



**XUNTA DE GALICIA**

CONSELLERÍA DE INNOVACIÓN  
E INDUSTRIA

Dirección Xeral de Promoción Industrial  
e da Sociedade da Información



Fundación para o Fomento  
da Calidade Industrial e  
o Desenvolvemento  
Tecnolóxico de Galicia



# A PROTECCIÓN DE DATOS DE CARÁCTER PERSOAL

Revisión teórica e grao de cumprimento

## Coordinadores:

Manuel Martínez Carballo  
Eduardo Guillén Solórzano  
Susana Barbeito Roibal



**OBSERVATORIO GALEGO**  
DA SOCIEDADE DA INFORMACIÓN

## Colaboran:



UNIVERSIDADE DA CORUÑA



UNIVERSIDADE  
DE VIGO

**AENOR**

Asociación Española de  
Normalización y Certificación

### **Licenza de Uso**

Este documento distribúese baixo Licenza Creative Commons Atribución/Non Comercial/Compartir Igual. Vostede é libre de copiar, distribuír e comunicar publicamente a obra, e facer obras derivadas dela baixo as condicións seguintes:

**Recoñecemento:** Debe recoñecer os créditos da obra do xeito especificado pola (persoa) autora ou pola licenciadora (pero non de xeito que suxira que ten o seu apoio ou apoian o uso que fan da súa obra).

**Non comercial:** Non pode empregar esta obra para fins comerciais.

**Compartir baixo a mesma licenza:** Se altera ou transforma esta obra, ou xera unha obra derivada, só pode distribuír a obra xerada baixo unha licenza idéntica a esta.

Teña en conta que ao reutilizar ou distribuír a obra, ten que deixar ben claro os termos da licenza desta obra; algunha destas condicións pode non aplicarse se se obtén o permiso da persoa titular dos dereitos de autoría e nada nesta licenza menoscaba ou restrinxen os dereitos morais dela.

Os dereitos derivados de usos lexítimos ou outras limitacións non se ven afectados polo anterior. Isto é un resumo facilmente lexible do texto legal (licenza completa) que pode obterse na seguinte URL: <http://creativecommons.org/licenses/by-nc-sa/3.0/deed.gl>

Este documento foi elaborado polos autores para a Fundación para o Fomento da Calidade Industrial e o Desenvolvemento Tecnolóxico de Galicia, pertencente á Consellería de Innovación e Industria.

A publicación deste informe correspóndese coa iniciativa CES-LA2-14 -Acceso libre aos contidos de orixe pública- do Plano Estratéxico Galego da Sociedade da Información (PEGSI).

O contido deste informe non representa necesariamente unha posición oficial da Xunta de Galicia.

### **A PROTECCIÓN DE DATOS DE CARÁCTER PERSOAL**

Revisión teórica e grao de cumprimento

© 1ª edición - Santiago de Compostela, decembro de 2007

#### **Coordinadores:**

Manuel Martínez Carballo  
Eduardo Guillén Solórzano  
Susana Barbeito Roibal

#### **Autores:**

Susana Álvarez González  
Manuel Martínez Carballo  
Eduardo Guillén Solórzano  
Susana Barbeito Roibal  
Mª Cruz del Río Rama  
Martín Pita López

#### **Edita:**

Fundación para o Fomento da Calidade Industrial e o Desenvolvemento Tecnolóxico de Galicia  
Dirección Xeral de Promoción Industrial e da Sociedade da Información  
Consellería de Innovación e Industria  
Xunta de Galicia

#### **ISBN:**

Depósito Legal: C 4254-2007

# ÍNDICE

# ÍNDICE DE CONTIDO

<b>CAPÍTULO 1. MARCO NORMATIVO E CONCEPTUAL DA PROTECCIÓN DE DATOS DE CARÁCTER PERSOAL.....</b>	<b>5</b>
1. INTRODUCCIÓN.....	6
2. CONCEPTO.....	8
3. A CONSOLIDACIÓN DO DEREITO Á AUTODETERMINACIÓN INFORMATIVA: O PAPEL DO TRIBUNAL CONSTITUCIONAL.....	10
4. O MARCO NORMATIVO.....	13
5. PRINCIPIOS DE CALIDADE DOS DATOS E DEREITOS DO INTERESADO: O CONTIDO DO DEREITO Á PROTECCIÓN DE DATOS NA LOPD.....	16
5.1. DEFINIÇÕES LEGAIS.....	16
5.2. PRINCIPIOS DE PROTECCIÓN DE DATOS. REQUISITOS PARA O TRATAMENTO DOS DATOS PERSOAIS.....	18
5.3. DEREITOS DOS INTERESADOS.....	20
6. NOTIFICACIÓN E INSCRICIÓN REXISTRAL.....	22
7. INFRACCIÓN E SANCIÓNS.....	23
8. RESUMO DOS DEBERES E OBRIGAS DO RESPONSABLE DO FICHEIRO E DO ENCARGADO DO TRATAMENTO.....	24
<b>CAPÍTULO 2. PASOS PRÁCTICOS PARA A APLICACIÓN DA LOPD.....</b>	<b>26</b>
<b>CAPÍTULO 3. NIVEL OU GRADO DE CUMPRIMENTO DA LOPD.....</b>	<b>30</b>
1. INTRODUCCIÓN.....	31
2. FICHEIROS DE TITULARIDADE PRIVADA.....	31
2.1. INTRODUCCIÓN.....	31
2.2. GRAO DE CUMPRIMIENTO EN ESPAÑA.....	32
2.3. GRAO DE CUMPRIMIENTO EN GALICIA.....	40
3. FICHEIROS DE TITULARIDADE PÚBLICA.....	42
4. SOPORTE DAS OPERACIÓNS ANTE O RGPD.....	45
<b>CAPÍTULO 4. A SOCIEDADE DA INFORMACIÓN E A PROTECCIÓN DE DATOS DE CARÁCTER PERSOAL. ESPECIAL REFERENCIA Á LEI 25/2007.....</b>	<b>47</b>
<b>CAPÍTULO 5. CONCLUSIÓNS E REFLEXIÓNS FINAIS.....</b>	<b>58</b>
<b>REFERENCIAS BIBLIOGRÁFICAS E PÁXINAS WEB DE INTERESE.....</b>	<b>62</b>
<b>ANEXOS</b>	
<b>ANEXO I. A LOPD E AS AUDITORÍAS DE CALIDADE.....</b>	<b>67</b>

# CAPÍTULO 1

## **MARCO NORMATIVO E CONCEPTUAL DA PROTECCIÓN DE DATOS DE CARÁCTER PERSOAL**

Susana Álvarez González  
*Universidade de Vigo*

## 1. INTRODUCCIÓN

A preocupación pola protección dos datos de carácter persoal ten a súa orixe no desenvolvemento das denominadas tecnoloxías da información. A expresión “sociedade da información” fai referencia ao papel absolutamente central que a información e a comunicación ten na actualidade no interior da organización social, do mundo produtivo, dos procesos políticos e de todo mecanismo decisorio (Toniatti, 1991:141). É sen dúbida a nosa unha época caracterizada pola acumulación da información (Garriga Domínguez, 2004:12). Existen bases de datos sobre as cuestións máis dispares. Este afán por recoller e acumular datos non exclúe aqueles que fan referencia de forma directa ás persoas. Pola contra, pode dicirse que este tipo de información é a máis prezada e valorada, ata o punto que forma parte do activo de calquera empresa, asociación ou Administración Pública.

O uso das tecnoloxías da información e comunicación posibilitan a recollida e utilización de información sobre as persoas de xeito ilimitado, permitindo ademais a interrelación de datos de carácter persoal con independencia de que estes se encontren en arquivos distintos, se refiran a diferentes etapas da vida da persoa ou do lugar onde foron recollidos. O tratamento da información constitúe pois una fonte inesgotable de poder para aqueles que a posúen, que se fai efectivo cando as novas tecnoloxías permiten converter informacións parciais en informacións en masa e organizadas (Del Peso y Ramos, 1994:13) ou encontrar de forma inmediata e comunicar coa mesma rapidez informacións obtidas deste xeito (Vizcaíno Calderón, 2001: 34).

Pero, o tratamento da información de carácter persoal leva tamén aparelado una serie de riscos para a persoa e para os seus dereitos fundamentais. As posibles agresións aos dereitos fundamentais serán máis directas e violentas canto máis sensible sexa a información manexada. Este perigo consiste esencialmente na construción dos denominados perfís da personalidade mediante a interrelación de informacións de carácter persoal en función dos que se tomen decisións (Lucas Murillo de la Cueva, 1999:38). Este perfil, con independencia do seu tipo, permite obter unha radiografía de toda ou parte da vida dunha persoa, así como prever ou intuír reaccións e comportamentos futuros (Garriga Domínguez, 2004:25). A elaboración de perfís da personalidade permite, por unha parte, o establecemento dunha correlación entre a posesión de determinadas características e comportamentos concretos e, por outra, a posibilidade de predicir, mediante certas operacións, o comportamento futuro dunha persoa, en función do que se adoptarán decisións, favorables ou desfavorables. Dende este punto de vista, o individuo queda exposto ao que Frosini (1982:178) denomina xuízo universal permanente. Cada persoa fichada nun banco de datos encóntrase polo tanto exposto a unha vixilancia continua e, na maioría dos casos, inadvertida (Pérez Luño, 2003:134).

Por este motivo, preséntase como imprescindible a busca do equilibrio entre a necesidade de solicitar datos e a necesaria protección da “privacidade” da persoa. Consecuencia da busca deste equilibrio foi o recoñecemento no Ordenamento xurídico español dun novo dereito fundamental: o dereito á

protección de datos persoais, coñecido tamén como dereito á autodeterminación informativa ou liberdade informática<sup>1</sup>.

O citado dereito está recollido de forma expresa no artigo 18.4 do texto Constitucional español nos seguintes termos:

“A Lei limitará o uso da informática para garantir o honor e a intimidade persoal e familiar dos cidadáns e o pleno exercicio dos seus dereitos”.

Como desenvolvemento deste precepto constitucional foi aprobada a Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal (LOPD)<sup>2</sup>. Esta Lei obriga a tódalas persoas ou empresas que recollan datos de carácter persoal a facer un bo uso e utilización deses datos, xa sexan datos dos seus clientes, traballadores, etc. Con esta finalidade impón unha serie de obrigas ao denominado responsable do ficheiro, entendido como persoa física o xurídica, de natureza pública o privada, ou órgano administrativo, que decida sobre a finalidade, contido e uso dos datos e, no seu caso, ao encargado do tratamento definido pola Lei como a persoa física ou xurídica, autoridade pública, servizo ou calquera organismo que, só ou conxuntamente con outros, trate datos persoais por conta do responsable do tratamento. O incumprimento destas obrigas legais pode derivar en sancións económicas que van dende os 601, 01 € ata 601.012,1 € no ámbito privado.

De xeito paralelo a estas obrigas, outorga a citada Lei una serie de dereitos ao titular dos datos de carácter persoal para facer efectivo o control da información tanto no momento da recollida, como posteriormente, especialmente nos casos de cesión ou comunicación.

O cumprimento deste requisitos afectarán polo tanto a todas as entidades que recollan e traten datos de carácter persoal, independente do arquivo informático o non dos datos. Neste senso, fronte a derogada LORTAD<sup>3</sup> que deixaba fóra do seu ámbito de aplicación aos ficheiros non automatizados, a vixente LOPD inclúe dentro do seu ámbito a tódolos datos de carácter persoal rexistrados en soporte físico que os faga susceptibles de tratamento e toda modalidade de uso posterior deses datos, de tal forma que inclúe tamén os datos persoais contidos en ficheiros manuais. As razóns desta inclusión pódense encontrar na Normativa Comunitaria. A LOPD, establecía, en todo caso, un prazo de adaptación xeneroso en relación cos denominados pola Lei “ficheiros preexistentes”<sup>4</sup>: doce anos dende o 24 de outubro de 1995. O citado prazo rematou o pasado 24 de outubro de 2007.

---

<sup>1</sup> Conven matizar que é habitual utilizar estes tres termos como sinónimos. Pero, como sinala Pérez Luño (1990:139,141), a citada asimilación non é tecnicamente correcta, posto que aínda que o dereito a autodeterminación informativa coincide co alcance da liberdade informática, é necesario diferenciar ambos os dous da expresión “protección de datos persoais”. Esta última, aínda que alude a unha mesma realidade, fai referencia ao conxunto de bens e intereses que poden verse afectados pola elaboración de informacións referentes a persoas identificadas ou identificables e non a un dereito fundamental.

<sup>2</sup> BOE de 14 de decembro de 1999.

<sup>3</sup> Lei Orgánica 5/1992, de 29 de outubro, de Regulación do Tratamento Automático dos Datos de Carácter Persoal (LORTAD). BOE núm. 262, de 31 de outubro de 1992.

<sup>4</sup> Disposición Adicional Primeira da LOPD.

Unicamente quedan excluídos do ámbito de aplicación da LOPD:

- a) Os ficheiros utilizados por persoas físicas no exercicio de actividades exclusivamente persoais ou domésticas.
- b) Os ficheiros sometidos á normativa sobre protección de materias clasificadas.
- c) Os ficheiros para a investigación de terrorismo e de formas graves de delincuencia organizada.

Por outra parte, réxense polas súas disposicións específicas e polo previsto, no seu caso, pola LOPD:

- a) Os ficheiros regulados pola lexislación de réxime electoral.
- b) Os tratamentos destinados a fins exclusivamente estatísticos e que estean amparados pola lexislación estatal ou autonómica sobre a función estatística pública.
- c) Os ficheiros que teñan por obxecto o arquivo dos datos contidos en informes persoais de cualificación aos que se refire a lexislación do réxime do persoal das Forzas Armadas
- d) Os ficheiros derivados do Rexistro Civil e do Rexistro Central de Penados e Rebeldes.
- e) Os ficheiros procedentes de imaxes e sons obtidos da utilización de videocámaras polas Forzas e Corpos de Seguridade.

## 2. CONCEPTO

Pódese definir o dereito fundamental á protección de datos persoais como a facultade do individuo de control e disposición sobre as súas informacións de carácter persoal, isto é, como a facultade do individuo de decidir basicamente por si mesmo cando e dentro de que límites procede revelar situacións relativas a vida propia<sup>5</sup>.

Enténdese por dato de carácter persoal o conxunto de informacións relativas a unha persoa física identificada ou identificable, que permiten ampliar ou precisar o coñecemento sobre o individuo (Garriga Domínguez, 2004:24). En efecto, como sinala Heredero Higuera (1997:74), a vinculación dos datos persoais coa persoa pode establecerse de distintos xeitos; de forma directa, mediante un nome; ou de forma indirecta, mediante un determinado número - pasaporte, teléfono, Seguridade Social-, ou mediante un conxunto de riscos distintivos que permitan illar a unha persoa nun grupo determinado por

---

<sup>5</sup> Sentenza do Tribunal Constitucional alemán de 15 de decembro de 1983. Boletín de Xurisprudencia Constitucional núm. 33, páx. 152.

distintas características -idade, posto de traballo, etc.- ou pola imaxe ou a voz, as pegadas dixitais ou as características xenéticas.

Todo os datos de carácter persoal son susceptibles de ser encadrados dentro dunha categoría xeral e homoxénea (Sánchez Bravo, 1998:100). Existen determinadas informacións susceptibles dunha reconsideración en relación con esta categoría xeral polas súas particulares características, como son os denominados datos sensibles (Sánchez Bravo, 1998:100). Pódense definir os datos sensibles como aqueles que teñen unha especial incidencia na vida privada, no exercicio das liberdades ou risco de prácticas discriminatorias (Pérez Luño, 1990:152).

España e os países do entorno europeo optaron maioritariamente por establecer unha categoría pechada de datos sensibles, aos que outorga unha tutela reforzada fronte aos datos ordinarios. Os datos sensibles encóntranse recollidos na LOPD baixo a rúbrica “datos especialmente protexidos”. A Lei diferencia tres grupos de datos sensibles. O primeiro está constituído polos datos relativos á ideoloxía, relixión, crenzas e afiliación sindical. O segundo grupo está formado polos datos relativos á saúde, vida sexual e orixe racial. O terceiro fai referencia aos datos de carácter persoal sobre infraccións penais ou administrativas. Todos eles se caracterizan por un reforzo das garantías previstas para o seu tratamento<sup>6</sup>. A tipificación dos datos sensibles no Dereito interno foi realizada en función do disposto nos artigos 16 e 18, apartado primeiro, da Constitución Española, respectivamente (Garriga Domínguez, 2004:189).

O dereito á autodeterminación informativa<sup>7</sup> foi formulado, nun primeiro momento, pola Doutrina e Xurisprudencia xermanas, consolidándose despois da Sentenza do Tribunal Constitucional alemán, de 15 de decembro de 1983<sup>8</sup>, que resolve o recurso interposto contra a Lei do Censo de Poboación, Profesións, Vivendas e Centros de Traballo de 1983 (Lei do Censo), aprobada polo Bundestag o 4 de marzo de 1982<sup>9</sup>. Esta Lei constituía o inicio dunha operación censual que esixía a recollida de forma exhaustiva de información dos cidadáns e o seu posterior tratamento informático polo Estado. A obrigatoriedade de aportar tales datos xerou temor e inqueda entre a poboación, contraria a un posible control da personalidade efectuado a través da utilización destas informacións, dando lugar a debates públicos sobre a Lei, a movementos de desobediencia civil e a recursos de amparo (Heredero Higuera, 1983:140). Froito dos recursos interpostos contra a Lei de Poboación é a Senteza de 15 de decembro de 1983, coñecida como “Sentencia Zensus” (Denninger, 1987:273).

O debate sobre o recoñecemento dun novo dereito entendido como facultade do individuo para controlar as súas propias informacións, trasladouse ao Ordenamento xurídico español, dando lugar a unha elaboración doutrinal do

---

<sup>6</sup> Artigo 7 da Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal.

<sup>7</sup> Denominación utilizada pola Doutrina alemá a partires dos anos setenta para facer referencia a distintos aspectos da informática, como aspecto xeral da personalidade (Ortí Vallejo, 1994:39).

<sup>8</sup> BJC, núm.33, xaneiro, 1984, pp. 126-170.

<sup>9</sup> Sobre esta Sentenza pode consultarse Heredero Higuera (1983:139-158) e Pérez Luño (1986:58 e ss.).

dereito fundamental<sup>10</sup> (Pérez Luño, 1990:137 e ss.; Lucas Murillo de la Cueva, 1990:156; Garriga Domínguez, 2004:23; entre outros).

Este dereito constitúe unha nova modalidade de liberdade persoal tendente a protexer xuridicamente a identidade persoal (Pérez Luño, 1992:107). O ben xurídico protexido, en palabras de Lucas Murillo de la Cueva (1993:33), é a autodeterminación informativa, consistente no control que lle corresponde á persoa sobre a súa información de carácter persoal para conservar dese modo a propia identidade e, en último extremo, a dignidade e a liberdade.

A singularidade deste dereito fundamental traduciuse no obxecto de protección máis amplo que o protexido polo dereito á intimidade. Fronte a este último, a liberdade informática estende a súa garantía no só á intimidade, senón á esfera dos bens da personalidade que pertencen ao ámbito da vida privada (Sentenza do Tribunal Constitucional 292/2000, de 30 de novembro)<sup>11</sup>. Desta forma, actúa como protección, non exclusivamente da intimidade, senón tamén dos dereitos e liberdades públicas en sentido amplo, fronte aos excesos e abusos que implicaría un poder absoluto e incontrolado da Administración e doutras entidades sobre estes datos (Sánchez Bravo, 1998:63). Trátase, en definitiva, de protexer a liberdade do individuo e non unicamente a súa intimidade, que non deixa de ser unha manifestación desta.

Como consecuencia, a protección non abarca unicamente as informacións de carácter persoal íntimas, senón tamén aquelas que fan referencia a aspectos non íntimos da persoa, ampliando a garantía a aqueles datos que identifiquen ou permitan identificar a unha persoa. O carácter íntimo non é unha condición necesaria para a súa protección, é dicir, deixa de ser o valor de prevalecer na problemática da súa protección e aténdese á posibilidade de disposición sobre estes con independencia do carácter secreto ou non secreto do dato (Sánchez Bravo, 1998:56). A área de confidencialidade que identifica ao dereito á intimidade deixa de ser relevante.

O dereito á protección de datos entendido nestes termos preséntase como a resposta do Estado de Dereito fronte á ameaza que continúen as novas tecnoloxías para as liberdades e dereitos fundamentais (Sánchez Bravo, 1998:58).

