

## **La aplicación de las tecnologías de la información y la comunicación por los gobiernos y las administraciones locales: exigencias legales y requerimientos de gestión. Especial referencia a los temas de procedimiento administrativo electrónico, protección de datos de carácter personal y gestión de propiedades y bienes inmateriales**

1. Introducción.
2. El paradigma del *informacionalismo* y sus consecuencias en la configuración jurídica y organizacional de las administraciones públicas.
  - 2.1. El paradigma del *informacionalismo*. 2.2. Consecuencias jurídicas y configuración de las administraciones públicas. 2.3. Exigencias legales y requerimientos de gestión. 2.3.1. Normativa reguladora. 2.3.1.1. Sobre telecomunicaciones y sociedad de la información. 2.3.1.2. Sobre procedimiento administrativo. 2.3.1.3. Sobre protección de datos de carácter personal. 2.3.1.4. Sobre otras materias conexas. 2.3.1.5. Directivas comunitarias. 2.3.2. Requerimientos legales y de gestión. Especial referencia al ámbito local.
3. El procedimiento administrativo electrónico.
  - 3.1. Consideraciones preliminares. 3.2. El documento electrónico. 3.3. El registro telemático. 3.3.1. Requisitos de los registros telemáticos. 3.3.2. Utilización de modelos normalizados de solicitudes. 3.3.3. El recibo telemático. 3.3.4. Eficacia temporal de la presentación telemática. 3.4. El circuito administrativo electrónica (*workflow*). 3.5. La firma electrónica. 3.6. La notificación electrónica. 3.7. El archivo y conservación de los documentos electrónicos. 3.8. Valoración de la situación en el ámbito de las administraciones locales.
4. La protección de datos de carácter personal y las administraciones locales.
  - 4.1. Evolución normativa y jurisprudencial. 4.2. El sistema de protección de datos de carácter personal. 4.2.1. Conceptos básicos. 4.2.2. Principios generales. 4.3. Ficheros y competencias locales. 4.3.1. Ficheros públicos locales. 4.3.2. Competencias locales. 4.4. Protección de datos de carácter personal y políticas públicas locales. 4.4.1. Observancia de las obligaciones formales establecidas. 4.4.2. Cumplimiento de las medidas de seguridad. 4.4.3. Cesión y comunicación de datos en el ámbito de las administraciones públicas
5. Condicionantes a la gestión pública local desde el ámbito de la normativa de las propiedades y los bienes inmateriales.
  - 5.1. Consideraciones preliminares. 5.2. Derechos inmateriales de autoría intelectual. 5.2.1. El uso imperativo de los instrumentos contractuales. 5.2.2. Limitaciones en las facultades de la propiedad de los soportes de las obras. 5.2.3. Los niveles de protección de las BD. 5.3. Derechos inmateriales de propiedad industrial. 5.4. Derecho de acceso a la información pública. 5.4.1. Condicionamientos generales. 5.4.2. Condicionamientos específicos sectoriales en el nivel local: tensión entre las exigencias de los derechos de autor y los de acceso a la documentación en la gestión de los contenidos y de los flujos informativos en las administraciones públicas.
6. Reflexiones finales.
7. Bibliografía.

José Luis Martínez-Alonso Camps  
(coordinador)

*Profesor asociado de la Universidad de Barcelona  
(Departamento de Derecho Constitucional y  
Ciencia Política)  
y letrado de la Diputación de Barcelona*

Joan Guasch Marimon  
*Letrado de la Diputación de Barcelona*

Albert Ortiz Villuendas  
*Licenciado en Ciencias Políticas y  
de la Administración y técnico superior de  
la Diputación de Barcelona*

## Abreviaturas

AGE: Administración General del Estado.  
 AEPD: Agencia Española de Protección de Datos.  
 BD: Bases de datos.  
 BOE: Boletín Oficial del Estado.  
 BOP: Boletín Oficial de la Provincia.  
 CE: Constitución española de 27 de diciembre de 1978.  
 CEAL: Carta Europea de la Autonomía Local, ratificada por España el 20 de enero de 1988 y publicada en el BOE 47, del 24 de febrero de 1989.  
 DLM: Données Lisibles par Machine (Datos legibles por ordenador).  
 DOGC: Diario Oficial de la Generalidad de Cataluña.  
 EAC: Estatuto de autonomía de Cataluña, aprobado por la Ley orgánica 4/1979, de 18 de diciembre.  
 EDPP: Entidades de derecho público sometidas al derecho privado.  
 EPE: Entidades públicas empresariales.  
 FJ: Fundamento jurídico.  
 IDESCAT: Instituto de Estadística de Cataluña.  
 INE: Instituto Nacional de Estadística (estatal).  
 JCA: Jurisdicción Contenciosa Administrativa.  
 JCCA: Junta Consultiva de Contratación Administrativa.  
 Ley 30/1984: de 2 de agosto, de medidas para la reforma de la función pública (estatal).  
 Ley 7/1985: de 2 de abril, reguladora de las bases del régimen local (estatal).  
 LRHL: Ley 39/1988: de 28 de diciembre, reguladora de las haciendas locales (estatal).  
 Ley 13/1989: de 14 de diciembre, de organización, funcionamiento y régimen jurídico de la Administración de la Generalidad de Cataluña.  
 Ley 30/1992: de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común (estatal).  
 LOFAGE: Ley 6/1997: de 14 de abril, de organización y funcionamiento de la Administración General del Estado (estatal).  
 LOPD: Ley 15/1999: Ley de protección de datos de carácter personal (estatal orgánica).  
 LORTAD: Ley 5/1992: Ley de regulación del tratamiento automatizado de los datos de carácter personal (estatal orgánica).  
 LJCA/1998: de 13 de julio, reguladora de la jurisdicción contenciosa administrativa (estatal) (núm. 29).  
 Ley 4/1999: de 13 de enero, de modificación de la Ley 30/1992 (estatal).  
 Ley 11/1999: de 21 de abril, de modificación de la Ley 7/1985 (estatal).  
 LOU/2001: de 21 de diciembre, de universidades (estatal orgánica) (núm. 6).  
 LM: Ley 17/2001, de 7 de diciembre, de marcas (estatal).  
 MAP: Ministerio de Administraciones Públicas.  
 NARA: U.S National Archives and Record Administration (archivos y administración nacionales de los expedientes).  
 PIL: Acrónimo de personificación/ones instrumental/es local/es.  
 PKI: Public Key Infrastructure (Infraestructura de clave pública).  
 PMH: Padrón municipal de habitantes.  
 RMS/1999: Reglamento estatal de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, aprobado por el Real decreto 994/1999, de 11 de junio.  
 ROF/1986: Reglamento de organización, funcionamiento y régimen jurídico de las entidades locales, aprobado por el Real decreto 2568/1986, de 28 de noviembre (estatal).  
 ROAS/1995: Reglamento de obras, actividades y servicios de los entes locales, aprobado por el Decreto 179/1995, de 13 de junio.  
 SAN: Sentencia de la Audiencia Nacional.  
 SI: Sociedad de la información.  
 SIAL: Sistema de Información de la Administración Local.  
 SMP: Acrónimo de sociedad/es mercantil/es pública/s.  
 TC: Tribunal Constitucional.  
 TIC: Tecnologías de la información y de la comunicación.  
 TR/1986: Texto refundido de las disposiciones legales vigentes en materia de régimen local, aprobado por el Real decreto legislativo 781/1986, de 18 de abril (estatal).  
 TRET/1995: Texto refundido de la Ley del Estatuto de los trabajadores, aprobado por el Real decreto legislativo /1995, de 24 de marzo (estatal).  
 TRLCAP/2000: Texto refundido de la Ley de contratos de las administraciones públicas, aprobado por el Real decreto legislativo 2/2000, de 16 de junio (estatal).  
 TRLCat/2003: Texto refundido de la Ley municipal y de régimen local de Cataluña, aprobado por el Real decreto legislativo 2/2003, de 28 de abril de 2003.  
 TRLPI: Texto refundido de la Ley de propiedad intelectual, aprobado por el Real decreto legislativo 1/1996, de 12 de abril de 1996 (estatal).  
 TU/1997: Texto único de los preceptos de determinados textos legales vigentes en Cataluña en materia de función pública, aprobado por el Decreto legislativo 1/1997, de 31 de octubre.  
 UE: Unión Europea.  
 URL: Localización de un fichero o directorio en internet que permite acceder a él.

## 1. Introducción

El subsistema local, conjunto de instituciones públicas agrupadas en torno a los municipios, se caracteriza por su multiplicidad y, con carácter general, por su atomización. Con todo, un número importante de indicios apunta que los gobiernos y las administraciones locales se han sumado decididamente al proceso de renovación tecnológica. Haciendo de la necesidad virtud, el uso de los sistemas de información puede permitir superar, de manera eficiente, las dificultades de tiempo y espacio inherentes a la fragmentación de ese subsistema local. Las posibilidades de estas tecnologías de la información y de la comunicación (TIC) son muchísimas y se proyectan internamente (mejora de la gestión) y externamente, y ello en un sentido doble: relación más fluida entre administraciones, cooperación en red, y entre la Administración y la ciudadanía.

Sobre la base de la configuración de este subsistema, el trabajo analiza las exigencias legales y los requerimientos de gestión con los que se encuentran los responsables de las administraciones y de los gobiernos locales a la hora de aplicar las TIC. Se trata, pues, de poner de manifiesto esta suerte de *variables independientes* que, obviamente, no deberían erigirse en escollos del proceso, pero que han de ser conocidas de antemano con vistas al diseño de las políticas públicas locales.

El trabajo consta de cinco partes. Se inicia con una visión general de la aplicación de las TIC y de sus consecuencias en la configuración jurídica y organizacional de las administraciones públicas y de las locales en particular (epígrafe 2). Siguen después los análisis pormenorizados del procedimiento administrativo electrónico (epígrafe 3), la protección de datos de carácter personal (epígrafe 4) y la gestión de propiedades y bienes inmateriales (epígrafe 5), y se cierra con unas reflexiones finales (epígrafe 6).

El antecedente del texto lo constituye la ponencia presentada en el *VI Congreso de la Asociación Española de Ciencia Política y de la Administración (AECPA)*, que se celebró en Barcelona, los días 18, 19 y 20 de septiembre de 2003. Dicho texto ha sido actualizado normativamente con motivo de la presente publicación.

Finalmente, hay que reseñar que éste es un trabajo conjunto, si bien la elaboración y redacción de los epígrafes 2 y 4 han correspondido a José Luis Martínez-Alonso, el 3 a Albert Ortiz y los 5 y 6 a Joan Guasch.

## 2. El paradigma del informacionalismo y sus consecuencias en la configuración jurídica y organizacional de las administraciones públicas

### 2.1. El paradigma del informacionalismo

Como punto de partida de nuestras reflexiones estimamos conveniente hacer una referencia a lo que se ha

venido en llamar el *informacionalismo* (Castells, 1997: 39-40). Con palabras recientes de este autor, se trata de un "nuevo paradigma tecnológico que actualmente está sustituyendo al industrialismo como matriz dominante de las sociedades del siglo XXI (y que) está constituido en torno a la importancia estratégica de las tecnologías de la información y la comunicación" (Castells, 2003: 10).

Conceptuarlo como *paradigma tecnoeconómico* supone caracterizarlo como un grupo de innovaciones técnicas, organizativas y gerenciales interrelacionadas que por su trascendencia constituyen una revolución o un proceso de cambio científicos (Castells, 1997: 87; Kuhn, 1977).

Las características principales del *paradigma del informacionalismo* son, en síntesis, las siguientes (Castells, 1997: 87-92; Castells, 2003: 10-14):

1.ª. Su materia prima la constituyen *tecnologías para actuar sobre la información*, no sólo información para actuar sobre la tecnología, como era el caso en las revoluciones tecnológicas previas.

2.ª. El nuevo paradigma tiene una *creciente y automultiplicada capacidad de procesamiento, tanto desde el punto de vista de volumen, como de complejidad y de velocidad*.

3.ª. La *lógica de la interconexión* preside todo el sistema o conjunto de relaciones que utilizan estas nuevas tecnologías de la información y de la comunicación (TIC).

4.ª. El *paradigma del informacionalismo se basa en la flexibilidad*, de suerte que su *capacidad de recombinación o reconfiguración* supone la *reversibilidad de los procesos* y la *posibilidad de modificación de las organizaciones y la reordenación de sus componentes*.

5.ª. El nuevo paradigma se apoya en la *convergencia creciente de tecnologías específicas en un sistema altamente integrado*, dentro del cual las antiguas trayectorias tecnológicas separadas (microelectrónica, telecomunicaciones, optoelectrónica e informática/ordenadores) se vuelven prácticamente indistinguibles.

La evolución del sistema se prevé que tienda a la complejidad y a la diversidad, que sus reglas sean creadas y cambiadas en un proceso constante que fluye, y cuyo resultado es una *red multifacética*.

### 2.2. Consecuencias jurídicas y configuración de las administraciones públicas

De las consecuencias que derivan del impacto de este nuevo paradigma interesa analizar inicialmente las que tienen una dimensión jurídica. En este sentido, las TIC tienen, en primer lugar, una incidencia tanto en el ámbito del Derecho privado (relaciones entre particulares y transacciones de todo tipo), como en el del Derecho

público (relaciones entre administraciones públicas y ciudadanos o personas jurídicas, entre las propias administraciones públicas y entre éstas y los operadores tecnológicos, por distinguir las categorías más significativas).

Sin negar la virtualidad de la distinción entre los ámbitos privado y público, en ocasiones se borran las fronteras. Tal es el caso de lo que podríamos calificar como *derecho de la ciudadanía* (con previsiones normativas sobre intimidad, privacidad, libertades de expresión y de comunicaciones, entre otras), cuya regulación contiene tanto normas de Derecho público como privado, y cuyo tronco común deriva de su configuración garantista, adecuada a los derechos que lo integran. En cualquier caso, como primera conclusión podemos sentar la de la *incidencia progresiva en todos los ámbitos jurídicos del paradigma del informacionalismo*.

En segundo lugar, el *informacionalismo* deja sentir sus efectos en lo que atañe a la propia configuración del Derecho, y más concretamente a dos de sus principios más estructurales. El primero de ellos, el de seguridad jurídica, se ve afectado en dos de sus máximas:

1.ª. La estabilidad de la legislación, como consecuencia de que es objeto de modificaciones continuas (el fenómeno de la llamada *“legislación motorizada”*).

2.ª. El conocimiento y la comprensión de las normas, en la medida en que su volumen aumenta de manera incesante (multiplicidad de poderes normativos) y que una parte importante de las nuevas normas presenta una alta complejidad técnico-jurídica, lo que hace difícil su inteligencia y, por tanto, su cumplimiento. Tal es el caso de la normativa vinculada a las TIC, y cuya causa obedece a la dificultad de regular la *configuración virtual* de sus contenidos (la información como flujo y la comunicación como proceso).

El segundo de los principios, el de integridad del ordenamiento jurídico, se resiente de las limitaciones de las categorías jurídicas al uso y la necesidad constante de nuevas regulaciones. Así, por ejemplo, la Ley general de telecomunicaciones de 1998 produjo el *descarte* de la concesión como título habilitante para la prestación de servicios de telecomunicaciones (aunque se mantuviera, excepcionalmente, en el de televisión), y su sustitución por una pluralidad heterogénea de licencias y autorizaciones para los de última generación (licencias tipos A1, A2, B1... C2, en telefonía, y autorizaciones provisionales, en otros servicios de telecomunicación). La nueva Ley general de telecomunicaciones, la 32/2003, que deroga la 11/1998, se pronuncia en los términos siguientes: “Se avanza en la liberalización de la prestación de servicios y la instalación y explotación de redes de comunicaciones electrónicas. En este sentido, cumpliendo con el principio de intervención mínima se entiende que la habilitación para dicha prestación y explotación a terceros viene concedida con carácter general e inmediato por la ley. Únicamente será requisito previo la notificación a la

Comisión del Mercado de las Telecomunicaciones para iniciar la prestación del servicio. Desaparecen, pues, las figuras de las autorizaciones y licencias previstas en la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, como títulos habilitantes individualizados de que era titular cada operador para la prestación de cada red o servicio” (Exposición de motivos, II, párrafo sexto).

Como segunda conclusión, pues, constatamos la *crisis de las categorías jurídicas tradicionales y la necesidad de nuevos instrumentos adecuados a las realidades faltas de regulación*.

Un tercer grupo de consecuencias con dimensión jurídica, derivadas también del impacto de las TIC, podemos considerarlo bajo la perspectiva de la función normativa en el marco de un Estado social y democrático de derecho, y más concretamente en relación con:

a) El componente garantista, apreciable significativamente en la regulación de los derechos fundamentales de la ciudadanía [intimidad, honor, imagen, producción y creación literaria, artística, científica y técnica, *ex* artículos 18 y 20 de la Constitución española (CE)], y cuya función es, cabalmente, protegerlos frente a las acciones de terceros que, de una manera efectiva o potencial, puedan perturbarlos.

b) El componente participativo que, como mandato dirigido a los poderes públicos, y en aplicación del modelo de Estado social y democrático (*ex* artículo 9.2 de la CE), promueve las condiciones y desarrolla políticas públicas para que la comunicación y participación ciudadanas sean reales y efectivas.

c) Finalmente, el componente derivado de los requerimientos exigidos a los poderes públicos por los principios de eficacia y eficiencia (*ex* artículos 103 y 31.2 de la CE, respectivamente), que tiende también a estimular la cooperación y colaboración (entre administraciones públicas, principalmente) y a reducir actuaciones que generen costes (para los poderes públicos o para la ciudadanía).

Del contraste entre los diferentes componentes de este tercer grupo de consecuencias, y como tercera conclusión, podemos apuntar una cierta paradoja que se pone de manifiesto al advertir los *efectos diferentes de las TIC*, en ocasiones contrapuestos, *en los ámbitos señalados: unos en sentido proactivo (participación y eficacia y eficiencia), y otros en sentido restrictivo (garantía de derechos fundamentales)*.

Una vez reseñadas, de manera sintética, las consecuencias jurídicas derivadas del paradigma del *informacionalismo*, estamos en condiciones de abordar el análisis de los efectos que se perciben en relación con la configuración de las administraciones públicas.

Con carácter meramente descriptivo, podemos señalar los siguientes hitos o características:

a) La Administración General del Estado (AGE) ha desarrollado considerables esfuerzos encaminados, básica-

mente, en dos direcciones: responder a los retos del paradigma del *informacionalismo* y asumir un papel de liderazgo en el conjunto de las administraciones públicas españolas.

A estos objetivos obedecen, por citar las más recientes, las iniciativas de:

–La comisión de expertos que, presidida por Juan Soto, elaboró –por encargo del Ministerio de Ciencia y Tecnología– el informe “Aprovechar la oportunidad de la sociedad de la información en España” (presentado el 1 de abril de 2003).<sup>1</sup>

–El denominado *Plan de choque*, elaborado por los ministerios de Ciencia y Tecnología y de Administraciones Públicas (presentado el 8 de mayo de 2003).<sup>2</sup>

–El plan de actuación denominado *España.es*, aprobado por el Consejo de Ministros en fecha 11 de julio de 2003, que aborda diversas actuaciones y que, a los efectos que nos interesan, centra la relativa a la *administración.es* en los objetivos de:<sup>3</sup>

“–Facilitar el acceso público a los usuarios (DNI electrónico, puntos de acceso a internet gratuitos en las oficinas de registro y atención al público).

–Impulsar el desarrollo de servicios para los usuarios (servicios públicos básicos establecidos por la UNE, cartas de servicios electrónicas, perfeccionamiento del Portal del Ciudadano, uso de lenguas cooficiales e internaciones de las páginas web de la Administración, accesibilidad a las personas con discapacidad, formularios, registros y notificaciones telemáticas, pagos vía internet).

–Facilitar el intercambio de información entre las administraciones públicas (intercambio de certificados telemáticos y transmisiones de datos, Portal de servicios para las entidades locales, integración de las nuevas tecnologías en la comunicación interna de la Administración).

–Apoyar la reorganización interna de las administraciones públicas (impulso al Portal del Empleado Público, reforma del Consejo Superior de Informática, coordinación de las administraciones territoriales, revisión de los procedimientos administrativos para su prestación por vía telemática, apoyo técnico a los distintos ministerios, archivo de documentación electrónica).”

Y este mismo documento acaba señalando en el apartado *administración.es*:

“El Ministerio de Administraciones Públicas liderará el esfuerzo a través del Consejo Superior de Informática y Administración Electrónica (CSIAE) y una conferencia sectorial como órgano de cooperación con las comuni-

dades autónomas y corporaciones locales. El Ministerio de Ciencia y Tecnología, a través de la Entidad Pública Empresarial Red.es, desarrollará servicios comunes y ofrecerá el apoyo técnico necesario para la implantación.”

b) De las administraciones autonómicas puede decirse que han oscilado entre dos polos de actuación: del papel de una cierta subordinación a la Administración General del Estado (AGE) a los intentos de diseñar iniciativas y aplicar políticas de las TIC propias. La heterogeneidad de las diecisiete administraciones autonómicas hace difícil un juicio global, como arriesgadas las consideraciones parciales.

Para intentar progresar en el análisis de las políticas de las TIC de las administraciones autonómicas contamos con el *Informe sobre recursos informáticos de las administraciones públicas (IRIA)*,<sup>4</sup> que tiene como ámbito las administraciones local y autonómica y se actualiza bienalmente en el marco de la *Comisión Nacional para la Cooperación entre las Administraciones Públicas en Sistemas y Tecnologías de la Información (COAXI)*, en base al sistema de información constituido. El sistema de información IRIA, pues, contiene referencias a las administraciones autonómicas y al considerar indicadores objetivos (evolución de los gastos informáticos y referencia al porcentaje presupuestario que suponen, entre otros), permite una aproximación más documentada. Algunos datos que resaltan son:

En diez años (1991-2001), el incremento porcentual presupuestario ha sido del 293% (de 160 a 470 millones de euros); de 1997 a 2001, del 200% (de 235 a 470 millones de euros), y de 1999 a 2001, del 139% (de 338 a 470 millones de euros).

Entre las administraciones autonómicas que en 2001 más presupuesto destinan a gastos informáticos se sitúan:

- 1) País Vasco (2,54% del presupuesto total, 72.763 miles de euros);
- 2) Región de Murcia (1,91%, 16.515 miles de euros);
- 3) Comunidad Valenciana (1,39%, 62.924 miles de euros);
- 4) Comunidad de Madrid (1,25%, 48.311 miles de euros);
- 5) Andalucía (1,21%, 103.837 miles de euros);
- [...]
- 8) Cataluña (0,92%, 67.464 miles de euros).<sup>5</sup>

Sin perjuicio de la remisión a los indicadores de los sucesivos informes *IRIA*, no hay que olvidar algunas iniciativas singulares, de entre las cuales destacaremos dos:

1. Se puede descargar en la siguiente URL: [www.cdsi.es/documentos/presentacion\\_informe\\_final\\_cdsi.pdf](http://www.cdsi.es/documentos/presentacion_informe_final_cdsi.pdf) (23.7.2003).

2. Disponible en la siguiente URL: [www.igsap.map.es/ticker/docs/plan\\_choque.pdf](http://www.igsap.map.es/ticker/docs/plan_choque.pdf) (23.7.2003).

3. Se puede consultar la nota de prensa en [www.mcyt.es/asp/ministerio\\_infoma/prensa/np11-07-03.htm](http://www.mcyt.es/asp/ministerio_infoma/prensa/np11-07-03.htm) (23.7.2003).

4. Se puede consultar la referencia en [www.csi.map.es/csi/pg5i30.htm](http://www.csi.map.es/csi/pg5i30.htm) (23.7.2003).

5. El resto se puede consultar en la referencia anterior.

En primer lugar, la de la Junta de Extremadura, que ha impulsado la utilización del *software* libre (Linux-Linux) en todos los colegios de esa comunidad; iniciativa que mereció el elogio, en noviembre de 2002, de *The Washington Post* (*El País*, 1 de mayo de 2003, Ciberp@is, 5).

En segundo lugar, la de Cataluña, que tiene como valor añadido que no se trata de una actuación exclusiva de la Administración autonómica, sino de una pluralidad de actores. Sus aspectos más relevantes son los siguientes:

–El inicio tiene lugar merced a un acuerdo institucional entre la Administración autonómica y Localret (consorcio que agrupa la casi totalidad de los municipios de Cataluña y cuyo objeto es el desarrollo de las redes de telecomunicaciones y de las nuevas tecnologías),<sup>6</sup> acuerdo que recibe el aval del Parlament (18 de noviembre de 1998).

–A partir de este consenso inicial se desarrollará un proceso complejo (intervención de 250 expertos, elaboración de 38 iniciativas que darán lugar a 155 acciones, enmarcadas en 7 ámbitos de actuación), que culminará con la elaboración del *Pla Estratègic, Catalunya en Xarxa*,<sup>7</sup> el cual pivota a partir del consenso institucional y se implementa mediante la *xarxa* (red) de colaboraciones entre actores públicos y privados.

–Quizá la concreción más emblemática del plan sea la denominada *CAT365*, portal y plataforma tecnológica de servicios que aspira a integrar y distribuir los servicios de las administraciones públicas catalanas.<sup>8</sup> Como se ha señalado, “esta herramienta ha de permitir, de un lado, simplificar los procesos que ha de seguir un ciudadano (también una empresa o una organización) para obtener los servicios de la Administración; por otro lado, ha de facilitar el intercambio de información entre las diferentes administraciones, necesario para hacer posible la simplificación de los procesos de cara al ciudadano” (Sanromà, director de CAT365, 2002).<sup>9</sup>

c) El elevado número de administraciones locales, su diversidad y heterogeneidad impiden fijar unas conclusiones precisas sobre el grado de aplicación de las TIC.

A lo sumo podemos hablar de tendencias, y siempre ponderando el riesgo de que éstas no se produzcan de manera uniforme.

De la consulta del *Informe sobre recursos informáticos de las administraciones públicas*, del IRIA ya citado, podemos destacar los siguientes datos:

En diez años (1991-2001), el incremento presupuestario en términos porcentuales ha sido del 224% (de 162 a 363 millones de euros); de 1997 a 2001, del 163% (de 267 a 363 millones de euros); y de 1999 a 2001, del 123% (de 294 a 363 millones de euros).<sup>10</sup>

La relación entre presupuestos y población de los municipios nos proporciona una ratio (euros/habitante) que, agrupando los municipios por tramos, nos permite apuntar las siguientes consideraciones:<sup>11</sup>

–En las ciudades de más de 100.000 habitantes (56 municipios, que suponen el 0,7% del total), la razón oscila de los 8,36 a los 9,40 euros/habitante.

–En el tramo de municipios comprendido entre los 10.001 y los 100.000 habitantes (595, el 7,34%), la ratio va de los 5,33 a los 6,61 euros/habitante.

