, 2007.

WARREN, Samuel y BRANDEIS, Louis. "The Right to Privacy". *Harvard Law Review*. Vol. IV, nº. 5, Diciembre 1890.

ZANELLA DI PIETRO, Maria Sylvia. Direito Administrativo. São Paulo: Atlas, 2001.

ZENO-ZENCOVICH, Vincenzo. “Dieci anni di legislazione sui dati personali: tentativo di un bilancio”. En FRANCO FERRARI, Giuseppe (coord.). La legge sulla privacy dieci anni dopo. Milano: Egea, 2008.

## C. Bibliografía digital

### C.1. Artículos

ABREU DALARI, Dalmo. Derecho a la autodeterminación informativa y acción de Habeas Data en Iberoamérica [en línea]. Disponible en

[http://derecho.otalca.cl/pgs/revistas/ius/3-1-97/071\\_080\\_abreu.pdf](http://derecho.otalca.cl/pgs/revistas/ius/3-1-97/071_080_abreu.pdf)

BADIN Arthur; CARAZZA DOS SANTOS, Bruno; RIBEIRO DAMASO, Otávio. “Os Bancos de Dados de Proteção ao Crédito, o CDC e o PL 5.870/2005: comentários sobre Direito e Economia” [en línea]. Disponible en

<http://www.fazenda.gov.br/spe//publicacoes/reformasinstitucionais/estudos/ArtigoRevistaDireitoConsumido-BancosDados.pdf> , agosto de 2007.

BARBOSA MOREIRA, José Carlos. “O Habeas Data Brasileiro e a sua Lei Regulamentadora” [en línea]. Disponible en:

[www.senado.gov.br/web/cegraf/ril/Pdf/pdf\\_138/r138-09.pdf](http://www.senado.gov.br/web/cegraf/ril/Pdf/pdf_138/r138-09.pdf)

DABOVE, Maria Isolina. "Personas Jurídicas Publicas: ¿Titulares de Derechos Humanos? Algunas reflexiones desde la Filosofía del Derecho en España" [en línea], texto disponible en la pagina web:

<http://www.cartapacio.edu.ar/ojs/index.php/iyd/article/view/770/575>

GIOFFRÈ, Giovanni. "La privacy nella Pubblica Amministrazione e la sua tutela" [En línea], documento disponible en la pagina web:

<http://www.diritto.it/art.php?file=/archivio/26450.html>

MARSICANO, Giorgia. "Il nuovo codice deontologico per le centrali rischi private", en *Magistra, Banca e Finanza*,

[www.magistra.it](http://www.magistra.it) , 19 settembre 2005.

MURILLO DE LA CUEVA, Pablo Lucas. "Perspectivas del derecho a la autodeterminación informativa". En: "III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas" [monográfico en línea]. IDP. Revista de Internet, Derecho y Política. n.º 5. UOC.

<http://www.uoc.edu/idp/5/dt/esp/lucas.pdf>

NEDER MENEGHELLI, José Eduardo. "Temas sobre a anotação do Nome do Consumidor em Cadastro de Entidades Prestadoras de Serviços e Concedentes de Crédito" [en línea]., Vol. 47, nº 264. São Paulo: Revista Jurídica, out./1999, p. 84/86. Disponible en:

<http://www.prr5.mpf.gov.br/nid/0nid0551.htm>

PASSARINHO JUNIOR, Aldir Guimarães. "Cadastros de consumidores: questões controvertidas sob a ótica do Superior Tribunal de Justiça". Jus Navigandi, Teresina, ano 11, n. 1258, 11 dez. 2006. Disponible en:

<http://jus2.uol.com.br/doutrina/texto.asp?id=9177>

RODOTÁ, Stefano. Democracia y Protección de Datos Personales [en línea]. Agencia Española de Protección de Datos. Disponible en:

[https://www.agpd.es/portalweb/.../DemocraciaMadrid\\_mayo\\_05.pdf](https://www.agpd.es/portalweb/.../DemocraciaMadrid_mayo_05.pdf)

SAMPAIO FERRAZ JUNIOR, Tercio. Sigilo de dados: o Direito à privacidade e os limites à função fiscalizadora do Estado [en línea].

<http://www.terciosampaioferrazjr.com.br/?q=/publicacoes-cientificas/49>

SANTANIELLO, Giuseppe. I fattori evolutivi della codificazione concernente la protezione dei dati personali [en línea]. Roma: Interlex. 07.10.04.

<http://www.interlex.it/675/santaniello11.htm>

SANTANIELLO, Giuseppe. “Le nuove garanzie nell'era del diritto alla protezione dei dati personali” [en línea]. Roma: Interlex. 07.10.04.