### **3. A CONSOLIDACIÓN DO DEREITO Á AUTODETERMINACIÓN INFORMATIVA: O PAPEL DO TRIBUNAL CONSTITUCIONAL**

Se ben parte da doutrina postula a existencia dun novo dereito fundamental recoñecido no artigo 18.4 da Constitución, non é ata 1993 cando o Tribunal Constitucional aporta unha solución ao debate existente sobre o recoñecemento

---

<sup>10</sup> Tamén se mostran partidarios do recoñecemento dun dereito fundamental recollido no texto constitucional Ull Pont (2000:46), Téllez Aguilera (2002:219 e ss.), Herrán Ortiz (2003:12 e ss.) e Serrano Pérez (2003:72 e ss.).

<sup>11</sup> Fundamento xurídico sexto.

constitucional dun dereito fundamental á protección de datos de carácter persoal distinto e independente do dereito á intimidade persoal e familiar.

O Tribunal proclama por primeira vez a existencia dun dereito fundamental á protección de datos recollido no artigo 18.4, na Sentenza 254/1993 (Sala Primeira), de 20 de xullo. Interpreta o citado precepto como unha incorporación na Constitución dunha nova garantía constitucional que actúa fronte a unha nova forma de ameaza concreta contra a dignidade, a liberdade e os dereitos da persoa, de dúas formas complementarias: por un lado, como garantía doutros dereitos, especialmente do dereito ao honor e á intimidade persoal e familiar, expresamente mencionados no seu tenor literal; e por outro, como dereito fundamental autónomo, como liberdade fronte ás agresións, reais ou potenciais, á dignidade e á liberdade derivadas do tratamento dos datos, o que a Constitución chama "á informática"<sup>12</sup>.

Posteriores pronunciamentos reflicten unha postura continuísta da interpretación iniciada pola mencionada Sentenza. Entre outras, hai que sinalar as Sentezas do "caso RENFE"<sup>13</sup> ou a Sentenza do Tribunal Constitucional 202/1999, de 8 de novembro<sup>14</sup>. Nestas, o Tribunal pronúnciase de xeito favorable ao recoñecemento dun dereito autónomo fronte a potenciais agresións á dignidade e á liberdade da persoa, dirixido a controlar o fluxo das informacións<sup>15</sup> e a preservar o pleno exercicio dos demais dereitos fundamentais<sup>16</sup>.

Esta doutrina constitucional consolídase nas Sentenzas 290/2000, de 30 de novembro, e 292/2000, de 30 de novembro, que resollen os recursos de inconstitucionalidade interpostos contra determinados preceptos da Lei Orgánica 5/1992, de 29 de outubro, de Regulación do Tratamento Automatizado de Datos de Carácter Persoal (LORTAD)<sup>17</sup>, xa derogada no momento do pronunciamento do Constitucional, e da Lei 15/1999, de 23 de

<sup>12</sup> Fundamento xurídico sexto, STC 254/1993 (Sala Primeira), de 20 de xullo.

<sup>13</sup> Todas teñen como obxecto de discusión a utilización por RENFE de datos de carácter persoal, como son os relativos á afiliación sindical, para unha finalidade distinta -desconto das horas correspondentes aos paros parciais a tódolos traballadores afiliados ao sindicato CCOO- daquela lexítima que xustificou a súa obtención -desconto da cota sindical a través da nómina salarial-. Os recursos de amparo fundaméntanse prioritariamente na vulneración do dereito a liberdade sindical (artigo 28 da Constitución española) en relación co dereito recoñecido no artigo 18.4. A doutrina que serve para o outorgamento do recurso de amparo expónse de xeito detallado nas Sentenzas 11/1998 (Sala Primeira), de 13 de xaneiro, STC 94/1998 (Sala Segunda), de 2 de maio. Así mesmo, o Tribunal reitera a súa doutrina na STC 33/1998 (Sala Primeira), de 11 de febreiro; STC 35/1998 (Sala Primeira), de 11 de febreiro; STC 45/1998 (Sala Primeira), de 24 de febreiro; STC 60/1998 (Sala Segunda), de 16 de marzo; STC 77/1998 (Sala Primeira), de 31 de marzo; STC 104/1998, 105/1998 e 106/1998 (Sala Segunda), de 18 de maio; STC 123/1998, 124/1998, 125/1998 e 126/1998 (Sala Segunda), de 15 de xuño; STC 158/1998 (Sala Segunda), de 13 de xullo; STC 198/1998 (Sala Primeira), de 13 de outubro; STC 223/1998 (Sala Primeira), de 24 de novembro; STC 30/1999 (Sala Primeira), de 8 de marzo e STC 44/1999 (Sala Segunda) e 45/1999 (Sala Segunda) de 22 de marzo.

En Cabeza Pereiro (2002:91-105) pode consultarse máis detalladamente o desconto da cota sindical e a protección de datos.

<sup>14</sup> Véxase Rodríguez Escanciano (2000).

<sup>15</sup> Fundamento xurídico único, STC 30/1999 (Sala Primeira), de 8 de marzo.

<sup>16</sup> Fundamento xurídico cuarto, STC 11/1998 (Sala Primeira), de 13 de xaneiro.

<sup>17</sup> Sobre os antecedentes normativos da regulamentación da informática no Dereito español pode consultarse a Pérez Luño (1981:33-34).

decembro, de Protección de Datos de Carácter Persoal (LOPD), respectivamente<sup>18</sup>. Nos dous pronunciamentos, o Tribunal reitera a existencia no artigo 18.4 da Constitución Española dun dereito fundamental autónomo e independente<sup>19</sup>. A fundamentación de tal decisión xira en torno a unha serie de cuestións. En primeiro lugar, o Tribunal retrotráese ao momento da elaboración polo poder constituínte do vixente artigo 18.4, resaltando, por un lado, a inclusión inicial dun apartado similar no anteproxecto do texto constitucional e, por outro, a constatación de que xa no debate parlamentario os demais dereitos recollidos no artigo 18, en atención ao seu contido, non ofrecían garantías suficientes fronte ás ameazas que o uso da informática podía supor para a protección da vida privada<sup>20</sup>. En segundo lugar, ratifica a insuficiencia do dereito á intimidade ante a nova realidade derivada do progreso tecnolóxico.

Unha excepción a esta doutrina constitucional foi a Sentenza 143/1994 (Sala Primeira), de 9 de maio. Esta resolveu o recurso de amparo interposto contra a Sentenza do Tribunal Supremo, de 7 de outubro de 1992, que declarou a inadmisibilidade do recurso formulado polo *Consejo General de Economistas de España* contra a normativa reguladora da composición e forma do NIF e da tarxeta acreditativa do mesmo -Real Decreto 338/1990, de 9 de marzo<sup>21</sup>, e Orden Ministerial de 14 de marzo de 1990<sup>22</sup>-. A Sentenza 143/1994 supón unha fenda na Doutrina fixada pola Sentenza 251/1993.

Neste caso a argumentación do Tribunal Constitucional xira exclusivamente en torno ao dereito á intimidade e á determinación de se as informacións relativas ás actividades desenvolvidas no tráfico económico e dos negocios forman parte do ámbito reservado e propio do individuo, excluído dos coñecementos dos demais. O Tribunal sinala expresamente a extrema dificultade para cualificar estas informacións como pertencentes ao núcleo da intimidade, pero centra o seu fallo no artigo 18, apartado primeiro, da Constitución e no estudo dos límites aos que pode ser sometido o dereito á intimidade.

Non entra o Tribunal na análise sobre a posible vulneración mediante a atribución dun código de identificación único, prohibido noutros Ordenamentos xurídicos<sup>23</sup>, nin tampouco sobre a forma de elaboración a través do Documento Nacional de Identidade<sup>24</sup>.

<sup>18</sup> A STC 290/2000, de 30 de novembro, resolve os recursos de inconstitucionalidade promovidos polo Consello Executivo da Generalitat de Cataluña, o Defensor do Pobo e polo grupo do Partido Popular contra os artigos 6.2, 19.1, 20.3, 22.1 e 2.1, 24, 31, 39.1 e 39.2, 40.1 e 22.2 e a disposición adicional terceira da LORTAD. Por outra parte, a STC 292/2000, de 30 de novembro, resolve o recurso de inconstitucionalidade presentado polo Defensor do Pobo contra os artigos 21.1 e 24.1 e 2 da LOPD.

<sup>19</sup> Fundamento xurídico sétimo, STC 290/2000, de 30 de novembro.

<sup>20</sup> Fundamento xurídico terceiro, STC 292/2000, de 30 de novembro.

<sup>21</sup> BOE núm. 63, de 14 de marzo de 1990.

<sup>22</sup> BOE núm. 64, de 15 de marzo de 1990.

<sup>23</sup> O artigo 35 da Constitución Portuguesa prohibe expresamente a asignación dun número nacional de identidade a cada cidadán. Así mesmo, en Francia fracasou o programa SAFARI con idéntica pretensión.

<sup>24</sup> Neste contexto, Madrid Conesa (1984:87) sinala que o N.I.F. debería prohibirse porque as interconexións realizadas mediante este número resultaban máis doadas e porque era previsible o seu traspaso ó sector privado e, neste sector si sería un perigo.

## 4. O MARCO NORMATIVO

A Constitución Española de 1978 foi unha das primeiras do noso entorno en recoller a denominada polo Tribunal Constitucional liberdade informática como dereito fundamental no artigo 18, apartado cuarto.

O desenvolvemento normativo do citado precepto constitucional non se realizou, sen embargo, ata o ano 1992, coa aprobación da Lei Orgánica 5/1992, de 29 de outubro, de Regulación do Tratamento Automatizado de Datos de Carácter Persoal (LORTAD). Esta Lei pola súa banda foi desenvolvida polo Real Decreto 428/1993, de 26 de marzo, que aproba o Estatuto da *Agencia de Protección de Datos*<sup>25</sup> -reformado polo Real Decreto 156/1996, de 2 de febreiro, que modifica o Estatuto da *Agencia de Protección de Datos* para designala como representante español no grupo de protección de persoas previsto na Directiva 95/46/CE de 24 de outubro<sup>26</sup>-, polo Real Decreto 1332/1994, de 20 de xuño, que desenvolve determinados aspectos da LORTAD<sup>27</sup> e polo Real Decreto 994/1999, de 11 de xuño, polo que se aproba o Regulamento de Medidas de Seguridade dos Ficheiros Automatizados que conteñan Datos de Carácter Persoal<sup>28</sup>. A LORTAD outorgou así unha resposta xurídica no Ordenamento xurídico interno ao tratamento de datos persoais.

Ata a súa promulgación, o marco xurídico da protección de datos estaba constituído polo artigo 18.4 da Constitución Española e polo Convenio 108 para a Protección de Persoas en relación co Tratamento Automatizado de Datos de Carácter Persoal, aprobado en Estrasburgo o 28 de xaneiro de 1981 e ratificado por España o 27 de xaneiro de 1984<sup>29</sup>, que recolle os principios e dereitos básicos que rexen na materia. Ambos os dous conteñen un mandato ao legislador español consistente na elaboración dunha norma con finalidade de garantir o pleno exercicio dos dereitos dos cidadáns<sup>30</sup>.

Os efectos despregados polo Convenio en relación cos dereitos fundamentais e, especialmente, co dereito recoñecido no artigo 18, apartado cuarto, do texto constitucional, foron analizados na Sentenza do Tribunal Constitucional 254/1993 (Sala Primeira), de 20 de xullo. O Tribunal Constitucional non entra a valorar o cumprimento ou non dos compromisos derivados de acordos internacionais por non estar incluída esta materia dentro do ámbito do recurso de amparo, pero si se pronuncia sobre as consecuencias da ratificación do citado Convenio en relación co dereito á protección de datos de carácter persoal. Partindo do feito de que os Tratados Internacionais poden servir para configurar o senso e o alcance dos dereitos recollidos na Constitución, segundo

---

<sup>25</sup> BOE núm. 106, de 4 de maio de 1993.

<sup>26</sup> BOE núm. 37, de 12 de febreiro de 1996.

<sup>27</sup> BOE núm. 147, de 21 de xuño de 1994.

<sup>28</sup> BOE núm. 151, de 25 de xuño de 1999.

<sup>29</sup> BOE núm. 274, 15 de novembro de 1985.

<sup>30</sup> O artigo 4 do citado Convenio sinala expresamente o compromiso dos Estados asinantes do texto de adoptar no Dereito interno, as medidas necesarias para a efectividade dos principios de protección de datos enumerados no mesmo, así como, a obriga de instaurar estas medidas como moi tarde no momento da entrada en vigor do texto no Estado parte.

o previsto no artigo 10, apartado segundo<sup>31</sup>, o Tribunal Constitucional complementa o tenor literal do artigo 18.4 cun elemento positivo, de disposición sobre as informacións persoais, derivado dunha interpretación do contido do Convenio 108.

A resposta normativa ao compromiso nacional e internacional foi atrasada ata a aprobación da LOPD que, en palabras de Pérez Luño, chegou tarde e mal; tarde porque o atraso lexislativo permitiu o tráfico de informacións persoais co inevitable risco para os dereitos do individuo ante a pasividade do lexislador; e mal porque a LORTAD, lonxe de beneficiarse das experiencias previas de Dereito comparado, presentaba deficiencias que puideron e deberon evitarse.

A LORTAD desenvolveu o contido do dereito, recollendo en certa medida a distinción entre intimidade e a liberdade informática ou protección de datos. A súa exposición de motivos contiña unha referencia expresa ao que a Lei entendeu como protección da privacidade, coa finalidade de distinguir entre esta expresión e a intimidade nos seguintes termos: “En tanto que a intimidade protexe a esfera en que se desenvolven as facetas máis singularmente reservadas da vida da persoa -o enderezo onde se realiza a vida cotiá, as comunicacións nas que expresa os sentimentos, por exemplo-, a privacidade constitúe un conxunto máis amplo, máis global, de facetas da súa personalidade que, illadamente consideradas, poden carecer de significación intrínseca pero que, coherentemente enlazadas entre si, ten como resultado un retrato da personalidade do individuo que este ten dereito a manter reservado. E si a intimidade, en sentido estrito, está suficientemente protexida polas previsións dos tres primeiros parágrafos do artigo 1 da Constitución e pola leis que o desenvolven, a privacidade pode resultar menoscabada pola utilización das tecnoloxías informáticas de tan recente desenvolvemento”.

Deste xeito, o lexislador optou por introducir no Ordenamento xurídico español un termo alleo a nosa linguaxe que é a tradución literal do vocábulo inglés “privacy” (Sánchez Bravo, 1998:46). O problema que formula a introdución desta palabra é a confusión conceptual que provoca a súa utilización, xa que, no noso Ordenamento xurídico co termo privacidade faise referencia tanto á intimidade como á vida privada; círculos concéntricos pero de distinta amplitude, posto que, si a vida privada inclúe o que é íntimo, non todo o que é íntimo pode estenderse á vida privada. O obxectivo de tal asimilación pódese encontrar quizais na necesidade de eliminar a problemática que xurdiu nos Ordenamentos xurídicos coa necesidade de protexer os datos persoais, isto é, de encontrar a sede axeitada, constitucional ou legal, para situar a protección dos individuos fronte ao acopio de información (Sérrano Pérez, 2003:34). Foi tal o impacto deste termo que tanto a Xurisprudencia como a Doutrina fixeron uso do mesmo, seguindo o sinalado pola LORTAD<sup>32</sup>.

A marxe destas cuestións, a LORTAD recolleu por primeira vez unha serie de principios e dereitos que desenvolven o contido do dereito fundamental á

---

<sup>31</sup> Fundamento xurídico sexto.

<sup>32</sup> A título de exemplo, pode citarse o fundamento xurídico quinto da STC 11/1998 (Sala Primeira), de 13 de xaneiro, que sinala en relación co artigo 18.4 da Constitución Española, que este “consagra un dereito fundamental autónomo ó controlar o fluxo de informacións referentes a cada persoa (...)” ou o fundamento xurídico segundo da STC 44/1999 (Sala Segunda), de 22 de marzo, que se pronuncia en termos semellantes.

protección de datos. Cuestión diferente é se este desenvolvemento cumpriu o obxectivo de desenvolver de maneira real é efectiva o contido do artigo 18.4 da Constitución. A doutrina mostrouse unánime ao sinalar a falta de garantías contidas na LORTAD fronte á utilización dos datos persoais, especialmente dos datos contados en ficheiros públicos ou a presenza de numerosas excepcións ou limitacións ás mesmas (Sánchez Bravo, 1998:47).

A derogación da LORTAD produciuse con certo atraso trala aprobación da Directiva 95/46/CE do Parlamento Europeo e do Consello, de 24 de outubro de 1995, relativa á protección das Persoas Físicas en relación co Tratamento de Datos Persoais e a Libre Circulación dos Datos<sup>33</sup>, que colma a ausencia existente no Dereito Comunitario sobre a protección de datos<sup>34</sup>. Esta norma introduce unha serie de "novidades"<sup>35</sup> que obrigan a modificar a LORTAD ou a aprobar unha nova Lei, optando o lexislador español por esta segunda opción.

Trátase, segundo Heredero Higuera (1997:44), dunha Directiva marco que contén unha serie de principios xerais pero que deixa aos Estados membros unha marxe de manobra na transposición e na elección dos medios e procedementos que permitan garantir a observancia dos principios. O texto supón a consagración dos principios de protección de datos, que son definidos como un conxunto de obrigas e dereitos -obrigacións relativas á calidade dos datos, á seguridade técnica, á notificación das autoridades de control, ás circunstancias nas que se pode efectuar o tratamento e dereitos outorgados ás persoas titulares dos datos-<sup>36</sup>.

A transposición da Directiva tivo o seu reflexo na vixente Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal, que substitúe a antiga LORTAD. Esta recolle en termos xerais a estrutura da Lei anterior -disposicións xerais, principios da protección de datos, dereitos das persoas, disposicións sectoriais, movemento internacional de datos, disposicións relativas á *Agencia Española de Protección de Datos* e normas relativas á infraccións e sancións-. Tamén introduce algunhas variacións impostas pola Directiva ás que non fai alusión por non conter esta nova Lei unha Exposición de Motivos. A influencia da Directiva pódese apreciar no artigo primeiro -obxecto da Lei<sup>37</sup>-, artigo segundo -ámbito de aplicación<sup>38</sup>- ou no apartado cuarto do artigo 6 que recolle o dereito de oposición<sup>39</sup>.

---

<sup>33</sup> DOCE 281/1995, de 23 de novembro.

<sup>34</sup> Sobre as iniciativas e propostas comunitarias previas á aprobación da Directiva pode consultarse a referencia de Heredero Higuera (1997:17-42).

<sup>35</sup> Por exemplo, cabe sinalar a inclusión dentro do seu ámbito de protección aos ficheiros manuais ou o recoñecemento dun dereito de oposición do afectado.

<sup>36</sup> Considerando 25º, Directiva 95/46/CE.

<sup>37</sup> Se abandona o tenor literal do artigo 18.4 da Constitución Española relativo á limitación do uso da informática e faise referencia expresa ó tratamento de datos persoais. Sobre esta cuestión pode consultarse a Garriga Domínguez (2004:51-53).

<sup>38</sup> A vixente LOPD da cabida a tódolos datos de carácter persoal rexistrados en soporte físico, susceptibles de tratamento, fronte a limitación contida na antiga LORTAD. Esta ampliación supón un xiro favorable na protección do dereito fundamental á protección de datos.

<sup>39</sup> A diferenza do que sucede na Directiva 95/46/CE, a LOPD non contén un artigo dedicado integramente ao dereito de oposición, senón que o inclúe no precepto relativo ao consentimento.

## 5. PRINCIPIOS DE CALIDADE DOS DATOS E DEREITOS DO INTERESADO: O CONTIDO DO DEREITO Á PROTECCIÓN DE DATOS NA LOPD

As disposicións sobre protección de datos establecen unha serie de cautelas, límites e pautas que terán que ser respectadas, tanto no momento de obtención dos datos como en posteriores fases do tratamento.

Este obxectivo conséguese, aínda que non exclusivamente, co establecemento dunha serie de garantías en forma de límites e modos nos que as informacións persoais poden e deben obterse, rexistrarse e ser tratadas e en forma de dereitos subxectivos que dotan de contido efectivo as anteriores cautelas e cos que se consegue un sistema eficaz de protección dos cidadáns.

A LOPD integra os dous tipos de garantías baixo os Títulos II e III, coa denominación de principios de protección de datos e dereitos das persoas (Garriga Domínguez, 2004:73). Ambos os dous desenvolven o contido do dereito fundamental formado polas facultades necesarias para dar cumprimento a súa función instrumental de garantía doutros dereitos e polas facultades de control outorgadas ao individuo en relación cos seus datos persoais, así como, polos deberes e obrigas que afectan ao suxeito pasivo do dereito.

Para a correcta comprensión destas garantías é necesario deterse previamente na definición de determinados termos legais.

### 5.1. DEFINICIÓNS LEGAIS

A LOPD recolle unha serie de definicións legais en consonancia co establecido na Directiva 95/46/CE e que son as seguintes:

- Dato de carácter persoal.