–En el tramo comprendido entre los 1.001 y los 10.000 habitantes (2.513, el 30,99%), la razón se sitúa en los 3,66 euros/habitante.

–De los municipios cuya población no supera los 1.000 habitantes (4.944, el 60,98%), sólo disponemos de datos de los comprendidos entre los 501 y los 1.000 habitantes, para los cuales la ratio alcanza los 4,15 euros/habitante.

Junto a los datos reseñados creemos relevante analizar los aspectos siguientes:

–Las iniciativas de los ayuntamientos de mayores dimensiones con vistas a la mejora de sus servicios por internet. En un estudio reciente, *Radiografía de las webs municipales* (Ciberp@aís, 26 de junio de 2003), se analizan las de todas las capitales de provincia, Ceuta, Melilla y todas las ciudades de más de 75.000 habitantes (un total de 78 webs), y, entre otras, se ponen de manifiesto, en relación con el estudio de esta misma publicación realizado en el 2002, las conclusiones siguientes:

6. Las referencias sobre este consorcio pueden consultarse en [www.localret.es](http://www.localret.es).

7. Se puede descargar en [http://dursi.gencat.net/ca/de/pla\\_estrategic.htm](http://dursi.gencat.net/ca/de/pla_estrategic.htm).

8. <http://www.cat365.net>.

9. A diferencia de la definición material del portal CAT365, que se muestra relativamente sencilla y comprensible, la configuración jurídica y organizativa es ciertamente compleja. Ese portal es gestionado por una empresa pública (*Serveis Públics Electrònics, SA*), que es uno de los dos agentes operativos de la *Administració Oberta de Catalunya* (AOC), consorcio constituido por la Generalidad de Cataluña y Localret (como se recordará, consorcio que agrupa a la mayoría de los ayuntamientos de Cataluña). El otro agente operativo de la AOC lo constituye la *Agència Catalana de Certificació* (CATCert), que adopta la modalidad de organismo autónomo de carácter comercial. Y a éstas hay que añadir nuevas entidades constituidas bajo la forma de fundaciones privadas (como, por ejemplo, la OBSI– *Observatori per a la Societat de la Informació*–, integrada por la Generalitat, Localret y la UOC –*Universitat*

*Oberta de Catalunya*–). En fin, una muestra más de la capacidad de *partenogénesis* de las administraciones catalanas, fenómeno éste del cual ya nos hemos ocupado (MARTÍNEZ-ALONSO, J. L. e YSA, T., 2003).

Los estatutos de la AOC fueron publicados en el *Diari Oficial de la Generalitat de Catalunya* –DOGC 3064, del 27.3.2002 (páginas 5384-6)–, y los de CATCert en el DOGC 3895, del 30.5.2003 (páginas 11207-8); el acuerdo para constituir *Serveis Públics Electrònics, SA* lo fue en el DOGC 3469, del 7.9.2001 (página 13682), con corrección de errores en el n.º 3475, del 18.9.2001 (página 14097). La referencia al OBSI se puede consultar en [http://dursi.gencat.net/generados/catala/societat\\_informacio/noticia/1020\\_12\\_13620.html](http://dursi.gencat.net/generados/catala/societat_informacio/noticia/1020_12_13620.html).

10. Los incrementos porcentuales son significativos, aunque menores que los de las administraciones autonómicas, especificados anteriormente.

11. Las fuentes que utilizamos para la interrelación son:

<http://www.csi.map.es/csi/pg5i3039.htm> (22.7.2003).

[http://www.dgal.map.es/cgi-bin/webapb/webdriver?Mlval=REEL\\_mun\\_tramo\\_1](http://www.dgal.map.es/cgi-bin/webapb/webdriver?Mlval=REEL_mun_tramo_1) (22.7.2003).

–Ha aumentado el número de ayuntamientos con web oficial, y, en un porcentaje significativo (casi el 50%), han perfeccionado el diseño.

–Se han mejorado e incrementado los servicios que se ofrecen y que, con variaciones de unos u otros municipios, cubre ya un catálogo que incluye: trámites en red, descarga de impresos, pagos en red, callejero, transporte urbano, información sobre sesiones plenarios, buscador, mapa de web, enlaces y buzón ciudadano.<sup>12</sup>

Hay que prestar atención también a la situación de los municipios pequeños y medianos, entendiendo por tales:

–Como pequeños, los de población no superior a 5.000 habitantes (6.948, el 85,7% del total);

–Como medianos, los que tienen entre 5.001 y 20.000 habitantes (841, el 10,37%).<sup>13</sup>

De acuerdo con el estudio ya citado de Ciberp@aís, sólo el 25% de municipios españoles tiene página web. Si tomamos los datos que ofrece dicho estudio por provincias, y los relacionamos con las comunidades autónomas que tienen mayor número de municipios (juntas suman 6.514 municipios, el 76% del total),<sup>14</sup> podemos fijar las tendencias siguientes:

–La extensión es reducida en Aragón (730 municipios, el 9% del total), donde las tres provincias tienen un porcentaje de municipios con web que no llega al 8% (Huesca del 2,4%, Teruel del 2,5% y Zaragoza del 7,5%).

–Similar es el caso de Castilla y León (2.248 municipios, el 27,33% del total), donde la mayoría de las provincias tienen un porcentaje de municipios con web inferior al 9%, salvo Ávila (16,1%) y Palencia (31,34%).

–Bastante parecido es el de Castilla-La Mancha (919 municipios, el 11,33%), donde el porcentaje de webs municipales es inferior al 11%, salvo el caso ejemplar de Albacete (todos los municipios tienen página).

–Desigual es Cataluña (946 municipios, el 11,66%), donde los municipios de Barcelona y Tarragona (con unos porcentajes de webs municipales del 90% y 84,7%, respectivamente) contrastan con los de Girona y Lleida (10,5% y 10,8%).

–Gradual es el caso de Andalucía (770 municipios, el 9,49%), donde en el punto bajo se sitúan los municipios de Jaén (sólo el 6,2% de los municipios con web), y los de Granada, Huelva y Málaga (en torno al 10-13%), para alcanzar valores superiores en Cádiz (el 38,6%) y Almería (el 82,3%), y la totalidad de páginas municipales, en Sevilla y Córdoba.

12. Sobre la base de la valoración de estos diez servicios y del *Test de Accesibilidad Web* (TAW), el estudio establece una clasificación final cuyos tres primeros puestos ocupan Madrid, Zaragoza y Sabadell, y los últimos del estudio (76, 77 y 78), respectivamente, Toledo, Segovia y Castellón.

13. El resto de los municipios supone ya un porcentaje reducido (el 3,93%) donde cabe suponer que los del tramo 20.001-50.000 habitantes (201, el 2,48%) se irán incorporando, si no lo han hecho ya, a las tendencias de los de grandes dimensiones.

–Finalmente, progresivo también es el caso de la Comunidad Valenciana (541 municipios, el 6,67% del total): Valencia (el 18,1% con web), Alicante (el 32,6%) y Castellón (el 97,7%).

Para el resto de las comunidades autónomas las tendencias son las siguientes:

–En las uniprovinciales (que juntas suman 917 municipios, el 11,31% del total), la ordenación es la siguiente: Islas Baleares (el 86,5% de los 67 municipios tiene web); Murcia (el 53,3% de los 45 municipios); Asturias (el 41% de los 78 municipios); Cantabria (el 22,5% de los 102 municipios); Madrid (el 20,1% de los 179 municipios); La Rioja (el 20,1% de los 174 municipios), y Navarra (el 17,6% de los 272 municipios).

–En el País Vasco (250 municipios, el 3,08% del total): Guipúzcoa (el 100% con web municipal), Álava (el 60%) y Vizcaya (el 58,5%); en Galicia (315 municipios, el 3,88%): A Coruña (el 100% con web municipal), Pontevedra (el 32,2%), Lugo (el 13,4%) y Ourense (el 10,5%); en Canarias: Las Palmas (el 79,4% de los 34 municipios tienen web) y Tenerife (el 32% de los 53 municipios); y, finalmente, en Extremadura: Badajoz (el 19% de los 163 municipios cuentan con web) y Cáceres (el 6,4% de los 219 municipios).

Dado el elevado número de municipios pequeños y medianos (como ya hemos visto, agrupan a 7.789, el 96% del total) es evidente que ése es el ámbito más necesitado de intervención. Y es por ello que en dicho ámbito es capital la función de las administraciones cooperadoras: diputaciones en las provincias, *consells insulars* y cabildos en los archipiélagos balear y canario, comunidades autónomas uniprovinciales y comarcas donde han sido instituidas como tales (Cataluña y, recientemente, Aragón).

Por hablar del caso que mejor conocemos, la Diputación de Barcelona ha contribuido decisivamente a la extensión de las TIC en los municipios de la provincia.<sup>15</sup> Y ello mediante la combinación de acciones e instrumentos: conexión de todos los ayuntamientos con la Diputación punto a punto con RDSI (Red Digital de Servicios Integrados); servicio de *hosting* gratuito para webs municipales; confección de un buen número de páginas web y gestión informatizada de servicios municipales, tales como: el padrón de habitantes (Martínez-Alonso, 1998b), la contabilidad o la gestión de tributos y recaudación (que alcanza a 282 municipios, el 91% de la provincia, y que incluye la firma digital y el pago electrónico), entre los más significativos.<sup>16</sup>

14. Los datos sobre el número de municipios se pueden extraer del propio estudio Ciberp@aís (por provincias) y de [http://www.dgal.map.es/cgi-bin/webapb/webdriver?Mlval=REEL\\_mun\\_tramo\\_1](http://www.dgal.map.es/cgi-bin/webapb/webdriver?Mlval=REEL_mun_tramo_1) (22.7.2003) (por comunidades autónomas).

15. Ese papel lo reconoce también el artículo de Ciberp@aís (28.6.2003, página 11).

16. La explicación sobre estos servicios y el resto de los ofrecidos se puede consultar en [www.diba.es](http://www.diba.es). También en Diputación de Barcelona (*Guía de serveis*: 2003).

### 2.3. Exigencias legales y requerimientos de gestión

Una vez hemos ofrecido e interrelacionado algunos datos con vistas a mostrar una panorámica general de la aplicación de las TIC por las administraciones públicas, es el momento de hacer una mención a la normativa que regula su actividad.

#### 2.3.1. Normativa reguladora<sup>17</sup>

##### 2.3.1.1. Sobre telecomunicaciones y sociedad de la información

–Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

–Real decreto ley 14/1999, de 17 de septiembre, sobre firma electrónica, vigente hasta el 19 de marzo de 2004, por derogación de la ley que se indica a continuación.

–Ley 59/2003, de 19 de diciembre, de firma electrónica, vigente a partir del 20 de marzo de 2004, y que deroga el Real decreto ley 14/1999.

–Ley 32/2003, de 3 de noviembre, general de telecomunicaciones, en vigor desde el 5 de noviembre de dicho año, y que derogó los siguientes textos: Ley 11/1998, de 24 de abril, general de telecomunicaciones; Ley 12/1997, de 14 de abril, de liberalización de las telecomunicaciones, y Ley 42/1995, de 22 de diciembre, de las telecomunicaciones por cable.

##### 2.3.1.2. Sobre procedimiento administrativo

–Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común.

–Real decreto 263/1996, de 16 de febrero, de regulación de la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

–Real decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones, la expedición de copias de documentos y devolución de los originales y el régimen de las oficinas de registro.

–Real decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

Normativa autonómica catalana:

–Ley 10/2001, de 13 de julio, de archivos y documentos.

–Decreto 324/2001, de 4 de diciembre, relativo a las relaciones entre los ciudadanos y la Administración de la Generalidad de Cataluña a través de internet.

##### 2.3.1.3. Sobre protección de datos de carácter personal

–Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

–Real decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

–Real decreto 1332/1994, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley orgánica 5/1992, de 29 de octubre.

–Real decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

–Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios (BOE 62, de 13 de marzo de 1996).

–Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación (BOE 25, de 29 de enero de 1998).

Normativa autonómica:

–Ley 8/2001, de 13 de julio, por la que se aprueban las Normas reguladoras de la protección de datos de carácter personal de la Comunidad de Madrid (BOE 245, de 12 de octubre de 2001).

–Ley 5/2002, de 19 de abril, de creación de la Agencia Catalana de Protección de Datos (BOE 115, de 14 de mayo de 2002).

–Decreto 48/2003, de 20 de febrero, por el cual se aprueba el Estatuto de la Agencia Catalana de Protección de Datos (ACPD).

–Resolución de 15 de diciembre de 2004, de la Presidencia de la ACPD, por la cual se aprueban los soportes normalizados para formalizar las inscripciones en el Registro de Protección de Datos de Cataluña (DOGC 4046, del 12 de enero de 2004).

##### 2.3.1.4. Sobre otras materias conexas

–Ley 17/2001, de 7 de diciembre, de marcas.

–Real decreto legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto refundido de la Ley de propiedad intelectual.

##### 2.3.1.5. Directivas comunitarias

–Directiva 2002/58/CE del Parlamento Europeo y del

Entre las últimas novedades destaca la de *elciutada.net*, un buscador de servicios públicos locales, autonómicos y estatales de interés para la ciudadanía de la provincia de Barcelona, con referencias por municipios y comarcas.

17. Se citan las principales disposiciones legales y reglamentarias, cuyos contenidos hay que entenderlos referidos a los vigentes en la actualidad.



Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

–Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información.

–Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

–Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre, por la que se establece un marco comunitario para la firma electrónica.

–Directiva 1995/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, 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.

### 2.3.2. Requerimientos legales y de gestión. Especial referencia al ámbito local

Con anterioridad ya señalamos la cierta paradoja que se produce al advertir los efectos diferentes de la regulación de las TIC, en ocasiones incluso contrapuestos. Así:

–De un lado, encontramos mandatos normativos en un sentido proactivo, que al perseguir como objetivos la eficacia (CE, artículo 103) o la eficiencia (CE, artículo 31.2), demandan un uso intensivo de las TIC. Tal sería el caso del artículo 45 de la Ley 30/1992 (“Incorporación de medios técnicos”), donde se señala que “las administraciones públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias [...]” (número 1 del citado artículo 45).

En esta misma línea, si consultamos la legislación local de carácter general podremos observar cómo se atribuyen a los municipios numerosas competencias, que al hacerlo se formula en clave de obligación, y con bastante frecuencia mediante el uso de verbos como garantizar, promover o asegurar, o sus sustantivos.<sup>18</sup> Se sigue de todo ello una exigencia a las autoridades y responsables locales para que optimicen los recursos disponibles, y para lo cual las posibilidades de las TIC son naturalmente inmensas.

–De otro lado, en cambio, la legislación sobre derechos fundamentales de la ciudadanía (intimidad, creación literaria, artística, científica y técnica, y el resto de los previstos en la Constitución), como le es propio, habilita y desarrolla una serie de mecanismos de garantía y protección que, enfrentados con la aplicación de las TIC, tenderán a reducir sus posibilidades. Y ahí tenemos la limitación sobre el uso de la informática en relación, entre otros, con la intimidad personal (*ex CE*, artículo 18.4).

El conflicto entre dos bienes o principios jurídicos se halla en la misma raíz del Derecho, y por tanto no nos debe extrañar esa tensión en relación con las TIC. El tema, pues, hay que centrarlo en los casos concretos, y sobre todo en las medidas o regulaciones específicas, y todo ello con vistas a intentar fijar los términos, si equilibrados o no, de dicha tensión.

Pondremos un ejemplo:

–El envío a un grupo de ciudadanos de una carta personalizada, remitida por el concejal de Cultura, con el anuncio del debate que centrará su objeto en los problemas de la inmigración en el municipio y de las acciones a emprender, y que tendrá lugar en la biblioteca municipal.

–Un vecino puede considerarlo del máximo interés y celebrar la iniciativa del ayuntamiento, como expresión de su interés por “facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social” (*ex CE*, artículo 9.2, *in fine*, uno de los contenidos de la cláusula del Estado social).

–Otro vecino puede interpretarlo como una intolerable agresión a su intimidad por el hecho de haberse servido de la lista de usuarios de la biblioteca para remitir la carta del concejal.

Otro supuesto en el que podremos percibir una cierta oposición entre alternativas lo encontramos en el desarrollo de las TIC aplicadas a las relaciones entre Administración y ciudadanía, y al papel de liderazgo que le corresponde a aquélla. Liderazgo que debemos considerar en todas sus facetas: desde la que se refiere a los recursos económicos empleados (y que, por tanto, no podrán dedicarse a otras necesidades), hasta la que se pregunta por la *relevancia* en términos de demanda social de algunas iniciativas de compleja implementación y acceso difícil (generando así una especie de *privilegios telemáticos* para los *elegidos*), y pasando por la

18. La Ley 7/1985, reguladora de las bases del régimen local, en sus artículos 25, 26 y 28 (sobre competencias municipales), es un buen ejemplo de lo dicho. En el mismo sentido, la legislación autonómica catalana, Texto refundido de la Ley municipal y de régimen local de Cataluña, aprobado por el Decreto legislativo 2/2003, de 28 de abril, artículos 66, 67 y 71.

Como manifestación específica hay que consignar la modificación introducida por la Ley 57/2003, de 16 de diciembre, en la Ley 7/1985, cuyo artículo 70.bis, sobre *participación ciudadana*, prevé en su apartado 3 lo siguiente: “Asimismo, las entidades locales y, especialmente, los municipios, deberán

impulsar la utilización interactiva de las tecnologías de la información y la comunicación para facilitar la participación y la comunicación con los vecinos, para la presentación de documentos y para la realización de trámites administrativos, de encuestas y, en su caso, de consultas ciudadanas.

Las Diputaciones provinciales, Cabildos y Consejos insulares colaborarán con los municipios que, por su insuficiente capacidad económica y de gestión, no puedan desarrollar en grado suficiente el deber establecido en este apartado.”

propia configuración de lo que han de ser los servicios públicos. Ejemplos que podemos vincular con estas cuestiones son los relativos al procedimiento administrativo electrónico, o las reticencias que ha levantado ante la Comisión del Mercado de las Telecomunicaciones (CMT), la propuesta de Localret de dar cobertura de acceso a internet de alta velocidad en determinados municipios catalanes con déficit de dicho acceso y con carácter gratuito.<sup>19</sup>

Un tercer ámbito donde suelen producirse controversias es el que se centra en la información (considerada en su sentido más amplio) de que disponen las administraciones públicas, y concretamente en relación con el acceso a la misma y su difusión a la ciudadanía. En este ámbito, al principio de libre acceso a archivos y registros y difusión de la información se contrapondrán derechos fundamentales, como la intimidad o el relativo a la creación artística o técnica. La previsión de la tensión o conflicto entre ambos grupos está ya en la Constitución [*ex* artículos 105.b) y 20.1.b)], en relación con el número 4 y con el artículo 53.1], de suerte que, nuevamente, se tratará de una cuestión de ponderación entre las medidas y garantías de unos y otros.

De unas u otras maneras, esta paradoja de la que venimos hablando no es infrecuente en el ámbito de las administraciones públicas del Estado social o de bienestar, atendidas tanto la extensión de sus tareas y estructuras como la fragmentación funcional y territorial de sus agentes (Baena, 1988: 32-35). De los supuestos en que concurren esos mandatos o prescripciones contrapuestas hemos elegido los tres que ya se perciben de las reflexiones que se acaban de hacer: procedimiento administrativo electrónico, privacidad o protección de datos de carácter personal, y gestión de propiedades y bienes inmateriales.

No obstante, antes de abordar el análisis pormenorizado de esos ámbitos, creemos necesario reseñar una serie de factores que caracterizan a los gobiernos y a las administraciones locales, y en razón de los cuales la problemática en dichos ámbitos adquiere unos perfiles singulares. Tales factores son los siguientes:

–Una atribución de capacidad y competencias generales a los municipios, lo que tiene como consecuencia

práctica que ningún sector quede fuera de su ámbito de responsabilidad.<sup>20</sup>

–El hecho de ser la instancia más próxima a la ciudadanía, unido a otros factores estructurales, configura unas administraciones municipales en las que se *palpa* la presión de la ciudadanía y se percibe el impacto que ello produce en la organización.<sup>21</sup> Se sigue de ello una mayor capacidad de la ciudadanía para incidir y conseguir que los gobiernos y las administraciones locales atiendan a sus demandas.

–Una *constelación* de organizaciones públicas locales, formada por entes obligatorios (municipios, provincias, e islas en los archipiélagos balear y canario) y voluntarios (mancomunidades, consorcios, etc.),<sup>22</sup> que se relacionan e interactúan continuamente, lo que en determinados supuestos (por ejemplo, en el apartado de cesión de datos personales entre administraciones) puede suponer problemas añadidos.

–Una planta municipal donde predominan las organizaciones de dimensiones reducidas, de lo que se derivan graves dificultades de gestión.<sup>23</sup>

–Una relativa presencia de grupos u organizaciones surgidas de la sociedad civil (asociaciones y fundaciones), cuyo número, en algunas comunidades, como es el caso de Cataluña, puede ser muy elevado, y que con frecuencia se vinculan con el ayuntamiento mediante relaciones heterogéneas (partenariado, voluntariado, prestación de servicios públicos, entre otras), y que incluyen a menudo el uso de medios y recursos municipales (locales, equipos informáticos, etcétera).

–Una dosis apreciable de *voluntarismo* en las actitudes de una parte importante de las autoridades locales, vinculada a la característica de no profesionalización de la mayoría de los electos, que tiene como consecuencia práctica el desarrollo de iniciativas proactivas con vistas a apurar el diseño y la aplicación de las políticas en el cuatrienio del mandato electoral.

–Finalmente, una limitación de los poderes locales que, como es sabido, tienen vedado el *acceso* directo a la ley, a diferencia de las administraciones central y autonómicas, las cuales disponen de más posibilidades de que se incluyan aquellas medidas que les resulten nece-

19. A juicio de la CMT, "la oferta gratuita del servicio de acceso a internet y del uso de la red pública a los usuarios en este caso sería, *a priori*, y sin perjuicio de lo manifestado en el punto 5.2.d) del presente informe, considerada como una actividad susceptible de producir distorsiones a la libre competencia en el servicio de acceso a internet y en la explotación de la red pública de telecomunicaciones y, por lo tanto, contraria a los principios informadores de la normativa en vigor reguladora del sector de las telecomunicaciones". (Conclusión cuarta de la Resolución aprobada el 5.6.2003 en relación con el expediente RO 2003/622). Se puede consultar en <http://www.cmt.es/cmt/decisiones/ultima.html>, búsqueda RO 2003/622.

20. La atribución de competencias a los municipios se estructura a partir de largas listas de sectores y materias en los que se les garantiza su actuación, y que se describen en los artículos 25.2 (competencias propias), 26 (ser-

vicios mínimos) y 28 (actividades complementarias) de la Ley 7/1985. Y para cerrar el círculo, en esta misma ley, el artículo 5 les reconoce plena capacidad y el 25.1 prevé que "el municipio, para la gestión de sus intereses y en el ámbito de sus competencias, puede promover toda clase de actividades y prestar cuantos servicios públicos contribuyan a satisfacer las necesidades y aspiraciones de la comunidad vecinal".

21. De este factor y de sus consecuencias nos hemos ocupado ya en un trabajo anterior (Martínez-Alonso, 1998: 344-345).

22. Sobre las *personificaciones instrumentales locales* nos remitimos a nuestro estudio (Martínez-Alonso, J. L. e Ysa, T., 2003).

23. Sobre la problemática de las organizaciones locales nos remitimos a nuestro trabajo (Martínez-Alonso, 1998: 339-342).

sarias para su gestión y que requieran de su previsión en una ley formal, ya sea con su inclusión en las leyes de acompañamiento de los presupuestos,<sup>24</sup> ya sea mediante su incorporación a leyes generales.<sup>25</sup>

### 3. El procedimiento administrativo electrónico

#### 3.1. Consideraciones preliminares

En el ámbito jurídico es muy conocida la Sentencia del Tribunal Supremo, de 3 de noviembre de 1997 (Aranzadi: RJ 1997/8251), en la cual se declara:

“[...] estamos asistiendo, en cierto modo, al ocaso de la civilización del papel, de la firma manuscrita y del monopolio de la escritura sobre la realidad documental. El documento, como objeto corporal que refleja una realidad fáctica con transcendencia jurídica, no puede identificarse ya en exclusiva con el papel como soporte, ni con la escritura como unidad de significación. El ordenador y los ficheros que en él se almacenan constituyen hoy día una nueva forma de entender la materialidad de los títulos valores y en especial de los documentos mercantiles.”

Si existe alguna organización que haya girado históricamente alrededor del papel, ésta es, sin ninguna duda, la Administración pública, a la que gráficamente le hemos asociado siempre la imagen del funcionario rodeado y cubierto de documentos, legajos, expedientes administrativos, etcétera.

Pero también el ámbito estrictamente administrativo se acerca a una realidad sin papel, de la mano de las nuevas tecnologías, las cuales han de permitir en un corto espacio de tiempo acercarnos al paradigma de la Administración electrónica; una administración que se podrá constituir en un nuevo modelo organizativo, en el que no tan sólo existirá un conjunto de información al alcance de los ciudadanos sino donde todas o gran parte de las gestiones administrativas se podrán llevar a cabo por medios electrónicos, informáticos o telemáticos. Pero el concepto de Administración electrónica no está relacionado únicamente con la necesidad de trabajar con equipamientos tecnológicamente avanzados, sino también, y sobre todo, a un profundo cambio cultural en cómo se ha de entender la Administración, tanto desde su funcionamiento interno como en las relaciones con los ciudadanos.

En el año 2000, el Gobierno Blair puso en funcionamiento el programa “UK on-line”, partiendo de la pre-

misas que el 53% de la población británica estimaba que el Gobierno no necesitaba más medios económicos para el ejercicio de su actividad, sino sencillamente una mayor eficacia. Entre los objetivos del programa se encuentran tanto el que en el año 2005 se puedan realizar el 100% de las gestiones con los ciudadanos por medios electrónicos como que la contratación pública se realice por este mismo canal en un 90% del total.

A este respecto, hay que señalar el importante impacto económico favorable que el programa “UK on-line” puede suponer para los presupuestos estatales: se estima que el coste administrativo de cada gestión realizada por un ciudadano de manera presencial es de unos 7 euros; si la misma gestión se hace por teléfono su coste baja hasta los 1,8 euros; pero si se gestiona por internet este coste baja todavía más, hasta situarse alrededor de los 0,9 euros, es decir, se produce un ahorro del 87% sobre el coste presencial. Y no sólo esto, ya que el beneficio no es tan sólo para la Administración, sino que, lógicamente, los propios ciudadanos percibirán directamente los beneficios en forma de ahorro de tiempo, facilidad de relación con la administración, mayor eficiencia en las actuaciones, etcétera.