<http://www.interlex.it/675/santaniello9.htm>

SETZER, Valdemar W. “Dado, Informação, Conhecimento e Competência” [en línea]. Disponible en la página web:

<http://www.ime.usp.br/%7Evwsetzer/dado-info.html>

SAFFO, Paul “Sensors: The Next Wave of Infotech Innovation” [en línea]. Disponible en

<http://www.saffo.com/essays/sensors.php>

TANG, Deyou; XI, Jianqing; YOU, Jinguo [et. al.]. “Data Evolution and Its Modeling” [en línea]. En IEEE Computer Society. Proceedings of the 2008 Fifth international Conference on Fuzzy Systems and Knowledge Discovery Volume 05 (18-20 Octubre 2008). Washington: 2008.

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4666596&number=4666476>

TEDLOW, Richard S. "Tecnologías que evolucionan y perduran" [en línea]. El País, documento disponible en la pagina web:

[http://www.elpais.com/articulo/espana/Tecnologias/evolucionan/perduran/elpeputec/20080412elpepunac\\_10/Tes](http://www.elpais.com/articulo/espana/Tecnologias/evolucionan/perduran/elpeputec/20080412elpepunac_10/Tes)

VILLAR MIR, Juan Miguel. La crisis económica actual. Sus orígenes y características. Medidas para salir de la crisis [en línea].

<http://www.copitiba.com/portal/DW/Ponencia.pdf>

C.2. Periódicos y documentos electrónicos.

El País. "Multa a Telefónica por hacer contratos de móviles a niños".

[http://www.elpais.com/articulo/sociedad/Multa/Telefonica/hacer/contratos/moviles/ninos/elpepisoc/20081209elpepisoc\\_2/Tes](http://www.elpais.com/articulo/sociedad/Multa/Telefonica/hacer/contratos/moviles/ninos/elpepisoc/20081209elpepisoc_2/Tes)

El Mundo. "El Crash de 2008. Borrachera de dinero".

<http://www.elmundo.es/especiales/2008/10/economia/crisis2008/lascausas/index.html>



Universo Online. "Site reúne dados sigilosos de cidadãos; senhas são vendidas".

<http://noticias.uol.com.br/ultnot/multi/2009/10/08/0402386EC4B94366.jhtm?site-reune-dados-sigiliosos-de-cidadaos-senhas-sao-vendidas-0402386EC4B94366>

Comitato parlamentare di controllo sull'attuazione ed il funzionamento della Convenzione di applicazione dell'Accordo di Schengen e di vigilanza sull'attività dell'unità nazionale Europol.

[http://www.camera.it/\\_bicamerali/schengen/notaintro/introfr.htm](http://www.camera.it/_bicamerali/schengen/notaintro/introfr.htm)

ComScore "'Digital World: State of the Internet' Report Highlights Growth in Emerging Internet Markets".

<http://www.comscore.com/press/release.asp?press=2115>

Relazione parlamentare di accompagnamento al testo del "codice in materia di protezione dei dati personali".

<http://www.privacy.it/codprivacyattiparl.html>

Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data.

[http://ec.europa.eu/justice\\_home/fsj/privacy/law/implementation\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm)

Secretaria da Justiça e Defesa da Cidadania. “Cadastro de reclamações fundamentadas. Período 2008”. São Paulo, 2009.

[http://www.procon.sp.gov.br/pdf/ACS\\_Ranking\\_de\\_reclama%C3%A7%C3%B5es\\_2008.pdf](http://www.procon.sp.gov.br/pdf/ACS_Ranking_de_reclama%C3%A7%C3%B5es_2008.pdf)

Sistema de Informações de Crédito do Banco Central.

<http://www.bcb.gov.br/fis/crc/ftp/cartilhascr.pdf>

SPC Brasil. “Indicador e Vendas e Inadimplência Dezembro de 2009”.

[http://www.spcnegocios.org.br/imprensa/Releases/Release\\_Indicador\\_CNDL\\_SPCBRASIL\\_Dezembro2009.pdf](http://www.spcnegocios.org.br/imprensa/Releases/Release_Indicador_CNDL_SPCBRASIL_Dezembro2009.pdf)

C.3. Fuentes digitales consultadas.

Agencia Española de Protección de Datos.

<https://www.agpd.es/>

Banca d'Italia.

<http://www.bancaditalia.it>

Banco Central do Brasil

<http://www.bacen.gov.br>

EUR-Lex.

<http://eur-lex.europa.eu>

Garante per la protezione dei dati personali.

<http://www.garanteprivacy.it>

Ministério da Fazenda do Brasil.

<http://www.fazenda.gov.br>

Naciones Unidas – Derechos Humanos.

<http://www.ohchr.org>

Presidencia da República Federativa do Brasil.

<http://www.planalto.gov.br>

Privacy International.

<http://www.privacyinternational.org>

Senado Federal de Brasil.

<http://www.senado.gov.br>

Serasa-Experian.

<http://www.serasa.com.br>

Società Interbancaria per l'Automazione (SIA) - Società per i Servizi Bancari (SSB).

<http://www.siasb.eu>