Conxunto de informacións concernentes a unha persoa física identificada ou identificable.

Esta definición complétase co disposto no artigo 1, apartado cuarto, do Real Decreto 1332/1994, de 20 de xuño, que segundo o disposto na Disposición Transitoria Terceira da LOPD segue en vigor en todo o que non se opoña a esta. Este define como dato de carácter persoal, toda información numérica, alfabética, gráfica, fotográfica, acústica ou de calquera outro tipo susceptible de recollida, rexistro, tratamento ou transmisión relativa a unha persoa física identificada ou identificable. É necesario, polo tanto, que a persoa poida ser identificada ou identificable por medio dos datos persoais.

Segundo o artigo 2, apartado a, da Directiva 95/46/CE, de 24 de outubro, considérase identificable toda persoa con identidade determinable, de forma directa ou indirecta, en particular mediante un número de identificación ou un ou varios elementos específicos

característicos da súa identidade física, fisiolóxica, psíquica, económica, cultural ou social.

- Ficheiro.

Todo conxunto organizado de datos de carácter persoal, calquera que sexa a forma ou modalidade de creación, arquivo, organización e acceso.

- Tratamento de datos.

Operacións e procedementos técnicos de carácter automatizado ou non que permitan a recollida, gravación, conservación, elaboración, modificación, bloqueo e cancelación, así como, as cesións de datos que resulten de comunicacións, consultas, interconexións e transferencias.

Este precepto ten que completarse co previsto no artigo primeiro, puntos 1, 3 e 6 do Real Decreto 1332/1994 que aclara o que debe entenderse por bloqueo de datos, cesión de datos e tranferenza de datos.

- Responsable do ficheiro ou tratamento.

Persoa física ou xurídica, de natureza pública ou privada, ou órgano administrativo, que decida sobre a finalidade, contido e uso do tratamento.

- Afectado ou interesado.

Persoa física titular dos datos que sexan obxecto de tratamento.

- Procedemento de disociación.

Todo tratamento de datos persoais de maneira que a información que se obteña do mesmo non poida asociarse á persoa identificada ou identificable.

En definitiva, supón a conversión dos datos persoais en datos anónimos, entendidos como aqueles que de ningunha maneira, a través de ningún procedemento, se poderán relacionar de xeito directo ou indirecto co individuo (Garriga Domínguez, 2004:76).

- Encargado do tratamento.

Persoa física ou xurídica, autoridade pública, servizo ou calquera organismo que, só ou de forma conxunta con outros, trate datos por conta ou encargo do responsable do tratamento.

- Consentimento.

Toda manifestación de vontade libre, inequívoca, específica e informada pola que o interesado consinta o tratamento das informacións.

- Cesión de datos.

Revelación realizada a unha persoa distinta do interesado.

- Fontes accesible ao público.

Ficheiros de datos que poderán ser consultados por calquera persoa, sempre e cando, esta consulta non se impida por unha norma limitativa ou sen máis esixencia que unha contraprestación.

Son fontes accesibles ao público exclusivamente o censo promocional, os repertorios telefónicos, as listas de persoas de grupos profesionais que conteñan exclusivamente o nome, título, profesión, actividade, grado académico, enderezo e indicación da pertenza ao grupo. Tamén serán fontes accesibles ao público os diarios, os boletíns oficiais e os medios de comunicacións.

## 5.2. PRINCIPIOS DE PROTECCIÓN DE DATOS. REQUISITOS PARA O TRATAMENTO DOS DATOS PERSOAIS

A LOPD, no Título II, recolle os chamados “principios de protección de datos”. Neste Título regúlanse cuestións tan dispares como os principios de calidade dos datos, o dereito á información na recollida dos mesmos, o consentimento do afectado, a comunicación dos datos, etc.

Non todos eles poden considerarse, en sentido estrito, principios de protección de datos. Unicamente poden ser considerados como tales os que forman parte do denominado contido negativo do dereito á protección de datos, que se traducen en esixencias relativas á obtención, tratamento e uso dos datos persoais. Principios que debe garantir a persoa ou entidade que os recolla e archive (Garriga Domínguez, 2004: 37).

O conxunto dos principios de calidade dos datos de carácter persoal estará formado polas seguintes esixencias: principio de pertinencia, principio de finalidade, principio de veracidade e exactitude, principio de lealdade e principio de seguridade.

### 1. Principio de pertinencia.

A adecuación ao principio de pertinencia esixe que os datos sexan adecuados e non excesivos para a finalidade que da lugar ao seu tratamento (Garriga Domínguez, 2004: 37).

Este principio encóntrase recollido, de maneira xenérica, no artigo 4 da LOPD -“os datos de carácter persoal só poderán recollese (...) cando sexan adecuados, pertinentes e non excesivos en relación coas finalidades determinadas, explícitas e lexítimas”-, no artigo 5, letra c, do Convenio 108 -“os datos de carácter persoal (...) serán adecuados, pertinentes e non excesivos en relación coas finalidades con que foron rexistrados”- e, no artigo 6, apartado primeiro, letra c, da Directiva 95/46/CE -“os Estados membros disporán que os datos persoais sexan: c) adecuados, pertinentes e non

excesivos en relación aos fins para os que se soliciten e para os que posteriormente se traten”-.

O principio de pertinencia, entendido neste sentido, obriga a unha avaliación da necesidade e proporcionalidade dos datos para un fin determinado, de forma previa a súa obtención.

## 2. Principio de finalidade.

Pódese definir o principio de finalidade como a necesidade de conexión entre a información persoal que se recaba e o fin para o que se solicita (Lucas Murillo de la Cueva, 1993:65). O citado principio encóntrase conectado ao de pertinencia, ata tal punto que o cumprimento dun implica necesariamente o respecto ao primeiro (Garriga Domínguez, 2004: 78).

O respecto do principio é imprescindible para evitar a difusión incontrolada da información que, segundo o disposto no artigo 18.4 da Constitución Española, se pretende limitar<sup>40</sup>.

Está recollido no artigo 4 da LOPD nos seguintes termos: “só se poderán recoller e tratar datos persoais que sexan adecuados (...) en relación co ámbito e as finalidades determinadas, explícitas e lexítimas para as que os datos foron recollidas”. Tamén o artigo 5, letra b, do Convenio 108 e o artigo 6, apartado primeiro, letra b, da Directiva 95/46/CE recollen este principio como límite á obtención e ao tratamento de datos de carácter persoal.

## 3. Principio de lealdade.

Esixe que os datos non se obteñan con falsidades ou enganos, a través de medios fraudulentos, desleais ou ilícitos, permitindo á persoa coñecer en todo momento que datos se obtén e para que.

## 4. Principio de veracidade e exactitude.

Pódese definir a veracidade como a perfecta correspondencia entre o discurso que marcan os feitos e o que se transmite ao receptor da información.

A LOPD recolle este requisito no artigo 4, apartado terceiro, esixindo a quen recolla e trate os datos que estes sexan exactos e postos ao día de forma que mentres se utilicen respondan á veracidade da situación do afectado.

## 5. Principio de seguridade.

Enténdese por seguridade da información o conxunto de sistemas e procedementos que garanten a confesionalidade, a integridade e a dispoñibilidade da información. Este principio actúa fronte á alteración, perda ou acceso indebido aos datos persoais (Pérez Luño, 2001: 346).

---

<sup>40</sup> A importancia deste principio foi reseñada na primeira Sentenza do Tribunal Constitucional favorable ao recoñecemento dun novo dereito fundamental. Fundamento xurídico sétimo da STC 254/1993, de 20 de xullo.

Recollido no artigo 9 LOPD, este principio esixe que se adopten as medidas precisas para garantir a seguridade dos datos, tendo en conta o estado da tecnoloxía, a natureza dos mesmos e os riscos aos que van a estar expostos.

Os riscos que poden afectar á seguridade dos datos dependen do sector concreto no que se encontre o ficheiro e do tipo de datos que se inclúen no mesmo. Polo tanto, para dar cumprimento a esta esixencia legal non é suficiente coa adopción de calquera medida, senón que deben ser as necesarias para garantir estes obxectivos, nin tampouco coa aprobación formal das medidas de seguridade, senón que é necesario que estas se adopten e se poñan en práctica.

O Regulamento de Medidas de Seguridade dos Ficheiros, aprobado polo Real Decreto 994/1999, de 11 de xuño, contén un marco de referencia obrigada sobre as medidas que ten que implantar o responsable do ficheiro. Esta norma complétase co Real Decreto 195/2000, de 11 de febreiro, que establece o prazo para implantar as medidas de seguridade.

Este Regulamento de Medidas de Seguridade distingue tres niveis de seguridade en función da natureza dos datos e da maior ou menor necesidade de confidencialidade e integridade dos mesmos (artigos 3 e 4). Contén ademais uns prazos de implantación das medidas para os sistemas de información que estaban xa en funcionamento previamente á entrada en vigor do texto normativo (Disposición Transitoria).

Directamente relacionado co deber de implantar as medidas de seguridade está a obriga de segredo profesional recollida no artigo 10 da LOPD, que esixe tanto ao responsable do ficheiro como a toda persoa que interveña en calquera fase do tratamento o deber de segredo sobre a información de carácter persoal coñecida. Este segredo esténdese ao longo do tempo e debe manterse tamén unha vez rematada a relación co responsable do ficheiro.

### **5.3. DEREITOS DOS INTERESADOS**

Concrétanse nunha serie de facultades que garanten a todo cidadán o coñecemento sobre quen, que, cando e con que motivo coñece datos que lle concirnen. Estas facultades reciben o nome de habeas data.

a) O dereito a recibir información.

A LOPD, no artigo 5, establece a obriga de informar ao interesado; de maneira previa á recollida dos datos, expresa, precisa e inequívoca; dos seguintes aspectos:

- Da existencia dun ficheiro ou tratamento de datos, da finalidade e dos destinatarios da información.
- Do carácter obrigatorio ou facultativo das respostas.
- Das consecuencias da obtención dos datos ou da negativa a proporcionarlos.
- Da posibilidade de exercitar os dereitos de acceso, rectificación, cancelación e oposición.

- Da identidade e dirección do responsable do tratamento ou, no seu caso, do seu representante.

Cando se utilicen cuestionarios ou outros impresos para a recollida dos datos figurarán as advertencias sinaladas.

A lexislación vixente soamente exclúe o requisito de información nos seguintes supostos: cando unha Lei así o recolla; cando o tratamento teña fins históricos, estatísticos ou científicos; cando a información resulte imposible ou esixa esforzos desproporcionados, segundo a *Agencia General de Protección de Datos* ou Organismo Autónomo equivalente, atendendo ao número de interesados, á antigüidade dos datos e as posibles medidas compensatorias ou; cando os datos procedan de fontes accesibles ao público e se destinen á actividade de publicidade ou prospección comercial.

- b) Dereito do afectado a que se requira o seu consentimento para a recollida, tratamento e cesión dos datos persoais.

Este consentimento debe ser libre e informado, isto é, non derivado de calquera tipo de presión ou coacción, de forma que o interesado poida sopesar os riscos e as vantaxes do tratamento dos datos e exercer os dereitos que lle asisten.

Como regra xeral o tratamento dos datos requirirá o consentimento inequívoco do titular dos mesmos, segundo o previsto no artigo 6 da LOPD.

Sen embargo, o artigo 7 da LOPD prevé un fortalecemento do consentimento e da forma en que este deberá outorgarse en relación cos denominados datos sensibles ou especialmente protexidos. Así, para o tratamento de datos médicos e de orixe racial, a LOPD esixe que o consentimento se preste de forma expresa. Maiores garantías establece aínda para os datos incluídos no primeiro grupo de datos sensibles -datos sobre ideoloxía, crenzas, relixión ou afiliación sindical- requirindo que o consentimento se preste ademais de expresamente por escrito.

Quedan prohibidos os ficheiros con finalidade exclusiva de archivar datos relativos a ideoloxía, afiliación sindical, relixión, crenzas, orixe racial ou vida sexual. Así mesmo, os datos relativos á comisión de infraccións penais ou administrativas só poderán ser incluídos en ficheiros de titularidade pública.

- c) Dereito de oposición, de acceso, de rectificación e de cancelación sobre os datos persoais.

O dereito de acceso pode definirse como a facultade de control do interesado para comprobar que datos sobre a súa persoa forman parte dun banco de datos (Frosini, 1987:51), cal é a orixe deses datos e que cesións foron efectuadas ou se pretenden realizar.

Está recollido no artigo 15 da LOPD que regula tamén a forma de exercitalo. En relación co período temporal, sinala a Lei, que esta facultade non poderá exercitarse en intervalos inferiores a 12 meses. En canto á forma, a Lei indica unha serie de métodos a través dos cales se pode obter a información. Os medios sinalados son: a visualización directa dos datos ou a indicación destes

por escrito, copia, telecopia ou fotocopia. Permítese calquera mecanismo que possibilite ao interesado saber de forma certa e efectiva cales son os datos que existes sobre el nun ficheiro e quen é o responsable do mesmo, así como, a quen foron comunicados.

Os dereitos de rectificación e cancelación foron recollidos de forma conxunta no artigo 16 da LOPD, aínda que se trata de dúas facultades diferentes con funcións distintas. O primeiro ten como función a corrección de datos inexactos ou incompletos, mentres que o segundo ten como finalidade eliminar datos que non deben figurar nun ficheiro porque foron recollidos de maneira ilícita ou porque existe algunha causa que esixe a súa supresión.

Pola contra, fronte ao que ocorre cos dereitos de acceso, rectificación e cancelación, o dereito de oposición supón un control previo ao tratamento dos datos persoais, configurándose como un instrumento garante de carácter preventivo ou cautelar (Corripio Gil-Delgado, 1996:287).

Recollido este último no artigo 6.4 da Lei é aplicable naqueles casos nos que non sexa necesario o consentimento do interesado, sempre e cando existan motivos fundados e lexítimos e unha Lei non dispoña o contrario. O responsable do ficheiro non incluírá os datos relativos ao afectado.

- d) Dereito a non verse sometido a unha decisión con efectos xurídicos baseada exclusivamente no tratamento dos datos e a impugnar estas valoracións.

O afectado, segundo a Lei, poderá impugnar decisións, sempre e cando estas teñan efecto xurídico, baseadas única e exclusivamente nun tratamento de datos que ofrezca unha definición das súas características ou un perfil da personalidade.

- e) Dereito ao esquecemento.

A súa finalidade é protexer ao individuo fronte a recuperación de determinados datos despois dun período de tempo longo ou despois da desaparición da finalidade lexítima para a que foron solicitados. Ten como misión evitar que informacións que se manteñen nun banco de datos se sigan utilizando co paso de decenas de anos, o que significa a desaparición da garantía que supuña para a intimidade das persoas a fragilidade da memoria humana (Garriga Domínguez, 2000: 306).

## 6. NOTIFICACIÓN E INSCRIPCIÓN REXISTRAL

Un dos deberes impostos pola LOPD é a notificación á *Agencia Española de Protección de Datos* (AGPD) da creación e existencia dun ficheiro de datos para a súa inscrición no *Registro General de Protección de Datos* (RGPD)<sup>41</sup>.

---

<sup>41</sup> Artigos 26 e 39 da LOPD.

Son numerosas as funcións da AGPD establecidas no artigo 37 da Lei e desenvoladas no Capítulo II do seu Estatuto: velar polo cumprimento da lexislación de protección de datos; realizar unha función informativa e de publicidade; colaborar cos órganos competentes na aplicación das normas que incidan na materia ditando instrucións e recomendacións precisas; informar, con carácter preceptivo, dos proxectos de disposicións xerais de desenvolvemento da Lei e dos proxectos de Lei ou regulamentos que incidan na protección de datos; realizar funcións de control e cooperación internacional; así como, levar a cabo unha función inspectora e unha función instrutora e de sanción nos termos previstos no Título VII da LOPD.

A imposición desta obriga de notificación dos ficheiros ten unha dobre función: facilitar o control pola *Agencia de Protección de Datos* e permitir o exercicio do dereito de información do interesado a través da consulta do *Registro General de Protección de Datos* para coñecer os ficheiros existentes e intentar dilucidar en cales poden estar os seus datos.

O RGPD é órgano da AGPD que ten que velar pola publicidade dos ficheiros. Son obxecto de inscrición no mesmo os seguintes ficheiros, actos e documentos:

- Os ficheiros de datos dos que sexan titulares a Administración Xeral do Estado, as Entidades e Organismos da Seguridade Social, os Organismos Autónomos do Estado, as Sociedades Estatais e Entes do sector público aos que se refire o artigo 6 da Lei Xeral Presupostaria, as Administracións das Comunidades Autónomas e Territorios Históricos, así como os seus Entes e Organismos Dependentes, sen prexuízo de que se inscriban ademais nos rexistros dependentes dos Entes de Protección de Datos Autonómicos, as Entidades que integran a Administración Local e os Organismos Dependentes das mesmas e calquera outra persoa xurídico pública.

- Os ficheiros de datos persoais dos que sexan titulares as persoas privadas, tanto físicas como xurídicas.

Nos asentos de inscrición destes ficheiros incluírase a información contida na notificación do ficheiro, así como, os cambios de finalidade do ficheiro, do responsable e do seu emprazamento.

- As autorizacións para a transmisión internacional de datos persoais cando sexa perceptiva a autorización do Director da AGPD.
- Os códigos tipo elaborados segundo o disposto no artigo 32 da LOPD.

## 7. INFRACCIÓNS E SANCIÓNS

O réxime sancionador está previsto no Título VII da LOPD. Fronte á realización de condutas irregulares contrarias ás disposicións da Lei ou con descoñecemento dos dereitos dos afectados, a Lei prevé unha serie de sancións. Tanto os responsables dos ficheiros como os encargados do tratamento están suxeitos ao réxime sancionador desta Lei.

A LOPD, no artigo 44, prevé tres tipos de infraccións: leves, graves ou moi graves.

A Lei establece un dobre réxime sancionador en función da titularidade dos ficheiros. Así, se o responsable do ficheiro é un particular, o réxime sancionador é o regulado no articulado da LOPD e o procedemento sancionador é o dos artigos 18 e 19 do Real Decreto 1332/1994. Cando o responsable do ficheiro sexa unha Administración Pública estarase a o disposto no artigo 46 da LOPD.

En relación co réxime sancionador xeral que afecta aos ficheiros de titularidade privada, o artigo 45 fixa a contía das multas en función da gravidade da infracción cometida. As infraccións leves serán sancionadas con multa de 601,01 a 60.101,21 €, as graves con multa de 60.101,21 a 300.506,05€ e as moi graves con multa de 300.506,05 a 601.012,10 €

A contía das sancións graduarase atendendo á natureza dos dereitos dos afectados, aos volumes dos tratamentos, aos beneficios obtidos, ao grado de intencionalidade, á reincidencia, aos danos e prexuízos ocasionados e a calquera outra circunstancia que sexa relevante para determinar o grao de antixuridicidade e culpabilidade presentes na conduta infractora. Ademais, cando en función das circunstancias concorrentes no caso se aprecie unha diminución cualificada da culpabilidade ou antixuridicidade do feito, a contía da sanción establecerase aplicando a escala relativa á clase de infracción que preceda inmediatamente en gravidade a esta.

## **8. RESUMO DOS DEBERES E OBRIGAS DO RESPONSABLE DO FICHEIRO E DO ENCARGADO DO TRATAMENTO**

Tanto o responsable do ficheiro como o encargado do tratamento están obrigados por todas e cada unha das disposicións previstas na LOPD. Neste senso, a Lei establece expresamente unha serie de deberes que garanten os dereitos dos titulares dos datos mentres que outros deberes se deducen do contido destes.

Sen ánimo exhaustivo e de maneira exemplificativa relaciónanse aquelas obrigas impostas ao responsable do ficheiro das que se derivan dereitos para o titular dos datos:

1. No primeiro grupo de obrigas, a LOPD reconece o deber de segredo do responsable dos ficheiros públicos e privados e de todas as persoas que interveñan en calquera fase do tratamento (artigo 10). O noso Ordenamento xurídico reforza a obriga de sxiilo profesional de todos os que teñan coñecementos de informacións de carácter persoal por razón do seu cargo, profesión ou oficio, tanto no ámbito privado como no público, tipificado no Título X do Código Penal á revelación de segredo.

2. Notificación á *Agencia Española de Protección de Datos* da creación e existencia dun ficheiro para a súa inscrición no *Registro General de Protección de Datos*.
3. Deber de informar ao afectado antes da recollida dos datos nos termos fixados no artigo 5 e, no momento no que se efectúe a primeira cesión nos termos sinalados no artigo 11.
6. Deber de solicitar o consentimento do interesado para a recollida, tratamento e comunicación de datos.
7. Deber de adoptar as medidas de seguridade correspondentes.
8. Deber de garantir o acceso do afectado aos seus propios datos e de rectificar as informacións de carácter persoal erróneas ou inexactas, na forma e prazos previstos no Regulamento de desenvolvemento da Lei.