Ahora bien, muchas organizaciones pretenden utilizar las tecnologías de la información como el único medio para resolver sus problemas más complejos, pero las TIC por sí solas no son la solución, ya que su incorporación de forma aislada puede crear más problemas de los que pretende resolver.

De igual modo que el paso de la agricultura a la industria supuso un cambio radical en las relaciones sociales, el paso de la era post-industrial a la del conocimiento esta suponiendo otro cambio en el mismo sentido, excepto por el hecho que este último no se puede percibir físicamente.

Se puede afirmar que actualmente la Administración tiene a su alcance un conjunto de instrumentos para reorientar su función de forma inigualable en la historia. A pesar de ello, los elementos que pueden complicar las acciones a implementar se encuentran más vinculados a los fundamentos organizativos que a los tecnológicos o materiales, ya que el cambio depende de la capacidad de cada uno de los organismos en la reorganización de sus actividades para que sea factible el uso de las nuevas tecnologías en las relaciones con los ciudadanos.

No se pueden contemplar las iniciativas de impulso de la sociedad de la información como un simple conjunto de cambios tecnológicos y de infraestructuras. La

24. En la denominación actual, leyes de medidas fiscales, administrativas y del orden social, cuyos proyectos son aprobados por los gobiernos respectivos.

25. Como ejemplo de este último supuesto podemos citar el de la L 33/2003, de 3 de noviembre, del patrimonio de las administraciones públicas, que en su disposición adicional décima regula el Régimen jurídico de la “Sociedad Estatal de Gestión Inmobiliaria de Patrimonio, Sociedad Anónima” (SEGIPSA), y

cuyo apartado 10 dispone lo siguiente: “Para la realización de los trabajos que se le encomienden de acuerdo con la presente disposición, SEGIPSA podrá recabar de la Dirección General del Catastro, en los términos previstos en el artículo 64 de esta Ley, la información de que disponga en relación con los bienes o derechos objeto de las actuaciones que se le hayan encomendado, sin que sea necesario el consentimiento de los afectados.”

sola automatización de procesos, sin un rediseño de éstos, provocará un efecto multiplicador de los defectos de las organizaciones.

Por lo tanto, para ofrecer servicios ligados a la gestión administrativa electrónica, se tiene que repensar la organización en el sentido de:

–Conocer qué hacemos y cómo.

–Rediseñar los procedimientos y las metodologías de trabajo internas.

–Implantar sistemas de información que soporten la gestión interna de los procedimientos.

–Transmitir una cultura de calidad y de cambio a la organización.

Además, este proceso de repensar las organizaciones no tiene final, ya que las posibilidades de utilización de las TIC son tan grandes que siempre será posible mejorar nuestras actividades, todo esto acompañado siempre de importantes inversiones efectuadas de una manera sostenida a lo largo de los años.

Así pues, la gestión del procedimiento administrativo electrónico deberá llevarse a cabo contemplando todas y cada una de las fases del procedimiento, considerándose para cada una de ellas los elementos y factores que intervienen, tanto desde la perspectiva tecnológica como de los requerimientos jurídicos y de gestión sobre los que desarrollar el procedimiento.

En este sentido, creemos necesario hacer una reflexión inicial sobre los aspectos y elementos que intervienen en la gestión del procedimiento electrónico, como son: la configuración del documento electrónico, el registro electrónico de entrada/salida, la gestión del procedimiento mediante herramientas de *workflow*, la validez del procedimiento en relación con la firma electrónica, la notificación electrónica y finalmente, y no por ello con una menor importancia, la conservación y validez de los documentos electrónicos a lo largo del tiempo.

### 3.2. El documento electrónico

Antes de empezar a plantear los aspectos jurídico-técnicos que definen los documentos electrónicos, es necesario prestar atención al concepto básico que lo sustenta. En este sentido, una concepción amplia de documento nos remite a considerar como tal cualquier fuente de datos recuperable en el tiempo y en el espacio.

Partiendo de este concepto amplio de documento, comprensivo tanto de los creados o almacenados en soporte papel como los que lo son en soporte electrónico, deben establecerse las diferencias existentes entre ambas tipologías de documentos, las cuales deberán tenerse presentes en la configuración y legitimación de todo proyecto de procedimiento administrativo electrónico.

La primera nota diferenciadora es aquella que hace referencia al soporte material sobre el que se registra. Mientras que en el documento no electrónico el soporte sobre el que se produce su registro es un soporte tangible y directamente accesible e interpretable sin que sea necesaria ninguna forma de intervención técnica, en el documento electrónico se da la circunstancia que la información ha pasado a ser intangible ya que se almacena como una sucesión de ceros y unos que no se pueden tocar y, al mismo tiempo, no se pueden encontrar e interpretar si no es mediante alguna herramienta de soporte que nos facilite su localización y conversión al lenguaje natural en el que se creó, siendo esta cuestión la que hace referencia a su contenido textual.

La segunda diferencia se puede encontrar dentro del ámbito de la validez del documento y más concretamente en aquel elemento que garantiza su autenticidad. El documento electrónico, si no se acompaña de algún elemento accesorio, como la firma electrónica, que garantice su autoría, es anónimo por naturaleza, ya que no contiene ninguna nota diferenciadora, como sí la incorpora el documento manuscrito y hasta el mecanizado pero identificado por su autor a partir de su firma autógrafa.

Para el resto de los factores, se puede decir, sin ninguna duda, que coinciden en su formulación tanto en los documentos electrónicos como los que no lo son, y por lo tanto hace falta poner el acento en los factores diferenciales a la hora de abordar cualquier aproximación al marco normativo del documento electrónico.

Una primera aproximación al concepto de documento electrónico sería la que ofrece el Real decreto 263/1996, de 16 de febrero:

“Documento: entidad identificada y estructurada que contiene texto, gráficos, sonidos, imágenes o cualquier otra clase de información que puede ser almacenada, editada, extraída e intercambiada entre sistemas de tratamiento de la información o usuarios como una unidad diferenciada.” [artículo 3.d)]

De esta nueva definición de documento se pueden extraer tres categorías diferenciadas de documentos electrónicos, como son:

a) Los registros de las bases de datos y ficheros, en los cuales se almacena información estructurada y organizada siguiendo criterios previamente definidos.

b) Los documentos digitalizados, es decir, aquellos documentos creados en soporte papel y que posteriormente han sido escaneados y transformados en un fichero de imagen, fiel reproducción del original.

c) El documento electrónico, *stricto sensu*, es decir, aquel cuyo ciclo de producción y reproducción es íntegramente electrónico o digital, incorporando los elementos de autenticidad necesarios para garantizar la identificación de su autor y la integridad de su contenido.

Así pues, en la configuración de todo procedimiento administrativo electrónico deberemos tener en cuenta qué tipo de documentos vamos a tratar y la validez jurídica que a cada uno de ellos le podemos atribuir.

Como veremos más adelante, únicamente a los documentos pertenecientes al grupo c) les podemos atribuir validez jurídica plena, puesto que son los únicos que gozan de las características de validez y autenticidad en términos análogos al documento manuscrito.

Por otro lado, será necesario contemplar la conveniencia de mantener archivos físicos en tanto que en los expedientes puedan o deban incorporarse documentos en soporte papel, los cuales, aun cuando hayan sido digitalizados, mantendrán todo su valor probatorio en tanto que ostentan la condición de original, por lo que la validez del documento digitalizado se regulará a partir de lo que dispone el artículo 46 de la Ley 30/1992.

Finalmente, para los documentos del grupo a) deberemos tener presente que principalmente formarán el grueso de los actos de trámite en la ejecución del expediente, y que tendrán validez y eficacia en cuanto se cumpla con los requisitos enunciados en el artículo 45.5 de la Ley 30/1992, es decir, se pueda garantizar su autenticidad, integridad y conservación.

### 3.3. El registro telemático

Con las modificaciones incorporadas por la Ley 24/2001 se ha legalizado la existencia de registros telemáticos, es decir, para recibir y dar salida a los escritos, documentos y comunicaciones que se realicen en soporte informático sin la presencia física de los sujetos que la efectúen. Se puede afirmar que el registro telemático constituye una modalidad de registro informatizado caracterizado por su aptitud para dejar constancia de las actuaciones administrativas o las de los ciudadanos realizadas a distancia, sobre el que cabe plantearse ciertas especificidades respecto del registro tradicional de las organizaciones administrativas clásicas. Es esta una materia de gran actualidad que ya ha sido tratada en diversos trabajos, entre los que destaca el del profesor Valero Torrijos (2002).

Es evidente que en las relaciones administrativas, el registro constituye uno de los principales puntos en la gestión del expediente administrativo, puesto que en él confluyen los actos que las partes del procedimiento ponen en conocimiento de los otros actores.

Aunque en un primer momento pueda parecer sencilla la implantación de un registro telemático, a medida que se avanza en su configuración van apareciendo una serie de elementos, los cuales se desarrollarán a continuación, que es necesario tener en cuenta en cuanto a su implementación y correcto tratamiento.

#### 3.3.1. Requisitos de los registros telemáticos

De acuerdo con lo que se dispone en el artículo 38.9 de la Ley 30/1992, los registros telemáticos tendrán que respetar las exigencias fijadas con carácter general por los registros administrativos, es decir, tendrán que garantizar “la constancia en cada asiento que se practique, de un número, epígrafe extensivo de su naturaleza, fecha de entrada, fecha y hora de su presentación, identificación del interesado, órgano administrativo remitente, si procede y persona u órgano administrativo al que se envía, y, en su caso, referencia al contenido del escrito o comunicación que se registra” (Ley 30/1992: 38.3).

Así pues, es necesario que las aplicaciones informáticas que se diseñen tengan en cuenta todas estas circunstancias, además, por supuesto, de las exigidas en función del soporte informático en que se almacenen: disponibilidad, autenticidad, integridad, confidencialidad y conservación de la información, garantías generales que quedan recogidas en el Real decreto 263/1996 visto antes.

Además, el artículo 7 del mismo real decreto obliga a la implementación de medidas de seguridad orientadas a evitar la interceptación y alteración de las comunicaciones, los accesos no autorizados, así como garantizar la compatibilidad técnica entre el sistema empleado por el emisor y el receptor de la comunicación.

El propio registro telemático ha de informar de los problemas que aparezcan mientras se produce la presentación de los documentos, tanto si éstos se dan por la inexactitud de los datos facilitados por el ciudadano como si se produce un error o avería de los sistemas informáticos en ambos extremos de la comunicación.

Desde la perspectiva de las limitaciones a que se encuentran sujetas las actuaciones que se pueden realizar a través de los registros telemáticos, el artículo 38.9 de la Ley 30/1992 ha establecido dos: la primera, desde un punto de vista subjetivo, ya que sólo se podrán realizar actuaciones que correspondan a la competencia del órgano o entidad que ha creado el registro, y la segunda, desde una perspectiva objetiva, en tanto que los procedimientos y trámites que admitan la comunicación telemática tendrán que haberse especificado previamente en la norma de creación del registro.

#### 3.3.2 Utilización de modelos normalizados de solicitudes

El artículo 70.4 de la Ley 30/1992 prevé de manera genérica la posibilidad de utilizar modelos normalizados de solicitudes, aspecto que en el ámbito de la presentación telemática adquiere una especial relevancia por el hecho que facilita la automatización en la recogida de la información remitida, evitando una actividad posterior de sistematización y archivo de esta información.

Como dispone el artículo 70.4, párrafo segundo, en relación con el uso de modelos normalizados “los solicitantes podrán acompañar los elementos que estimen

convenientes para precisar o completar los datos del modelo, los cuales deberán ser admitidos y tenidos en cuenta por el órgano al que se dirijan". Es decir, el ciudadano tiene el derecho de ampliar la información suministrada a la Administración cuando las posibilidades de espacio y formato que le pongan a disposición no le permitan comunicar toda la información que considere necesaria para la defensa de sus derechos e intereses legítimos.

El principal problema que plantea esta posibilidad es el de garantizar la identidad del autor del documento y su integridad, de tal modo que cualquier alteración de éste pueda ser advertida por el órgano administrativo destinatario de la información.

La solución de este problema se encuentra en las posibilidades que ofrece la firma electrónica como mecanismo que garantiza, de forma razonable, la identidad del autor de los documentos y su integridad. Es por eso que las aplicaciones informáticas utilizadas en los registros telemáticos se tendrían que adaptar a las necesidades específicas de la presentación de documentos, de manera que se permitiera firmar electrónicamente todos aquellos que se adjunten a los modelos normalizados de solicitudes.

### 3.3.3. El recibo telemático

Según dispone el artículo 70.3 de la Ley 30/1992, el ciudadano podrá exigir el correspondiente recibo de las solicitudes, las comunicaciones y los escritos que presente ante la Administración pública, cuestión que queda precisada en el artículo 6 del Real decreto 772/1999. En concreto, este precepto prevé el supuesto de que el ciudadano realice la presentación telemática, en el sentido que "el recibo se expedirá de acuerdo con las características del soporte, medio o aplicación y deberá reunir los requisitos expresados en los apartados anteriores".

En relación con el contenido del recibo, el citado artículo exige de manera alternativa que la acreditación pueda consistir en una copia fiel del documento donde se haga constar el lugar y la fecha de la presentación o bien que sea un recibo en sentido estricto, en el cual se haga constar "el remitente, el órgano destinatario y un extracto del contenido de la solicitud, escrito o comunicación". Es decir, no es suficiente que el registro telemático ofrezca al ciudadano tan sólo un número o código de registro o epígrafe indicativo de la naturaleza del documento presentado, sino que hace falta al menos un resumen de su contenido.

Un ejemplo de cómo se materializa este requisito lo encontramos en la Resolución de 11 de diciembre de 2001, de la Dirección General de la Agencia Estatal de Administración Tributaria, en cuya disposición cuarta se prevé que el registro devolverá "en pantalla el escrito de presentación de la solicitud validado con un código

electrónico de 16 caracteres, además de la fecha y hora de presentación".

Finalmente, hay que señalar que el artículo 6.1 del mismo Real decreto 772/1999 exige que la expedición del recibo se efectúe "en el mismo momento de la presentación de la solicitud", de tal manera que la emisión de la acreditación ha de ser automática y se tiene que poner a disposición del interesado con la mayor agilidad posible.

### 3.3.4. Eficacia temporal de la presentación telemática

Uno de los problemas que puede provocar la tramitación telemática es el relativo a la determinación del momento en que se debe considerar como presentado el escrito en el registro del órgano competente, cuestión ésta que adquiere una gran trascendencia cuando se debe dar por agotado un plazo máximo para la resolución de un asunto o para la notificación de la resolución y la consecuente convalidación o no del acto administrativo para la actuación del silencio.

La resolución de esta cuestión se encuentra en la regulación general de los registros administrativos. El artículo 4.2, párrafo 2.º, del Real decreto 772/1999 considera como registro del órgano competente cualquiera de los correspondientes al departamento que tenga atribuida la tramitación, por lo que la remisión de los escritos, solicitudes y comunicaciones a través del registro telemático, y más concretamente, la recepción en el mismo, podrá determinar automáticamente el inicio del plazo para dictar resolución expresa y para su notificación. Consecuentemente, como regla general, se ha de admitir que en el supuesto de la utilización por parte del ciudadano de los registros telemáticos, la fecha de registro en éste coincidirá con la de la entrada de la solicitud en el registro del órgano competente para su tramitación.

En relación con la eficacia temporal de las actuaciones realizadas a través de un registro telemático, es necesario resaltar que el artículo 38.9 de la Ley 30/1992 establece con carácter básico que puedan presentarse las solicitudes, escritos y comunicaciones "todos los días del año durante las veinticuatro horas". A estos efectos, si la recepción se produjera en un día inhábil para el órgano o entidad destinataria, la presentación se entenderá efectuada el día hábil siguiente.

Finalmente, será necesario prever en qué medida quedan afectadas las reglas generales sobre el cómputo de los plazos si se diera el supuesto que por razones técnicas no imputables al interesado, el registro telemático quedara fuera de servicio durante un tiempo determinado, sobre todo si esta falta de disponibilidad se produce el último día del plazo fijado.

A este respecto, es necesario tener presente que por ser el registro el punto de entrada / salida de los documentos electrónicos, no por ello con su implantación se

puede considerar que ya se tiene en marcha la gestión electrónica de un asunto; es necesario contar con otros elementos, con la gestión electrónica del expediente, la notificación electrónica o la gestión documental, para con la suma de todos ellos disponer de un verdadero procedimiento administrativo electrónico.

De poco sirve contar con un punto de entrada por el canal electrónico si el resto del procedimiento se ejecuta siguiendo los mismos trámites y circuitos que los utilizados en el procedimiento manual.

Actualmente, estamos asistiendo a una carrera de implantación de cuantos más procedimientos en línea mejor, como una muestra de la modernización de las administraciones públicas, pero sin abordar con profundidad el rediseño de los circuitos y procesos para obtener una mayor agilidad en su resolución.

Es evidente que el ciudadano agradece cualquier iniciativa que le facilite las relaciones con las administraciones públicas, pero este agradecimiento se desvanecerá rápidamente si una vez iniciado el procedimiento los requisitos (presentación de documentación complementaria, notificación, seguimiento del expediente, etc.), trámites y periodificación en la resolución no son ostensiblemente mejores que en el procedimiento tradicional.

### 3.4. El circuito administrativo electrónico (*workflow*)

Se puede entender como circuito administrativo electrónico aquel sistema de tramitación soportado por una herramienta informática que facilite y ayude a todos los actores involucrados en todas y cada una de las fases de un procedimiento administrativo, con indicación expresa de los datos que hay que incorporar al sistema y los documentos que se han de emitir o tratar en cada una de ellas, impidiendo la realización de ciertas fases de los procedimientos si no se han cumplido una serie de requerimientos previos.

El inicio de todo expediente administrativo se puede producir por alguno de los siguientes canales:

–El interesado (ciudadano o empresa), de manera presencial o virtual a través del portal que la Administración tenga a internet.

–El funcionario, mediante una actuación de oficio.

Una vez iniciado el expediente e identificadas sus partes integrantes, entrará en funcionamiento el núcleo de la aplicación de tramitación. Un aplicativo de esta clase ha de permitir diseñar diferentes tipologías de expedientes con las correspondientes estructuras de datos y metadatos, todo esto enlazado por un motor de *workflow* que permita definir fielmente las reglas de los procedimientos (normativa aplicable, directrices de ges-

tión, fases del circuito, etc.) y la estructura jerárquica o funcional de la Administración o ente público. Toda esta información, en su conjunto, tendrá que posibilitar a la herramienta de *workflow* dirigir el expediente en cada momento al responsable de su tramitación.

El sistema así definido se ve complementado por todo un conjunto de herramientas y aplicaciones que facilitan la tramitación y aumentan el nivel de información disponible. Algunas de estas herramientas pueden ser los mecanismos de seguridad (infraestructura PKI),<sup>26</sup> los sistemas de explotación de la información geográfica (SIG) o los sistemas de gestión documental para el almacenamiento y tratamiento masivo de la documentación. Es esencial que todas estas herramientas queden integradas en un único sistema de información y gestión administrativa que sea transparente al usuario y le permita obtener en cada momento la información que necesita.

El expediente definido en el sistema de información incluirá tanto documentos electrónicos (es decir, otros documentos del sistema) como físicos. Estos últimos pueden ser de dos tipos: escaneados, la imagen electrónica de los cuales se anexa al expediente, o documentos físicos en papel a los que se identificará mediante un código y de los que habrá que incorporar un extracto al expediente electrónico.

En un entorno como el descrito, la integración de los datos maestros es más una necesidad que no una herramienta complementaria. Implica tener en cuenta la consigna “un dato en un solo lugar y una sola vez”. Esto quiere decir que los datos han de ser únicos y compartidos, siempre que se tenga el consentimiento del interesado cuando se haga tratamiento de datos de carácter personal, desde las tablas auxiliares hasta los datos transaccionales, de modo que el sistema no tenga información redundante y se pueda acceder a ella desde donde sea y cuando sea necesario.

Otro aspecto fundamental es el de la seguridad. Es básico garantizar la seguridad y confidencialidad de la información, preferentemente mediante la utilización de certificados reconocidos emitidos por prestadores de servicios de certificación.

Es, por tanto, la implantación de un circuito electrónico un elemento fundamental que coadyuvará a la materialización efectiva del procedimiento administrativo electrónico, no sólo en los aspectos de “escaparate” como el registro, sino también en la agilización en la tramitación de los expedientes, alcanzándose con ello la verdadera esencia de la aplicación de las nuevas tecnologías de la información y las comunicaciones en la gestión de los procedimientos por las administraciones públicas.

26. *Public Key Infrastructure*.

Con la implantación de este tipo de herramientas se podrá ofrecer a los ciudadanos utilidades que generen valor añadido al procedimiento, como la modificación de datos *on-line* o el seguimiento y situación del trámite en tiempo real, cuestiones que, además de suponer una mejora en las relaciones Administración/ciudadano, incorporan elementos de transparencia que ayudan a mejorar el funcionamiento de las administraciones públicas.

### 3.5. La firma electrónica

En primer lugar, es necesario fijar el concepto de tramitación electrónica, en cuanto se refiere a las relaciones que un ciudadano mantiene con la Administración a través de los canales telemáticos (principalmente internet), así como a la información y documentación que las dos partes se intercambian por este canal, normalmente en el curso de un procedimiento administrativo.

Mientras que los artículos 70 y 110 de la Ley 30/1992 hacen referencia a la necesidad de identificación del interesado o de la persona que le represente, así como la firma del solicitante o la acreditación de la autenticidad de su voluntad expresada por cualquier medio, en sede electrónica el artículo 7.2.b) del Real decreto 263/1996 se limita a exigir que se identifique de forma fehaciente al remitente y al destinatario de la comunicación, no considerándose por lo tanto la cuestión de la representación.

Los mecanismos de autenticación simple, como son los basados en los tradicionales códigos de usuario y *password*, no resultan suficientes para acreditar fehacientemente la identidad del interesado que se dirige a un órgano administrativo, ya que es posible que una tercera persona pueda hacer uso de estos mecanismos con relativa facilidad. Es por eso que será necesario dotarse de mecanismos de autenticación, como los vinculados a las técnicas de criptografía asimétrica y a la utilización de certificados electrónicos, para que quede garantizada la identidad y voluntad del interesado en la tramitación de cualquier procedimiento administrativo.

La cuestión de la autenticidad queda garantizada con la firma electrónica, regulada por la recién aprobada Ley 59/2003, de 19 de diciembre, de firma electrónica, y definida en el punto 1 de su artículo 3 como "El conjunto de datos en forma electrónica, consignados junto a otros asociados con ellos, que pueden ser utilizados como medio de identificación del firmante".

Normalmente, la forma de firmar electrónicamente un documento consiste en su cifrado mediante una clave que se encuentra en posesión tanto del emisor

como del receptor. Este mecanismo de cifrado en el cual las dos partes utilizan una misma clave para cifrar y descifrar el documento se llama sistema de clave simétrica.

Explicado de una manera gráfica, el cifrado con clave simétrica consiste en que el particular (A) que dirige un escrito o solicitud a un órgano administrativo (B) cifra el documento aplicando la clave que comparten ambos agentes, mientras que el órgano administrativo utilizará la clave para hacer inteligible el documento que le llega cifrado.

A pesar de parecer seguro, este mecanismo de cifrado no cumple los requisitos que exige el artículo 70.1 de la Ley 30/1992 a los escritos o solicitudes que los particulares dirijan a la Administración por vía telemática, en tanto que, además de exigir la identificación del interesado [letra a)], también exige la firma del solicitante o la acreditación de la autenticidad de su voluntad expresada por cualquier medio [letra d)], y es en este último punto donde el cifrado de clave simétrica no puede garantizar la voluntad del interesado ya que, como se ha visto, la clave está a disposición de ambas partes y con los mismos efectos materiales.

El modo como la tecnología ha conseguido verificar la garantía de la integridad del documento y por lo tanto que quede acreditada la autenticidad de la voluntad del interesado sin que sea posible su manipulación, desde el punto de vista subjetivo de la comunicación, es mediante el cifrado de clave asimétrica. Este sistema de firma electrónica se fundamenta en la utilización de dos claves asociadas mediante una función matemática, de manera que del conocimiento de una de las claves no se puede obtener la configuración de la segunda.

Una de estas dos claves es privada, es decir, queda dentro del ámbito personal de su poseedor, mientras que la otra es pública, y por lo tanto accesible e utilizable por cualquier persona. La combinación de estas claves en el proceso de comunicación entre las partes garantiza que la autenticidad se asocie no sólo a la identificación del interesado (autenticidad), sino también a su voluntad (integridad). Si el interesado firma digitalmente un documento con su clave privada y la dirige a la Administración, y ésta la puede descifrar y verificar su integridad aplicando la clave pública del interesado, quedará totalmente garantizada la autenticidad e integridad del documento intercambiado.

Por lo tanto, si un particular quiere dirigir una solicitud o escrito a un órgano administrativo, tan sólo necesita disponer de un par de claves facilitadas por una tercera parte de confianza, un prestador de servicios de certificación<sup>27</sup> que no interviene en el procedimiento, del mismo modo que el órgano administrativo que

27. Las autoridades de certificación o prestadores de servicios de certificación tienen por función, además de facilitar el par de claves (pública y privada), la de actuar como fedatarios de la identidad de su proveedor, así como

garantizar las condiciones óptimas de mantenimiento y depósito de los algoritmos y mecanismos que han permitido la generación de las claves.



interviene, sin que sea necesario que ambas partes se intercambien previamente ninguna clave.

El particular sólo necesita firmar con su clave privada el escrito o solicitud dirigido al órgano administrativo competente, para que éste pueda comprobar con la clave pública del interesado la autenticidad de la comunicación. Con esta fórmula sí que existe una garantía total y absoluta de que el documento se ha generado por quien dice haberlo hecho, y, además, la voluntad que transmite por medio de este documento es la que se contiene en él y no otra.

Esta firma digital mediante el sistema de claves asimétricas es la que se recoge en la Ley 59/2003 con el nombre de firma electrónica avanzada [artículo 2.b)], y se define como "La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a los que se refiere, y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control".

A pesar de las mayores garantías ofrecidas por la firma electrónica avanzada y con el fin de proporcionar un instrumento de firma electrónica equiparable a la firma manuscrita, la Ley 59/2003 introduce el mecanismo de firma electrónica reconocida (artículo 3.3) como: "Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma".

Por lo tanto, las características propias de la firma electrónica avanzada, siempre que sea reconocida, serán conciliables con los requisitos que la Ley 30/1992 exige para las comunicaciones ordinarias que los interesados dirijan a la Administración y viceversa. En contraposición, la firma electrónica ordinaria, por el hecho de no encontrarse vinculada a su propietario ni al contenido de los documentos, no permite garantizar material ni jurídicamente la autenticidad ni la integridad de una comunicación, requisitos estos forzosamente exigibles en las comunicaciones dirigidas a la Administración.