## CAPÍTULO 2

# PASOS PRÁCTICOS PARA A APLICACIÓN DA LOPD

M<sup>a</sup> Cruz del Río Rama  
*Universidade de Vigo*

Manuel Martínez Carballo  
Susana Barbeito Roibal  
Eduardo Guillén Solórzano  
*Universidade da Coruña*

O obxectivo deste segundo capítulo é recoller de forma moi breve unha serie de etapas ou fases que sirvan de guía ás entidades para o cumprimento da normativa vixente en materia de protección de datos de carácter persoal. O proceso estrutúrase en catro pasos prácticos que lles permitirá ás empresas entender e levar a cabo as accións correspondentes para cumprir a Lei Orgánica de Protección de Datos (LOPD) dunha forma moi sinxela e así garantir aos cidadáns os dereitos fundamentais recollidos na Constitución neste sentido.

Estes pasos son os seguintes:

### 1. INVENTARIO OU IDENTIFICACIÓN DOS FICHEIROS

Nesta fase a entidade correspondente terá que realizar unha identificación de todos os ficheiros existentes na súa organización, distinguindo aqueles que conteñan datos de carácter persoal dos que non almacenen este tipo de datos, con obxecto de identificar así os ficheiros aos cales lles é de aplicación a LOPD.

Respecto dos ficheiros con datos persoais, haberá que determinar os datos que se almacenan (nome, apelidos, enderezo, etc.); o responsable do ficheiro; e no seu caso, do encargado do tratamento; a unidade de acceso á cal se debe dirixir o responsable para exercer os seus dereitos; os niveis de seguridade aplicables aos ficheiros (nivel básico, medio e alto); entre outros aspectos.

### 2. DECLARACIÓN DOS FICHEIROS NO RGPD

Unha vez realizada a etapa anterior e determinada a existencia de ficheiros que conteñen datos de carácter persoal, o seguinte paso é levar a cabo a inscrición destes ficheiros no *Registro General de Protección de Datos* (RGPD) da *Agencia Española de Protección de Datos* (AGPD) que é a entidade encargada, en España, de velar polo cumprimento da lexislación sobre protección de datos. Para iso, haberá que especificar a finalidade para a que foi creado o ficheiro; o responsable do mesmo; a estrutura e organización; a orixe e a procedencia dos datos; os dereitos correspondentes (acceso, rectificación, cancelación e oposición); etc.

A inscrición destes ficheiros pódese realizar mediante formularios en papel, en soporte magnético ou vía Internet<sup>42</sup>.

### 3. ADOPCIÓN DE MEDIDAS DE SEGURIDADE

A maiores, todas aquelas entidades que traten datos de carácter persoal tamén teñen que adoptar as medidas de seguridade de índole técnica e organizativa necesarias para garantir a seguridade dos datos obxecto de tratamento que han de ser plasmadas no denominado documento de seguridade.

---

<sup>42</sup> Véxase apartado 4 do capítulo 2. Ademais pode consultarse a Resolución de 1 de setembro de 2006 da AGPD pola que se determina a información que contén o catálogo de ficheros inscritos no RGPD (BOE núm. 227, de 22 de setembro de 2006; a Resolución do 12 de xullo de 2006 da AGPD pola que se crea o rexistro telemático da AGPD (BOE núm. 181, de 31 de xullo de 2006; e a Resolución de 12 de xullo de 2006 da AGPD pola que se aproban os formularios electrónicos mediante os cales deberán efectuarse as solicitudes de inscrición de ficheros no RGPD, así como, os formatos e requirimentos aos que deben axustarse as notificacións remitidas en soporte informático e telemático (BOE núm. 181, de 31 de xullo de 2006).

Dentro destas medidas de seguridade distínguense tres niveis: nivel básico, medio (datos protexidos) e alto (datos especialmente protexidos); xa que, non é o mesmo tratar datos como o nome, apelidos ou o enderezo postal de datos persoais relativos á personalidade, á sexualidade ou á saúde. Ademais, os ficheiros con nivel de seguridade medio e alto han de ter expresamente designado un responsable de seguridade, así como, someterse, polo menos bianualmente, a unha auditoría interna ou externa con obxecto de verificar o cumprimento das medidas establecidas regulamentariamente.

O documento de seguridade ha de ser divulgado dentro da empresa, de maneira que o persoal da mesma coñeza as normas que afectan ao desenvolvemento das súas funcións e as consecuencias derivadas do seu incumprimento, asegurándose en todo momento o deber de segredo profesional.

#### 4. ADOPCIÓN DE CLÁUSULAS DE PROTECCIÓN DE DATOS

Nesta etapa a empresa debe incluír nos seus formularios, contratos, páxina Web, entre outros documentos; todas aquelas cláusulas necesarias para a recollida e o tratamento dos datos, os tratamentos por terceiros, as cesións ou comunicacións e, as transferencias internacionais.

Na recollida e no tratamento dos datos hai que ter en conta a calidade e a exactitude dos mesmos, así como a finalidade para o que se recolleron, polo que teñen que cumprirse as seguintes premisas:

- A entidade ten que informar ao interesado da recollida dos datos, o fin para os que se vai a utilizar e, o consentimento para o seu tratamento.
- Os datos só se poderán utilizar para os fins para os que foron recollidos.
- Os datos que non sexan necesarios para tal fin non se poden recoller.
- Aqueles datos que xa non sexan útiles teñen que ser cancelados.
- Os datos teñen que manterse actualizados en todo momento.

Cando o tratamento dos datos sexa realizado por un terceiro para a prestación dun servizo (confección de nóminas, realización de auditorías, contabilidade, etc.) ten que asinarse un contrato co encargado do tratamento polo que se garanta o adecuado tratamento dos datos pola súa parte.

No caso de que se produza unha cesión de datos (por exemplo, a unha empresa do grupo), a entidade ten que informar ao interesado de a quen e para que cede os datos, así como, obter o seu consentimento para a cesión dos mesmos.

Para as transferencias internacionais debe terse en conta:

- Se o destino do dato é a Unión Europea ou un país declarado "seguro":
  - Hai que notificalo á *Agencia Española de Protección de Datos*.
  - Informar ao interesado de a quen e para que se transfiren os datos, así como, o seu consentimento para levar a cabo a devandita transferencia.

- Se o destino do dato son terceiros países:
  - Hai que notificalo á *Agencia Española de Protección de Datos*.
  - Informar ao interesado de a quen e para que se transfiren os datos, así como, o seu consentimento para levar a cabo a devandita transferencia.
  - Solicitar a autorización do Director da AGPD.

A empresa debe ser tamén coñecedora das obrigacións que se derivan dos dereitos que os afectados poden solicitarlle. Moi brevemente, estes dereitos son:

- Dereito de acceso.

Mediante este dereito o interesado pode solicitar á entidade que datos ou que tipo de datos ten sobre el. A solicitude dirixirase ao responsable do ficheiro que debe responder no prazo máximo dun mes.

- Dereito de rectificación.

O titular dos datos poderá solicitar á empresa a rectificación daqueles datos persoais que sexan inexactos, incompletos, inadecuados ou excesivos. O responsable do ficheiro deberá atender esta solicitude no prazo máximo de dez días.

- Dereito de cancelación.

É un dereito no que o afectado pode solicitar o borrado dos datos persoais tratados nun ficheiro cando sexan inexactos incompletos, inadecuados ou excesivos. O responsable do ficheiro deberá atender tamén esta solicitude no prazo máximo de dez días.

- Dereito de oposición.

Trátase dun dereito polo que o interesado pode opoñerse ao tratamento dos seus datos cando non foi necesario o seu consentimento. O responsable do ficheiro debe proceder á exclusión destes datos no prazo máximo dun mes.

- Dereito á indemnización.

Fai referencia ao dereito a unha indemnización naqueles casos que, como consecuencia do incumprimento da LOPD por parte da empresa, o afectado sufra un dano ou lesión nos seus bens ou dereitos.

## CAPÍTULO 3

# NIVEL OU GRAO DE CUMPRIMENTO DA LOPD

Manuel Martínez Carballo  
Eduardo Guillén Solórzano  
Susana Barbeito Roibal  
*Universidade da Coruña*

M<sup>a</sup> Cruz del Río Rama  
*Universidade de Vigo*

## 1. INTRODUCCIÓN

Unha vez abordado o marco normativo e conceptual da protección de datos de carácter persoal no capítulo 1, así como, os pasos básicos para a aplicación da LOPD no capítulo 2, a continuación imos realizar unha análise detallada do grao ou nivel de cumprimento da lexislación vixente nesta materia, tanto no ámbito privado como no ámbito público. Non obstante, centrarémonos con moito maior detalle no terreo privado por ser este o de maior importancia na actualidade en canto ao volume de ficheiros inscritos no *Registro General de Protección de Datos* (RGPD), xa que, ao 30-9-2007, os ficheiros inscritos de titularidade privada representan o 93,11% da totalidade das inscricións (758.955 ficheiros no ámbito privado fronte a 56.138 ficheiros de titularidade pública).

Así mesmo, a investigación se levará a cabo para o conxunto de España e, en particular, para Galicia.

## 2. FICHEIROS DE TITULARIDADE PRIVADA

### 2.1. INTRODUCCIÓN

Neste segundo apartado efectuarase un estudo pormenorizado do nivel de cumprimento no ámbito privado a partir de datos da *Agencia Española de Protección de Datos* (AGPD) e do *Instituto Nacional de Estadística* (INE), principalmente. Para iso, utilizaranse e calcularanse os seguintes indicadores que a continuación se describen:

1. Tratamentos inscritos e Entidades con ficheiros inscritos
2. [Ficheiros inscritos] / [Entidades con ficheiros inscritos]
3. [Entidades con ficheiros inscritos] / [Entidades totais] x 100

#### **Tratamentos inscritos e Entidades con ficheiros inscritos**

O primeiro indicador é o relativo aos tratamentos inscritos que fan referencia ao volume neto de ficheiros inscritos no RGPD da AGPD (altas-baixas). As entidades con ficheiros inscritos, representan como o seu propio nome indica, o número total de entidades (empresas, asociacións de empresarios, outras organizacións sen ánimo de lucro, etc.) que teñen algún ficheiro inscrito no RGPD. Ambos indicadores recollen o volume de inscrición en valor absoluto e por si mesmos representan moi pouca información para analizar o verdadeiro grao de cumprimento desta lexislación. O ideal sería comparar estes dous indicadores entre si, ou ben, o número de entidades con ficheiros inscritos co número total de entidades.

**[Ficheiros inscritos] / [Entidades con ficheiros inscritos]**

Este ratio complementa a información dos indicadores anteriores e representa o número total de ficheiros que por termo medio ten inscrito cada entidade que iniciou algunha actuación para o cumprimento da LOPD no RGPD.

**[Entidades con ficheiros inscritos] / [Entidades totais] x 100**

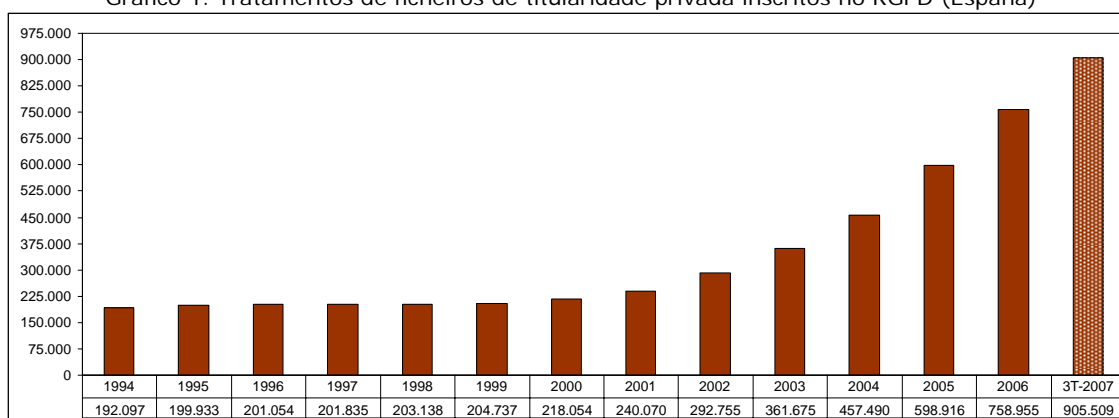
Outro indicador relevante neste contexto resulta de comparar o número de entidades que teñen algún ficheiro inscrito no RGPD co número total de entidades existentes. A ausencia de cifras oficiais deste último parámetro impediranos o seu cálculo exacto. Sen embargo, de forma aproximada, procederáse igualmente ao seu cálculo comparando o número de entidades con ficheiros inscritos co número total de empresas segundo datos recabados do Instituto Nacional de Estadística (INE). Neste caso, é moi importante apreciar e ter claro que os resultados obtidos aínda serían moito máis baixos se tivéssemos en conta todo tipo de entidades e non soamente o número total de empresas.

A continuación imos a proceder ao cálculo de todos estes indicadores para analizar o nivel ou grao de cumprimento da lexislación vixente en materia de protección de datos, tanto no Estado español como na Comunidade galega.

**2.2. GRAO DE CUMPRIMIENTO EN ESPAÑA**

En primeiro lugar, consideremos o volume neto de ficheiros inscritos no RGPD. A súa evolución a nivel nacional é a que aparece reflexada no gráfico 1, no que se observa unha primeira etapa de estancamento e, é a partir do ano 2000, que ademais coincide coa entrada en vigor da nova Lei, cando realmente se aprecian incrementos significativos. A 30-9-2007 o número total de tratamentos inscritos ascendía a 905.509 ficheiros (case o dobre dos ficheiros inscritos ata o ano 2004). O sector comercio; comunidades de propietarios; sanidade; contabilidade, auditoría e asesoría fiscal; xunto con actividades inmobiliarias; encabezan o ranking de distribución por sector de actividade.

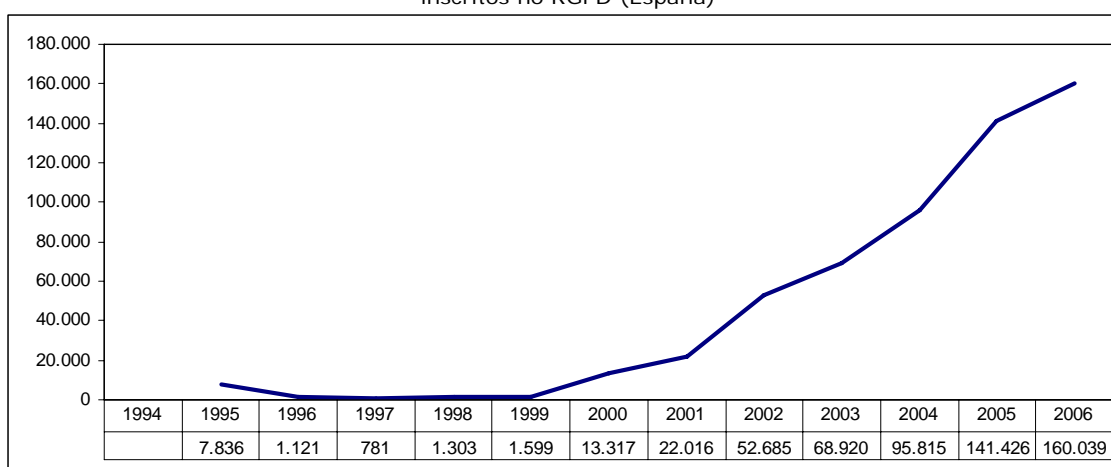
Gráfico 1. Tratamentos de ficheiros de titularidade privada inscritos no RGPD (España)



Fonte: Elaboración propia a partir de estadísticas da AGPD

O incremento habido no número de tratamentos inscritos durante o ano 2006 respecto ao ano anterior foi do 26,72% (gráfico 2), porcentaxe moi inferior ao incremento do 2005 (30,91%). Así mesmo, o aumento medio dos últimos 5 anos completos (2002-2006) foi do 26,92%, mentres que o dos últimos 10 anos (1997-2006) foi do 16,41%. No futuro, supoñendo un crecemento igual á media dos últimos 5 anos, situariámonos no ano 2015 con 6.484.856 ficheiros inscritos (case oito veces máis que a data de hoxe), ou ben, unha inscrición neta de 2.978.330 ficheiros segundo a media dos últimos 10 anos. No período que levamos do presente ano (2007) podemos falar dun incremento do 19,31% ata o terceiro trimestre, o que equivalería aproximadamente a un incremento anual do 25,75%, en calquera caso inferior ao aumento acaecido nos últimos anos.

Gráfico 2. Incremento anual de tratamentos de ficheiros de titularidade privada inscritos no RGPD (España)



Fonte: Elaboración propia a partir de estadísticas da AGPD

En canto ás entidades con ficheiros inscritos, no ano 2006 existían un total de 317.722 entidades (táboa 1), o que supón un aumento do 24,28% respecto ao ano anterior, porcentaxe tamén moi inferior ao incremento do 2005 que foi do 31,21%. A distribución deste indicador por Comunidades Autónomas a 30-9-2007 é a que se mostra no gráfico 3, onde as Comunidades situadas nas seis primeiras posicións aglutinan a case o 80% do total. O aumento que houbo nestes nove primeiros meses do ano 2007 en termos anuais sería do 23,72%, inferior tamén ao dos últimos anos.

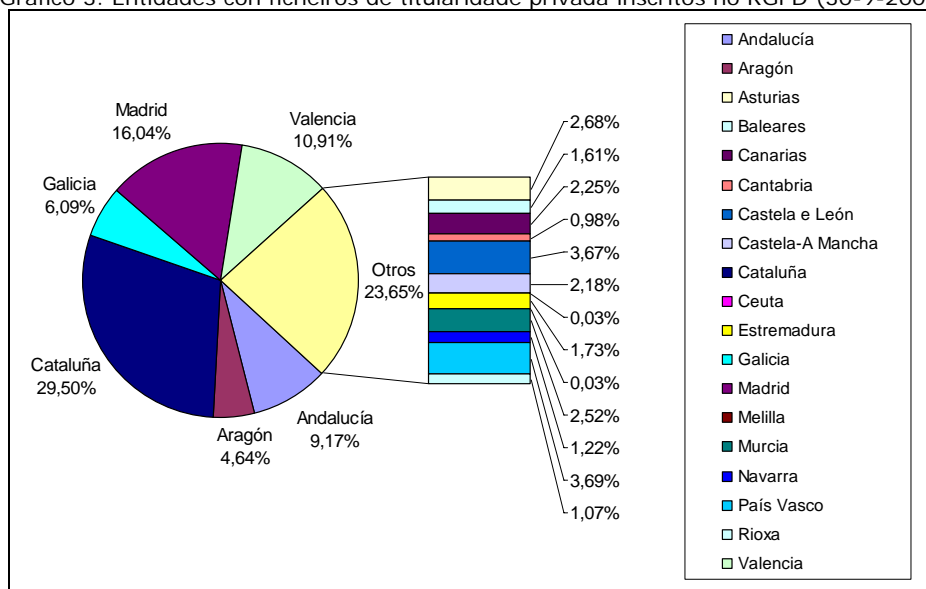
Táboa 1. Entidades con ficheiros de titularidade privada inscritos no RGPD (2006)

Comunidade Autónoma	Entidades
Andalucía	27.849
Aragón	15.836
Asturias	8.067
Baleares	4.328
Canarias	6.750
Cantabria	2.759
Castela e León	10.931
Castela-A Mancha	6.630

Comunidade Autónoma	Entidades
Cataluña	99.182
Ceuta	114
Estremadura	5.272
Galicia	19.100
Madrid	50.228
Melilla	76
Murcia	8.050
Navarra	4.006
País Vasco	11.461
Rioxa	3.493
Valencia	33.590
<b>Total</b>	<b>317.722</b>

Fonte: Elaboración propia a partir de estadísticas da AGPD

Gráfico 3. Entidades con ficheiros de titularidade privada inscritos no RGPD (30-9-2007)



Fonte: Elaboración propia a partir de estadísticas da AGPD

En xeral, a tendencia incremental do volume de tratamentos inscritos e o das entidades con ficheiros inscritos é moi similar ao longo dos últimos anos. Non obstante, tal e como se explicou anteriormente, estes dous indicadores non son unha reseña moi significativa para analizar o cumprimento real da lexislación vixente en materia de protección de datos, xa que, por si mesmos representan moi pouca información. En cambio, se comparamos ambos indicadores entre si ([Ficheiros inscritos] / [Entidades con ficheiros inscritos]), o que temos é o número de ficheiros que por termo medio inscribiu cada entidade no RGPD. A media anual deste ratio no ano 2005 ascendía a 2,34 ficheiros (táboa 2), no ano 2006 a 2,39 (táboa 3) e a 30-9-2007 crecía ata 2,42 (táboa 4); o que significa que cada vez hai máis entidades que inscriben os seus ficheiros no RGPD ou aquelas que xa inscribían algún deciden dar de alta máis ficheiros. Na nosa opinión, trátase igualmente de ratios excesivamente baixos, xa que, calquera entidade dispón xeralmente de ficheiros con datos de carácter persoal

correspondentes aos seus empregados, provedores, clientes e un longo etcétera.

Nestas táboas tamén se poden consultar as cifras deste indicador desglosadas por Comunidades Autónomas, onde os datos das celas en *negrita* representan aquelas Comunidades que están por encima da media nacional.

Táboa 2. Ficheiros inscritos e Entidades con ficheiros inscritos (2005)

Comunidade Autónoma	Entidades	Ficheiros	[Fich.]/[Entid.]
Andalucía	22.667	56.441	<b>2,49</b>
Aragón	13.817	26.605	1,93
Asturias	5.549	16.234	<b>2,93</b>
Baleares	2.865	8.936	<b>3,12</b>
Canarias	5.614	19.199	<b>3,42</b>
Cantabria	1.697	4.115	<b>2,42</b>
Castela e León	8.863	19.424	2,19
Castela-A Mancha	5.444	14.520	<b>2,67</b>
Cataluña	82.037	175.088	2,13
Ceuta	109	244	2,24
Estremadura	4.531	10.368	2,29
Galicia	15.189	38.406	<b>2,53</b>
Madrid	38.741	99.338	<b>2,56</b>
Melilla	59	137	2,32
Murcia	6.176	13.607	2,20
Navarra	3.328	7.842	<b>2,36</b>
País Vasco	8.658	22.834	<b>2,64</b>
Rioxa	3.043	6.348	2,09
Valencia	27.263	59.180	2,17
Outras	----	50	----
<b>Total</b>	<b>255.650</b>	<b>598.916</b>	<b>2,34</b>

Fonte: Elaboración propia a partir de estadísticas da AGPD

Táboa 3. Ficheiros inscritos e Entidades con ficheiros inscritos (2006)

Comunidade Autónoma	Entidades	Ficheiros	[Fich.]/[Entid.]
Andalucía	27.849	74.718	<b>2,68</b>
Aragón	15.836	31.645	2,00
Asturias	8.067	25.423	<b>3,15</b>
Baleares	4.328	13.979	<b>3,23</b>
Canarias	6.750	23.652	<b>3,50</b>
Cantabria	2.759	6.023	2,18
Castela e León	10.931	25.439	2,33
Castela-A Mancha	6.630	19.001	<b>2,87</b>
Cataluña	99.182	210.150	2,12
Ceuta	114	275	<b>2,41</b>

Comunidade Autónoma	Entidades	Ficheiros	[Fich.]/[Entid.]
Estremadura	5.272	12.552	2,38
Galicia	19.100	53.398	<b>2,80</b>
Madrid	50.228	123.868	<b>2,47</b>
Melilla	76	186	<b>2,45</b>
Murcia	8.050	17.495	2,17
Navarra	4.006	9.742	<b>2,43</b>
País Vasco	11.461	29.597	<b>2,58</b>
Rioxa	3.493	8.175	2,34
Valencia	33.590	73.582	2,19
Outras	----	55	----
<b>Total</b>	<b>317.722</b>	<b>758.955</b>	<b>2,39</b>

Fonte: Elaboración propia a partir de estadísticas da AGPD

Táboa 4. Ficheiros inscritos e Entidades con ficheiros inscritos (30-9-2007)

Comunidade Autónoma	Entidades	Ficheiros	[Fich.]/[Entid.]
Andalucía	34.328	94.603	<b>2,76</b>
Aragón	17.376	35.098	2,02
Asturias	10.019	32.500	<b>3,24</b>
Baleares	6.008	19.130	<b>3,18</b>
Canarias	8.438	30.030	<b>3,56</b>
Cantabria	3.677	7.517	2,04
Castela e León	13.727	31.590	2,30
Castela-A Mancha	8.148	23.486	<b>2,88</b>
Cataluña	110.389	237.150	2,15
Ceuta	124	338	<b>2,73</b>
Estremadura	6.467	15.086	2,33
Galicia	22.784	65.700	<b>2,88</b>
Madrid	60.020	146.098	<b>2,43</b>
Melilla	99	251	<b>2,54</b>
Murcia	9.439	20.915	2,22
Navarra	4.568	11.380	<b>2,49</b>
País Vasco	13.795	35.719	<b>2,59</b>
Rioxa	3.996	9.914	<b>2,48</b>
Valencia	40.831	88.426	2,17
Outras	----	578	----
<b>Total</b>	<b>374.233</b>	<b>905.509</b>	<b>2,42</b>

Fonte: Elaboración propia a partir de estadísticas da AGPD

O último ratio significativo que utilizaremos para analizar o nivel ou grao de cumprimento da lexislación sobre protección de datos a nivel nacional é o número de entidades que teñen algún ficheiro inscrito no RGPD co número total de empresas segundo o INE, ante a ausencia do número total de entidades

existentes no ámbito privado. No ano 2005 tan só unha media do 8,05% das entidades a nivel nacional iniciaron algunha acción en materia de protección de datos de carácter persoal inscribindo todos/algúns dos seus ficheiros no RGPD (táboa 5). No 2006 este ratio ascendía a 9,52% (táboa 6). A variación 2006-2005 do volume de empresas activas foi do 5,1%. Para o ano 2007 aínda non contamos con estatísticas oficiais referentes ao número total de empresas. Loxicamente trátase de valores moi baixos. Ademais, hai que destacar que se tivéssemos en conta todo tipo de entidades e non soamente empresas, os resultados deste índice serían aínda inferiores.

Táboa 5. Entidades con ficheiros inscritos en relación ao número total de empresas (2005)

Comunidade Autónoma	Entidades con ficheiros inscritos [1]	Total Empresas [2]	% [1]/[2]x100
Andalucía	22.667	486.674	4,66
Aragón	13.817	87.941	15,71
Asturias	5.549	70.115	7,91
Baleares	2.865	88.027	3,25
Canarias	5.614	132.810	4,23
Cantabria	1.697	37.690	4,50
Castela e León	8.863	163.856	5,41
Castela-A Mancha	5.444	124.413	4,38
Cataluña	82.037	578.340	14,18
Ceuta	109	3.700	2,95
Estremadura	4.531	63.084	7,18
Galicia	15.189	191.642	7,93
Madrid	38.741	478.202	8,10
Melilla	59	3.657	1,61
Murcia	6.176	90.698	6,81
Navarra	3.328	41.083	8,10
País Vasco	8.658	161.376	5,37
Rioxa	3.043	22.393	13,59
Valencia	27.263	348.692	7,82
Total	255.650	3.174.393	8,05

Fonte: Elaboración propia a partir de estatísticas da AGPD e do INE

Táboa 6. Entidades con ficheiros inscritos en relación ao número total de empresas (2006)

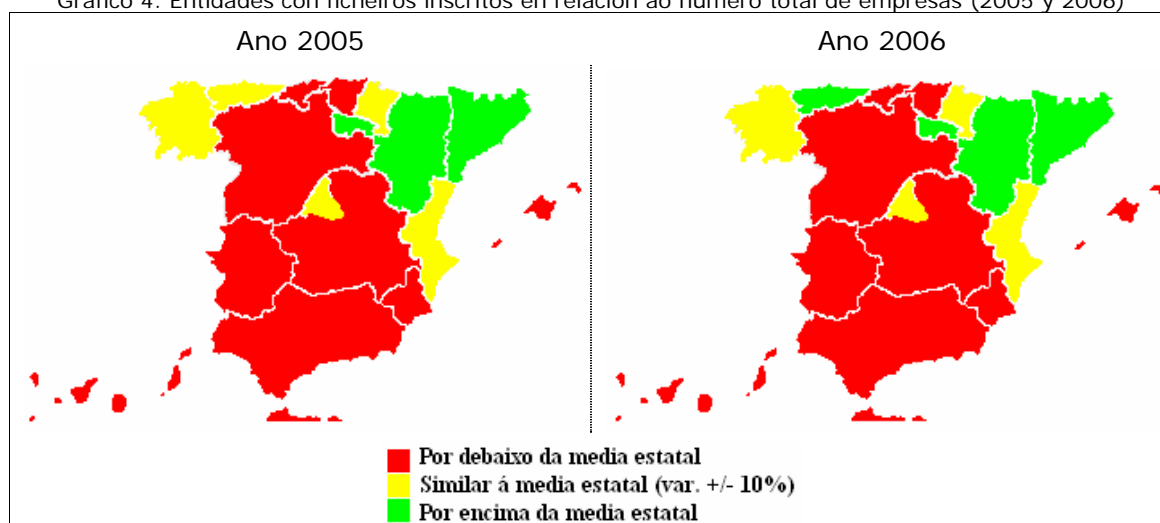
Comunidade Autónoma	Entidades con ficheiros inscritos [1]	Total Empresas [2]	% [1]/[2]x100
Andalucía	27.849	511.728	5,44
Aragón	15.836	92.162	17,18
Asturias	8.067	72.276	11,16
Baleares	4.328	91.254	4,74
Canarias	6.750	140.414	4,81
Cantabria	2.759	39.560	6,97

Comunidade Autónoma	Entidades con ficheiros inscritos [1]	Total Empresas [2]	% [1]/[2]x100
Castela e León	10.931	170.319	6,42
Castela-A Mancha	6.630	132.906	4,99
Cataluña	99.182	612.404	16,20
Ceuta	114	3.752	3,04
Estremadura	5.272	66.232	7,96
Galicia	19.100	200.020	9,55
Madrid	50.228	503.000	9,99
Melilla	76	3.693	2,06
Murcia	8.050	97.374	8,27
Navarra	4.006	43.142	9,29
País Vasco	11.461	164.431	6,97
Rioxa	3.493	23.404	14,92
Valencia	33.590	368.586	9,11
<b>Total</b>	<b>317.722</b>	<b>3.336.657</b>	<b>9,52</b>

Fonte: Elaboración propia a partir de estadísticas da AGPD e do INE

No gráfico 4 resúmese claramente a visión nacional por Comunidades Autónomas deste indicador de cumprimento da LOPD.

Gráfico 4. Entidades con ficheiros inscritos en relación ao número total de empresas (2005 y 2006)



Fonte: Elaboración propia a partir de estadísticas da AGPD e do INE

Táboa 7. Nivel ou grao de cumprimento da lexislación en materia de protección de datos de carácter persoal no ámbito privado (cadro-resumo)

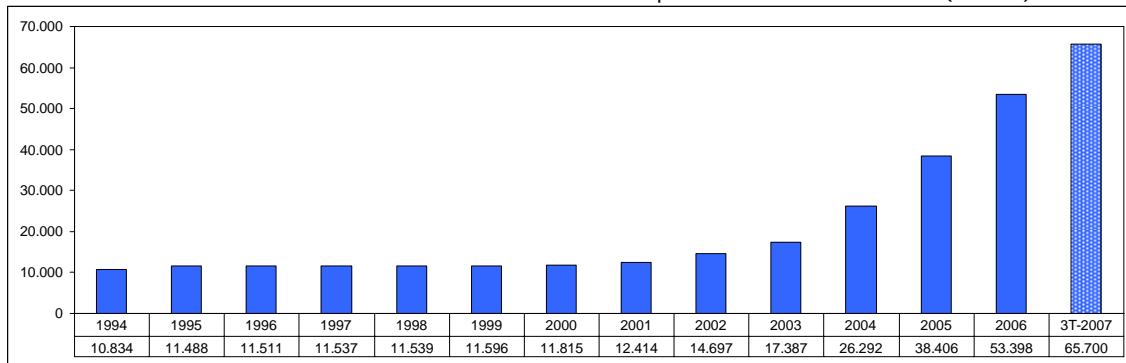
Comunidades Autónomas	Ano 2005					Ano 2006					Variación 2006-2005	
	Entidades con ficheiros inscritos [1]	Ficheiros inscritos [2]	Ficheiros/Entidades [2]/[1]=3	Total Empresas [4]	% [1]/[4]x100=5	Entidades con ficheiros inscritos [6]	Ficheiros inscritos [7]	Ficheiros/Entidades [7]/[6]=[8]	Total Empresas [9]	% [6]/[9]x100=[10]	Entidades con ficheiros inscritos	Ficheiros inscritos
Andalucía	22.667	56.441	2,49	486.674	4,66	27.849	74.718	2,68	511.728	5,44	22,86	32,38
Aragón	13.817	26.605	1,93	87.941	15,71	15.836	31.645	2,00	92.162	17,18	14,61	18,94
Asturias	5.549	16.234	2,93	70.115	7,91	8.067	25.423	3,15	72.276	11,16	45,38	56,60
Baleares	2.865	8.936	3,12	88.027	3,25	4.328	13.979	3,23	91.254	4,74	51,06	56,43
Canarias	5.614	19.199	3,42	132.810	4,23	6.750	23.652	3,50	140.414	4,81	20,24	23,19
Cantabria	1.697	4.115	2,42	37.690	4,50	2.759	6.023	2,18	39.560	6,97	62,58	46,37
Castela e León	8.863	19.424	2,19	163.856	5,41	10.931	25.439	2,33	170.319	6,42	23,33	30,97
Castela-A Mancha	5.444	14.520	2,67	124.413	4,38	6.630	19.001	2,87	132.906	4,99	21,79	30,86
Cataluña	82.037	175.088	2,13	578.340	14,18	99.182	210.150	2,12	612.404	16,20	20,90	20,03
Ceuta	109	244	2,24	3.700	2,95	114	275	2,41	3.752	3,04	4,59	12,70
Extremadura	4.531	10.368	2,29	63.084	7,18	5.272	12.552	2,38	66.232	7,96	16,35	21,06
Galicia	15.189	38.406	2,53	191.642	7,93	19.100	53.398	2,80	200.020	9,55	25,75	39,04
Madrid	38.741	99.338	2,56	478.202	8,10	50.228	123.868	2,47	503.000	9,99	29,65	24,69
Melilla	59	137	2,32	3.657	1,61	76	186	2,45	3.693	2,06	28,81	35,77
Murcia	6.176	13.607	2,20	90.698	6,81	8.050	17.495	2,17	97.374	8,27	30,34	28,57
Navarra	3.328	7.842	2,36	41.083	8,10	4.006	9.742	2,43	43.142	9,29	20,37	24,23
Pais Vasco	8.658	22.834	2,64	161.376	5,37	11.461	29.597	2,58	164.431	6,97	32,37	29,62
Rioxa	3.043	6.348	2,09	22.393	13,59	3.493	8.175	2,34	23.404	14,92	14,79	28,78
Valencia	27.263	59.180	2,17	348.692	7,82	33.590	73.582	2,19	368.586	9,11	23,21	24,34
Outras	----	50	----	----	----	----	55	----	----	----	----	10,00
<b>Total</b>	<b>255.650</b>	<b>598.916</b>	<b>2,34</b>	<b>3.174.393</b>	<b>8,05</b>	<b>317.722</b>	<b>758.955</b>	<b>2,39</b>	<b>3.336.657</b>	<b>9,52</b>	<b>24,28</b>	<b>26,72</b>

Fonte: Elaboración propia a partir de estatísticas da AGPD e do INE

### 2.3. GRAO DE CUMPRIMENTO EN GALICIA

A continuación imos realizar unha análise semellante para o caso concreto de Galicia. Neste sentido, a evolución do volume neto de ficheiros inscritos no RGPD da AGPD pódese apreciar no gráfico 5. A finais de setembro de 2007 (3T-2007) o número total de tratamentos inscritos na comunidade galega elevábase a 65.700 ficheiros (máis do dobre dos ficheiros inscritos ata o ano 2004), dos cales 26.923 (40,98%) correspondían á provincia da Coruña, 10.105 (15,38%) á de Lugo, 5.096 (7,76%) a Ourense e, 23.576 (35,88%) á provincia de Pontevedra.

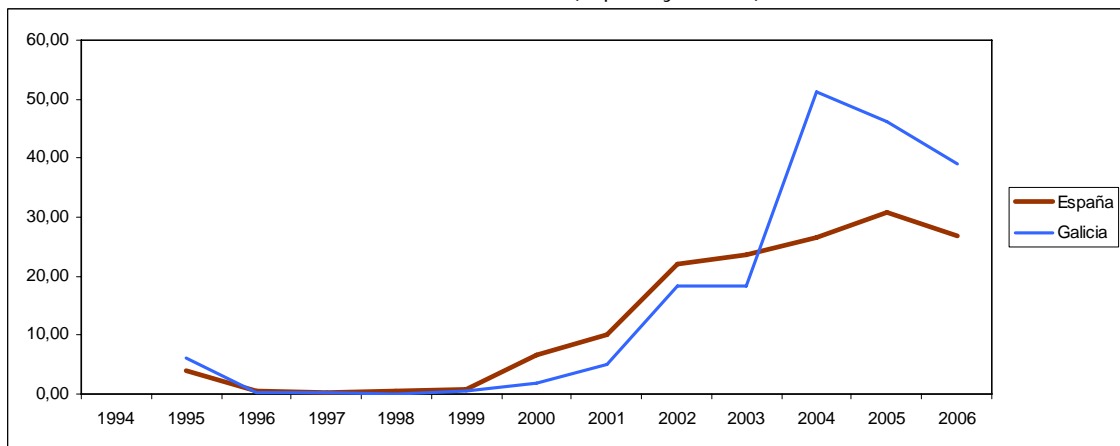
Gráfico 5. Tratamentos de ficheiros de titularidade privada inscritos no RGPD (Galicia)



Fonte: Elaboración propia a partir de estadísticas da AGPD

Agora ben, se comparamos o incremento anual habido neste contexto cos datos nacionais, temos que o aumento na comunidade galega foi moi superior ao de España nos últimos anos (gráfico 6). Houbo unha primeira etapa de igualdade ata o ano 1999, desde este ano ata o 2003 o crecemento foi superior a nivel estatal, pero a partires desta data o incremento en Galicia do volume de ficheiros inscritos foi moi superior. O desglose da variación 2006-2005 nas catro provincias galegas foi do 26,31% na Coruña, do 33,79% en Lugo, do 35,59% en Ourense e, do 65,06% en Pontevedra (variación media 39,04%).

Gráfico 6. Incremento porcentual anual de tratamentos de ficheiros de titularidade privada inscritos no RGPD (España y Galicia)



Fonte: Elaboración propia a partir de estadísticas da AGPD

No referente a entidades con ficheiros inscritos en Galicia, no ano 2006 había un total de 19.100 entidades que tiñan todos/algúns dos seus ficheiros inscritos

no *Registro General de Protección de Datos*, o que supón un incremento do 25,75% respecto ao ano anterior, porcentaxe moi similar ao aumento acontecido a nivel estatal que foi do 24,28%.

Por outra banda, dado que estes dous indicadores analizados nos parágrafos precedentes representan por si mesmos moi pouca información para analizar o nivel ou grao de cumprimento da LOPD, a continuación imos proceder a comparalos entre si ( $[\text{Ficheiros inscritos}] / [\text{Entidades con ficheiros inscritos}]$ ) e co volume total de empresas activas ( $[\text{Entidades con ficheiros inscritos}] / [\text{Total empresas}] \times 100$ ). As táboas seguintes recollen os resultados dos anos 2004, 2005 e 2006 (táboa 8, táboa 9 e táboa 10).