### 3.6. La notificación electrónica

El tratamiento de la notificación electrónica en el procedimiento administrativo electrónico no es en absoluto una cuestión pacífica, sino todo lo contrario, ya que con la correcta formalización de este trámite administrativo se puede dar por concluido, por lo menos en una primera etapa, el procedimiento o por el contrario abrir la vía de resolución judicial. Un excelente trabajo al respecto es el realizado por el profesor Hernández González, a partir del cual se han desarrollado las notas que siguen (Hernández González, 2002).

Después de las reformas incorporadas por la Ley 4/1999, el texto de la Ley 30/1992 señala en nueve ocasiones diferentes que el plazo máximo legal de duración de los procedimientos se entiende que es para resolver y notificar la resolución (artículos 42.1, 2 y 5; 43.1 y 5; 44; 115.2; 117.2; y 119.3). Es decir, la notificación de la resolución se conforma como un elemento esencial que determina la finalización del procedimiento y, por lo tanto, la interrupción del cómputo tanto del silencio administrativo como de la caducidad del procedimiento.

A estos efectos, hay que recordar que el artículo 59.1 de la Ley 30/1992 establece que la notificación se practicará por cualquier medio que permita obtener la constancia de la recepción por el interesado o su representante, así como de la fecha, la identidad y el contenido del acto notificado, lo que posibilita de manera implícita la utilización de la notificación telemática.

Es por ello que el artículo 7 del Real decreto 263/1996 establece que las notificaciones realizadas por medios o con aplicaciones informáticas, electrónicas o telemáticas entre la Administración General del Estado y cualquier persona física o jurídica queden condicionadas al cumplimiento de un conjunto de requisitos técnicos que garanticen la disponibilidad y el acceso, la compatibilidad y la seguridad de las comunicaciones, con la finalidad de evitar la interceptación y alteración de los mensajes, así como los accesos no autorizados. Así pues, de acuerdo con el apartado segundo de este artículo, las notificaciones electrónicas serán válidas siempre que:

Exista constancia de la transmisión y recepción de sus datos y del contenido íntegro de las comunicaciones, de acuerdo con lo que se prevé en los artículos 58.2 y 59 de la Ley 30/1992, por lo que también será preciso incorporar elementos como: si la resolución es o no definitiva en vía administrativa, los recursos posibles y el órgano ante el cual se pueden presentar, así como el plazo máximo para interponerlo.

Que el remitente y el destinatario de la comunicación se puedan identificar de manera fehaciente. Como se ha visto en el apartado anterior, esta identificación fehaciente se consigue mediante la firma electrónica avanzada reconocida facilitada por un prestador de servicios de certificación.

Que el interesado en el procedimiento haya determinado como medio preferente de comunicación, en cualquier momento del procedimiento administrativo, el medio electrónico, tal y como se prevé en el artículo 70.1 de la Ley 30/1992 cuando permite "la identificación del medio preferente o del lugar que se señale a efectos de notificación". No obstante, la notificación telemática se considerará, con carácter general, como medio preferente cuando se incardine en procedimientos que se desarrollen íntegramente en soportes informáticos, en

los cuales se produzcan comunicaciones caracterizadas por su regularidad, número o volumen entre la Administración General del Estado y determinadas personas físicas o jurídicas (Real decreto 263/1996: 7.3).

La voluntariedad del medio de notificación se recoge también en el artículo 59.3 de la Ley 30/1992, en la redacción dada por la Ley 24/2001, señalando que “para que la notificación se practique utilizando medios telemáticos se requerirá que el interesado haya señalado dicho medio como preferente o consentido expresamente su utilización, identificando, además, la dirección electrónica correspondiente”.

Cuando se cumpla con todos estos requisitos y de acuerdo con el artículo 7.4 del Real decreto 263/1996, los datos de transmisión y recepción acreditados en la notificación telemática serán válidos a los efectos del cómputo de los plazos, habiéndose de anotar en los registros generales o auxiliares previstos en el artículo 38.3 de la Ley 30/1992.

El principal problema que plantean las notificaciones electrónicas remitidas a los particulares es que los protocolos de no-rechazo y la firma electrónica avanzada garantizan la confidencialidad (por el cifrado del documento), la autenticidad e integridad del mensaje o documento (mediante la firma electrónica), pero no que la notificación haya sido efectivamente recibida por el interesado o por otra persona que pueda ser identificada.

Una primera aproximación a la resolución de dicho problema es la planteada para la Administración General del Estado en el Real decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos, mediante el cual se añaden una serie de artículos a los reales decretos 263/1996 y 772/1999, también de aplicación exclusiva para la Administración General del Estado y los entes públicos de ella dependientes.

Aunque no parezca ésta la solución mejor, por cuanto exige a los interesados el disponer de una dirección de correo electrónico única, en contraposición con lo establecido para el procedimiento no electrónico, como indica el artículo 12.3 del citado RD 209/2003:

“3. Para la eficacia de lo dispuesto en el presente artículo, todo interesado que manifieste su voluntad de ser notificado por medios telemáticos en cualesquiera procedimientos deberá disponer, con las condiciones que se establezcan, de una dirección electrónica habilitada para ello, que será única para todas las posibles notificaciones a practicar por la Administración General del Estado y sus organismos públicos [...]”

Condiciones que han sido fijadas por la Orden PRE/1551/2003, de 10 de junio, por la que se desarrolla la disposición final primera del RD 209/2003, de 21 de febrero, en sus artículos octavo y noveno

Sí que constituye un primer intento de abordar la cuestión de validez de la notificación electrónica. El tiempo y las experiencias que se obtengan marcarán el camino a seguir, aunque no parece descabellado aventurar que, más pronto que tarde, será necesario flexibilizar un sistema que *a priori* parece, y es, demasiado rígido, básicamente como consecuencia de las incertidumbres que se plantean en este campo.

En cualquier caso, estos inconvenientes quedan en segundo plano por la voluntariedad de la comunicación electrónica. Por lo tanto, una vez los interesados hayan manifestado su consentimiento y facilitado una dirección electrónica, de acuerdo con los requisitos establecidos reglamentariamente, las notificaciones transmitidas por correo electrónico a esta dirección, con las correspondientes garantías, tendrán total validez; excepción hecha que se pueda demostrar la imposibilidad material de acceder al texto notificado o que se haya producido una interceptación o alteración del mensaje durante la transmisión.

De todos modos, es evidente que la notificación por correo ordinario no está exenta de riesgo de pérdida, por lo tanto parece fuera de toda lógica exigir mayores garantías al procedimiento telemático que al ordinario, por lo que el artículo 59.3 de la Ley 30/1992, en la redacción dada por la Ley 4/1999, incorpora una doble presunción:

–Presunción de notificación mediante la recepción del mensaje en la dirección electrónica facilitada por el interesado: “La notificación se entenderá practicada a todos los efectos legales en el momento en que se produzca el acceso a su contenido en la dirección electrónica.”

–Presunción en el rechazo de la notificación por el transcurso de diez días naturales sin que el destinatario acceda al contenido del mensaje: “Cuando, existiendo constancia de la recepción de la notificación en la dirección electrónica, transcurrieran diez días naturales sin que se acceda a su contenido, se entenderá que la notificación ha sido rechazada con los efectos previstos en el siguiente apartado, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso.”

La finalidad de esta segunda presunción parece clara: evitar una conducta elusiva del interesado a recibir la notificación, retrasando de esta forma la continuación o finalización del procedimiento, para, de este modo, poder obtener un silencio positivo o la caducidad del procedimiento. De acuerdo con la remisión que realiza este mismo precepto, los efectos que se derivan de esta presunción son los previstos en el artículo 59.4 de la Ley 30/1992, según el cual cuando el interesado rechace la notificación “se hará constar en el expediente [...] y se tendrá por efectuado el trámite siguiéndose el procedimiento”.

Dicho de otra forma, la recepción del mensaje en el buzón de correo electrónico sin que en el plazo de diez días naturales se produzca el acceso a su contenido, queda equiparado al rechazo de la notificación y no a la ausencia del interesado de su domicilio. En este sentido no será de aplicación el doble intento de notificación que el artículo 59.2 de la Ley 30/1992 exige cuando ninguna persona puede hacerse cargo de la notificación en el domicilio del interesado, lo que podría interpretarse como una situación discriminatoria en razón de la tecnología empleada, ya que la falta de acceso al correo bien podría producirse por una conducta dilatoria del interesado, pero también podría darse el caso de un error en la transcripción de la dirección de correo electrónico, cuestión que dejaría el error sin posibilidad de rectificación en un segundo intento por parte de la Administración.

### 3.7. El archivo y conservación de los documentos electrónicos

Fijados los contornos jurídico-materiales a los que se sujetan los procedimientos electrónicos, hay que ver si existen las garantías de conservación de los documentos para que sus efectos sean perdurables en el tiempo.

Si bien es cierto que ésta es una cuestión que desde hace mucho tiempo no se plantea para los documentos en soporte papel, dado que este proceso de conservación se encuentra plenamente arraigado y normativizado en el seno de las organizaciones, el hecho que en este momento se disponga de un nuevo soporte documental hace necesario afrontar el tema, aunque sea de manera sucinta, y ver cuál es el estado de la cuestión en el ámbito normativo español.

En primer lugar, hay que decir que los documentos electrónicos con valor jurídico, en tanto que equiparados a los autógrafos, han de conservar su vigencia por el mismo período de tiempo que éstos, y por lo tanto se ha de garantizar su legibilidad y el mantenimiento de sus efectos jurídicos, mientras así lo establezcan los procedimientos en los cuales se encuentren incluidos.

A este respecto, la Ley 59/2003 incorpora una regulación más detallada que la que figuraba en el derogado RDL 14/1999, sobre las obligaciones de conservación de los certificados reconocidos por parte de los prestadores de servicios de certificación que expidan certificados reconocidos, tanto en relación con la verificación de las firmas efectuadas como con la fiabilidad de los sistemas de almacenamiento de dichos certificados. Todo ello por un período de quince años contados desde el momento de su expedición [artículos 20.1, letras f) y g), y 21.3].

Este período previsto de conservación de quince años parece suficiente como para garantizar la validez de los

documentos en las fases activa y semiactiva, pero, ¿qué pasará una vez transcurrido este período?

Como muy bien indica Jordi Serra en su trabajo "Gestión de los documentos digitales: Estrategias para su conservación", "¿qué sentido tiene garantizar la fiabilidad de una transacción electrónica y la autenticidad de sus intervinientes, así como de su contenido, si esta información no se puede utilizar como prueba pasado un tiempo?" (Serra, 2001: 5).

La firma digital es un serio problema para la conservación a largo plazo. Si se trata de documentos que han de mantener su valor legal durante un largo período de tiempo, deberemos tener presente que la migración a un nuevo formato puede invalidar la firma digital que acompaña al documento. El *National Archives and Record Administration* (NARA) de los Estados Unidos de América recomienda que el nombre de la persona que firma el documento, juntamente con la fecha de la firma, consten escritos de una forma humanamente inteligible en el propio documento, con la finalidad de poder preservar la autoría del documento en el caso que la migración invalide la firma digital (Serra, 2002: 35).

Por lo tanto, si se produce la migración mencionada, lo que parece del todo posible y recomendable si lo que se pretende es mantener vivos los archivos administrativos y al mismo tiempo adaptarse al constante cambio tecnológico, nos encontraremos de aquí a unos años con una ingente cantidad de documentos electrónicos que en su día fueron firmados digitalmente pero que en el futuro puede ser que hayan perdido parte de los requisitos de validez que los equipararon a los documentos autógrafos.

Debe decirse que no existe una única solución al problema ya que la evolución tecnológica hará muy difícil mantener la legibilidad íntegra de estos documentos a lo largo del tiempo, en este sentido, y para ilustrar un poco el problema, a continuación se reproduce una parte de la solución adoptada por el NARA (Serra, 2002: 44):

"Cuando un documento electrónico está en fase administrativa y son activos sus valores primarios se hace preciso un mecanismo que garantice su autenticidad, y la forma de hacerlo es mediante sistemas de autenticación como la firma digital o los códigos de acceso al sistema. El documento incorpora el código de seguridad como metadato y el fichero que contiene el significado de ese código pasa a ser, a partir de ese momento, parte del contexto del documento. Sin embargo, cuando el documento pierde sus valores primarios y se convierte en documento de 'archivo', este cambio va asociado a un cambio de espacio: el documento es transferido a un espacio que denominamos 'archivo digital', y que identifica a los documentos como históricos por el solo hecho de residir en ese espacio [...]. Este es un espacio cerrado, reservado al acceso de

un único usuario autorizado y responsable de la custodia. Por lo tanto, la autenticación particular de cada documento se convierte en una autenticación general: todos los documentos electrónicos, por el mero hecho de residir en el espacio del 'archivo virtual' se consideran auténticos, y lo hacen en virtud de dos condiciones:

“–Que el espacio de archivo es un espacio inmodificable, reservado al acceso del archivero.

“–Que se tiene la certeza de que los documentos han ingresado auténticos en el archivo, puesto que lo han hecho mediante un proceso controlado.”

Pero el problema de la conservación y el archivo de la documentación electrónica no se vincula exclusivamente con la problemática que incorpora la firma electrónica, sino que también se ha de extender al resto de los documentos que se generen en las organizaciones.

En este sentido, los documentos son activos críticos en las administraciones públicas, y por lo tanto se ha de encontrar la mejor forma de gestionarlos, ya que con carácter general se puede decir que:

–Los archivos de documentación ocupan mucho espacio físico y éste aumenta significativamente en cortos espacios de tiempo.

–El espacio físico es caro y escaso.

–Los sistemas de organización de los archivos existentes no se utilizan adecuadamente.

–La documentación archivada no es fácilmente accesible.

–La documentación se puede deteriorar con el tiempo si no se archiva en óptimas condiciones de conservación.

Como dijo el Sr. Erkki Liikanen, comisario europeo para la Empresa y la Sociedad de la Información, durante la celebración del DLM Fórum de 1999, “la importancia de ofrecer acceso público y conservación de la información electrónica a largo plazo se considera hoy en día un requisito crucial para conservar la memoria de la sociedad de la información y, al mismo tiempo, mejorar los procesos de negocio de cara a un gobierno más efectivo”.

Fruto de esta sensibilidad por la gestión electrónica de los documentos, la Comisión Europea encargó la confección de un informe que analizara de forma exhaustiva los requisitos de la gestión de los registros electrónicos.

Ultimados los trabajos por un grupo de auditores expertos con la colaboración de profesionales de diversos países de la Unión Europea, se presentó a mediados del año 2001 la especificación MoReq, en la que se describen los requisitos funcionales de un modelo de sistema de gestión de registros electrónicos (SGRE) o sistema de gestión documental.

El documento analiza con detenimiento todos los elementos substanciales que intervienen en la gestión electrónica de los documentos, como son:

–El sistema de clasificación a utilizar.

–Los controles de acceso y de seguridad a implementar.

–Las normas a considerar en la conservación y eliminación de los documentos.

–La captura de los registros.

–Cómo referenciar los registros para vincularlos con los documentos.

–Aspectos relacionados con la búsqueda, recuperación y reproducción de los documentos.

–Las funciones de administración del sistema que hay que incorporar.

–La gestión de aspectos como la firma electrónica, la encriptación, los registros no electrónicos, etcétera.

Otra norma internacional que se debe tener presente en el momento de abordar la gestión documental es la norma ISO 15489 sobre Información y documentación. Gestión documental.

Esta norma es aplicable a la gestión de documentos, en sus fases activa y semiactiva, de todos los formatos o soportes, creados o recibidos por cualquier organización pública o privada en el ejercicio de sus actividades o por cualquier responsable de crear y mantener documentos, sirviendo de referencia para el diseño e implementación de un sistema de gestión documental.

Los sistemas de gestión documental deben incorporar documentos que se caractericen por su autenticidad, fiabilidad, integridad y utilidad. Asimismo, los sistemas de gestión documental han de ser fiables, garantizar la integridad, adecuarse al entorno normativo, responder a las necesidades de toda la organización, y todo esto siguiendo un modelo sistematizado que permita crear, mantener y gestionar los documentos mediante políticas bien documentadas, responsabilidades asignadas y metodologías formales para asignarlas.

Como se ha podido ver, existe una gran preocupación en el ámbito archivístico sobre cómo se ha de gestionar la conservación de los documentos en un momento en que las nuevas tecnologías están provocando el desbordamiento de los mecanismos de archivo tradicionales, bien por la aparición de nuevos formatos de documentos o bien por una explosión en la creación de documentos provocada por la aparición de nuevos medios de comunicación y difusión de la información.

En este sentido, y recogiendo la sensibilidad que al respecto han manifestado los profesionales de la archivística, la Ley catalana 10/2001, de 13 de julio, de archivos y documentos, prevé en su artículo 7 que:

“Responsabilidades de los titulares de documentos públicos.

“Todas las administraciones y las entidades titulares de documentos públicos han de disponer de un único sistema de gestión documental que abarque la producción, la tramitación, el control, la evaluación y la conservación de los documentos y el acceso a éstos y

que garantice el tratamiento correcto mientras sean utilizados administrativamente en las fases activa y semiactiva.”

### 3.8. Valoración de la situación en el ámbito de las administraciones locales

El impacto de las TIC en las administraciones públicas se puede medir, básicamente, desde tres perspectivas diferentes: (1) su utilización en la organización y gestión interna con el objetivo de mejorar los sistemas de integración de la información y coordinación de las distintas instancias de la Administración pública; (2) el desarrollo de nuevas aplicaciones basadas en internet y en las TIC, destinadas a favorecer el contacto y la comunicación con los ciudadanos, y (3) la implantación de un verdadero canal electrónico de tramitación de los asuntos que acerque definitivamente la Administración a los ciudadanos, ofreciendo un auténtico valor añadido a la gestión administrativa de los expedientes.

Por lo que respecta a la primera de las perspectivas, cabe decir que su estudio, aun teniendo una relación directa con el presente trabajo, no es objeto de su análisis, ya que al situarse en el ámbito organizativo interno de las administraciones públicas, requeriría de un detallado estudio prospectivo de los procesos y circuitos mecanizados en cada organización.

En relación con el segundo de los ámbitos citados, debemos mencionar los datos recientemente publicados en sendos estudios sobre el uso de las TIC en las relaciones Administración/ciudadano (e-España, 2002 y Ciberp@ís) a través de internet, de los que cabe destacar la presencia en este medio de más del 90% de los municipios de las provincias de A Coruña, Guipúzcoa, Albacete, Córdoba, Sevilla, Castellón y Barcelona, mientras que en el polo opuesto de la horquilla se sitúan provincias como Salamanca, Segovia, Soria, Teruel, Huesca y Guadalajara, todas ellas con una presencia en la red inferior al 5% del total de sus municipios.

Por último, siguiendo con los datos mostrados en el estudio “Radiografía de las webs municipales” (Ciberp@ís, 26.06.2003), en relación con el análisis de la tercera de las perspectivas apuntadas al inicio del presente epígrafe, es importante poner de manifiesto que de las setenta y ocho webs analizadas, un 28,2% no ofrece la posibilidad de realizar ningún trámite por internet, y el 29,5% lo ofrece en un número inferior a cinco, mientras que únicamente el 23,1% proporciona las herramientas para la tramitación *on-line* de más de quince asuntos, la

mayoría de los cuales sólo proporcionan un medio de transmisión telemática de la solicitud.

Aun cuando pueda parecer que se están alcanzando mayores niveles de interactividad *on-line*, es preciso matizar que en muy pocos trámites se facilita una herramienta de seguimiento del estado de la tramitación, con lo que la gestión electrónica es más aparente que real, si atendemos a la configuración que del procedimiento administrativo electrónico hemos desarrollado en este mismo capítulo.

La implantación de un verdadero procedimiento administrativo electrónico requiere no sólo unas elevadas inversiones en equipamiento y desarrollo de *software*, sino también un ejercicio de rediseño de la gestión administrativa en su globalidad, integrando sistemas y herramientas de tal manera que se consiga la agilización y transparencia de los procedimientos.

Es evidente que, a la luz de los datos reseñados, el subsistema local se caracteriza por su gran heterogeneidad, y por lo tanto nos encontramos con realidades muy diferentes que hacen muy difícil una valoración general del estado del arte en la tramitación electrónica, por lo que sólo cabe extraer una conclusión: se avanza, pero muy lentamente, y posiblemente no siempre en la dirección adecuada.

## 4. La protección de datos de carácter personal y las administraciones locales

### 4.1. Evolución normativa y jurisprudencial

El punto de partida en la consideración jurídica de la protección de datos de carácter personal lo constituye la Constitución de 1978, y concretamente el artículo 18, que, entre otras, formula las siguientes prescripciones:

“1. Se garantiza el derecho [...] a la intimidad personal y familiar [...].

“4. La ley limitará el uso de la informática para garantizar [...] la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.”

Catorce años más tarde se da cumplimiento al mandato de los constituyentes y se promulga la Ley orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos de carácter personal (LORTAD). Con esta ley se produce una ampliación de garantías, puesto que, en rigor, su objeto no es sólo la protección de la intimidad, sino la *privacidad*, entendida como un conjunto de facetas de la personalidad más amplias que las íntimas (Exposición de motivos, I).<sup>28</sup> Con

28. La Exposición de motivos (I, segundo párrafo) dice así: “El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad. Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas

de la vida de la persona –el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo–, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a

todo, el artículo 1 ceñía su objeto al mandato constitucional:

“La presente Ley Orgánica, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.”

Poco tiempo después es aprobada la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de julio de 1995, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la circulación de estos datos*. Esta directiva contiene algunas diferencias respecto a la LORTAD/1992,<sup>29</sup> lo que determinará la ineludible adecuación de esta ley.

A mediados de 1999, es aprobado por el Consejo de Ministros el proyecto de ley de modificación de la LORTAD, que afectaba a un número determinado de artículos, precisamente para adecuarlos a la Directiva 95/46/CE antes citada. En el curso de la tramitación parlamentaria, sin embargo, el objeto de la modificación se amplía y el resultado será una ley íntegramente nueva, la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD).

Entre las modificaciones substanciales que introduce cabe destacar la ampliación de su objeto: incluye cualquier “tratamiento de datos personales” (no sólo los automatizados, también los que no lo sean), y la garantía y protección se extienden también a “las libertades públicas y los derechos fundamentales de las personas físicas” (LOPD/1999, 1).<sup>30</sup>

En marzo de 2000, el Defensor del Pueblo interpuso recurso de inconstitucionalidad contra determinados incisos de los artículos 21.1 (“Comunicación de datos entre administraciones públicas”) y 24.1 y 2 (“Otras excepciones a los derechos de los afectados”) de la LOPD/1999, recurso que fue estimado por el Tribunal Constitucional (TC) mediante la Sentencia 292/2000, de 30 de noviembre. Más adelante trataremos el tema de la cesión o comunicación de datos entre administraciones. Ahora interesa dejar constancia de que con dicha sentencia se produce la *constitucionalización* de lo que,

con términos sinónimos, se denomina “derecho a la autodeterminación informática”, “libertad informática”, “*habeas data*” o “derecho fundamental a la protección de datos” de la persona física. El contenido de dicho derecho fundamental puede resumirse así (STC 292/2000, fundamentos jurídicos 5, 6 y 7):

–Derecho a saber y a ser informados sobre el destino y uso de los datos personales recogidos.

–Poder de disposición y control sobre los datos personales propios, susceptible de ejercerse frente a otros (privados o poderes públicos).

Tras esta apretada síntesis sobre la evolución normativa y jurisprudencial, vemos cómo hay un sucesivo desplazamiento o ampliación del objeto protegido: de la intimidad se pasa a la privacidad, y de ésta a la autodeterminación informativa de la persona física.

## 4.2. El sistema de protección de datos de carácter personal

### 4.2.1. Conceptos básicos

Uno de los factores que ayuda a explicar el porqué de las dificultades en la aplicación de la legislación y las medidas de protección de datos es, sin duda, el de su complejidad. Complejidad que deriva del hecho de aunar elementos técnico-informáticos y una configuración jurídica con un alto nivel de abstracción.<sup>31</sup>

Para paliar los efectos de tales dificultades, la propia LOPD/1999 (artículo 3) ofrece las siguientes definiciones:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, la grabación, la conservación, la elaboración, la modificación, el bloqueo y la cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.” La Exposición de motivos de la LORTAD/1992 tenía párrafos que, como el transcrito, ilustraban certeramente sobre el objeto y las consecuencias de la ley.

29. Así, por ejemplo, la figura del *encargado de tratamiento* [artículo 2.e) de la directiva], no contemplada en la ley.

30. Las valoraciones sobre esta nueva ley han sido diversas: es bastante crítico Davara (2000), y lo es menos Vizcaíno (2001). En cualquier caso, si ya la LORTAD/1992 era considerada una de las leyes más protectoras de todas las de la Unión Europea (Fernández López, 2000), la LOPD/1999 ha acentuado este carácter. Otros aspectos, como la falta de una exposición de motivos o

algunas imprecisiones que son fuente de dudas interpretativas, suponen sendas deficiencias de la ley.

31. En el seno de las organizaciones (hablamos de las públicas, que son las que conocemos) se produce por ello una situación un tanto paradójica: los técnicos informáticos no acaban de entender el sistema de protección de la LOPD, lo que atribuyen a su complejidad jurídica, y a los juristas y responsables administrativos les resulta difícil comprender las implicaciones de conceptos y locuciones como *ficheros* o *tratamientos automatizados de datos*, o la diferencia entre *bloqueo* y *cancelación* de datos (LOPD, artículo 3), atendido que para ello se requieren conocimientos informáticos. Afortunadamente, se están ya superando las iniciales actitudes de rechazo mutuo (una especie de *conflicto negativo de competencias*), y ya es norma el análisis y la actuación conjuntos, así como la consideración de que la protección de datos personales es una cuestión que concierne a todos.

d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o juntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.”

No obstante el hecho de que la LOPD/1999 sea el resultado último de la modificación (derogación finalmente) de la LORTAD/1992 para adecuarla a la Directiva 95/46/CE, lo cierto es que la adaptación presenta deficiencias. De entre ellas destacan las siguientes:

–El olvido en la LOPD/1999 del concepto de *tercero*, que en la directiva es definido como “persona diferente del interesado, del responsable o encargado del tratamiento, o de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o encargado del tratamiento” [Directiva 95/46/CE, artículo 2.f)].

Dicho olvido tiene repercusiones graves, por ejemplo, a la hora de discernir qué supuestos constituyen *cesión o comunicación de datos* (muy limitadas en la LOPD) en el seno de las administraciones públicas.

–Imprecisión en la definición de *responsable* del fichero o del tratamiento, que la LOPD/1999 refiere también a *órgano* [3.d)], mientras que la Directiva 95/46/CE lo remite al término más amplio de organismo [2.d)].