Táboa 8. Nivel ou grao de cumprimento da LOPD no ámbito privado (Galicia 2004)

Provincia	Entidades con ficheiros inscritos [1]	Ficheiros inscritos [2]	Ficheiros/Entidades [2]/[1]=[3]	Total Empresas [4]	% [1]/[4]x100=[5]
A Coruña	5.516	13.344	2,42	77.023	7,16
Lugo	1.992	3.940	1,98	23.122	8,62
Ourense	909	2.229	2,45	22.452	4,05
Pontevedra	2.695	6.779	2,52	63.125	4,27
Diferenzas	-24	---	---	---	---
Total Galicia	11.088	26.292	2,37	185.722	5,97
España	194.842	457.490	2,35	3.064.129	6,36

Fonte: Elaboración propia a partir de estatísticas da AGPD e do INE

Táboa 9. Nivel ou grao de cumprimento da LOPD no ámbito privado (Galicia 2005)

Provincia	Entidades con ficheiros inscritos [1]	Ficheiros inscritos [2]	Ficheiros/Entidades [2]/[1]=[3]	Total Empresas [4]	% [1]/[4]x100=[5]
A Coruña	7.510	18.413	2,45	79.170	9,49
Lugo	2.841	6.292	2,21	23.780	11,95
Ourense	1.120	3.060	2,73	22.843	4,90
Pontevedra	3.759	10.641	2,83	65.849	5,71
Diferenzas	-41	---	---	---	---
Total Galicia	15.189	38.406	2,53	191.642	7,93
España	255.650	598.916	2,34	3.174.393	8,05

Fonte: Elaboración propia a partir de estatísticas da AGPD e do INE

Táboa 10. Nivel ou grao de cumprimento da LOPD no ámbito privado (Galicia 2006)

Provincia	Entidades con ficheiros inscritos [1]	Ficheiros inscritos [2]	Ficheiros/Entidades [2]/[1]=[3]	Total Empresas [4]	% [1]/[4]x100=[5]
A Coruña	8.933	23.267	2,60	82.873	10,78
Lugo	3.491	8.418	2,41	24.609	14,19
Ourense	1.392	4.149	2,98	23.520	5,92
Pontevedra	5.336	17.564	3,29	69.018	7,73
Diferenzas	-52	---	---	---	---
Total Galicia	19.100	53.398	2,80	200.020	9,55
España	317.722	758.955	2,39	3.336.657	9,52

Fonte: Elaboración propia a partir de estatísticas da AGPD e do INE

A táboa 11 recolle un adianto dos resultados ata o terceiro trimestre do ano 2007, no que aínda non se contan con estatísticas oficiais referentes ao número total de empresas.

Táboa 11. Nivel ou grao de cumprimento de la LOPD no ámbito privado (Galicia 3T-2007)

Provincia	Entidades con ficheiros inscritos [1]	Ficheiros inscritos [2]	Ficheiros/Entidades [2]/[1]=[3]
A Coruña	10.025	26.923	2,69
Lugo	4.025	10.105	2,51
Ourense	1.680	5.096	3,03
Pontevedra	7.118	23.576	3,31
Diferenzas	-64	---	---
Total Galicia	22.784	65.700	2,88
España	374.233	905.509	2,42

Fonte: Elaboración propia a partir de estatísticas da AGPD

Á vista dos resultados anteriores, obsérvase que na actualidade as entidades galegas de ámbito privado inscriben por termo medio un volume de ficheiros no RGPD superior á media estatal. Pasouse dunha inscrición de 2,37 ficheiros no ano 2004 a 2,88 no 3T-2007 fronte a unha media en España de 2,35 e 2,42; respectivamente. Ourense e Pontevedra sitúanse por encima de 3 ficheiros por entidade. Non obstante, seguimos opinando que o número de ficheiros que por termo medio inscribiu cada entidade da comunidade galega que deu algún paso para o cumprimento da lexislación vixente en materia de protección de datos de carácter persoal ante o propio *Registro General de Protección de Datos* é aínda moi baixo, se ben este ratio aumenta lentamente co paso dos anos.

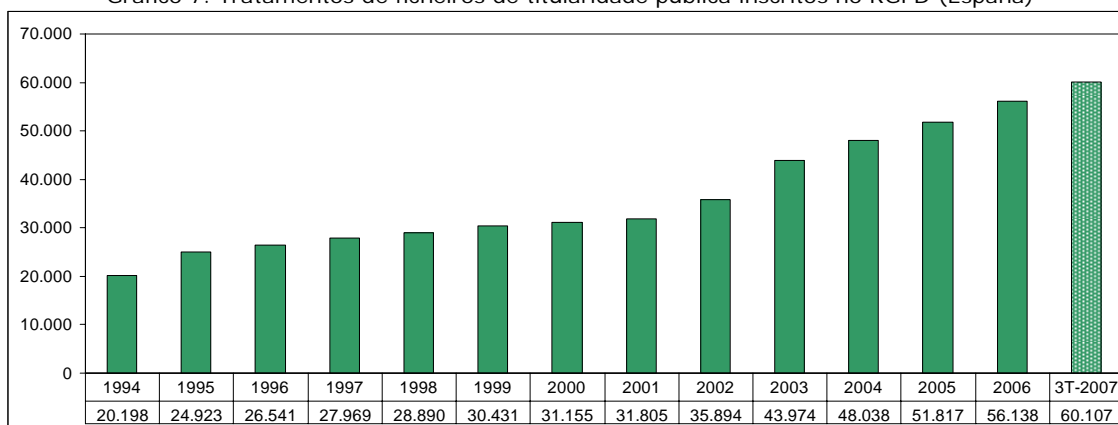
As cifras relativas ao número de empresas galegas que iniciaron algunha actuación nesta materia inscribindo todos ou parte dos seus ficheiros no RGPD ( $[\text{Entidades con ficheiros inscritos}] / [\text{Total empresas}] \times 100$ ) corrobora os comentarios anteriores. No caso de Galicia este ratio evolucionou do 5,97% no ano 2004 ao 9,55% no 2006 fronte a un 6,36% e 9,52%; respectivamente a nivel nacional. Hai que resaltar a provincia de Lugo cun índice de 14,19%. En xeral, situámonos a uns niveis superiores á media española. Hai que recordar tamén que se tivéssemos en conta todo tipo de entidades (empresas, asociacións de empresarios, outras organizacións sen ánimo de lucro, etc.), os resultados deste índice serían aínda moito máis baixos.

### 3. FICHEIROS DE TITULARIDADE PÚBLICA

A análise do nivel ou grao de cumprimento da lexislación vixente en materia de protección de datos de carácter persoal no ámbito público en base aos indicadores expostos no apartado anterior resulta moito máis complexo, xa que, na maioría dos casos non dispoñemos do número de entidades que se corresponden coa inscrición dos ficheiros correspondentes e, en calquera caso, non dispoñemos con certeza da cifra total de entidades públicas ás que fan referencia os datos. Non obstante, procedemos igualmente a realizar un estudo moito máis breve.

A evolución a nivel nacional do volume neto de ficheiros de titularidade pública inscritos no RGPD da AGPD aparece reflexada no gráfico 7. Nos últimos cinco anos completos (2002-2006) o incremento habido foi do 11,99% e nos últimos dez anos (1997-2006) foi do 8,21%. No que levamos do ano 2007 (ata o 30 de setembro) este aumento estaría cifrado no 7,07% que se correspondería aproximadamente cun incremento anual do 9,43%, superior á media dos últimos dez anos a diferenza do que ocorría cos ficheiros de titularidade privada

Gráfico 7. Tratamentos de ficheiros de titularidade pública inscritos no RGPD (España)



Fonte: Elaboración propia a partir de estadísticas da AGPD

A distribución da inscrición destes ficheiros por tipo de Administración Pública pódese consultar na táboa seguinte (táboa 12), onde case o 60% dos mesmos corresponden á Administración Local.

Táboa 12. Tratamentos de ficheiros de titularidade pública inscritos no RGPD (España)

Tipo Administración	Ano 2006		3T-2007	
	Ficheiros	%	Ficheiros	%
Administración Xeral do Estado	3.173	5,65	3.657	6,08
Administración e Organismos CC.AA.	12.488	22,25	13.183	21,93
Administración e Organismos Entes Locais	32.891	58,59	35.342	58,80
Cámaras Oficiais de Comercio e Industria	335	0,60	360	0,60
Colexios Profesionais	573	1,02	768	1,28
Notariado	5.905	10,52	5.940	9,88
Universidades	544	0,97	581	0,97
Outras	229	0,41	276	0,46
<b>Total</b>	<b>56.138</b>		<b>60.107</b>	

Fonte: Elaboración propia a partir de estadísticas da AGPD

Na táboa 13 recóllese o volume de ficheiros inscritos correspondentes á Administración Autónoma dos dous últimos anos, así como, a variación existente entre estes períodos. A diferenza experimentada en Galicia (2,54%) é superior á da media estatal (2,02%).

Táboa 13. Tratamentos de ficheiros da Administración Autónoma inscritos no RGPD

Comunidade Autónoma	Ficheiros 2005	Ficheiros 2006	Variac. 2006-2005
Andalucía	1.486	1.363	-8,28
Aragón	237	237	0,00
Asturias	230	241	4,78
Baleares	61	72	18,03
Canarias	382	397	3,93
Cantabria	51	57	11,76
Castela e León	391	467	19,44
Castela-A Mancha	238	363	52,52
Cataluña	548	581	6,02
Ceuta	23	23	0,00
Estremadura	146	163	11,64
Galicia	749	768	2,54
Madrid	6.051	6.066	0,25
Melilla	62	62	0,00
Murcia	286	304	6,29
Navarra	116	125	7,76
País Vasco	446	458	2,69
Rioxa	229	187	-18,34
Valencia	509	554	8,84
Total	12.241	12.488	2,02

Fonte: Elaboración propia a partir de estatísticas da AGPD

No referente á Administración Local podemos calcular o ratio de ficheiros inscritos en relación ao número de entes locais que inscribiron estes ficheiros. Segundo os datos acumulados ata o ano 2006, o número total de ficheiros que por termo medio ten inscrito cada entidade de ámbito local era de 7,53 ficheiros (táboa 14), un resultado moi superior ao que ocorría cos ficheiros de titularidade privada (2,39 ficheiros por entidade). Neste caso concreto, Galicia sitúase por debaixo da media estatal cunha inscrición media por entidade de 5,73 ficheiros (A Coruña 6,22 ficheiros; Lugo 5,05; Ourense 6,72 e; Pontevedra 4,67 ficheiros por entidade)

Táboa 14. Ficheiros inscritos e Entidades con ficheiros inscritos da Administración Local (2006)

Comunidade Autónoma	Entidades	Ficheiros	[Fich.]/[Entid.]
Andalucía	715	6.260	8,76
Aragón	468	2.966	6,34
Asturias	53	416	7,85
Baleares	71	758	10,68
Canarias	92	602	6,54
Cantabria	49	453	9,24
Castela e León	526	2.443	4,64
Castela-A Mancha	377	2.345	6,22

Comunidade Autónoma	Entidades	Ficheiros	[Fich.]/[Entid.]
Cataluña	598	4.100	6,86
Estremadura	203	1.656	8,16
Galicia	281	1.609	5,73
Madrid	141	1.671	11,85
Murcia	41	589	14,37
Navarra	105	541	5,15
País Vasco	201	2.588	12,88
Rioxa	31	171	5,52
Valencia	415	3.723	8,97
<b>Total</b>	<b>4.367</b>	<b>32.891</b>	<b>7,53</b>

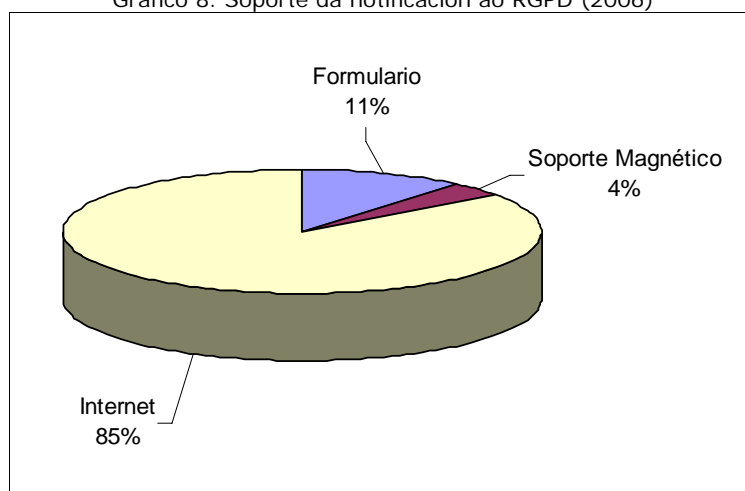
Fonte: Elaboración propia a partir de estatísticas da AGPD

#### 4. SOPORTE DAS OPERACIÓNS ANTE O RGPD

Como último apartado deste capítulo e, logo de facer mención ao nivel ou grao de cumprimento da LOPD, tanto no ámbito privado como no público, cabe resaltar moi brevemente o medio que utilizan as distintas entidades para inscribir os seus ficheiros no *Registro General de Protección de Datos* (RGPD).

No ano 2006 o RGPD tramitou de media máis de 900 operacións diarias, das que 700 correspondían a inscricións de novos ficheiros. Na actualidade máis de 260 novas entidades diarias inscriben os seus ficheiros con datos de carácter persoal neste rexistro, mentres que no 2003 a media diaria era de 136. Tomando como referencia os últimos cinco anos (2002-2006), os documentos de entrada segundo o tipo de soporte para a notificación das operacións (altas, modificacións, baixas e subsanacións) proceden, na súa maior medida, dunha presentación vía Internet. O gráfico 8 recolle as estatísticas dos soportes da notificación correspondentes ao ano 2006.

Gráfico 8. Soporte da notificación ao RGPD (2006)



Fonte: Agencia Española de Protección de Datos (AGPD)

Por outra banda, a propia AGPD informa que dos máis de 160.000 ficheiros inscritos no 2006, preto de 6.000 se inscribiron mediante o novo *Sistema de Notificaciones Telemáticas a la Agencia* (Sistema NOTA). Este novo sistema vén a substituír ao antigo programa de inscrición de ficheiros que estivo en funcionamento nos últimos anos e que aínda se segue utilizando, pero cada vez menos. O Sistema NOTA presenta unha navegación máis intuitiva e permite que o responsable non se perda entre os diferentes apartados que ten que cubrir. Unha das maiores novidades é a posibilidade de realizar a inscrición e o envío por Internet mediante a utilización da firma electrónica. Este sistema está sendo moi ben acollido polas entidades, xa que, ao 30-9-2007 o volume total anual de descargas do Formulario NOTA era de 84.464 fronte a 3.057 do programa de axuda anterior.

Grazas a este *Sistema de Notificaciones Telemáticas a la Agencia* tamén se puido incorporar o trámite obrigatorio de inscrición de ficheiros con datos de carácter persoal na constitución de sociedades de responsabilidade limitada e das sociedades limitadas nova empresa que se realicen de forma telemática a través do sistema de tramitación telemática do *Centro de Información y Red de Creación de Empresas* (CIRCE).

## **CAPÍTULO 4**

# **A SOCIEDADE DA INFORMACIÓN E A PROTECCIÓN DE DATOS DE CARÁCTER PERSOAL**

**Especial referencia á Lei 25/2007**

Susana Álvarez González  
*Universidade de Vigo*

As Tecnoloxías da Información e da Comunicación (TIC) permiten acelerar o ritmo dos avances técnicos, a modernización e o axuste estrutural da economía. Tendo en conta o enorme potencial de crecemento deste sector é necesario aplicar políticas específicas e adaptar as políticas actuais aos novos avances.

A expansión das redes de telecomunicacións, en especial de Internet como vehículo de transmisión e intercambio de informacións, así como, a paulatina incorporación dos móbiles multimedia son un reflexo do comportamento dos cidadáns fronte as TIC. Nestes intres asistimos ao nacemento do denominado "mercado electrónico globalizado". Grazas a esta evolución a comunicación non só se converte nunha actividade comercial mundial, senón que apoia a mundialización e a posta en rede de actividades económicas.

A aplicación das novas tecnoloxías desenroladas no marco da sociedade da información supón a superación das formas tradicionais de comunicación mediante a expansión dos contidos transmitidos e os soportes e formatos utilizados. Esta expansión está acompañada en grande medida por un descenso dos custos deste tipo de comunicacións que as fai accesibles para a maioría das persoas.

A sociedade da información xera por si mesma un marco de evolución que provoca cambios constantes no contorno xurídico e con facilidade créanse ámbitos baleiros de regulamentación. As posibilidades técnicas das redes abertas xa están poñendo a proba as estruturas xurídicas en numerosas áreas, sendo a protección dos datos persoais e a confidencialidade da información unha delas.

E é que na era na que o uso da tecnoloxía facilita a relación entre os individuos e chega con acceder a Internet ou a unha rede similar para coñecer datos e informacións relativas a unha persoa determinada, resulta imprescindible a adopción de mecanismos xurídicos que faciliten, por unha banda, o desenvolvemento da sociedade da información e, por outra parte, fronteiras legais para impedir, cando a persoa o desexe, accesos non autorizados á súa información.

Son numerosos, polo tanto, os cambios normativos como a adopción de novos instrumentos xurídicos que pretenden regular os distintos aspectos da sociedade da información. A aparente natureza neutra destes avances non impide que do seu uso poidan derivarse fins indexados ou incluso delictivos. Por este motivo, na actualidade estamos presenciando unha transformación normativa consistente nun intento de conciliación entre o uso de novas tecnoloxías e a necesaria protección da seguridade pública por unha banda e, da privacidade dos cidadáns e o segredo das comunicacións doutro lado.

Sen ánimo exhaustivo, é necesario citar en primeiro lugar os cambios vencellados á "revolución" normativa producida no ano 2003, consecuencia en gran medida da necesidade de adaptación ao Dereito Comunitario.

Neste marco, apróbase a Lei 32/2003, de 3 de novembro, Xeral de Telecomunicacións<sup>43</sup>. Trátase dun novo marco regulador das comunicacións electrónicas provocado pola transposición das seguintes Directivas Comunitarias: a Directiva 2002/21/CE, do Parlamento Europeo e do Consello, de 7 de marzo de 2002, relativa a un marco regulador común de redes e servizos de comunicacións electrónicas; a Directiva 2002/20/CE, Parlamento Europeo e do Consello, de 7 de marzo de 2002, relativa á autorización de redes e servizos de comunicacións electrónicas; a Directiva 2002/22/CE, do Parlamento Europeo e do Consello, de 7 de marzo de 2002, relativa ao servizo universal e aos dereitos dos usuarios en relación cas redes e os servizos de comunicacións electrónicas; a Directiva 2002/19/CE, do Parlamento Europeo e do Consello, de 7 de marzo de 2002, relativa ao acceso ás redes de comunicacións electrónicas e recursos asociados e a súa interconexión; a Directiva 2002/58/CE, do Parlamento Europeo e do Consello, de 12 de xullo de 2002, relativa ao tratamento de datos persoais e a protección da intimidade no sector das comunicacións electrónicas; a Directiva 2002/77/CE, da Comisión, de 16 de setembro de 2002, relativa á competencia nos mercados de redes e servizos de comunicacións electrónicas e, finalmente, a Decisión núm. 676/2002/CE, do Parlamento Europeo e do Consello, de 7 de marzo de 2002, sobre un marco regulador da política do espectro radioelétrico na Unión Europea.

A mencionada Lei ten por obxecto regular exclusivamente o sector das telecomunicacións, polo que exclúe expresamente da súa regulación os contidos difundidos a través de medios audiovisuais e a prestación de servizos sobre redes de telecomunicacións que non consistan principalmente no transporte de sinais a través das citadas redes<sup>44</sup>. En relación cos dereitos dos usuarios recolle a ampliación das prestacións, que, como mínimo, deben prestarse aos cidadáns baixo a denominación de "Servizo Universal"<sup>45</sup>.

O segredo das comunicacións e a protección dos datos persoais e dereitos e obrigas vinculados con redes e servizos de comunicación electrónica encóntranse recollidos nos artigos 33 e seguintes da Lei 32/2003. O artigo 34 da citada Lei 32/2003, de 3 de novembro, está dedicado en particular á protección de datos persoais. Establece a obriga dos operadores que exploten redes públicas de comunicacións electrónicas ou que presten servizos de comunicacións electrónicas dispoñibles ao público de garantir, no exercicio da actividade, a protección de datos de carácter persoal, sen prexuízo das limitacións establecidas no artigo, apartado 6, e artigo 33, parágrafo segundo, da citada Lei así na restante normativa aplicable.

No sector das telecomunicacións constitúen exemplos prácticos do intento de conxugar o modelo tecnolóxico coa protección da privacidade a prohibición de envío de comunicacións comerciais non solicitadas ou a obriga de que os datos de tráfico dos usuarios non se almacenen máis alá dun período de tempo determinado, que cede unicamente ante necesidades públicas prevalentes,

---

<sup>43</sup> BOE núm 264, de 4 de novembro de 2003.

<sup>44</sup> Exposición de motivos da Lei 32/2003, de 3 de novembro.

<sup>45</sup> Sección Segunda, do Capítulo I do Título III da Lei 32/2003, de 3 de novembro.

recollidas legalmente, ou no eido dunha investigación xudicial (Erdozáin López, 2007).

A este marco regulador hai que engadir a aprobación do Real Decreto 2296/2004, de 10 de decembro, que establece o novo regulamento sobre mercados de comunicacións electrónicas, acceso ás redes e numeración<sup>46</sup> e o Real Decreto 424/2005, de 15 de abril sobre as condicións de servizos de comunicacións electrónicas, o servizo universal e a protección dos usuarios<sup>47</sup>.

Dende a óptica da protección de datos no sector das telecomunicacións este último Regulamento mencionado é especialmente importante, pois desenvolve o previsto no artigo 34 da Lei 32/2003. Adica o Título V integramente á protección dos datos persoais na explotación de redes e na prestación dos servizos de comunicacións electrónicas dispoñibles ao público.

Esta regulación está realizada dende unha tripla perspectiva, como é o tratamento dos datos que obren no poder dos operadores relativo ao tráfico, facturación e localización dos abonados e usuarios, a elaboración das guías telefónicas dos números de abonados e a prestación de servizos avanzados de telefonía, como a identificación da liña de orixe e o desvío de chamadas (Marín Pérez, 2005). Estas tres temáticas son abordadas polos artigos 65 e seguintes do Regulamento.

En primeiro lugar o artigo 65 regula o tratamento de datos persoais relativos ao tráfico e a facturación, establecendo a obriga de eliminar ou facer anónimas as informacións de carácter persoal referidas a una comunicación e relacionadas cos usuarios e abonados tratados e almacenados co fin de establecer unha comunicación, sempre e cando xa non sexan precisos para tal finalidade.

Poderán ser tratados os datos do tráfico que sexan necesarios para realizar a facturación e os pagos das interconexións durante o prazo no que poida impugnarse a factura ou esixirse o pago. Transcorrido este prazo, deberán eliminarse ao facerse anónimos os datos de carácter persoal sinalados.

Tamén autoriza o citado artigo aos operadores o tratamento dos datos de tráfico con fins de promoción comercial de servizos de comunicacións electrónicas ou para a prestación de servizos con valor engadido, na medida e durante o tempo preciso para a prestación de tales servizos ou a súa promoción comercial, sempre e cando o abonado outorgase o seu consentimento informado. A estes efectos, os suxeitos obrigados deberán dirixirse aos abonados polo menos cun mes de antelación ao inicio da promoción ou da prestación do servizo con valor engadido, informalos do tipo de servizos para os que se efectuará o tratamento, os tipos de datos que serán obxecto do mesmo, a duración que terá e solicitar o seu consentimento. Deberá en todo caso posibilitarse que o suxeito poida manifestar a súa negativa ao tratamento dos datos. Deberá ademais comunicarlle ao afectado a posibilidade de manifestar a súa negativa ao tratamento dos datos.

---

<sup>46</sup> BOE núm. 314, de 30 decembro 2004.

<sup>47</sup> BOE núm. 102, de 29 abril de 2005.

Dentro deste marco normativo merece especial mención a aprobación da Directiva 2006/24/CE, do Parlamento Europeo e do Consello, de 15 de marzo de 2006, sobre a conservación de datos xerados ou tratados en relación coa prestación de servizos de comunicacións electrónicas de acceso público ou de redes públicas de comunicacións, pola que se modifica a Directiva 2002/58/CE<sup>48</sup>.

Son obxectivos da citada Directiva harmonizar as obrigas dos provedores de conservar determinados datos e asegurar que estean dispoñibles con fins de investigación, detección e enxuzamento de delitos graves. Presta especial atención a Directiva ao respecto aos dereitos fundamentais, facendo especial referencia aos recoñecidos pola Carta de Dereitos Fundamentais da Unión Europea. En particular, tal e como sinala no seu considerando vixésimo segundo, este texto normativo xunto coa Directiva 2002/58/CE intenta garantir o pleno cumprimento do dereito dos cidadáns á vida privada, o segredo das comunicacións e á protección de datos de carácter persoal.

A ninguén se lle escapa as posibilidades que estes avances ofrecen para transmitir información e poder pasar o mesmo tempo desapercibido no contido do transmitido (Erdozáin López, 2007). Con estas condicións técnicas as formas graves de delincuencia encontraron unha das armas máis prezadas. Neste contexto, poder acceder, rastrexar ou localizar unha comunicación electrónica constitúe na actualidade un obxectivo esencial na loita contra o terrorismo e as formas graves de delincuencia (Erdozáin López, 2007). Os datos de tráfico e localización desas comunicacións son eslavóns da cadea que levan ata a orixe e o destino, segundo sexa o sentido, da comunicación en xeral.

A Directiva, como excepción á obriga de eliminar os datos nos termos sinalados previamente prevé un prazo de conservación dos datos de carácter persoal de tráfico e de localización de persoas. Esta cuestión xa fora tratada no Dereito interno pola Lei 34/2002, de 11 de xullo, de Servizos da Sociedade da Información e do Comercio electrónico<sup>49</sup>. O obxecto da Lei é a regulación do réxime xurídico dos servizos da sociedade da información e a contratación por vía electrónica, no relativo ás obrigas dos prestadores de servizos incluídos os que actúan como intermediarios na transmisión de contidos polas redes de telecomunicacións, as comunicacións comerciais por vía electrónica, a información previa e posterior á celebración de contratos electrónicos, as condicións relativas a súa validez e eficacia e o réxime sancionador aplicable aos prestadores de servizos da sociedade da informacións.

A Lei 34/2002 establecía un prazo de conservación dos datos dun máximo de 12 meses. O problema que presentaba a Lei era que recollía un prazo máximo de conservación pero non un mínimo polo que algúns operadores optaron por un borrado inmediato (Erdozáin López, 2007). O artigo 12 da Lei foi derogado pola Disposición Derogatoria Única de Lei 25/2007, de 18 outubro.

A Directiva establece a obriga de garantir que se conserven na medida que son xerados ou tratados polos provedores de servizos de comunicacións de acceso público ou dunha rede de comunicacións os datos previstos no seu artigo 5:

---

<sup>48</sup> Diario Oficial de la Unión Europea L 105/54, de 13 de abril de 2006.

<sup>49</sup> BOE núm. 166, 12 xullo 2002.

- Datos necesarios para rastrear e identificar a orixe dunha comunicación.
  - 1) En relación coa telefonía de rede fixa e a telefonía móbil:
    - o número de teléfono de chamada,
    - o nome e o enderezo do abonado ou usuario
  - 2) No acceso a Internet, correo electrónico por Internet e Telefonía por Internet:
    - A identificación de usuario asignada.
    - A identificación de usuario e o número de teléfono asignados a toda comunicación que acceda á rede pública de telefonía.
    - O nome e o enderezo do abonado ou do usuario rexistrado o que se lle asignou no momento da comunicación un enderezo de Protocolo de Internet (IP), unha identificación de usuario ou un número de teléfono.
  
- Datos necesarios para identificar o destino dunha comunicación.
  - 1) En relación coa telefonía de rede fixa e a telefonía móbil:
    - O número ou números marcados e, no caso de que interveñan outros servizos, como o desvío ou a transferencia de chamadas, o número ou números aos que se transfíren as chamadas.
    - Os nomes e os enderezos dos abonados ou usuarios rexistrados.
  - 2) En relación ao correo electrónico por Internet e Telefonía por Internet:
    - A identificación de usuario ou o número do teléfono do destinatario ou destinatarios dunha chamada telefónica por internet.
    - Os nomes e enderezos dos abonados ou usuarios rexistrados e a identificación de usuario do destinatario da comunicación.
  
- Datos necesarios para identificar a data, hora e duración dunha comunicación.
  - 1) En relación coa telefonía de rede fixa e a telefonía móbil: a data e hora do comezo e fin da comunicación.
  - 2) No acceso a Internet, correo electrónico por Internet e Telefonía por Internet:
    - A data e hora da conexión e desconexión do servizo de acceso a Internet, baseadas nun determinado uso horario, así como o enderezo IP asignada polo provedor de acceso a Internet a unha comunicación e a identificación do usuario abonado e do usuario rexistrado.
    - Data e hora da conexión e desconexión do servizo de correo electrónico por Internet ou do servizo de telefonía por Internet, baseada nun determinado uso horario.

- Datos precisos para identificar o tipo de comunicación.
  - 1) En relación coa telefonía de rede fixa e a telefonía móbil: o servizo telefónico utilizado.
  - 2) En relación co correo electrónico por Internet e a telefonía por Internet: o servizo de Internet utilizado
- Datos necesarios para identificar a equipa de comunicación dos usuarios ou o que se considera o equipo de comunicación.
  - 1) En relación coa telefonía de rede fixa: os números de teléfono de orixe e destino.
  - 2) En relación coa telefonía móbil:
    - Os números de teléfono de orixe e destino.
    - A identidade internacional do abonado móbil (IMSI) da parte que efectúa a chamada.
    - A identidade internacional da equipa móbil (IMEI) da parte que efectúa a chamada.
    - A IMSI da parte que recibe a chamada.
    - A IMEI da parte que recibe a chamada.
    - No caso de servizos anónimos de pago por adiantado, data e hora da primeira activación do servizo e a etiqueta de localización dende a que está activado o servizo.
  - 3) En relación ao acceso a Internet, correo electrónico e telefonía por Internet:
    - O número de teléfono de orixe no caso de acceso mediante marcado de números.
    - A liña dixital de abonado (DSL) ou outro punto terminación identificador do autor da comunicación.
- Datos necesarios para identificar a localización da equipa de comunicación móbil.
  - 1) A etiqueta de localización ao comezo da comunicación.
  - 2) Os datos que permiten fixar a localización xeográfica da cela, mediante a referencia da etiqueta de localización durante o período no que se conservan os datos das comunicacións.

O período de conservación destes datos non será inferior a seis meses nin superior a dous anos a partir da data da comunicación.

Co obxectivo de dar cumprimento ao disposto na Directiva 2006/24/CE, recentemente aprobouse a Lei 25/2007, de 18 de outubro<sup>50</sup>, de conservación de datos relativos ás comunicacións electrónicas e ás redes públicas de comunicacións. Constitúe o obxecto da Lei a regulación da obriga dos operadores de conservar os datos xerados ou tratados no marco da prestación de servizos de comunicacións electrónicas ou de redes públicas de

---

<sup>50</sup> BOE núm. 251, de 19 de outubro.

comunicación, así como o deber de cesión dos citados datos aos axentes facultados sempre que lles sexan requiridos por autorización xudicial con fins de detección, investigación e enxuzamento de delitos graves contemplados no Código Penal o unas leis penais especiais.

Recolle a Lei a obriga de conservar os datos enumerados pola Directiva, estendendo esta obriga aos datos relativos ás denominadas chamadas infrutuosas. Enténdese por chamada infrutuosa “a comunicación no transcurso da cal se realizou con éxito a chamada telefónica pero sen contestación o na que houbo unha intervención por parte do operador ou operadores involucrados na chamada”<sup>51</sup>.

Están excluídos da Lei os datos relativos ás chamadas non conectadas, entendéndose por tal “aquela comunicación no transcurso da que se realizou unha chamada sen éxito, sen que houbera intervención do operador ou operadores involucrados”<sup>52</sup>.

Deroga a Lei 25/2007 o artigo 12 da Lei 34/2002 e regula o período de conservación dos datos nos seguintes termos:

“A obriga de conservación dos datos cesa aos doce meses computados dende a data na que se produciu a comunicación. Regulamentariamente, previa consulta aos operadores, poderá ampliarse ou reducirse o prazo de conservación para determinados datos ou unha categoría de datos ata un máximo de dous anos ou un mínimo de seis meses, tomando en consideración o custo do almacenamento e conservación dos datos, así como a interese dos mesmos para fins de investigación, detección e enxuzamento dun delito grave, previa consulta dos operadores”.

O establecemento destas obrigas, xustificadas na necesidade de protexer a seguridade pública, efectúase buscando o imprescindible equilibrio entre esta e os dereitos fundamentais que poidan verse afectados en especial a privacidade e o segredo das comunicacións<sup>53</sup>.

Co obxecto de preservar o segredo das comunicacións e a privacidade establece a Lei tres tipos de garantías:

1. Non se poderá conservar ningún dato que revele o contido da comunicación (artigo 3.2 da Lei 25/2007). Neste senso, busca a Lei ser respectuosa cos pronunciamentos do Tribunal Constitucional sobre o dereito o segredo das comunicacións. Os datos que a Lei obriga a conservar son única e exclusivamente os vinculados a unha comunicación, xa sexa telefónica ou efectuada por Internet, pero en ningún caso reveladores do seu contido.
2. A cesión dos datos que afecten a tal comunicación ou comunicacións concretas esixirá, sempre autorización xudicial previa.

---

<sup>51</sup> Artigo 4, apartado segundo (Lei 25/2007).

<sup>52</sup> Artigo 4, apartado terceiro (Lei 25/2007).

<sup>53</sup> Preámbulo da Lei 25/2007, de 18 de outubro.

As normas relativas á cesión encóntranse recollidas nos artigos 6 e 7 da Lei 25/2007 e tradúcense nas seguintes obrigas:

- Os datos só poderán ser comunicados para fins determinados e concretos e previa autorización xudicial.
- A resolución xudicial determinará os datos conservados que deben ser cedidos. Unicamente se poderán comunicar os datos conservados aos que se refire a Lei relativos á comunicacións que identifiquen a persoas. En todo caso, será necesario respectar os principios de necesidade e proporcionalidade.
- Os datos unicamente se cederán aos axentes facultados, sinalados no apartado segundo artigo 6 da Lei.
- O prazo de execución da orde de cesión será fixado pola resolución xudicial. Este terá en conta a urxencia e os efectos da investigación, así como a natureza e a complexidade técnica da operación.
- A cesión aos axentes facultados dos datos de conservación obrigatoria, efectuarase en formato electrónico. Así mesmo, os suxeitos obrigados pola Lei a conservar estes datos terán un prazo de seis meses dende a súa entrada en vigor para configurar, a súa costa, os equipos e estar preparados tecnicamente en disposición de cumprir coas obrigas de conservación e cesión de datos (Disposición Final Cuarta).

Fronte a estas garantías de protección do afectado polo tratamento dos datos persoais, en relación coa cesión, establece a Lei 25/2007 un límite ao dereito fundamental á protección de datos persoais. O responsable do tratamento non comunicará a cesión dos datos efectuada de conformidade co disposto na citada Lei.

### 3. A protección e seguridade dos datos.

Como non podía ser doutro xeito a Lei establece a obriga de que os datos persoais conservados estean suxeitos ás normas de seguridade. A seguridade dos datos esixe a adopción dunha serie de medidas con finalidade de garantir o principio de seguridade da información de carácter persoal.

O obriga de manter a seguridade dos datos encóntrase recollido do artigo 8 da Lei 5/2007 que impón as seguintes pautas:

- Identificación do persoal autorizado para acceder aos datos.
- Adoptar as medidas técnicas e organizativas que impidan a súa manipulación ou uso para fins distintos aos comprendidos na mesma, a súa destrución accidental ou ilícita e a perda accidental, así como o arquivo, tratamento, divulgación ou acceso non autorizado, de conformidade co disposto na Lei 15/1999 e na súa normativa de desenvolvemento.

- Cumprir as obrigas derivadas dos principios de calidade dos datos e a confidencialidade e seguridade no tratamento dos datos, segundo o disposto na LOPD e na súa normativa de desenvolvemento. No relativo ás medidas de seguridade haberá que acudir ao Real decreto 994/1999, de 11 de xuño. Así mesmo, o nivel de protección dos datos almacenados determinarase de conformidade coa LOPD, en particular co disposto no artigo 9.
- Designa á *Agencia Española de Protección de Datos* como autoridade pública responsable de velar polo cumprimento das previsións da LOPD e da normativa de desenvolvemento aplicables aos datos mencionados na Lei 5/2007.

Por último, hai que facer referencia á novidade establecida na Disposición Adicional Única da Lei relativa aos servizos de telefonía mediante tarxetas de prepago. Por primeira vez introdúcese na normativa a obriga de que os operadores de telefonía móbil que comercialicen servizos con sistema de activación mediante a modalidade de tarxetas de prepago deberán levar un libro rexistro no que conste a identidade dos clientes que adquiran unha tarxeta intelixente coa citada modalidade de pago. A citada obriga é esixible dende a entrada en vigor da Lei<sup>54</sup>.

Os operadores de telefonía móbil que comercialicen estes servizos terán un prazo de dous anos dende a entrada en vigor para cumprir coa obriga de inscrición das tarxetas adquiridas con anterioridade á entrada en vigor desta Lei. Transcorrido este prazo, os operadores terán que anular ou desactivar as tarxetas prepago, cando non puideran cumprir con esta obriga.

A identificación das persoas físicas farase co documento acreditativo da personalidade. No libro-rexistro deberá facerse constar os seguintes datos: nome e apelidos, nacionalidade, número, natureza e denominación correspondente o documento identificativo. A identificación das persoas xurídicas realizarase aportando a tarxeta de identificación fiscal e farase constar no libro-rexistro a denominación social e o código de identificación fiscal.

En relación co previsto coas tarxetas de modalidade prepago, sen prexuízo do disposto na LOPD, constitúen infraccións moi graves:

- O incumprimento de levar o libro-rexistro.
- A negativa á cesión e á entrega de datos das persoas nos casos previstos na disposición.

Constitúen infraccións graves:

- Levar de forma incompleta o libro-rexistro.
- A demora inxustificada, en máis de setenta e dúas horas na cesión e entrega dos datos nos casos legalmente previstos.

---

<sup>54</sup> Punto 7, da Disposición Adicional Única da Lei 25/2007.

Será de aplicación a estas infraccións o réxime sancionador establecido na Lei 32/2003, de 3 de novembro. A competencia sancionadora corresponde ao Secretario de Estado de Telecomunicacións e para a Sociedade da Información.

## CAPÍTULO 5

# CONCLUSIÓNS E REFLEXIÓNS FINAIS

Manuel Martínez Carballo  
Eduardo Guillén Solórzano  
Susana Barbeito Roibal  
*Universidade da Coruña*

M<sup>a</sup> Cruz del Río Rama  
Susana Álvarez González  
*Universidade de Vigo*

Para pechar esta breve monografía sobre a protección de datos de carácter persoal, a continuación indícanse unha serie de conclusións a modo de reflexións finais sobre o tema que nos incumbe.

En primeiro lugar, hai que destacar que, segundo o estudo de carácter exploratorio realizado no capítulo 3 desta obra, existe un claro incumprimento xeneralizado da lexislación vixente en materia de protección de datos de carácter persoal por parte das entidades do noso país, tanto privadas como públicas. No caso de Galicia os índices de cumprimento sitúanse entorno á media nacional.

Este suspenso xeneralizado en toda España parece ir en consonancia co feito de que a Lei Orgánica 15/1999 e o seu desenvolvemento regulamentario é considerada unha das leis máis estritas do mundo nesta materia. Non hai máis que ler algúns titulares aparecidos en prensa nos últimos meses para facernos eco da situación actual (táboa 15).

---

Táboa 15. Titulares de prensa sobre o nivel ou grao de cumprimento da LOPD

---

**Sólo el 10% de las pymes españolas cumple la Ley de Protección de Datos**

**El 90% de las empresas incumple la Ley de Protección de Datos**

**El 92% de los negocios gallegos no protegen bien nuestros datos**

---

Fonte: Prensa escrita do noso país

Polo tanto, o que realmente habería que preguntarse é se non se cumpre esta normativa porque é moi complexa, resulta moi custoso, as entidades non están preparadas técnica nin organizativamente, non existe a suficiente formación e información ou, resulta que se aprobou unha lexislación tan difícil de levar á práctica que hai un certo “pasotismo” por parte da Administración encargada do seu control e das entidades que teñen que cumprila; porque o que non é lóxico é que despois de case quince anos cunha normativa específica ao respecto esteamos cuns índices de cumprimento tan baixos, ou visto doutra forma, cun nivel ou grao de incumprimento tan elevado.

Certas investigacións levadas a cabo en ámbitos moi reducidos achégannos algúns indicios de partida. Un estudo realizado pola Consultora Helas no ano 2004 destaca que o incumprimento desta normativa débese ao descoñecemento que existe da mesma no tecido empresarial, así como, o seu verdadeiro contido. Ademais, aseguran que os principais incumprimentos céntranse na ausencia de medidas organizativas para protexer o uso da información e a carencia de medidas tecnolóxicas.

Neste contexto, unha enquisa realizada no ano 2003 pola Comisión Europea revelaba que o 70% dos españois nunca oíran falar da lexislación existente en materia de protección de datos de carácter persoal e do contido dos dereitos que lle asisten e, o 76% descoñecía ata a existencia dun organismo público encargado de recibir as súas reclamacións e queixas.

Na actualidade, aínda que existe un coñecemento crecente da normativa, especialmente por parte das grandes empresas, a maioría das entidades

privadas e máis concretamente as PEMES non teñen en conta a protección e o tratamento de toda a información de carácter persoal que van almacenando nas súas bases de datos, basicamente por dous motivos: o descoñecemento e o contido da lexislación vixente nesta materia e, a pouca importancia que lle prestan a este tipo de datos.

Outra reflexión que cabería facerse en comparación con outros temas, é porqué en materias como poden ser no ámbito laboral, fiscal ou mercantil cúmprese a lexislación de maneira rigoroso ou polo menos inténtase na súa grande parte. Será quizais por que en materia de protección de datos de carácter persoal as inspeccións/sancións non son tan habituais ou severas na práctica dado que a *Agencia Española de Protección de Datos* (AGPD) non conta coa suficiente infraestrutura (técnica e humana), a pesar do seu autofinanciamento.