–Introducción de la definición de *cesión o comunicación de datos*, que no se recoge en la directiva y que, en cambio, la LOPD/1999 incluye como sinónimos.

#### 4.2.2. Principios generales

Todo el sistema de protección de datos de carácter personal se asienta sobre una serie de principios, medidas y exigencias, cuya articulación en la LOPD/1999 responde a la finalidad garantista ya señalada y que es propia de toda ley orgánica reguladora de derechos fundamentales. Sucintamente enunciados, los principios generales del sistema y sus aspectos esenciales son los siguientes:

a) Principio de calidad de los datos (LOPD, 4), en cuya virtud los datos personales:

–Sólo se podrán recoger y tratar cuando sean adecuados, pertinentes y no excesivos, en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

–No podrán usarse para finalidades incompatibles.

–Deberán ser objeto de actualización y almacenamiento de forma que permita el ejercicio del derecho de acceso por su titular.

–Serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

b) Derecho de información en la recogida de datos (LOPD, 5), del que se derivan las obligaciones siguientes:

–Los interesados a los que se soliciten datos personales deberán ser previamente informados de la existencia de un fichero o tratamiento de datos de carácter personal y del resto de las previsiones y con las garantías fijadas en la LOPD.

–Cuando los datos no hayan sido recabados del interesado, éste será informado en el plazo de los tres meses siguientes al registro.

c) Consentimiento inequívoco del afectado para el tratamiento de datos que le será requerido, salvo que la ley disponga otra cosa, y que podrá ser revocado (LOPD, 6).<sup>32</sup>

32. De conformidad con el número 2 del artículo 6 de la LOPD:

“No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente ley (*diagnóstico médico y prestación sanitaria*), o cuando los datos figuren en fuentes

accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.”

Y para estos casos añade: “[...] y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal” (número 4, artículo 6, de la LOPD).

d) Consentimiento expreso y otras previsiones más garantistas en relación con datos especialmente protegidos (ideología, religión, creencias y afiliación sindical), sensibles (salud, origen racial o étnico y vida sexual) y relativos a la comisión de infracciones penales y administrativas (sólo susceptibles de incluir en ficheros de las AP competentes) (LOPD, 7 y 8).

e) Obligación para el responsable del fichero y el encargado del tratamiento de adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal (LOPD, 9 y Reglamento aprobado por el Real decreto 994/1999).

f) Deber de secreto del responsable del fichero y de quienes intervengan en cualquier fase del tratamiento de datos personales (LOPD, 10).

g) Consentimiento previo e informado del interesado como requisito de la comunicación de sus datos personales a un tercero, para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, susceptible de ser revocado y que no será preciso sólo en los supuestos previstos legalmente (LOPD, 11).<sup>33</sup>

h) Derechos de las personas en relación con sus datos personales que son objeto de tratamiento:

–No ser objeto de una valoración que se base únicamente en un tratamiento de datos, y derecho a impugnarla (LOPD, 13).

–Derecho de consulta al Registro General de Protección de Datos sobre la existencia de tratamientos, sus finalidades y la identidad del responsable del mismo (LOPD, 14).

–Derecho del interesado a solicitar y obtener información del responsable del tratamiento sobre el origen y las comunicaciones de sus datos personales (LOPD, 15).

–Derecho del interesado a que sus datos sean rectificados o cancelados cuando resulten incorrectos o incompletos, o su tratamiento no se ajuste a la LOPD (16).

–No se exigirá contraprestación alguna por el ejercicio de tales derechos (LOPD, 17).

l) Tutela de los derechos de las personas a partir de la formulación por los interesados de las reclamaciones ante la Agencia Española de Protección de Datos (AEPD)<sup>34</sup> u organismo competente de la comunidad autónoma respectiva, y la interposición de recurso contencioso-administrativo contra sus resoluciones (LOPD, 18).

La AEPD es calificada como “ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las administraciones públicas en el ejercicio de sus funciones” (LOPD, 35.1). Encargada de velar por el cumplimiento de la legislación sobre protección de datos, controlar su aplicación y ejercer las atribuciones y potestades conferidas (dictar instrucciones, efectuar requerimientos, ordenar la cesación de tratamientos, ejercer la potestad sancionadora, entre otras, detalladas en la LOPD, 37), la Agencia Española de Protección de Datos integra el supuesto de las denominadas *administraciones independientes*, “organizaciones administrativas de carácter institucional, no representativas, que desarrollan funciones propias de la Administración activa y que están configuradas legalmente de forma que el Gobierno y el resto de la Administración gubernativa carecen de las facultades de dirección que configuran típicamente su relación con la Administración institucional instrumental, y ello con la finalidad de neutralizar políticamente una actividad integrada en la órbita del poder ejecutivo” (Magide, 2000: 33).

El régimen de independencia de la AEPD se refleja en una serie de garantías que recoge la LOPD/1999: elaboración y aprobación del anteproyecto de presupuesto (artículo 35.5), configuración del cargo (36) y de las funciones del director (que “no estará sujeto a instrucción alguna en el desempeño de aquéllas”, 36.2) y previsión de un Consejo Consultivo, de composición plural (38), entre las más significativas.

La LOPD prevé también que las comunidades autónomas podrán crear sus respectivas autoridades de control, con competencias sobre los ficheros creados o gestionados por la propia comunidad y por la Admi-

33. Tal consentimiento, dice el núm. 2 del artículo 11 de la LOPD, no será preciso:

“a) Cuando la cesión esté autorizada en una ley.

“b) Cuando se trate de datos recogidos de fuentes accesibles al público.

“c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

“d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

“e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

“f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.”

A este respecto, hay que tener en cuenta que no se considera comunicación o cesión de datos personales el acceso que tiene a éstos el encargado del tratamiento (cuya definición transcribimos al principio del apartado 2.1). Se trata del supuesto tan frecuente del *outsourcing* o *externalización* de tareas (gestión de nóminas, envío de correspondencia, etc.). Obviamente, todo ello está legalmente admitido si bien hay que adoptar una serie de garantías (contrato formalizado, medidas de seguridad, no-comunicación o cesión de los datos a un tercero y devolución o destrucción de los datos al finalizar la prestación) (LOPD, 12).

34. La L 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social (artículo 79) ha añadido el calificativo de *Española* a la denominación inicial de *Agencia de Protección de Datos* que figuraba en la LOPD/1999, y que ahora ha sido modificada.



nistración local de su ámbito territorial (LOPD, 41 y 42). Hasta la fecha han sido instituidas la Agencia de Protección de Datos de la Comunidad de Madrid (Ley autonómica 8/2001, de 13 de julio), y la Agència Catalana de Protecció de Dades (Ley autonómica 5/2002, de 19 de abril).

j) Derecho del interesado a ser indemnizado por el daño o lesión sufrido en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en la LOPD por el responsable o el encargado del tratamiento (LOPD, 19).

k) Establecimiento de un régimen sancionador que se configura a partir de:

–La tipificación de infracciones leves, graves o muy graves por el incumplimiento de las obligaciones exigidas a los responsables y encargados de los tratamientos de datos personales (LOPD, 43 y 44).

–En los supuestos de infracciones cometidas por sujetos distintos de las administraciones públicas, la fijación de sanciones en función del carácter leve, grave o muy grave (su escala va desde 601,01 hasta 60.101,21, desde esta última hasta 300.506,05, y desde ésta hasta 601.012,1 euros) (LOPD, 45).

–Si las infracciones son cometidas en ficheros de los que sean responsables las administraciones públicas, las consecuencias son otras: resolución de la AEPD para que cesen o se corrijan los efectos de la infracción y propuesta de actuaciones disciplinarias (de lo que deberá darse cuenta al director de la AEPD) y comunicación al Defensor del Pueblo (LOPD, 46).

–Determinación de las previsiones sobre prescripción de las infracciones muy graves (a los tres años), graves (a los dos años) y leves (al año), y de las sanciones, con los mismos plazos (LOPD, 47); sobre el procedimiento sancionador (LOPD, 48 y Real decreto 1332/1994, 18) y sobre la potestad de la AEPD de inmovilización de ficheros en supuestos muy graves (LOPD, 49).

### 4.3. Ficheros y competencias locales

#### 4.3.1. Ficheros públicos locales

##### a) Configuración general.

Los datos personales pueden almacenarse en ficheros de titularidad privada o pública. Centrándonos en éstos, cabe definir el *fichero público* como *todo conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de creación, almacenamiento, organización y acceso, que gestiona una administración pública*.

Regulados en los artículos 20 a 24 de la LOPD/1999, la tipología de ficheros públicos es muy variada, lo que se explica por la diversidad de competencias de las administraciones públicas. Y será precisamente el ámbito de las competencias respectivas lo que determinará si la actuación de una administración determinada es o no legítima.<sup>35</sup>

De conformidad con la LOPD, “la creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general sólo publicada en el *Boletín Oficial del Estado* o Diario Oficial correspondiente” (artículo 20.1).

El tema de la naturaleza jurídica de la *disposición general* de creación del fichero plantea bastantes dudas. De entrada, este término, en la acepción usual del Derecho administrativo, se vincula con el reglamento.<sup>36</sup>

Sin embargo, a nuestro entender, concurren diversos argumentos para rechazar la naturaleza reglamentaria del acto de aprobación de ficheros públicos. En síntesis, tales argumentos son los siguientes:

1.º. En rigor, con el fichero no se produce ningún tipo de *normación*, ni su contenido puede constituir la más mínima *innovación de ordenamiento jurídico*, características estas del reglamento como fuente de Derecho. Por el contrario, lo que se produce es una mera declaración formal de los aspectos materiales que definen el contenido del fichero. Es en este sentido que el artículo 20.2 de la LOPD prevé:

“Las disposiciones de creación o modificación de ficheros deberán indicar:

- a) La finalidad del fichero y los usos previstos para el mismo.
- b) Las personas o los colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
- c) El procedimiento de recogida de los datos de carácter personal.
- d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
- e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
- f) Los órganos de las administraciones responsables del fichero.
- g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

“disposición de carácter general” (artículo 52.2). A su vez, la Ley catalana 13/1989, de 14 de diciembre (de organización, procedimiento y régimen jurídico de la Administración de la Generalidad) también habla de “disposiciones administrativas de carácter general” (artículos 61 a 67). En todos estos textos se identifican con el reglamento.

En cambio, la Ley 50/1997, de 27 de noviembre, del Gobierno, usa profusamente la expresión “reglamentos” (artículos 23 y 24).

35. La LOPD/1999 utiliza con frecuencia referencias a la legitimidad (por ejemplo, en el artículo 4, sobre *calidad de los datos y finalidades legítimas de obtención de los mismos*).

36. La Ley 29/1998, de 13 de julio (reguladora de la jurisdicción contencioso-administrativa), utiliza los términos “disposición de carácter general” (artículos 25.1 y 26.1) y “disposición general” (artículos 26.2, 27 y 29.1). La Ley 30/1992 emplea los de “disposiciones administrativas” (artículos 51 y 52.1) y

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.”

Se trata de simples apuntes o referencias a los aspectos señalados, cuya regulación está específicamente detallada en la ley y sin que, mediante el acto de *creación* o aprobación del fichero, se pueda ir más allá de los límites prescritos por la LOPD.

Como tantos otros actos de las administraciones públicas, se consigna una declaración de voluntad, una decisión (recoger o tratar datos personales), y se hace pública mediante su inserción en un diario oficial.

2.º. Es también un argumento para negar la naturaleza reglamentaria la propia Sentencia del Tribunal Constitucional 292/2000. Dicha sentencia declaró inconstitucional un inciso del artículo 21 (sobre “Comunicación de datos entre administraciones públicas”), concretamente el que la admitía “cuando la comunicación hubiere sido prevista por las disposiciones de creación o por disposición de superior rango que regule su uso”. Y lo anula porque, como se precisa en los fundamentos jurídicos 14 y 15, posibilitaba que mediante reglamento (norma de superior rango a la disposición de creación del fichero) se autorizaran cesiones; y éstas, sin que medie consentimiento, dice la sentencia, sólo pueden autorizarse por ley. Luego si la sentencia proscribiera tanto la disposición de creación del fichero como la de (su inmediato) rango superior, esto es, la reglamentaria, queda claro que dicha disposición de creación del fichero se sitúa en un rango inferior al del reglamento.

3.º. Entre la doctrina administrativista, Heredero es categórico: “[...] la disposición de creación no es una ‘disposición general de desarrollo de la ley’, sino un acto de aplicación” (1996: 152); y, más adelante, concluye: “[...] la disposición creadora del fichero no es un reglamento, sino un acto administrativo con pluralidad indeterminada de destinatarios” (1996: 153).<sup>37</sup> En el ámbito local,

37. Es cierto que el comentario de Heredero se refiere al artículo 18 de la LORTAD/1992, pero éste es uno de los preceptos que mantuvo su redacción en la LOPD/1999; de ahí que sea igualmente aplicable al artículo 20 de esta ley.

38. Estos autores señalan la competencia del alcalde para la aprobación de los ficheros municipales, de lo que desprende que no les confieren naturaleza de reglamento [cuya aprobación corresponde al Pleno, Ley 7/1985, artículo 22.2.d)]. También Villaverde (2003b: 75) admite que la creación del fichero se realice mediante decreto del alcalde.

Entre los que atribuyen naturaleza reglamentaria a la disposición de creación del fichero hay que citar a González Pérez y González Navarro (1999: 1043) y Herrán (2002: 265-266).

39. O que desaparezca en una futura ley que sustituya a la LOPD/1999.

Entre las opiniones críticas con la diferenciación entre ambos tipos de ficheros se encuentra Alonso (1997: 145), que es citada por Herrán (2002: 264-265).

40. Piénsese, por otro lado, que la exigencia de reglamento para crear un fichero público plantearía graves dificultades a todas aquellas entidades públicas distintas de las que tienen reconocida la potestad reglamentaria, esto es, las territoriales: la general del Estado (Ley 50/1997, de 27 de noviembre, del *Gobierno*, artículos 23 a 25), las autonómicas (así, por ejemplo, la Generalidad de Cataluña, Ley catalana 13/1989, artículos 61 a 67), y la muni-

se adscriben igualmente a la posición que defendemos, Chacón y Cortés (2002: 767).<sup>38</sup>

4.º. Finalmente, la tesis de la naturaleza no reglamentaria del acto de aprobación de ficheros públicos puede argumentarse a partir de la identidad material entre éstos y los de titularidad privada. Esta no-diferencia entre unos y otros nace ya de la Directiva 95/46/CE, que no establece distinción alguna entre personas privadas y públicas, sino la obligación del responsable del tratamiento de efectuar una notificación a la autoridad de control con anterioridad a la realización de tratamientos (artículo 18.1 de la directiva). Como tampoco lo hace en relación con el contenido de la notificación (artículo 19 de la directiva), que, por tanto, es común.

La regulación separada en el título IV de la LOPD/1999 de los ficheros de titularidad pública (capítulo I, artículos 20 a 24) y privada (capítulo II, artículos 25 a 32) es una peculiaridad de la legislación española, que ya se inició con la LORTAD/1992 (título IV, capítulo primero, artículos 18 a 22, para los públicos, y capítulo II, artículos 23 a 31, para los privados), pero que bien pudiera no haberse producido.<sup>39</sup>

La reglamentaria es una potestad y, por ello, una prerrogativa del poder público, y sus manifestaciones (las normas jurídicas), ni formal ni materialmente podrían coincidir con la actividad de una persona jurídica privada.<sup>40</sup>

En conclusión, por tanto, la disposición de creación, modificación o supresión de un fichero público tiene la naturaleza de acto administrativo general que, en razón de ser su destinatario una pluralidad indeterminada de personas, debe publicarse en el diario oficial correspondiente a la Administración que es titular del mismo [LOPD/1999, 20.1, y Ley 30/1992, 59.6.a) y 60.1].<sup>41</sup>

#### *b) Aplicación al ámbito local.*

Con referencia al ámbito local podemos fijar las siguientes especificaciones:

la municipal, la provincial y la insular [Ley 7/1985, artículo 4.1.a) y 49]; y aquellas otras que la tienen atribuida con carácter limitado: el Consejo General del Poder Judicial (que “podrá dictar Reglamentos sobre su personal, organización y funcionamiento en el marco de la legislación sobre la función pública”, artículo 110.1 de la Ley orgánica 6/1985, de 1 de julio, del poder judicial); y las denominadas *administraciones independientes*, con potestad restringida a sus ámbitos específicos (*circulares* del Banco de España, *disposiciones* de la Comisión Nacional del Mercado de Valores e *instrucciones* de la Agencia de Protección de Datos, entre las más importantes; véase Magine, 2000: 426-450).

Pero la limitación en razón de su especialidad en estos casos, o la no-previsión legal en otros (así, por ejemplo, las universidades públicas), plantean problemas irresolubles si se mantiene la naturaleza reglamentaria de la disposición de creación del fichero.

Sobre la potestad reglamentaria y su remisión a las administraciones territoriales, véase García de Enterría, E. y Fernández, T. R., 2002: 188-189; Morell, 1998: 106-114; y Cobo, 2002: 330.

41. Sobre los actos administrativos generales o que tengan por destinatarios una pluralidad indeterminada de sujetos, véase García de Enterría, E. y Fernández, T. R. (2002: 548 y 572), y respecto de su diferencia con los reglamentos, los mismos autores (2002: 187-188).

En los ayuntamientos, el acto de aprobación del fichero corresponderá al alcalde, en aplicación de la cláusula residual de competencia [asignación al municipio y no atribución a otros órganos municipales, artículo 21.1.s) de la Ley 7/1985]; y en las diputaciones, al presidente, en aplicación de la regla análoga [artículo 34.1.o) de la Ley 7/1985].

La publicación de la creación, modificación o supresión del fichero deberá realizarse en el *Boletín Oficial de la Provincia* –BOP– (Ley 5/2002, de 4 de marzo, reguladora de los boletines oficiales de las provincias).

En relación con las indicaciones del fichero cabe señalar las siguientes opciones sobre:

–La *finalidad*, en el sentido que la definición sea adecuada, ni muy genérica, ni demasiado específica, puesto que determina y condiciona el uso posterior.

–La *estructura básica del fichero*, en el de que la descripción no emplee excesivos tecnicismos dado que su objeto es informar a los interesados.

–Los *tipos de datos*, con la sugerencia de que su referencia se agrupe por categorías (por ejemplo, de carácter identificativo, económico-financiero o de salud).

–Las *cesiones*, que deberán circunscribirse a aquellas que se prevean específicamente.

–El *responsable del fichero*, al respecto del cual proponemos que lo sea el alcalde (municipio) o el presidente (provincia), atribuida su condición de representante legal respectivo [Ley 7/1985, artículos 21.1.b) y 34.1.b)].<sup>42</sup>

–El *servicio o unidad ante los cuales pueden ejercerse los derechos*, sobre lo que consideramos conveniente una remisión al registro general de la entidad (Ley 30/1992, artículos 38.1 y 3).

#### 4.3.2. Competencias locales

Ya en la introducción hemos anticipado como factor relevante la atribución de capacidad y competencias generales a los municipios, lo que tiene como consecuencia práctica que ningún sector quede fuera de su ámbito de responsabilidad.

Efectivamente, la atribución de competencias a los municipios está regulada, esencialmente, en dos grupos normativos:

–El de la legislación general local, constituido por la Ley 7/1985 (artículos 1, 2, 25 a 28) y, en su caso, por la legislación autonómica (por ejemplo, en Cataluña, el

Texto refundido de la Ley municipal y de régimen local de Cataluña, aprobado por el Decreto legislativo 2/2003, de 28 de abril, artículos 9, 66 a 71 –TRLCat/2003–).

–El de la legislación sectorial aplicable a los diferentes ámbitos y materias.

Las diferentes previsiones que se contienen en estos grupos normativos sirven, a la vez, para garantizar la presencia de las autoridades municipales en el proceso de toma de decisiones y para fijar sus obligaciones y responsabilidades.

Sin que, obviamente, podamos detenernos en una especificación detallada de las competencias locales, sí interesa poner énfasis en su amplitud. Y así, por ceñirnos a la legislación general básica, hay que recordar que a los municipios (Ley 7/1985):

–Se les garantizan *competencias propias* en una larga lista de sectores y materias: desde la protección civil y la gestión urbanística, a la defensa de usuarios y consumidores, y pasando, entre otros muchos sectores, por las actividades culturales y la prestación de servicios sociales y de promoción y inserción social [Ley 7/1985, artículo 25.2, letras de la a) a la n)].

–Se les reconoce que puedan realizar *actividades complementarias* de las propias administraciones públicas y, en particular, las relativas a la educación, cultura, promoción de la mujer, vivienda, sanidad y protección del medio ambiente (Ley 7/1985, artículo 28).

Las obligaciones fijadas en tales previsiones son precisadas por la legislación sectorial (sobre urbanismo y vivienda, medio ambiente, sanidad, etc.), o incluso pueden ser ampliadas a otros sectores por la legislación autonómica general (tal es el caso del ya citado TRLCat/2003, que, en su artículo 66.2, reconoce competencia a los entes locales en nuevos ámbitos, tales como la *cohesión social*, las *infraestructuras de movilidad* y la *tecnología de la información y la comunicación*).

Y si, llegado el caso, quedara algún sector o parcela de la realidad social o económica no comprendida en los supuestos anteriores, es cuando entran en juego las previsiones sobre la *plena capacidad jurídica de las entidades locales* (Ley 7/1985, artículo 5) y que “el municipio, para la gestión de sus intereses y en el ámbito de sus competencias, puede promover toda clase de actividades y prestar cuantos servicios públicos contribuyan a satisfacer las necesidades y aspiraciones de la comunidad vecinal” (Ley 7/1985, artículo 25.1).

42. Como señala Vizcaíno (2001: 79), se trata de una identificación desde el punto de vista jurídico y no meramente técnico, de quien –citando a Davara– “tiene la capacidad de tomar decisiones sobre el objeto, utilización y fin del tratamiento o sobre el uso que se va a dar a los datos de carácter personal resultante del tratamiento o, en su caso, si van o no a ser cedidos” (la cita es de DAVARA, Miguel Ángel, *Guía práctica de protección de datos*. ASNEF. 1999, en Vizcaíno, 2001: 79).

Atribuir la figura del responsable a delegados del alcalde o del presidente de la Diputación conlleva el problema de tener que modificar el fichero

ro cuando se revoque la delegación o cambien las personas que las ostentan.

La identificación formal de la primera autoridad de la corporación local con la figura legal del responsable del fichero o tratamiento no excluye que se adopten otras medidas encaminadas a asegurar, materialmente, el conocimiento y la observancia de la LOPD en la organización. Así, en la Diputación de Barcelona se ha instituido la figura del *responsable de gestión*, que es el jefe de la unidad (normalmente, un servicio) que gestiona el fichero.

La amplitud, e incluso la *extensibilidad*, de las obligaciones y responsabilidades municipales tienen una consecuencia incontestable: califican como legítima la actuación del ayuntamiento que se desarrolle en los sectores o ámbitos en los que la legislación les atribuye competencia. Por otra parte, no hay que olvidar que las actuaciones municipales, en numerosas ocasiones, responden a demandas ciudadanas más o menos intensas, pero efectivas, de suerte que la *presión de la ciudadanía* actúa como mecanismo de fijación de las políticas públicas, lo que las legitima.

Y es en este punto donde engarzamos la problemática de la protección de datos personales y la legitimidad de todas las actuaciones municipales que se acometan en el marco de competencias reconocido por la legislación. Los puntos de fricción son frecuentes porque son muchos y variados los ámbitos y sectores en que se llevan a cabo dichas actuaciones municipales, que en la casi totalidad de supuestos tratan datos personales de esa ciudadanía a quien van destinadas.

La descripción de la problemática local quedaría incompleta si no pusiéramos de manifiesto cómo las ya señaladas características de amplitud y extensibilidad de la capacidad municipal tienen, además, unos efectos expansivos: definen también el ámbito de actuación de las diputaciones provinciales (y, en su caso, de los cabildos y los *consells insulars* y aquellas otras entidades previstas en la legislación autonómica),<sup>43</sup> que encuentran así la manera de cumplir las funciones asignadas legalmente de asistencia y cooperación con los ayuntamientos (Ley 7/1985, artículos 31 y 36, sobre competencias de las diputaciones), lo que, igualmente, también legitima sus actuaciones.

#### 4.4. Protección de datos de carácter personal y políticas públicas locales

Es obvio que, en nuestros días, cualquier actuación de cierta complejidad o duración que tenga que ver con personas en un número superior a las dos o tres decenas va a comportar, indefectiblemente, el uso de una herramienta de informática de gestión, desde el fichero más simple hasta la base de datos más sofisticada. Y en

tal caso nos hallaremos ya bajo la aplicación de la legislación de protección de datos personales.

Si esta constatación evidente la vinculamos con las reflexiones sobre las competencias locales realizadas en el apartado anterior, y todo ello lo ponemos en relación con la multiplicidad de entidades que integran el subsistema local,<sup>44</sup> es fácil deducir que el número de ficheros públicos locales será elevadísimo: varias decenas de miles.<sup>45</sup> Desde la perspectiva de la gestión de las políticas públicas en este subsistema habrá que atender, como es lógico, a los requerimientos derivados de la legislación sobre protección de datos de carácter personal. A continuación analizaremos algunos de los aspectos que pueden presentar cierta complejidad o incluso situaciones problemáticas.

##### 4.4.1. Observancia de las obligaciones formales establecidas

En primer lugar, dada la frecuencia con la que los diferentes servicios municipales recogen y tratan datos personales, deberán observarse previamente la serie de *obligaciones formales* establecidas. Entre las más significativas cabe destacar:

–En cualquier caso, proporcionar a los interesados la información definida y del modo establecido legalmente (“expreso, preciso e inequívoco” y referida dicha información a la existencia del fichero, a los derechos que les corresponden y al resto de los extremos detallados en la LOPD, artículo 5.1).

–Si se trata de datos especialmente protegidos (ideología, religión y los demás señalados en la LOPD, artículo 7), habrá que recabar el consentimiento expreso del afectado.

–Este consentimiento no será preciso si, tratándose de datos no especialmente protegidos, se recogen para el ejercicio de funciones propias del municipio en el ámbito de sus competencias (LOPD, artículo 6.2, primer inciso).

–Proceder a la tramitación y aprobación de la disposición general de creación del fichero y publicación en el BOP (LOPD, artículo 20).

–Cursar la notificación a la AEPD de la creación del fichero para su inscripción en el Registro General de Protección de Datos (LOPD, artículo 39; Real decreto 428/1993, artículo 24, y Real decreto 1332/1994, artículo 5).<sup>46</sup>

defensa de usuarios y consumidores, educación, sanidad, entre las más importantes); *participación y atención a la ciudadanía*; *registro de asociaciones*; *subvenciones, premios y becas*; *policía local* (infracciones de tráfico, grúa municipal, etc.), y *tributos y otros ingresos públicos* (desagregados o no en razón de los diferentes tipos de impuestos, tasas, contribuciones especiales, precios públicos y multas).