En relación con este aspecto, hai que ter en conta que o réxime sancionador español no ámbito privado é tamén un dos máis duros do mundo desde o punto de vista económico, polo que descoidar o cumprimento da LOPD pódese pagar moi caro con sancións de ata 601.012,10 euros que, en moitos casos, pode facer perigar a viabilidade do negocio e, noutros pode supor ata o peche do mesmo ao non poder facer fronte ao pago de tales contías. O réxime sancionador no ámbito público é de carácter disciplinario e non pecuniario.

O número de actuacións e procedementos iniciados e finalizados por parte da AGPD é cada vez maior nos últimos anos, aínda que, o crecemento habido no 2006 é menor en relación aos anteriores. No ano 2006 iniciáronse 1.182 actuacións previas de investigación fronte ás 1.158 no 2005, 978 no 2004, 574 no 2003, 723 no 2002, 405 no 2001 e, 319 no 2000. Respecto das actuacións e procedementos finalizados, no ano 2006 termináronse 1.539 fronte ás 1.456 no 2005, 1.184 no 2004 e, 1.037 no 2003. A Administración Pública ocupa no exercicio 2006 o terceiro posto por sector de actividade, tanto nas actuacións iniciadas como nas finalizadas. Galicia ocupa nese mesmo ano o quinto lugar no ranking de procedementos iniciados por Comunidade Autónoma, tanto do denunciado como tamén do principal investigado. No referente a procedementos sancionadores iniciados no 2006 por Comunidade Autónoma do principal imputado, Galicia ocupa tamén o quinto posto por detrás de Madrid, Cataluña, Andalucía e País Vasco. Sen embargo, ocupa o sexto lugar en canto a procedementos sancionadores finalizados. Estas cifras do volume de actuacións e procedementos da *Agencia Española de Protección de Datos* corroboran dalgunha forma os comentarios anteriores.

Por outra banda, os indicadores ou ratios comentados no capítulo 3 reflexan entidades que iniciaron ou deron algún paso de cara ao cumprimento da lexislación vixente en materia de protección de datos de carácter persoal, porque o que si é certo, é que moitas entidades consideran que co simple feito de inscribir os ficheiros correspondentes na AGPD xa están cumprindo coa Lei e, esquécense dos documentos e medidas de seguridade que hai que adoptar segundo o tipo de dato que se almacene, así como, das auditorías pertinentes. A propia *Agencia Española de Protección de Datos* reconece neste sentido que existe un gran número de entidades que aínda non contan co respectivo documento de seguridade, polo que, o nivel ou grao de cumprimento analizado sería aínda menor. É máis, sendo estritos en todos os aspectos da norma,

poderíamos estar falando dunhas porcentaxes de cumprimento por baixo do 5%.

En definitiva, á vista de todos os comentarios anteriores, parece confirmarse tamén o dito a nivel xeral de que España é un dos países do mundo con máis normativa, pero tamén parece que somos os que menos a cumprimos e/ou facemos cumprir.

Ademais, o incumprimento da LOPD pode supor nalgúns casos a non certificación dos Sistemas de Xestión da Calidade (SGC) conforme á familia de normas ISO 9000 cando devanditos incumprimentos afecten directamente á calidade do produto/servizo (véxase Anexo I). Noutros casos, pode entrañar incluso a retirada temporal ou definitiva da mencionada certificación.

Outra implicación directa que pode ter o non cumprir coa lexislación vixente nesta materia é a efectos da Lei 19/1988, de 12 de xullo, de Auditoría de Contas (B.O.E. 15-07-1988) e do Real Decreto 1636/1990, de 20 de decembro, polo que se aproba o Regulamento que desenvolve a Lei 19/1988 (B.O.E. 25-12-1990). Neste sentido, cabería facerse a reflexión de se é responsabilidade do auditor de contas avaliar o risco do incumprimento da lexislación vixente en materia de protección de datos de carácter persoal na empresa auditada. Na nosa opinión, a resposta a esta pregunta é obvia na medida en que se profundice na transcendencia do tema, xa que, moi raras veces o auditor se para a avaliar o risco do incumprimento desta normativa no seu traballo de auditoría que podería dar lugar no informe final a unha opinión con excepcións, desfavorable ou ata unha opinión denegada dependendo da avaliación do risco. En cambio, si acostuma facelo no ámbito laboral, fiscal, etc.

En resumo, descoidar o cumprimento da LOPD págase moi caro en todos os sentidos, tanto desde o punto de vista económico como do lado da xestión. Non obstante, para superar os niveis de cumprimento nos que estamos na actualidade é necesario un cambio de actitude do titular dos ficheiros. Así mesmo, resulta moi importante o que se sigan levando a cabo políticas de formación, información, concienciación, fomento ou outras actividades análogas sobre a existencia real e práctica desta lexislación por parte das Asociacións de Empresarios, as Cámaras de Comercio, a propia *Agencia Española de Protección de Datos*, a Consellería de Innovación e Industria da Xunta de Galicia no caso da comunidade galega, entre outras. A cambio, as entidades públicas e privadas do noso país débense comprometer fortemente a adoptar as medidas necesarias (humanas, económicas, técnicas, etc.) para cumprir a mesma, xa que, esta normativa resulta transcendental para a sociedade española, cuxo éxito depende e é "obrigación" de todos.

A posta a disposición das empresas dun programa informático para facilitar a adaptación dos requisitos técnicos e legais impostos pola lexislación vixente nesta materia, por exemplo o programa "Sinxelo LOPD" da Consellería de Innovación e Industria da Xunta de Galicia, é outra das medidas a ter moi en conta de cara a aumentar os índices de cumprimento.

**REFERENCIAS BIBLIOGRÁFICAS E  
PÁXINAS WEB DE INTERESE**

CABEZA PEREIRO, J. (2002): El descuento de la cuota sindical, Tirant lo Blanch, Valencia.

CÁMARAS DE COMERCIO (2003): Estudio de la LOPD, Consejo Superior de Cámaras Oficiales de Comercio, Industria y Navegación de España.

CORRIPIO GIL-DELGADO, R. (1996): "Las nociones de interés público e interés legítimo en relación al ejercicio del derecho de oposición del interesado", en Jornadas sobre el Derecho Español de Protección de Datos Personales, Agencia de Protección de Datos, Madrid.

DEL PESO NAVARRO, E.; RAMOS GONZÁLEZ, M.A. (1994): Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas, Díaz de Santos, Madrid.

DEL RÍO RAMA, M.C.; MARTÍNEZ CARBALLO, M.; GUILLÉN SOLÓRZANO, E. (2007): "La protección de datos de carácter personal. Estudio en la Comunidad Autónoma de La Rioja", XVII Jornadas Hispano-Lusas de Gestión Científica: "Conocimiento, Innovación y Emprendedores. Camino al Futuro", febrero, Logroño (España), Actas del Congreso formato CD-ROM, pp. 2931-2943, Edita Universidad de La Rioja.

DENNINGER, E. (1987): "El derecho a la autodeterminación informativa", traducción de Antonio Enrique Pérez Luño, en PÉREZ LUÑO, A.E. [Dir.] (1986): Problemas actuales de la documentación y la informática jurídica, Actas do Coloquio Internacional celebrado na Universidad de Sevilla, Sevilla, 5 e 6 de marzo de 1986, Tecnos, Madrid.

ERDOZÁIN LÓPEZ, J.C. (2007): "La protección de datos de carácter personal en el sector de las telecomunicaciones", Aranzadi Civil núm. 1/2007.

FROSINI, V. (1982): Cibernética, Derecho y Sociedad, Tecnos, Madrid.

FROSINI, V. (1987): "Problemas jurídicos de la información y la documentación", traducción de Manuel Carrera, en PÉREZ LUÑO, A.E. [Dir.] (1986): Problemas actuales de la documentación y la informática jurídica, Actas do Coloquio Internacional celebrado na Universidad de Sevilla, Sevilla, 5 e 6 de marzo de 1986, Tecnos, Madrid.

GARRIGA DOMÍNGUEZ, A. (2000): "La nueva Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales, ¿un cambio de filosofía?", Anales de la Cátedra Francisco Suárez, núm. 34/2000.

GARRIGA DOMÍNGUEZ, A. (2004): Tratamiento de datos personales y derechos fundamentales, Dykinson, Madrid.

HELAS CONSULTORES (2004): "La aventura de viajar por la red", Helas Consultores y AECE.

HEREDERO HIGUERAS, M. (1983): "La sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de Población de 1983", Documentación Administrativa, núm. 198.

HEREDERO HIGUERAS, M. (1997): La Directiva Comunitaria de Protección de Datos de Carácter Personal. Comentario a la Directiva 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, Aranzadi Editorial, Pamplona.

HERRÁN ORTIZ, A.I. (2003): El derecho a la protección de datos personales en la sociedad de la información, Universidad de Deusto-Instituto de Derechos Humanos, Bilbao.

LUCAS MURILLO DE LA CUEVA, P. (1990): El derecho a la autodeterminación informativa. La protección de los datos personales frente al uso de la informática, Tecnos, Madrid.

LUCAS MURILLO DE LA CUEVA, P. (1993): Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal), Centro de Estudios Constitucionales, Madrid.

LUCAS MURILLO DE LA CUEVA, P. (1999): "La construcción del derecho a la autodeterminación informativa", Revista de Estudios Políticos y Constitucionales, núm. 104, abril-junio.

MADRID CONESA, F. (1984): Derecho a la intimidad e Informática, Universidad de Valencia. Valencia.

MARÍN PÉREZ, A. (2005): "Protección de los datos personales en la explotación de redes y en la prestación de los servicios de comunicaciones electrónicas disponibles al público", Revista de la Agencia de Protección de Datos de la Comunidad de Madrid, núm. 15, (mayo).

MARTÍNEZ CARBALLO, M. (2006): "La protección de datos de carácter personal, el gran reto de principio de Siglo", Más Profesionales. Revista Económica de la Asociación de Empresarios de Culleredo, núm. 6 (marzo), pp. 8-11, Culleredo (A Coruña).

MARTÍNEZ CARBALLO, M.; DEL RÍO RAMA, M.C.; GUILLÉN SOLÓRZANO, E.; BARBEITO ROIBAL, S. (2006): "¿Cumplen las empresas la normativa sobre protección de datos?", Harvard Deusto Marketing & Ventas, núm. 75 (julio-agosto), pp. 12-17.

MARTÍNEZ CARBALLO, M.; DEL RÍO RAMA, M.C.; GUILLÉN SOLÓRZANO, E.; BARBEITO ROIBAL, S. (2007): "El cumplimiento de la Ley de Protección de Datos en Galicia", Revista Gallega de Economía, vol. 16, núm. 2 (diciembre), pp. 177-190, Santiago de Compostela (A Coruña).

MARTÍNEZ CARBALLO, M.; DEL RÍO RAMA, M.C.; GUILLÉN SOLÓRZANO, E.; BARBEITO ROIBAL, S. (2005): "¿Las empresas gallegas incorporan en su gestión el cumplimiento de la protección de datos?", III Congreso de Economía de Galicia: "Galicia en una Europa ampliada: convergencia y bienestar", Actas del Congreso formato CD-ROM, pp. 1-14, Edita IDEGA-Universidad de Santiago de Compostela.

MARTÍNEZ CARBALLO, M.; DEL RÍO RAMA, M.C.; GUILLÉN SOLÓRZANO, E.; BARBEITO ROIBAL, S. (2006): "El cumplimiento de la legislación en materia de protección de datos de carácter personal a debate", VI Congreso Gallego de la Calidad: "Cambiar para Ganar", marzo, Santiago de Compostela-A Coruña (España), Actas del Congreso formato CD-ROM, pp. 1-10, Edita Asociación Congreso Gallego de la Calidad, Santiago de Compostela.

ORTÍ VALLEJO, A. (1994): Derecho a la intimidad e informática (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada), Editorial Comares, Granada.

PENTEIO (2004): "Estudio sobre el cumplimiento de la LOPD y de la LSSI", Grupo Penteio y Landewell-PWC.

PÉREZ LUÑO, A.E. (1981): "Informática y libertad. Comentario al artículo 18.4 de la Constitución española", Revista de Estudios Políticos (Nueva Época), núm. 24.

PÉREZ LUÑO, A.E. (1986): "La defensa del ciudadano y la protección de datos", en Jornadas Internacionales sobre Informática y Administración Pública, Instituto Vasco de Administración Pública, Bilbao.

PÉREZ LUÑO, A.E. (1990): "La libertad informática. Nueva frontera de los derechos fundamentales", en LOSANO, M.G; PÉREZ LUÑO, A.E. y GUERRERO MATEUS, M.F. (1990): Libertad informática y leyes de protección de datos, Centro de Estudios Constitucionales, Madrid.

PÉREZ LUÑO, A.E. (1992): "Vittorio Frosini y los nuevos derechos de la sociedad tecnológica", Informática e Diritto, Le Monnier, Firenze.

PÉREZ LUÑO, A.E. (2001): "Sobre el arte legislativo del birbiloque. La LOPRODA y la tutela de la libertad informática", Anuario de Filosofía del Derecho, Nueva Época, Tomo XVIII.

PÉREZ LUÑO, A.E. (2003): Trayectorias contemporáneas de la Filosofía y la Teoría del Derecho, Grupo Nacional de Editores, Sevilla.

RODRÍGUEZ ESCANCIANO, S. (2000): "La intimidad del trabajador en el uso de diagnósticos médicos informatizados (Comentario a la STCo 202/1999, de 13 de noviembre)", Revista Española de Derecho del Trabajo, núm. 101.

SÁNCHEZ BRAVO, A.A. (1998): La protección del derecho a la libertad informática en la Unión Europea, Universidad de Sevilla, Sevilla.

SERRANO PÉREZ, M.M. (2003): El derecho fundamental a la protección de datos. Derecho español y comparado, Thomson-Civitas, Agencia de Protección de Datos de la Comunidad de Madrid, Madrid.

TÉLLEZ AGUILERA, A. (2002): La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores, Edisofer, Madrid.

TONIATTI, R. (1991): "Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada", traducción de Alejandro Saiz Arnaiz, Revista Vasca de Administración Pública, número 29.

ULL PONT, E. (2000): Derecho Público de la Informática (Protección de datos de Carácter Personal), Universidad Nacional de Educación a Distancia, Madrid.

VIZCAÍNO CALDERÓN, M. (2001): Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal, Civitas, Madrid.

Agencia Española de Protección de Datos

<http://www.agpd.es>

Agencia Catalana de Protección de Datos

<http://www.apdcat.net>

Agencia de Protección de Datos de la Comunidad de Madrid

<http://www.madrid.org/apdcm>

Agencia Vasca de Protección de Datos

<http://www.avpd.euskadi.net>

# ANEXO I

## A LOPD E AS AUDITORÍAS DE CALIDADE

Martín Pita López  
*Director da Delegación de Galicia de AENOR*

Configurada como un dereito fundamental de todos os cidadáns, a Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos (LOPD) e a súa normativa concordante impón unha serie de obrigacións legais para todas aquelas persoas físicas ou xurídicas, organismos públicos ou privados que traten ou manexen datos de carácter persoal.

Aquela empresa ou profesional, que no ámbito da súa actividade, desenvolva algún tipo de tratamento que afecte a datos de carácter persoal deberá adoptar as medidas necesarias co fin de adecuar devandito tratamento á normativa vixente, evitando así a imposición de sancións.

Os activos de información forman parte esencial na xestión das empresas do Século XXI e non cabe dúbida de que a protección destes activos, a través da implantación dunha política de seguridade activa e eficiente, supón un maior grao de competitividade para todas aquelas organizacións que o desenvolvan.

Partindo da base de que todas as organizacións teñen datos de carácter persoal, se a organización mantén ficheiros (tanto en soporte informático como en papel), programas ou equipos que conteñan estes datos, durante as auditorías analizarase se a empresa coñece as obrigacións, dereitos e aplica medidas de seguridade para o tratamento destes datos.

De forma xeral revisarase:

- Alta de ficheiros ante a *Agencia Española de Protección de Datos*: Identificación dos ficheiros que inclúan datos de carácter persoal e notificación dos mesmos para a súa inscrición no *Registro General de Protección de Datos*.
- Establecemento das políticas de privacidade, determinación das diferentes cláusulas contractuais e contratos de acceso aos datos persoais.
- Existencia do documento de seguridade e implantación das súas medidas, acorde aos niveis de protección dos datos que posúa a organización.

A aplicación dos niveis de seguridade vai en función do carácter dos datos. A LOPD distingue tres niveis:

- Básico, que son os que conteñen datos de carácter persoal.
- Medio, que son os que inclúen datos relativos a infraccións administrativas ou penais, Facenda Pública e servizos financeiros, así como o conxunto de datos que permitan a avaliación do individuo.
- Alto, que son os de especial protección e están relacionados cos datos referentes a ideoloxía, afiliación sindical, relixión e crenzas, orixe racial, saúde ou vida sexual e os datos solicitados con fins policiais sen consentimento do afectado.

De forma específica, en función dos niveis de seguridade que a organización outorgue aos datos que manexe, revisarase:

### 1. Medidas de Seguridade de Nivel Básico:

- Definición de funcións e obrigacións do persoal en canto á protección de datos.
- Creación e mantemento dun rexistro de incidencias.
- Implantación de procedementos de identificación e autenticación. Asignación de contrasinais.
- Relación de usuarios con acceso autorizado.
- Xestión de soportes (identificación do tipo de información que conteñen, inventario actualizado e autorización de saída polo Responsable do Ficheiro).
- Xestión de copias de respaldo e recuperación.

### 2. Medidas de Seguridade de Nivel Medio (engadidas ás anteriores):

- Designación dun Responsable de Seguridade que coordine e controle as medidas definidas no documento de seguridade.
- Auditoría bienal e emisión de informe.
- Control de acceso físico aos locais de sistemas informáticos.
- Establecemento de medidas adicionais para a xestión de soportes (establecemento dun rexistro de entrada e saída e elaboración dun procedemento para a eliminación de soportes).
- Probas con datos reais.

### 3. Medidas de Seguridade de Nivel Alto (engadidas ás anteriores):

- A distribución de soportes realizarase previo cifrado dos datos.
- Do rexistro de accesos conservarase: a identificación do usuario, a data e hora de acceso, o tipo de acceso cun período mínimo de conservación de dous anos.
- Existencia de copias de respaldo e recuperación en lugar diferente a onde se atopen os equipos informáticos.
- Obrigación de cifrar os datos na transmisión de datos a través de redes.

A organización debe ter identificados e implantados os requisitos, a non implantación ou a implantación parcial dos mesmos pode dar lugar á aparición de non conformidades ou observacións durante as auditorías.

Verificarase que sempre que se capturen datos que se pretendan tratar para outros fins distintos daqueles para os que se capturaron, débese informar ao titular de devanditos datos da súa posible cesión a través dunha lenda incluída no documento, formulario ou ferramenta informática a través da cal se capturen os datos (os interesados aos que se soliciten datos persoais deberán ser informados da existencia dun ficheiro, do tratamento dos seus datos, da finalidade da recollida destes, dos destinatarios da información, e da identidade e enderezo do responsable de tratar devanditos datos).

Non obstante, a efectos de auditoría, o indicado anteriormente esixirase de forma expresa a aquelas organizacións que manexen datos de carácter medio e/ou alto, é dicir, a aquelas organizacións que como parte da súa actividade

xestionan datos (por exemplo: Administración Pública, Sector Bancario e de Seguros, Sector de Mercadotecnia, etc.) e aquelas outras que polo desenvolvemento da súa actividade teñen acceso a datos considerados de especial protección (por exemplo: Sector Sanitario, Despachos de Avogados, etc.).

O Marco normativo de aplicación xira entorno a:

- Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal (B.O.E. núm. 298, de 14 de decembro).
- Real Decreto 994/1999, de 11 de xuño, polo que se aproba o Regulamento de medidas de seguridade dos ficheiros que conteñan datos de carácter persoal (B.O.E. núm. 151, de 25 de xuño) (subsistente en virtude da Disposición Transitoria Terceira da Lei Orgánica 15/1999).
- Real Decreto 428/1993, de 26 de marzo, polo que se aproba o Estatuto da Agencia Española de Protección de Datos (modificado polo Real Decreto 156/1996, de 2 de febreiro)
- Real Decreto 1332/1994, de 20 de xuño, polo que se desenvolven determinados aspectos da Lei de Protección de Datos (B.O.E. núm. 147, de 21 de xuño) (subsistente en virtude da Disposición Transitoria Terceira da Lei Orgánica 15/1999).

Ademais existe unha variada lexislación complementaria á mencionada. A día de hoxe sinalar que está en trámite o novo Regulamento da LOPD.