En datos referidos al año 2000, de los 31.057 ficheros públicos, 23.521 (el 75,7 %) correspondían al ámbito local (Paricio, 2002: 6).

En 2001, de los 31.805 ficheros públicos, 23.757 (el 74,65%) eran locales (Agencia Española de Protección de Datos, 2002: 29).

En 2002, de los 35.894 ficheros públicos, 24.121 (el 67,2%) eran locales (Agencia Española de Protección de Datos, 2003: 86)

46. Además, deberá notificarse, en el caso de que se hayan constituido, a la agencia autonómica respectiva, como sucede en la Comunidad de

43. Tal sería el caso de las comarcas en Cataluña (TRLCat/2003, artículos 84 a 86).

44. Como se recordará, los datos sobre esta multiplicidad los hemos ofrecido en el apartado I.2, letra c).

45. Desde el punto de vista material, y con carácter meramente indicativo, encontraremos ficheros sobre: *padrón municipal de habitantes*; *registro de documentos* (entrada y salida); *recursos humanos* (agregadas o no sus diferentes explotaciones: nómina, selección de personal, provisión de puestos de trabajo, control de incompatibilidades, salud laboral, formación, acción social, actividad sindical, entre otras); *contratación* (proveedores, registros de licitadores y de contratistas); *usuarios de servicios públicos* (abastecimiento de agua potable, instalaciones deportivas, servicios sociales, juventud, servicios funerarios, mercados municipales, bibliotecas, actividades culturales, transporte colectivo urbano, promoción y gestión de viviendas,

En los supuestos de modificación y supresión de ficheros, deberán seguirse las mismas formalidades observadas para su creación, y en estos últimos, además, se establecerá el destino de los ficheros o, en su caso, las previsiones que se adopten para su destrucción.

#### 4.4.2. Cumplimiento de las medidas de seguridad

Un segundo aspecto, menos conocido pero de gran trascendencia en la práctica, es el referido a la adopción y cumplimiento de las *medidas de seguridad* a que resultan obligados el responsable del fichero y, en su caso, el encargado del tratamiento. Esta obligación, prescrita en los artículos 9 y 44.3 h) de la LOPD/1999, ya venía recogida en la LORTAD/1992 [artículos 9 y 43.3.h)], y en desarrollo de la cual se dictó el Real decreto 994/1999, de 11 de junio, por el que se aprobó el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (RMS/1999). Declarado expresamente en vigor el RMS/1999 en todo lo que no se opusiera a la nueva ley (LOPD/1999, disposición transitoria tercera),<sup>47</sup> dicho reglamento tiene por objeto:

"[...] establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal."

Sobre la aplicación de estas medidas de seguridad, y poniendo el acento en el ámbito local, podemos destacar, en síntesis, los aspectos siguientes:<sup>48</sup>

a) Se trata de un asunto que tiene una dimensión doble: formal, en la medida que requiere la adopción de decisiones o la confección de documentos que deben plasmarse fehacientemente (así, por ejemplo, la elaboración e implantación del *documento de seguridad*, LOPD, artículo 8); y material, toda vez que exige la aplicación de medidas organizativas y físicas en el seno de la entidad.

b) El punto de partida lo constituye el tipo de datos contenidos en el fichero y la asignación de niveles de seguridad correlativos que establece el RMS/1999. Y así:

–En cualquier caso, todos los ficheros que contengan *datos personales* deberán adoptar las medidas de seguridad calificadas como de nivel básico (RMS, artículo 4.1).

–Si los datos contenidos se refieren a la *comisión de infracciones administrativas o penales, hacienda pública, servicios financieros o de información sobre solvencia patrimonial y crédito, o permiten obtener una evaluación de la personalidad del individuo*, los ficheros deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio (RMS, artículo 4.2 y 4).

–Si los ficheros contienen datos sobre *ideología, religión, creencias, origen racial, salud o vida sexual, así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas*, sus medidas deberán ser, además de las de nivel básico y medio, las calificadas de nivel alto (RMS, artículo 4.3).<sup>49</sup>

c) En función, pues, del tipo de datos habrá que elaborar e implantar el documento de seguridad según se trate de datos de nivel básico,<sup>50</sup> medio<sup>51</sup> o alto.<sup>52</sup>

Madrid (Ley 8/2001, de 13 de julio) y en la de Cataluña (Ley 5/2002, de 19 de abril).

47. Uno de los extremos que hay que entender modificado es el ámbito subjetivo del RMS, que no se circunscribe al responsable del fichero, sino que alcanza también al *encargado del tratamiento*, figura no contemplada en la LORTAD y sí en la LOPD/1999, y al que incluye, precisamente, en el artículo 9 sobre medidas de seguridad.

48. Entre las aportaciones más completas en relación con la protección de datos de carácter personal y, en particular, las medidas de seguridad hay que destacar la de Sibina Tomàs (1999).

49. La referencia a la *afiliación sindical* como dato que demanda medidas de nivel alto no se contiene, específicamente, en el artículo 4.3 del RMS/1999. Ello no obstante, no ha de haber ninguna duda sobre que es éste el nivel exigido, ya sea porque se trata de una especificación de la *ideología* o las *creencias* (sí detalladas en el citado artículo), ya porque la *afiliación sindical* se califica como dato especialmente protegido en la LOPD, artículo 7.2. En el mismo sentido, Vizcaino (2001:147-150), que, además, ofrece la explicación del porqué el RMS/1999 no la incluye en la relación: este reglamento, anterior en unos meses a la LOPD, sigue la enumeración que efectuaba la LORTAD/1992, que tampoco mencionaba, expresamente, la *afiliación sindical* como dato especialmente protegido en su artículo 7.

50. El documento de seguridad deberá contener, como mínimo, los siguientes aspectos de carácter básico (RMS, artículo 8.2):

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

51. Cuando los datos sean de nivel medio, el documento de seguridad, además de los señalados en la nota anterior, deberá contener:

a) Identificación del responsable o responsables de seguridad, con la función de coordinar y controlar las medidas de seguridad definidas (RMS, artículos 15 y 2.11).

b) Procedimientos de verificación del cumplimiento de las medidas de seguridad establecidas en el documento, tales como auditorías y otros controles periódicos (RMS, artículos 15 y 17).

c) Procedimientos y protocolos a seguir en relación con la gestión de soportes informáticos que contengan datos de carácter personal, su entrada y salida, su reutilización o destrucción (RMS, artículos 15 y 20).

d) Mecanismos y controles relativos a la autorización de personas para los accesos a los sistemas de información en los cuales se traten datos de carácter personal (RMS, artículo 18), y a los locales en que éstos se encuentran (RMS, artículo 19).

52. Cuando los datos sean de nivel alto, además de las medidas de nivel básico y medio descritas en el documento de seguridad, se adoptarán otras medidas sobre:

a") Distribución de soportes y telecomunicaciones mediante el cifrado de datos u otro mecanismo que garantice que la información no sea inteligible ni manipulable durante su transporte (RMS, artículo 23) o transmisión telemática (RMS, artículo 26).

d) El reglamento, pues, prescribe la obligación formal relativa al *documento de seguridad*: “[...] el responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y los sistemas de información” (RMS, artículo 8.1).

En el plano práctico, sin embargo, surgen dudas sobre la manera más conveniente de proceder: disponer de un solo documento de seguridad; de tantos como niveles de protección de los datos sean exigibles en función de las medidas de seguridad (niveles básico, medio y alto); o, en fin, de tantos documentos como ficheros se hayan creado, ya sean individualizados o agrupados.<sup>53</sup> Se trata de una decisión que ha de ponderar las ventajas y los inconvenientes, y responder también a la exigencia de que el documento de seguridad “deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo” (RMS, artículo 8.3).

En cualquier caso, tratándose de una administración pública y para garantizar su validez y eficacia, el documento de seguridad deberá ser aprobado “por el órgano competente ajustándose al procedimiento establecido” (Ley 30/1992, artículo 53.1), lo que en el ámbito de la Administración local nos lleva a considerar que:

–Su aprobación corresponderá al alcalde del ayuntamiento [Ley 7/1985, artículo 21.1.s)] o al presidente de la Diputación [Ley 7/1985, 34.1.o)], en aplicación de la cláusula residual de competencia.

–A diferencia de la disposición sobre creación, modificación o supresión de ficheros, el documento de seguridad no necesita ser publicado en un diario oficial, ni notificado a la Agencia Española de Protección de Datos.<sup>54</sup>

–Finalmente, las previsiones de ese documento pueden ser complementadas con otras actuaciones de la

entidad local, con grados diversos de formalización administrativa.<sup>55</sup>

e) Para cerrar el tema de la seguridad queremos insistir en que, además de la dimensión formal del documento, su aplicación conlleva una serie de medidas organizativas, que afectan al personal y al funcionamiento de la entidad, y también de orden físico y logístico (sobre locales, accesos, mobiliario, etc.). La efectiva implantación de tales medidas puede resultar más difícil de lo que, en principio, pudiera parecer, y, desde luego, suele tener un coste económico considerable.<sup>56</sup>

En cualquier caso, y como ya enfatizara Sibina (1999: 43 y 47), con remisión expresa a la STC 290/2000, de 30 de noviembre, la exigencia de tales medidas de seguridad podrá producir, en un primer momento, perplejidad, pero debe tomarse conciencia de que el sistema de protección de datos de carácter personal tiene un “carácter básicamente preventivo”, y el legislador, al dar cumplimiento al mandato contenido en el artículo 18.4 de la CE, “no ha querido [...] que la protección de datos personales frente al uso de la informática se lleve a cabo exclusivamente en la vía judicial, esto es, cuando ya se ha producido una lesión del derecho fundamental”, y de ahí “este carácter tuitivo o preventivo” (los párrafos entrecomillados se contienen en el fundamento jurídico 9, de la STC 290/2000, de 30 de noviembre, al hilo de la justificación de la atribución de funciones y potestades a la Agencia Española de Protección de Datos).

#### 4.4.3. Cesión y comunicación de datos en el ámbito de las administraciones públicas

El tema de la cesión y comunicación de datos de carácter personal es uno de los más complejos y controvertidos en la materia que estamos analizando. Trataremos por ello de sistematizar la explicación y fijar los principios o criterios generales aplicables.

##### a) Identificación y regulación.

b”) Registro de accesos, que, como mínimo, guardarán la siguiente información: identificación del usuario, fecha y hora en que se realizó, fichero accedido, tipo de acceso, autorización o no del acceso y registro accedido; en relación con esta información se elaborará un informe mensual por el responsable de seguridad (RMS, artículo 24).

c”) Copias de respaldo y recuperación, su conservación en lugar diferente de aquel en que se encuentran los equipos informáticos y con sus propias medidas de seguridad (RMS, artículo 25).

53. En la Diputación de Barcelona, sobre la base de que en el documento de seguridad se incluyen dos bloques de información, una general (sobre medidas, procedimientos, etc.), y otra específica del fichero, se ha optado por confeccionar un documento de seguridad por sistema de información que incluya las especificidades propias del sistema, remitiendo los aspectos comunes o generales a todos los niveles de protección a documentos externos o transversales que contemplen las exigencias referidas a cada aspecto concreto.

54. La página web de la APD informa de que no hay obligación de presentar el documento de seguridad en la Agencia, sino tan sólo tenerlo disponible por si les fuera requerido ([www.agenciaprotecciondatos.org/consulta12.htm](http://www.agenciaprotecciondatos.org/consulta12.htm), 25.8.2003).

55. Así, en la Diputación de Barcelona, por citar tres de 16 de mayo 2002, remitido a todo el personal y que incluye un epígrafe expreso sobre la materia); la inclusión de la cláusula sobre el *deber de secreto* en todos los contratos con terceros que traten datos personales y la referencia a ese mismo deber en los nombramientos de personal.

56. Lógicamente, las dificultades y los costes económicos ejemplos de actuaciones, mediante el *Manual del usuario de los sistemas de información* (aprobado por la Comisión de Gobierno en sesión son mayores en proporción directa al nivel de medidas de seguridad exigibles. Ciertamente, en las administraciones locales, los ficheros de nivel básico son numerosos, pero también lo son los de nivel medio (así, los tributarios o los que permitan una evaluación de la personalidad, como es el caso de los relativos al personal o sobre fomento del empleo). Finalmente, son bastante frecuentes en las entidades locales, y exigirán medidas de seguridad de nivel alto, ficheros como los de nóminas (por recoger el dato sobre el descuento de la cuota sindical o el de minusvalías para el cálculo de retenciones del IRPF de los empleados) y los que incluyan datos sobre la salud (del personal, sanidad, bienestar social, etcétera).

Pese a que *comunicación* y *cesión* de datos son términos susceptibles de ser diferenciados, lo cierto es que la LOPD/1999 los emplea como sinónimos para definir “toda revelación de datos realizada a una persona distinta del interesado” [artículo 3.i)].<sup>57</sup>

Sobre la base de esta definición tan amplia es evidente que la cesión o comunicación de datos en el ámbito de las administraciones públicas plantearán un cúmulo de cuestiones. Y ello, de un lado, por la propia configuración en clave de concurrencia de la mayoría de las competencias de las mismas, y, de otro, por el número tan elevado de entidades públicas en presencia.<sup>58</sup>

Se sigue de ello que tales entidades, para llevar a cabo sus cometidos, y como es lógico suponer, forzosamente han de entrar en contacto, hasta el punto de que puede afirmarse que *las relaciones interadministrativas o intergubernamentales* constituyen una cuestión crucial en un sistema político-administrativo tan complejo como el español.<sup>59</sup>

Con tales antecedentes no es de extrañar que los problemas sobre cesión o comunicación de datos de carácter personal se planteen en tres órdenes con características diferentes:

–Entre las administraciones públicas autónomas, esto es, la central, las autonómicas y las locales (municipios, provincias e islas).

–Entre las administraciones públicas matriz y sus personificaciones instrumentales (organismos autónomos, entidades públicas empresariales y el resto de las “vinculadas o dependientes de cualquiera de las Administraciones públicas”, por emplear los términos del artículo 2.2 de la Ley 30/1992).

–Y entre los órganos de una misma administración pública.

En relación, pues, con la cesión y comunicación de datos en el ámbito de las administraciones públicas, serán de aplicación las previsiones de la LOPD siguientes:

–Artículo 6.2, sobre excepciones a la necesidad del consentimiento en la recogida de datos, con especial referencia al supuesto del “ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias”.<sup>60</sup>

–Artículo 7, sobre datos especialmente protegidos.<sup>61</sup>

–Artículo 11.2, sobre excepciones a la necesidad del consentimiento en la comunicación de datos.<sup>62</sup>

–Artículo 21, sobre comunicación de datos entre administraciones públicas.<sup>63</sup>

57. Aparicio (2000: 117-124 y 218-220) trata profusamente este tema y pone de manifiesto cómo en el borrador de modificación de la LORTAD se distinguía la simple *comunicación* como “toda revelación de datos realizada a una persona distinta del interesado” (*op. cit.*: 122), de la *cesión*, “que se reservaría semánticamente al supuesto de comunicación de datos en que se otorgara al destinatario el poder de disposición del tratamiento” (*op. cit.*: 123), y de la diferente trascendencia en orden a las infracciones graves y muy graves. En el texto aprobado se equiparan ambas conductas a la que era la definición inicial de comunicación y la infracción será calificada de muy grave en la LOPD, artículo 44.4.b).

58. La tarea de *recuento* del número de entidades públicas no debería descuidarse. Hace años dábamos la cifra de 16.600 actores públicos locales (municipios, provincias, islas, consorcios, etc.), y sin haber podido contar los organismos autónomos y sociedades públicas locales no catalanas (Martínez-Alonso, 1999: 13). Si a ello añadimos las administraciones central y autonómicas, sus personificaciones instrumentales y el resto de las entidades (universidades, autoridades independientes, etc.), no parece que la cifra total pueda ser inferior a 20.000 personas jurídico-públicas.

59. Y de ahí que, en desarrollo del principio de coordinación (CE, artículo 103) y en correspondencia con esa complejidad, se articule un verdadero *modelo de relaciones interadministrativas o intergubernamentales*.

Cronológicamente, la primera formulación del modelo se incluye en la Ley 7/1985 (artículos 10 y 55 y siguientes) y pretende regular las relaciones entre las administraciones locales, de un lado, y las comunidades autónomas y el Estado (sus administraciones respectivas), de otro. La bondad y la funcionalidad del modelo explican que siete años después, la Ley 30/1992 (artículo 4 y siguientes) reproduzca su formulación y la generalice para las relaciones entre todas las administraciones. Sobre las exigencias, efectividad y análisis de dicho modelo nos remitimos a nuestro trabajo (Martínez-Alonso, 1998: 353-361).

60. Tales excepciones se han transcrito en la nota 32.

61. Dicho artículo prevé lo siguiente:

“1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

“Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

“2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

“3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

“4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

“5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

“6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

“También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.”

62. Se han transcrito en la nota 33.

63. Dicho artículo dispone:

“1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

–Artículo 4, sobre calidad de los datos.<sup>64</sup>

*b) Criterios sobre cesiones o comunicaciones de datos entre administraciones públicas.*

El punto inicial del análisis se centra en la exigencia de consentimiento previo del interesado. Es obvio que si lo presta en el momento de ser recogidos los datos por la Administración (cedente), o si lo hace con posterioridad, pero antes de que ésta los ceda o comunique a la otra (cesionaria), se habrán cumplido las exigencias legales (LOPD, artículo 11.1).<sup>65</sup>

Sucede, sin embargo, que la mayoría de las demandas para cesión o comunicación de datos entre administraciones no cuentan con el antecedente del consentimiento previo del interesado, bien porque no fueron previstas al recoger los datos, bien porque, aun siendo presumibles las peticiones de cesión o comunicación, no era posible obtenerlo con todas las garantías legales sobre consentimiento *informado*.<sup>66</sup> A su vez, acometer la tarea de requerir siempre el consentimiento de los interesados cada vez que otra Administración los solicita puede resultar problemático.<sup>67</sup>

Se comprenderá por todo ello que lo verdaderamente relevante es analizar los *criterios sobre cesiones o comunicaciones admitidas legalmente sin que el consentimiento sea preciso*. Tales criterios son los siguientes:

1.º. Para el ejercicio de competencias no diferentes o que versen sobre materias no distintas (LOPD, 21.1).

La formulación de este criterio responde al estricto tenor legal (transcrito en la nota 63), que al haberse construido en forma negativa hace muy difícil precisar, sin equívocos, su sentido.<sup>68</sup> Lo cual se ve agravado, además, por la lógica interpretación restrictiva que debe hacerse al tratarse de una excepción al principio general (consentimiento previo del interesado).

Con todas las cautelas señaladas, nos inclinamos por fijar el de la identidad material como el criterio más ajustado para admitir la cesión o comunicación entre administraciones públicas.<sup>69</sup> Como se ha señalado, “cen-

tra el contenido del artículo (21.1) la aplicación del principio de finalidad en la cesión de datos que sólo se autorizará entre diferentes administraciones públicas y sin consentimiento del interesado cuando coincidan las materias” (Freixas, 2001: 235).

Sobre el principio de finalidad, no obstante, hay que consignar un problema añadido, derivado de la modificación introducida por la LOPD. Concretamente, la LORTAD/1992, disponía que:

“Los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para *finalidades distintas* de aquellas para las que los datos hubieran sido recogidos” (artículo 4.2).

La LOPD/1999, en cambio, prevé que:

“Los datos de carácter personal objeto de tratamiento no podrán usarse para *finalidades incompatibles* con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos” (artículo 4.2).

Es obvio que las limitaciones eran mayores con la LORTAD, y de ahí que se haya subrayado que el cambio introducido por la LOPD “supone una mayor flexibilidad respecto de la prohibición de alteración de la finalidad, pues no se prohíbe el uso cuando exista una simple diferencia entre el objeto para la obtención y aquel al que finalmente se aplican los datos, sino que es necesario que dicha diferencia llegue a suponer una auténtica incompatibilidad de objetivos” (Aparicio, 2000: 97).

De todas formas, no parece que esa fórmula de la no-incompatibilidad de finalidades autorice a ir más allá, en relación con la cesión o comunicación de datos, de lo que resulta de la aplicación del criterio sobre identidad material que hemos propuesto.

2.º. Cuando la cesión esté autorizada en una ley [LOPD, artículo 11.2.a)].

Fue precisamente sobre la base de la infracción del principio de reserva legal respecto a la regulación de los límites de un derecho fundamental (CE, artículo 53.1),

“2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

“3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

“4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente ley.”

(El inciso en cursiva es el que fue anulado por la STC 292/2000).

64. Reseñado en el apartado 2.2, letra a).

65. “Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado” (LOPD, artículo 11.1).

66. Una referencia genérica sobre *cesión a otras administraciones públicas* no cumpliría el estándar requerido por el artículo 5 de la LOPD (*derecho de información en la recogida de datos*), y sería *materialmente* imposible

incluir todas las administraciones que pudieran tener competencias sobre la materia.

67. Ya sea en términos de tiempo de demora, o del coste económico que suponga para la Administración cedente, si es que no asumiera los gastos la cesionaria. Y todo ello, naturalmente, sin olvidar la incidencia de los principios de eficacia, economía y eficiencia que deben presidir la actuación de las administraciones públicas (CE, artículos 103 y 31, y Ley 30/1992, artículos 3 y 4).

68. Esta construcción proviene ya del artículo 19 de la LORTAD/1992, del cual se dijo que era “oscura, difícil, yo diría que atormentada (ya que) construir una frase en forma negativa dificulta siempre la comprensión, porque obliga a invertirla previamente para captar un sentido positivo” (González Pérez y González Navarro, 1999: 1072).

69. Como criterio de distribución de competencias entre el Estado y las comunidades autónomas, la Constitución se refiere, precisamente, a *materias* (artículos 148 y 149). Igual sucede en la atribución de competencias a los municipios (Ley 7/1985, artículo 25.2).



por lo que la STC 292/2000 anuló la posibilidad de comunicación de datos entre administraciones prevista en la disposición de creación del fichero o en norma de superior rango (la reglamentaria) que regulase su uso.

Como cesiones autorizadas legalmente cabe reseñar las siguientes:

2.º.1. Cesión de datos del padrón municipal de habitantes.

El artículo 16.3 de la Ley 7/1985 dispone lo siguiente:

“Los datos del Padrón Municipal se cederán a otras Administraciones públicas que lo soliciten sin consentimiento previo del afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. “También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, y en las leyes de estadística de las comunidades autónomas con competencia en la materia.”<sup>70</sup>

Esa previsión se complementa con la del artículo 17.3, último inciso, de la L 7/1985, que prevé:

“El Instituto Nacional de Estadística remitirá trimestralmente a los Institutos estadísticos de las comunidades autónomas u órganos competentes en la materia, y en su caso, a otras Administraciones públicas los datos

relativos a los padrones en los municipios de su ámbito territorial en los que se produzcan altas o bajas de extranjeros en las mismas condiciones señaladas en el artículo 16.3 de esta ley.”<sup>71</sup>

El padrón municipal de habitantes (PMH) y las cesiones y comunicaciones de que pueden ser objeto los datos personales que contiene son fuente frecuente de controversias. Su análisis desborda los límites de la presente contribución, en la que sólo podemos ofrecer unas consideraciones generales.<sup>72</sup> En cualquier caso hay que señalar que el PMH es un registro muy completo, tanto porque sus resultados agregados ofrecen el total de la población del Estado, como por los datos que de cada vecino se recogen en los respectivos padrones de todos y cada uno de los municipios españoles.<sup>73</sup> Además, todos los padrones han de ser gestionados informatizadamente, por el propio municipio titular o por la Diputación o la Administración cooperadora respectiva (Ley 7/1985, artículo 17.1), lo que optimiza las posibilidades de consulta.

Todo ello explica que desde siempre haya sido habitual que las administraciones y sus diferentes órganos se dirijan a los ayuntamientos formulando peticiones sobre datos de una, varias o colectivos de personas. Y, lógicamente, en estos casos se plantean los temas relativos a sus derechos (*intimidad, privacidad y autodeter-*

70. El artículo 16.3 contenía un párrafo más hasta su supresión por la Ley orgánica 14/2003, de 20 de noviembre, de reforma de diversas leyes, entre ellas la 7/1985. Dicho párrafo era del siguiente tenor:

“Fuera de estos supuestos, los datos del padrón son confidenciales y el acceso a los mismos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (después LOPD/1999) y en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.”

Esta modificación formaba parte del bloque de medidas adoptadas en relación con la legislación de extranjería, y pretendía “perfeccionar la información contenida en el Padrón Municipal relativa a los extranjeros empadronados” (LO 14/2003, Exposición de motivos, III, párrafo cuarto).

71. Este párrafo del artículo 17.3 de la L 7/1985 también fue modificado por la LO 14/2003, que ha fijado la remisión por el INE con carácter imperativo sustituyendo la previsión potestativa anterior.

72. Para el análisis pormenorizado nos remitimos a nuestros trabajos (Martínez-Alonso, 1998b y 2000) y a los recientes de Villaverde (2003 y 2003b). Las memorias anuales de la Agencia de Protección de Datos recogen consultas y otras informaciones sobre el PMH. Finalmente, con fecha 25.3.1998, por resolución conjunta de la presidenta del INE (Instituto Nacional de Estadística) y del director general para la Administración local del MAP (Ministerio de las Administraciones Públicas) se aprobaron unas *Instrucciones técnicas sobre cesión de datos del padrón municipal*, muy detalladas y precisas, por lo que son de mucha utilidad.

No nos consta que se publicaran en el BOE, por lo cual para su consulta hay que remitirse al INE o al MAP, si bien está también disponible en la web de la Diputación de Barcelona ([www.diba.es/padro](http://www.diba.es/padro), apartado “Normativa sobre gestión del padrón”, epígrafe “Consultas resueltas por el Consell d'Empadronament”, subepígrafe “Datos padronales: uso y cesión”).

73. Sobre la base de que “toda persona que viva en España está obligada a inscribirse en el Padrón del municipio en el que resida habitualmente”, según prescribe el artículo 15, primer inciso, de la Ley 7/1985, el artículo 16.2 de esta misma ley prevé:

“La inscripción en el padrón municipal contendrá como obligatorios los siguientes datos:

“a) Nombre y apellidos.

“b) Sexo.

“c) Domicilio habitual.

“d) Nacionalidad.

“e) Lugar y fecha de nacimiento.

“f) Número de documento nacional de identidad o, tratándose de extranjeros:

*Número de la tarjeta de residencia en vigor, expedida por las autoridades españolas o, en su defecto, número del documento acreditativo de la identidad o del pasaporte en vigor expedido por las autoridades del país de procedencia, tratándose de ciudadanos nacionales de estados miembros de la Unión Europea, de otros Estados parte en el Acuerdo sobre el Espacio Económico Europeo o de Estados a los que, en virtud de un convenio internacional se extienda el régimen jurídico previsto para los ciudadanos de los Estados mencionados.*

*Número de identificación de extranjero que conste en documento, en vigor, expedido por las autoridades españolas o, en su defecto, por no ser titulares de éstos, el número del pasaporte en vigor expedido por las autoridades del país de procedencia, tratándose de ciudadanos nacionales de Estado no comprendidos en el inciso anterior de este párrafo.”*

“g) Certificado o título escolar o académico que se posea.

“h) Cuantos otros datos puedan ser necesarios para la elaboración del Censo Electoral, siempre que se garantice el respeto a los derechos fundamentales reconocidos en la Constitución.”

El redactado del apartado f) se introdujo por la LO 14/2003 en sustitución de una escueta redacción anterior (*tratándose de extranjeros, el documento que sustituya el DNI*).

El reglamento que desarrolla la ley prevé que se podrán recoger, con carácter voluntario, los siguientes datos: el número de teléfono y la designación de las personas que pueden representar a cada vecino ante la Administración municipal a efectos padronales (artículo 57.2 del Reglamento de población y demarcación territorial de las entidades locales –RPD–, en la redacción dada por el Real decreto 2612/1996, de 20 de diciembre).

minación informativa) y a los límites de la cesión y la comunicación de datos.

Durante años el tema fue muy controvertido y fueron sucediéndose opiniones doctrinales divergentes, pronunciamientos jurisprudenciales diversos (de entre los que destaca la STS del 12 de noviembre de 1996, repertorio Aranzadi 7942), la modificación de la Ley 7/1985 en los artículos relativos al PMH (modificación operada por la Ley 4/1996, de 10 de enero), e, incluso, una resolución conjunta del Instituto Nacional de Estadística y del Ministerio de las Administraciones Públicas, de 25 de marzo de 1998, relativa a *Instrucciones técnicas sobre cesión de datos del padrón municipal*.<sup>74</sup> Nuevamente se ha abierto la controversia con motivo de la Ley orgánica 14/2003, de 20 de noviembre, que modifica diversas normas en la relación con la reforma de la legislación de extranjería.

Con carácter general podemos decir que, al amparo del supuesto que venimos analizando, la cesión o comunicación de datos del PMH a otras administraciones públicas deberá producirse en los términos estrictos del artículo 16.3 de la Ley 7/1985, anteriormente transcrito, y previa evaluación de la concurrencia de todos los requisitos (*sobre ejercicio de competencias y exclusivamente para asuntos en que la residencia o el domicilio sean datos relevantes*), siempre en referencia a, como máximo, un grupo determinado de personas (no caben las *cesiones masivas*) y sólo de los datos personales que sean necesarios para atender la solicitud de la Administración peticionaria.<sup>75</sup>

Con carácter específico, el último eslabón de modificaciones al respecto lo ha constituido la Ley orgánica 14/2003, que ha añadido a la L 7/1985 la siguiente previsión:

“Disposición adicional séptima. Acceso a los datos del padrón.

Para la exclusiva finalidad del ejercicio de las competencias establecidas en la Ley orgánica de derechos y libertades de los extranjeros en España y su integración social, sobre control y permanencia de extranjeros en España, la Dirección General de la Policía accederá a los

datos de inscripción padronal de los extranjeros existentes en los Padrones Municipales, preferentemente por vía telemática.

A fin de asegurar el estricto cumplimiento de la legislación de protección de datos de carácter personal, los accesos se realizarán con las máximas medidas de seguridad. A estos efectos, quedará constancia en la Dirección General de la Policía de cada acceso, la identificación de usuario, fecha y hora en que se realizó, así como de los datos consultados.

Con el fin de mantener actualizados los datos de inscripción padronal de extranjeros en los padrones municipales, la Dirección general de la Policía comunicará mensualmente al Instituto Nacional de Estadística, para el ejercicio de sus competencias, los datos de los extranjeros anotados en el Registro Central de Extranjeros.

Se habilita a los Ministros de Economía y del Interior para dictar las disposiciones que regulen las comunicaciones de los datos de los extranjeros anotados en el Registro Central de Extranjeros por medios electrónicos, informáticos o telemáticos al Instituto Nacional de Estadística.”

2º. Cesión o suministro de datos a la Administración tributaria.

Sobre la base del deber constitucional de contribución de todas las personas “*al sostenimiento de los gastos públicos de acuerdo con su capacidad económica*” (CE, artículo 31.1), la Ley general tributaria (LGT) prevé la obligación de ceder o suministrar datos a la Administración tributaria. En relación con la LGT hay que distinguir:

–El texto que se corresponde con la L 230/1963, de 28 de diciembre, con las modificaciones de que fue objeto, que mantiene su vigencia hasta el 30 de junio de 2004, y que regula tales obligaciones en sus artículos 111 y 112.

–El nuevo texto de la LGT aprobado por la L 58/2003, de 17 de diciembre, cuya entrada en vigor se produce el 1 de julio de 2004, que las regula en sus artículos 93 (“Obligaciones de información”)<sup>76</sup> y 94 (“Autoridades sometidas al deber de informar y colaborar”).<sup>77</sup>

74. Véase nota 72, inciso final.

75. Las dos últimas precisiones suponen sendas exigencias derivadas del principio de calidad de los datos (“adecuados, pertinentes y no excesivos”, LOPD, artículo 4.2).

76. En lo que interesa, el artículo 93 de la LGT (que reproduce sustancialmente el 111 del texto anterior) dice lo siguiente:

“1. Las personas físicas o jurídicas, públicas o privadas, así como las entidades mencionadas en el apartado 4 del artículo 35 de esta ley (*herencias yacentes, comunidades de bienes y demás entidades que, carentes de personalidad jurídica, constituyan una unidad económica o un patrimonio separado susceptible de imposición*), estarán obligadas a proporcionar a la Administración tributaria toda clase de datos, informes, antecedentes y justificantes con trascendencia tributaria relacionados con el cumplimiento de sus propias obligaciones tributarias o deducidos de sus relaciones económicas, profesionales o financieras con otras personas. [...]

2. Las obligaciones a las que se refiere el apartado anterior deberán cumplirse con carácter general en la forma y plazos que reglamentariamente se

determinen, o mediante requerimiento individualizado de la Administración tributaria que podrá efectuarse en cualquier momento posterior a la realización de las operaciones relacionadas con los datos o antecedentes requeridos. [...]

77. En lo que interesa, el artículo 94 de la LGT (que reproduce sustancialmente el 112 del texto anterior) dice lo siguiente:

“1. Las autoridades, cualquiera que sea su naturaleza, los titulares de los órganos del Estado, de las comunidades autónomas y de las entidades locales; los organismos autónomos y las entidades públicas empresariales; las cámaras y corporaciones, colegios y asociaciones profesionales; las mutualidades de previsión social; las demás entidades públicas, incluidas las gestoras de la Seguridad Social y quienes, en general, ejerzan funciones públicas, estarán obligados a suministrar a la Administración tributaria cuantos datos, informes y antecedentes con trascendencia tributaria recabe ésta mediante disposiciones de carácter general o a través de requerimientos concretos, y a prestarle, a ella y a sus agentes, apoyo, concurso, auxilio y protección para el ejercicio de sus funciones. [...]

Los términos en que se recogen esas obligaciones de cesión y suministro de datos a la Administración tributaria son amplios y su régimen es especial, privilegiado si se quiere, pero en todo caso articulado para asegurar ese “*sistema tributario justo inspirado en los principios de igualdad y progresividad*”, del que habla la Constitución (artículo 31.1).

2º.3. Cesión o suministro de datos de la Administración tributaria a otros destinatarios públicos.

También la LGT prevé la cesión o el suministro de datos de la Administración tributaria en favor de otras administraciones tributarias y destinatarios públicos (órganos jurisdiccionales, ministerio público, Inspección de Trabajo y Seguridad Social, etcétera).<sup>78</sup>

3º. Cesiones a destinatarios públicos cualificados [LOPD, artículo 11.2.d)].

La propia LOPD/1999 detalla una relación de destinatarios públicos cualificados a los cuales deberán cederse o comunicarse los datos de carácter personal que soliciten, y sin que obviamente sea necesario el consentimiento previo de los interesados.

Dichos destinatarios son [LOPD, artículo 11.2.d)]: el Defensor del Pueblo y el Tribunal de Cuentas (y las ins-

tituciones autonómicas respectivas con funciones análogas), el Ministerio Fiscal, los jueces y los tribunales.

4º. Cesión para el tratamiento posterior con fines históricos, estadísticos o científicos [LOPD, artículos 11.2.e) y 21.1].

La autorización para la cesión o comunicación entre administraciones públicas para el tratamiento posterior con fines históricos, estadísticos o científicos se incluye, con una formulación idéntica, en dos artículos: el 11.2.e) y el 21.1, inciso final.

Estas previsiones se complementan con la que, en relación con el principio de calidad de los datos y su cancelación, se recogen en el artículo 5, párrafo tercero, de la LOPD:

“Reglamentariamente se determinará el procedimiento por el que, *por excepción*, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos” (la cursiva es nuestra).

Desde la perspectiva de la legislación de protección de datos de carácter personal esa excepción a la cancelación parece lógica. En cambio, el criterio es justamente el contrario si el tema se analiza a la luz de la legisla-

5. La cesión de datos de carácter personal que se deba efectuar a la Administración tributaria conforme a lo dispuesto en el artículo anterior, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito no será de aplicación lo dispuesto en el apartado 1 del artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.”

78. El artículo 95 (“Carácter reservado de los datos con trascendencia tributaria”) de la LGT, texto aprobado por la L 58/2003 (y que reproduce el 113 del texto anterior, si bien lo amplía con nuevas previsiones sobre cesiones), dice lo siguiente:

“1. Los datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada y para la imposición de las sanciones que procedan, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión tenga por objeto:

a) La colaboración con los órganos jurisdiccionales y el Ministerio Fiscal en la investigación o persecución de delitos que no sean perseguibles únicamente a instancia de persona agraviada.

b) La colaboración con otras Administraciones tributarias a efectos del cumplimiento de obligaciones fiscales en el ámbito de sus competencias.

c) La colaboración con la Inspección de Trabajo y Seguridad Social y con las entidades gestoras y servicios comunes de la Seguridad Social en la lucha contra el fraude en la cotización y recaudación de las cuotas del sistema de Seguridad Social, así como en la obtención y disfrute de prestaciones a cargo de dicho sistema.

d) La colaboración con las Administraciones públicas para la lucha contra el delito fiscal y contra el fraude en la obtención o percepción de ayudas o subvenciones a cargo de fondos públicos o de la Unión Europea.

e) La colaboración con las comisiones parlamentarias de investigación en el marco legalmente establecido.

f) La protección de los derechos e intereses de los menores e incapacitados por los órganos jurisdiccionales o el Ministerio Fiscal.

g) La colaboración con el Tribunal de cuentas en el ejercicio de sus funciones de fiscalización de la Agencia Estatal de Administración Tributaria.

h) La colaboración con los jueces y tribunales para la ejecución de resoluciones judiciales firmes. La solicitud judicial de información exigirá resolución expresa en la que, previa ponderación de los intereses públicos y privados afectados en el asunto de que se trate y por haberse agotado los demás medios o fuentes de conocimiento sobre la existencia de bienes y derechos del deudor, se motive la necesidad de recabar datos de la Administración tributaria.

i) La colaboración con el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, con la Comisión de Vigilancia de Actividades de Financiación del Terrorismo y con la Secretaría de ambas comisiones, en el ejercicio de sus funciones respectivas.

j) La colaboración con órganos o entidades de derecho público encargados de la recaudación de recursos públicos no tributarios para la correcta identificación de los obligados al pago.

k) La colaboración con las Administraciones públicas para el desarrollo de sus funciones, previa autorización de los obligados tributarios a que se refieran los datos suministrados.

2. En los casos de cesión previstos en el apartado anterior, la información de carácter tributario deberá ser suministrada preferentemente mediante la utilización de medios informáticos o telemáticos. Cuando las Administraciones públicas puedan disponer de la información por dichos medios, no podrán exigir a los interesados la aportación de certificados de la Administración tributaria en relación con dicha información.

3. La Administración tributaria adoptará las medidas necesarias para garantizar la confidencialidad de la información tributaria y su uso adecuado.

Cuantas autoridades o funcionarios tengan conocimiento de estos datos, informes o antecedentes estarán obligados al más estricto y completo sigilo respecto de ellos, salvo en los casos citados. Con independencia de las responsabilidades penales o civiles que pudieran derivarse, la infracción de este particular deber de sigilo se considerará siempre falta disciplinaria muy grave.

Cuando se aprecie la posible existencia de un delito no perseguible únicamente a instancia de persona agraviada, la administración tributaria deducirá el tanto de culpa o remitirá al Ministerio Fiscal relación circunstanciada de los hechos que se estimen constitutivos de delito. También podrá iniciarse directamente el oportuno procedimiento mediante querrela a través del Servicio Jurídico competente.

4. Los retenedores y obligados a realizar ingresos a cuenta sólo podrán utilizar los datos, informes o antecedentes relativos a otros obligados tributarios para el correcto cumplimiento y efectiva aplicación de la obligación de realizar pagos a cuenta. Dichos datos deberán ser comunicados a la Administración tributaria en los casos previstos en la normativa propia de cada tributo.

Salvo lo dispuesto en el párrafo anterior, los referidos datos, informes o antecedentes tienen carácter reservado. Los retenedores y obligados a realizar ingresos a cuenta quedan sujetos al más estricto y completo sigilo respecto de ellos.”

ción de protección del patrimonio cultural, en la medida en que se prescribe la conservación de cualesquiera documentos producidos por las administraciones públicas y atendido que en la definición de los mismos se incluyen los recogidos “en cualquier tipo de soporte material”, “incluso los soportes informáticos” (Ley estatal 16/1985, de 25 de junio, del *patrimonio histórico español*, artículos 1.2, 49 y 52; y leyes catalanas 9/1993, de 30 de septiembre, del *patrimonio cultural catalán*, artículos 19 y 21, y 10/2001, de 13 de julio, de *archivos y documentos*, artículo 7).

5º. Cesión de datos de carácter personal necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar estudios epidemiológicos de acuerdo con la legislación sobre sanidad (LOPD, artículo 11.2.1).

Como supuesto de cesión de datos entre administraciones públicas que no precisa del consentimiento del interesado se encuentra también el de que sea necesaria para solucionar una urgencia o realizar estudios epidemiológicos [LOPD, artículo 11.2.f)].

Se trata de un supuesto específico, bien que, no obstante, hay que ponerlo en relación con:

–El resto de las previsiones de la LOPD sobre la materia, entre las que destacan las de los artículos 6.2 (“proteger un interés vital del interesado”), 7 (“datos especialmente protegidos”, apartados 2, 3 y 6) y 8 (“datos relativos a la salud”).

–La legislación sobre sanidad, autonómica y estatal, de entre la que cabe destacar, en Cataluña, la Ley 7/2003, de 25 de abril, de protección de la salud, y las leyes estatales 41/2002, de 14 de noviembre, *básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica*, y 16/2003, de 28 de mayo, *de cohesión y calidad del Sistema Nacional de Salud* (especialmente, el capítulo V, *del sistema de información sanitaria*, artículos 53 a 58).

Atendida la complejidad de la materia nos limitamos a consignar el supuesto y a remitirnos a los estudios especializados.

6º. Comunicación de datos de carácter personal que una Administración obtenga o elabore con destino a otra (LOPD, 21.2 y 4).

La comunicación de datos entre dos administraciones públicas no requiere el consentimiento del interesado en el supuesto de que una de ellas (cedente) obtenga o elabore los datos con destino a la otra (cesionaria). Es evidente que en este caso, previsto en el artículo 21.2 de la LOPD, habrá un antecedente previo de colaboración

entre administraciones, que tendrá su correspondiente amparo normativo y, eventualmente, una formulación documental (convenio de delegación o encomienda de gestión, por ejemplo).

La concurrencia de tales circunstancias y condiciones son las que legitiman la recogida, elaboración y tratamiento de datos de carácter personal (LOPD, 4.1), y su comunicación entre cedente y cesionaria (LOPD, 21.2 y 4).

7º. Otras cesiones previstas con carácter general.

Previstas con carácter general, y, por tanto, susceptibles de aplicarse a las cesiones de datos entre administraciones públicas podemos reseñar los supuestos de:

–Datos recogidos de fuentes accesibles al público [LOPD, artículo 11.2.a) en relación con el 3.j)].

–Tratamiento de datos que responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros –en el caso que tratamos– de otra administración pública, y en el bien entendido que la comunicación será legítima en cuanto se limite a la finalidad que la justifique [LOPD, artículo 11.2.d)].

*c) Cesiones o comunicaciones de datos en el seno de una administración pública.*

Si el tema de las *cesiones o comunicaciones de datos de carácter personal* entre administraciones públicas resulta problemático, no lo es menos el relativo a las que se producen *en el seno de una administración pública*, esto es, *entre órganos de una misma administración*.

El principal factor que provoca las dudas lo constituye la falta de previsión expresa de la ley, a diferencia de lo que sucede entre administraciones públicas según hemos visto en el apartado anterior. De manera que la no-regulación de la cesión o comunicación de datos *intra-administrativa* deja la cuestión abierta, y a partir de ahí, los autores se manifiestan de maneras divergentes e, incluso, antagónicas.

Lo cierto es que el tema tampoco estaba resuelto con la LORTAD/1992, lo que dio pie a que se afirmara que “la ley no regula expresamente la cesión entre órganos de la misma Administración Pública, por lo que, en principio, parece deducirse que ello estaría permitido” (Del Peso y Ramos, 1994: 132). Ya vigente la LOPD, Freixas (2001: 235-237), tras poner de manifiesto la no-regulación específica y examinar las alternativas (aplicación de los artículos 11.1 y 21.1), se decanta por los argumentos que apoyan la cesión.<sup>79</sup>

79. Su argumentación merece ser reproducida de manera textual:

“Dos son las soluciones que se pueden dar a las cesiones entre órganos de una misma administración. La primera, y a falta de una regulación específica, la aplicación del artículo 11 de la LOPDCP, que regula la comunicación de datos de una manera general. Como hemos analizado en el capítulo 7, dicha cesión a un tercero requerirá el consentimiento del interesado y el

cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario. La segunda, entender que las limitaciones a las cesiones de datos con relación a competencias distintas sólo se aplican en los casos en que las administraciones públicas sean diferentes, por lo que nada impedirá que esta cesión se efectúe sin ningún tipo de requisito previo entre órganos de una misma administración.

En cambio, Vizcaíno (2001: 237-239) rechaza tajantemente que el “aparente olvido de las cesiones entre órganos de la misma Administración [signifique] que la ley lo admite en forma indiscriminada” (*op. cit.*: 237), y apela para ello al propio espíritu (restrictivo) y finalidad (defensa de la privacidad e intimidad de los ciudadanos) de la LOPD.<sup>80</sup>

*d) Necesidad de esclarecer los requisitos de las comunicaciones y las cesiones de datos en el ámbito de las administraciones públicas.*

La revisión que hemos efectuado en los apartados anteriores pone al descubierto la problemática en torno a las comunicaciones y las cesiones en el ámbito de las administraciones públicas. Son demasiadas las dudas que se plantean sobre los requisitos que deben cumplir las demandas que unas formulan, así como sobre los límites y las garantías que han de observar las destinatarias de las mismas para atenderlas. Y lo mismo puede decirse respecto de las cesiones y comunicaciones en el seno de una administración, entre sus órganos, y que, como es de suponer, adquiere unos perfiles más acusados a medida que disminuyen sus dimensiones.

Y en esa problemática no sólo cuenta la disyuntiva sobre el juicio legal acerca de si una cesión o comunicación concreta de datos debe admitirse o no, sino también –¡y mucho!– el *riesgo* del error, susceptible de ser calificado como infracción muy grave *ex* LOPD, artículo 44.b).

No creemos que se nos pueda tachar de alarmistas si reseñamos que los equívocos sobre estos temas están añadiendo tensiones a las relaciones interadministrativas y también en el seno de las propias administraciones. Y lo peor de todo es que pueden generar tendencias a la *estanquidad* y a la no-cooperación, justo lo contrario de lo que demandan los principios de coordi-

nación administrativa y lealtad institucional (CE, artículo 103, y Ley 30/1992, artículos 3 y 4).

La conclusión que se desprende de todo ello apunta claramente a la necesidad de esclarecer, con carácter general, los requisitos de las comunicaciones y las cesiones de datos de carácter personal en el ámbito de las administraciones públicas. En este sentido creemos que podría resultar muy útil distinguir los supuestos de comunicación y cesión de datos, en la línea propuesta por Aparicio (2000: 117-124 y 218-220). Y, en esta dirección, mantener la definición de *comunicación* como “toda revelación de datos realizada a una persona distinta del interesado” (*op. cit.*: 122), diferenciándola de la *cesión*, “que se reservaría semánticamente al supuesto de comunicación de datos en que se otorgara al destinatario el poder de disposición del tratamiento” (*op. cit.*: 123).

En el ámbito de las administraciones públicas deberían fijarse los requisitos, los límites y las garantías de las comunicaciones de datos, de un lado, y de las cesiones, de otro, y en el bien entendido que el nivel de exigencia en éstas habría de ser superior, obviamente, al de aquéllas. Creemos, asimismo, que el principio de finalidad en la recogida y el tratamiento de los datos debe servir de criterio en este ámbito, vinculándolo con el de la identidad material en el ejercicio de competencias de las administraciones públicas, y con el principio de confianza legítima como deber de actuación de éstas en sus relaciones con la ciudadanía (*ex* artículo 3.1, *in fine*, de la L 30/1992). Finalmente, todas esas tareas de delimitación y precisión de las condiciones de las comunicaciones y las cesiones de datos deberían consignarse en la ley, preferentemente en la propia LOPD, que, como se recordará, tiene el carácter de ley ordinaria en lo relativo, entre otros, a los preceptos sobre *ficheros de titula-*

“Si defendemos la primera de las interpretaciones estaremos estableciendo, para la cesión de datos entre órganos de una misma administración, un requisito adicional, el consentimiento del interesado, que no se exige en la comunicación de datos entre distintas administraciones públicas con competencias o materias coincidentes. Si defendemos la segunda interpretación, estaremos deslegalizando la comunicación de datos entre órganos de una misma administración, lo que podría vulnerar algunos derechos que la ley otorga a los afectados.

“La discusión está pendiente de que se plantee alguna controversia y así ver avanzar alguna solución judicial a esta problemática. Pero pienso que tiene difícil aceptación que a la comunicación de datos entre órganos de una misma administración se le apliquen los criterios generales del artículo 11 de la LOPDCP que limita ésta cuando intervengan terceros. No es éste el caso porque las administraciones públicas tienen personalidad jurídica única y están constituidas por órganos jerárquicamente ordenados. Por ello, no cabe interpretar, en mi opinión, que órganos de una administración pública tengan la consideración de terceras personas con relación a otros órganos de la misma administración y que, por este motivo, la comunicación de datos está sujeta al régimen general del artículo 11 de la LOPDCP.

“En este sentido, tampoco hemos de olvidar que el principio de eficacia que ha de regir las actuaciones de las administraciones públicas previsto en el artículo 103 de la CE comporta evitar al máximo la duplicidad de actuaciones. Por ello, carece de sentido que unos datos obtenidos por un órgano de una administración con competencias diferentes, obliguen a otro órgano

de la misma administración a crear unos datos que ya constan en un fichero. Es cierto que se podría crear otro fichero con los mismos datos con lo que no se produciría ninguna problemática en este aspecto. Pero ello, supondría un coste en tiempo y recursos económicos importantes y una actuación innecesaria. Por otro lado, si una administración pública puede obtener o elaborar datos con destino a otra, tal y como analizaremos en el punto siguiente sin consentimiento del interesado ¿qué sentido tiene que órganos de una misma administración no se puedan ceder datos?” (Freixas, 2001: 235-237).

80. A nuestro entender, sin embargo, el corolario de su argumentación acaba restringiendo en exceso el propio sentido de la cesión entre administraciones públicas *ex* artículo 21.1 de la LOPD:

“Dicho en otros términos. *A sensu contrario*, la norma permite la comunicación de datos personales de los administrados entre administraciones públicas para el ejercicio de competencias iguales o de competencias que versen sobre las mismas materias, pero ello, lógicamente, sólo puede entenderse, con naturalidad, *en la órbita de una misma Administración*.

“En consecuencia, puede concluirse razonablemente que para que los datos personales sean comunicados a órganos o entidades distintas del responsable del fichero, aun dentro de una misma Administración es necesario que la comunicación tenga por finalidad *el ejercicio de iguales competencias en las mismas materias* (lo cual sólo puede entenderse con naturalidad *en el seno de una misma Administración*).” (Vizcaíno, 2001: 238, las cursivas son nuestras).

*ridad pública* (artículos 20 a 24, en relación con la disposición final segunda de la LOPD/1999).

## 5. Condicionantes a la gestión pública local desde el ámbito de la normativa de las propiedades y los bienes inmateriales

### 5.1. Consideraciones preliminares

En este contexto en que nos movemos, aquende las lejanas atalayas de los despachos decisorios en las grandes administraciones públicas gubernamentales, que es el de proximidad o inmediatez de la gestión municipal, y, por extensión, toda la local, la presente contribución tiene por objeto aportar una reflexión sobre algunos de los condicionantes que se vienen planteando con insistencia creciente a esta gestión desde las exigencias de la evolución normativa sobre las propiedades y bienes inmateriales.

Los citados derechos y bienes incorporeales han sido frecuentemente olvidados en nuestra tradición jurídica y política por el lamentable lastre de una herencia, y aún realidad presente, de falta de cultura democrática y de concienciación colectiva de respeto a los valores genuinos de la creatividad y de su contribución al progreso social, inercia que afronta actualmente un nuevo reto en la adaptación forzada al último gran cambio tecnológico en los medios de tratamiento y transmisión de la información. Es, pues, tiempo de situar a los gestores locales ante la deuda histórica de asumir plenamente las implicaciones de los derechos de autor y el valor esencial del derecho de acceso a la información pública que gestionan, este último como barómetro fiel del grado real de democratización de nuestra sociedad.

### 5.2. Derechos inmateriales de autoría intelectual

Consideramos, como punto de partida, una realidad de gestión local cuyos agentes dinamizadores, en el marco de esta función pública, no sólo manejan grandes flujos de información de la propia entidad, de otras ajenas y, sobre todo, de los ciudadanos particulares y personas jurídicas privadas que acuden a este nivel de administración, sino que instrumentan de manera creciente su actividad de gestión sobre estos activos informacionales mediante servicios y técnicas tales como, entre otros muchos:

a) Creación de bases de datos (BD) en línea, que se constituyen en auténticos portales o centros de documentación pública telemática, contratación de empresas externas para su implementación de contenidos y para su mantenimiento técnico, y participación en la creación de BD transnacionales en el marco de las redes y asociaciones de cooperación internacional legitimadas por la Carta Europea de la Autonomía Local (CEAL).

b) Contratación de la realización de aplicaciones informáticas a medida para la difusión de los propios activos.

c) Contratación de la producción de contenidos de índole técnica, social, cultural, etc., de autoría individual, colectiva, o mediante fórmulas de colaboración plural, para su posterior edición digital.

d) Coproducción y gestión de exposiciones en régimen de itinerancia entre museos municipales, así como la gestión de éstos mismos y de sus archivos.

e) Programación y realización de programas de formación pública y profesional continuada de los propios recursos humanos, con su corolario de contratación de profesores. La multiplicidad de las formas aquí relacionadas a título indicativo no puede en ningún modo velar un común denominador a todas ellas en su imbricación con los derechos de autor.

#### 5.2.1. El uso imperativo de los instrumentos contractuales

La normativa general de contratación de las administraciones públicas clasifica los negocios jurídicos “sobre propiedades incorporeales” en el ámbito residual de “los restantes contratos”, aquellos que, en el contexto de una heterogénea lista indicativa, considera como privados (TRLCAP, artículo 5.3). La exigencia de formalización expresa y escrita de toda cesión de derechos de explotación económica de la propiedad intelectual (Real decreto legislativo 1/1996, de aprobación del Texto refundido de la Ley de la propiedad intelectual –TRLPI, en adelante–, artículos 43 y 45), sumada al incremento exponencial descrito en el punto anterior de actividades públicas locales con implicaciones de derechos de autoría, exige poner de relieve las consecuencias prácticas del no-seguimiento de aquella exigencia.

La experiencia de gestión en el ámbito de las unidades administrativas operativas de los entes locales, las mismas que dinamizan su actuación con la modernización instrumental técnica descrita, evidencia aún, desde la perspectiva del observatorio permanente que son las administraciones cooperadoras de segundo grado, un cierto déficit en la concienciación de sus recursos humanos sobre la necesidad de hacer uso de los instrumentos contractuales para el correcto tratamiento de los derechos de explotación de autor en toda nueva adquisición o encargo de contenidos y flujos informativos que impliquen creatividad en su generación por parte de terceros y que hayan de integrarse como un elemento o *input* en los circuitos de gestión pública de aquéllas (se constata el mismo déficit a escala de la AGE en MAP, 2003: 14).

La correcta aplicación del imperativo legal citado es de la máxima importancia puesto que su corolario es que no se puede considerar tener adquirido ningún derecho de explotación de propiedad intelectual que no conste documentado expresamente por escrito y de

manera circunstanciada en cuanto a las formas y modalidades cedidas, así como al ámbito territorial y temporal de tal cesión, en un contrato, convenio o acuerdo de cesión otorgado por el/los autor/es.

La recomendación a efectuar a los gestores locales en este sentido se centraría en la conveniencia de maximizar el privilegio legal otorgado a las administraciones públicas de instrumentar, mediante sus pliegos, contratos de condiciones generales de adhesión con prerrogativas exorbitantes de Derecho público, como manera de anticipar un tipo de cesión expresa de derechos en los términos y extensión perseguidos en el redactado de sus pliegos de cláusulas administrativas de contratación de los servicios o consultorías de creación de nuevos contenidos/formas. La sugerencia aquí formulada se extiende, naturalmente, a aquellos casos de procedimiento de contrato menor por razón de su cuantía (no superior a 12.020,24 euros), que estadísticamente concentran la mayor parte de este tipo de consultorías/cesiones.

### 5.2.2. Limitaciones en las facultades de la propiedad de los soportes de las obras

Existe una doble limitación, activa y pasiva, sobre las posibilidades de actuación de los titulares dominicales de los soportes materiales en que se plasman las obras protegibles por el derecho de autor:

1.ª. El adquirente de la propiedad del soporte al cual se haya incorporado la obra no tiene, por este sólo título, ningún derecho de explotación sobre aquella excepto el de su exposición pública si es una obra de artes plásticas o de fotografía (TRLPI, artículo 56).

2.ª. Los derechos morales del autor, y, por lo tanto, irrenunciables e inalienables, de: a) acceso al ejemplar único o raro de la obra, cuando se encuentre en poder de otro, a fin de ejercitar el derecho de divulgación o cualquier otro que le corresponda (TRLPI, artículo 14.7), y b) retirar la obra del comercio, por cambio de sus convicciones intelectuales o morales, previa indemnización de daños y perjuicios a los titulares de derechos de explotación (TRLPI, artículo 14.6).

Esta doble limitación tiene una incidencia directa en la gestión pública local de la difusión cultural, y, muy notablemente, en los ámbitos museístico y archivístico. Cabe, no obstante, apreciar que el mencionado derecho de acceso no permitirá exigir el desplazamiento de la obra y el acceso a la misma se llevará a efecto en el lugar y forma que ocasionen menos inconvenientes al poseedor, al que se indemnizará, en su caso, por los daños y perjuicios que se le irroguen. En un estadio preventivo, la recomendación de obligado cumplimiento es la previsión contractual expresa de la adquisición de los derechos de explotación de la obra junto con la adquisición de la propiedad del soporte al cual se incorpora ésta.

### 5.2.3. Los niveles de protección de las BD

La trascendencia del régimen jurídico de las BD para el propósito de la presente ponencia radica en el hecho conjunto de que, como se apreció en la nota introductoria de la misma, constituyen ya hoy en día una de las manifestaciones más relevantes de la actividad informativa sociocultural en general y de las administraciones públicas en particular, y de que las páginas web públicas locales (y, por tanto, de los llamados "portales" y "centros de documentación" electrónicos) revisten la consideración legal de BD. Se colige de ello la necesidad de tener en cuenta los diferentes niveles de protección de los elementos de éstas en la contratación de su elaboración o del arrendamiento (licencia de cesión de uso) de las ya creadas por terceros con carácter previo. Existe un cuádruple nivel de protecciones acumuladas, independientes y compatibles entre sí:

a) Protección mediante las modalidades de explotación económica del derecho de autor (reproducción, distribución, comunicación pública y transformación), protección referida exclusivamente a su estructura en tanto que forma de expresión de la selección o disposición de sus contenidos, pero no de éstos en sí mismos (TRLPI, artículo 12.1).

b) Protección mediante el llamado derecho *sui generis* sobre las BD: se confiere amparo a la inversión substancial realizada por el fabricante o productor de la BD, evaluada en términos cuantitativos o cualitativos, por un período de quince años desde la finalización del proceso de fabricación, renovables en caso de una transformación que suponga una nueva inversión substancial (TRLPI, artículo 133 y siguientes). Se mantiene aquí también la excepción relevante de las extracciones para fines ilustrativos de enseñanza o de investigación científica en la medida justificada por el objetivo no comercial que se persiga y siempre que se indique la fuente.

c) Protección mediante el régimen del derecho de autor sobre los programas de ordenador (TRLPI, artículo 95 y siguientes) para los que se usen en la fabricación y/o funcionamiento de BD accesibles por medios electrónicos ("en línea") (TRLPI, artículo 12.3).

d) Se ha de recordar en último término la independencia y compatibilidad de los tres niveles anteriores respecto a la protección mediante el derecho de autor u otros derechos previos de propiedad intelectual sobre los contenidos de la BD, además de los eventuales derechos también previos de propiedad industrial (véase *infra*, 5.3), derecho de la competencia, derecho contractual, protección del secreto empresarial/industrial, de los datos que encierran la privacidad personal, del patrimonio cultural-documental público, del acceso a los documentos públicos y de la tutela pública del derecho de acceso a la cultura (Directiva 2001/29/CE, artículo 9; TRLPI, artículos 137 y 40). Es, en razón de esta compatibilidad, recomendable a los gestores locales que gene-

ralicen la práctica de la inclusión en sus páginas web en internet de un punto de atención o “aviso legal” de exención de responsabilidad por las informaciones o contenidos provenientes de terceros que consten en ella directamente o por remisión de enlace telemático, así como por el eventual uso que los terceros hagan de las informaciones contenidas en la página.

### 5.3. Derechos inmateriales de propiedad industrial

Por contraste con los derechos inmateriales de propiedad intelectual, interesa poner de relieve que en los de propiedad industrial sí es un requisito constitutivo del propio derecho la inscripción del título correspondiente (marca, nombre comercial, patente, modelo de utilidad, modelos y dibujos industriales, etc.) en el Registro de la Propiedad Industrial, denominado Oficina Española de Patentes y Marcas desde 1992, en que se constituyó como organismo autónomo, adscrito hoy al Ministerio de Ciencia y Tecnología.

Al mismo tiempo, y respecto al más relevante de estos títulos industriales en relación con la gestión de los servicios públicos locales, cual es el de marca, interesa reseñar tres puntos de interés: las posibilidades legales de maximización de la imagen corporativa local a través de las redes telemáticas (a), la necesidad de despejar definitivamente dudas e inhibiciones respecto a las posibilidades de actuación de los entes públicos locales al respecto y de ser plenos titulares de derechos de propiedad industrial (b), y, por último, el recordatorio del recurso al instrumento contractual como garantía de que la gestión propia no pueda verse afectada por derechos preexistentes de terceros (c).

a) Uno de los derechos atribuidos por la Ley 17/2001, de 7 de diciembre, de marcas (LM), a los titulares del derecho de marca es la posibilidad de usar este signo como nombre de dominio en la dirección electrónica propia en las redes de comunicación telemática [artículo 34.3.e)]. Este último elemento de identidad corporativa, que sirve para la localización de la dirección de un ordenador a través de internet, ha adquirido, una vez ya superado venturosamente el lamentable primer período de desconocimiento absoluto de los derechos de propiedad industrial por parte de los gestores de la red telemática, una cierta virtualidad diferenciadora tanto en el ámbito empresarial privado como en el institucional público (“DIBA”, “BCN”, etc.). A fin de registrar un distintivo de marca bajo los dominios telemáticos de tercer nivel “.com.es”, “.nom.es”, “.org.es”, “.gob.es”, “.edu.es”, y el genérico de segundo nivel “.es” la solicitud ha de tramitarse dirigiéndola a la entidad pública empresarial “Red.es” (www.red.es). Y para inscribirla bajo los dominios genéricos de segundo nivel (como son los “.com”, “.net”, y “.org”), la solicitud ha de tramitarse a través de una entidad agente registradora acredi-

tada per la *Internet Corporation for Assigned Names and Numbers* (ICANN) (www.icann.org).

b) Los antecedentes tradicionales de inhibiciones en este campo, fruto de un contexto histórico degradado de falta de autonomía y de tutela administrativa gubernamental, así como en el más actual en que conviven el auge del municipalismo con un entorno de agresividad competitiva de los operadores mercantiles privados, hace que no sea superfluo remarcar la solidez de los títulos competenciales de que se ha dotado el ordenamiento jurídico administrativo local confiriendo a sus entidades la capacidad de ser titulares de derechos inmateriales de propiedad industrial. Con carácter general, el primer fundamento competencial objetivo es el reconocimiento constitucional de la iniciativa pública en la actividad económica (CE, artículo 128.2), que se ha de relacionar aquí con el fundamento institucional del principio de autonomía local (CE, artículo 137); ambos encuentran su despliegue conjunto a escala local en las bases jurídicas siguientes:

b.1) Formalmente, en la capacidad jurídica plena que les reconoce el texto ordinamental básico local para actuar en derecho y establecer servicios públicos bajo cualquier forma organizativa y modo de gestión, directa o indirecta, así como para interponer los recursos establecidos y ejercitar las acciones previstas en las leyes (Ley 7/1985, artículo 5).

b.2) Materialmente, la capacidad de crear, establecer y explotar servicios públicos (Ley 7/1985, 85; Decreto legislativo 2/2003 –TRLCat/2003–, 246; ROAS/95, títulos 5 y 6) y de ejercer actividades económicas en régimen de libre competencia (TRLCat/2003, artículo 243; ROAS/95, título 4), que podrán ser identificados y distinguidos con signos marcarios de propiedad industrial, se despliega a partir de un triple orden de fundamentos:

–Primero: En la potestad de autoorganización de los entes locales (Ley 7/1985, artículo 4.1), que les habilita a la creación de personificaciones instrumentales funcionales de gestión de servicios públicos, dos figuras relevantes de las cuales serán los organismos autónomos y las entidades públicas empresariales.

–Segundo: En el principio de cooperación económica, técnica y administrativa entre la Administración local y las restantes administraciones públicas que rige en las relaciones interadministrativas entre todas ellas, tanto en servicios locales como en asuntos de interés común (Ley 7/1985, artículo 57), en que se fundamentan los consorcios locales.

–Tercero: En la cláusula competencial de apoderamiento general de los municipios, y, con ellos, de todos los entes locales cooperadores de segundo grado, que, “[...] para la gestión de sus intereses y en el ámbito de sus competencias, puede promover toda clase de actividades y prestar cuantos servicios públicos contribuyan a satisfacer las necesidades y aspiraciones de la comunidad de vecino” (Ley 7/1985, artículo 25.1).



c) Es plenamente extensible a los derechos de propiedad incorporal industrial el mismo énfasis que se ponía respecto a la necesidad de concienciar a los agentes públicos locales del interés del uso de los instrumentos contractuales para garantizar una gestión pacífica de sus activos propios o cedidos sobre los cuales pudieran incidir derechos de autoría preexistentes. Puesto que la conexión material entre el objeto de estas propiedades inmateriales y los objetos típicos o especiales de contratación administrativa está siempre potencialmente presente, es así conveniente la inserción de sendas previsiones en el pliego de cláusulas administrativas de contratación pública de una entidad local en el doble sentido preventivo (enunciación de la obligación) y reactivo (responsabilidad y deber de indemnización) siguiente:

c.1) Obligaciones del contratista en relación con la propiedad industrial y comercial de los elementos utilizados instrumentalmente para la realización de su prestación contractual: el contratista deberá obtener las licencias, las cesiones, los permisos y las autorizaciones necesarios de los titulares de los derechos de propiedad industrial correspondientes, siendo a su cargo el pago de los derechos e indemnizaciones por estos conceptos (*Pliego de cláusulas*, 2002: cl. 47.2.b, p. 33).

c.2) Responsabilidad e indemnización por cuenta del contratista derivada de toda reclamación relativa a la propiedad industrial y comercial de los materiales, procedimientos y equipos utilizados en su prestación contractual: deber de indemnizar a la Administración contratante todos los daños y perjuicios que para ésta pudieran derivarse de la interposición de reclamaciones al respecto, incluidos los gastos derivados de las que eventualmente puedan interponerse contra ella (*Pliego de cláusulas*, 2002: cl. 42.4, p. 32). El interés de esta recomendación viene acentuado por el hecho de que la nueva regulación de la LM (artículo 43.5) refuerza el derecho a la percepción de indemnización de daños y perjuicios por el titular de la marca cuya violación haya sido declarada judicialmente (Otero Lastres, 2002: 60).

#### 5.4. Derecho de acceso a la información pública

##### 5.4.1. Condicionamientos generales

El derecho de acceso a los archivos y registros administrativos, esto es, a la documentación pública, consagrado en la CE, artículo 105.b), y desarrollado a escala de legislación básica del Estado en la Ley 30/1992, artículo 37 (Matas, 2000) sigue constituyendo un índice fiel lamentablemente actualizado, tanto en sus manifestaciones normativas como en sus últimos desarrollos

jurisprudenciales, de la falta de transparencia democrática que caracteriza todavía a una generalidad de actuaciones públicas en un Estado formalmente denominado de derecho. En sus manifestaciones normativas, porque el catálogo de excepciones básicas al derecho de acceso que se configura en la Ley 30/1992, artículo 37, es tan minucioso al tiempo que ambiguo en la mayoría de sus manifestaciones que llega a la paradoja de invertir completamente los términos y convertir en regla general lo que en aplicación fiel de la prescripción constitucional citada debería ser la excepción.<sup>81</sup> Y en sus desarrollos jurisprudenciales, porque éstos han caído en el abuso dialéctico de las amplias posibilidades ofrecidas por un catálogo tan generoso como ambiguo de excepciones, cuando no activamente, sí, las más de las veces, por mera tolerancia pasiva de los excesos administrativos de celo corporativista en este sentido. Se puede aportar como último testimonio la triste sentencia del Tribunal Supremo (Sala 3.<sup>a</sup>) de 19 de mayo de 2003 en la que se estima procedente en vía de casación la denegación a un periodista para acceder a expedientes administrativos referentes a los créditos FAD concedidos a la empresa pública FOCOEX durante los años 1985-1995: la solución de este alto tribunal se funda en una interpretación desmesuradamente restrictiva del requisito de “petición individualizada de los documentos, sin que quepa formular solicitud genérica sobre una materia o conjunto de materias” (Ley 30/1992, artículo 37.7), dando lugar en sus fundamentos de derecho cuarto y quinto a argumentaciones que, vaciando de contenido el sentido del precepto legal, firmarían los propios maestros de Abdera y Leontini: así, pareciendo olvidar la distinción entre “materia” y “expediente”, “La solicitud del recurrente, relativa a todos los expedientes administrativos que hacen referencia a los créditos FAD concedidos a la empresa pública FOCOEX durante los años 1985-1995, no es individualizada. No se concreta en ella qué documentos se desea consultar, en relación con uno o varios créditos determinados, para comprobar la veracidad de la información que se posee y que se quiere comunicar [...]” (fundamento quinto), o bien, “[...] la Administración, al dictar la resolución denegatoria [...], no ha impedido al periodista recurrente comunicar libremente la información veraz que poseyese por cualquier medio de difusión, ni correlativamente recibirla libremente a los lectores. Lo que le ha impedido es comprobar la veracidad de su información, negándole el acceso a los archivos y expedientes administrativos respecto a los expedientes [...]” (fundamento cuarto).

La evolución en parábola descendente descrita no deja mucho margen más que para suscribirse a la opi-

81. Para una crítica en este sentido, ALBERCH, Ramon, y CRUZ, José Ramón, 1999. *¡Archívese! Los documentos del poder, el poder de los documentos*. Madrid: Alianza Editorial, SA: 107 y ss.

nión ya expresada por diversos autores, y que en su momento podía parecer aventurada, según la cual, “El tiempo ha ido configurando una realidad muy del gusto de quienes abogaban por un modelo de burocracia paternalista, anclada en los viejos usos de la reserva, al servicio de una ciudadanía menor de edad perpetua. Por eso se ha ido sacudiendo paulatinamente los molestos controles democráticos, recurriendo a las más depuradas fórmulas del cinismo hasta dejar convertido el mandato constitucional en mera expresión de intenciones.” (Alberch, R.; Cruz, J. R., 1999: 108).

#### 5.4.2. Condicionamientos específicos sectoriales en el nivel local: tensión entre las exigencias de los derechos de autor y los de acceso a la documentación en la gestión de los contenidos y de los flujos informativos en las administraciones públicas

En el marco del contexto general descrito en el punto anterior, el objeto de la controversia planteada en torno a la colisión de los intereses de autores e investigadores debe delimitarse a los documentos o contenidos producidos fuera del marco de la función pública y de la acción política de gobierno que reúnen los mínimos de creatividad (“originalidad”) exigidos por el TRLPI para ser susceptibles de protección bajo su amparo.

La gestión no lucrativa de los archivos públicos locales entra de lleno en el catálogo de excepciones previstas legalmente a los derechos de explotación económica por parte de los autores de las obras en ellos custodiadas (TRLPI, artículo 37), excepción que permite la reproducción solicitada para fines de investigación y el préstamo sin necesidad de autorización, y ello en el bien entendido de que adoptamos un concepto amplio de “investigador”, que comprende desde el historiador profesional hasta el periodista de investigación o el simple reportero de un medio de comunicación local. Ello no obstante, la misma ley ha tenido que salir al paso de la visión excesivamente patrimonialista que los derechohabientes de los autores exhiben a la muerte o declaración de fallecimiento de éstos sobre la explotación de sus obras, mediante el establecimiento de otra excepción a aquellos derechos que no es sino una aplicación sectorial del principio general privatista de interdicción del abuso antisocial de derecho: si aquéllos ejerciesen su derecho a la no-divulgación de la obra en condiciones que vulneren el principio rector constitucional del derecho de todos al acceso a la cultura (CE, artículo 44), las corporaciones locales, o sus instituciones públicas de carácter cultural u otras personas con interés legítimo, podrán instar del juez las medidas adecuadas de protección del interés general.

Es ya por desgracia un referente histórico sin herencia el informe sobre los archivos de la Unión Europea realizado hace una década bajo los auspicios de las instituciones comunitarias (Comisión Europea, 1994), entre

cuyas recomendaciones conclusorias figuraba la propuesta de crear un grupo transnacional de expertos en derechos de autor y archiveros con la misión de analizar la disparidad de legislaciones de los estados miembros de la Unión Europea en esta materia y de realizar propuestas de armonización normativa centradas en la necesidad de conciliar los intereses de los autores y los de los ciudadanos interesados en la consulta de los documentos. Tal iniciativa de coordinación se perdió lamentablemente en los intrincados laberintos eurocráticos y sólo ha conocido concreciones más tarde y a un nivel local en el meritorio trabajo de elaboración de formularios contractuales tipo de cesión de derechos de explotación realizado más recientemente por un grupo de archiveros locales catalanes (Boadas *et al.*, 1998).

## 6. Reflexiones finales

Más allá del mero ejercicio descriptivo del tratamiento legal en nuestro ordenamiento jurídico local de las relaciones electrónicas y del estudio de sus requerimientos de gestión, el análisis valorativo de este régimen jurídico necesita previamente una contextualización institucional y normativa clara. La configuración material efectuada en este sentido ha partido de las consecuencias jurídicas del llamado paradigma del *informacionalismo* para el operador público local, abocado a gestionar cotidianamente en primera línea la conflictividad de derechos e intereses en una realidad social que no entiende de anacronismos en los textos legales que la rigen, y se ha centrado en el análisis de una panorámica general de la aplicación de las TIC por las administraciones públicas, de la normativa que regula su actividad y de los factores que caracterizan con perfiles singulares los gobiernos y las administraciones locales.

Con estas premisas, los operadores públicos locales implicados, como agentes del mercado de la información, en la gestión de documentos en todas sus fases (activa, semiaactiva e inactivo-histórica), asisten a la paradoja de constatar, de un lado, las grandes posibilidades técnicas ofrecidas en este mercado por la introducción de las TIC, y, de otro, las obvias limitaciones impuestas por una legislación que, obedeciendo a principios, exigencias y objetivos diferentes, todos ellos legítimos, se muestra a veces contradictoria, forzando equilibrios bastante difíciles. En este sentido, se puede consignar una serie nada desdeñable de tensiones que conforman el último escollo respecto a la plenitud de la seguridad jurídica en el ejercicio de las funciones de los operadores mencionados.

En el plano instrumental, queda pendiente la clarificación de los parámetros mínimos de servicio público y de reconocimiento mutuo en el mercado de la certificación digital que no ha sido resuelto ni por el Real decreto ley 14/1999, ni por la L 59/2003, de firma electrónica.

Esta tarea es tanto o más urgente en la agenda de los poderes públicos si se recuerda que la firma electrónica es la piedra de toque de todo el sistema del procedimiento administrativo electrónico, como materialización de los requisitos legales básicos para la validez jurídica de sus manifestaciones.

En el plano material, el operador público local en cuestión se encuentra sometido a una creciente responsabilización y constreñido, incluso mediante mecanismos de coerción jurídica en los respectivos regímenes sancionadores, justo en medio de un triángulo de exigencias legales centrífugas que no siempre son de fácil conciliación: es así como un mismo documento, fichero o base de datos puede ser a la vez objeto de los imperativos de conservación (interés histórico, científico y cultural), de acceso por terceros (transparencia administrativa), al tiempo que de los de confidencialidad, reserva patrimonial, secreto, y, en último extremo, de cancelación (privacidad, propiedad intelectual e industrial, secreto empresarial y defensa de la competencia en el marco de la economía de mercado).

Este peculiar triángulo se desequilibra por el mayor nivel de exigencia en su tercer lado, hijo de un movimiento exagerado de péndulo en la relación entre el ser y el deber ser de la actividad reguladora: por una parte, el abuso lucrativo de mercantilización de la privacidad de los ciudadanos en que ha incurrido el sector de la mercadotecnia a caballo de los avances informáticos, tanto desde las instancias privadas como públicas, ha provocado una reacción, por el extremo opuesto, plasmada en la adopción de una legislación protectora de los datos personales de inspiración reconocidamente maximalista; por otra parte, se puede constatar el mismo contraste evolutivo pendular entre una tradición histórica continuada de ignorancia, cuando no menosprecio, de los valores inherentes a la investigación y a su corolario de creación técnica e intelectual, y el reciente establecimiento de una normativa de signo claramente tuitivo de los autores de obras acreedoras de derechos de propiedad incorporada intelectual o industrial. En ambos casos se detectan rigideces operativas en el plano de su despliegue institucional que son a superar en pro de la mejor consecución de sus propios fines.

## 7. Bibliografía

- Agencia de Protección de Datos. *Memoria 2001*. Madrid: Agencia de Protección de Datos, 2002.
- Agencia de Protección de Datos. *Memoria 2002*. Madrid: Agencia de Protección de Datos, 2003.
- Alberch, Ramón y Cruz, José Ramón. 1999. *¡Archívese! Los documentos del poder, el poder de los documentos*. Madrid: Alianza Editorial: 107 y ss.
- Alonso, Diana. 1997. "La aplicación de la Directiva europea de protección de datos en España: reformas necesarias en la LORTAD". Encuentros sobre Informática y Derecho (1996-1997). Universidad Pontificia de Comillas. Facultad de Derecho, Instituto de Informática Jurídica, Madrid: Aranzadi.
- Amadeo, S. L. 2001. *Informática y Nuevas Tecnologías*. Madrid: La Ley.
- Aparicio, J. 2000. *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*. Navarra: Aranzadi.
- Arnaldo, E., y Delgado-Iribarren, M. 1999. *Código Electoral*. Madrid: El consultor de los Ayuntamientos y de los Juzgados.
- Baena del Alcázar, M. 1988. *Curso de Ciencia de la Administración*. 2a. ed. Madrid: Tecnos.
- Boadas, Joan, et al., 1998. *Patrimoni cultural i drets d'autor: Instruments per a la seva gestió*. Girona: Ed. Ajuntament de Girona, Col·lecció "Textos i Documents", 8.
- Castells, M. 1997. *La era de la información: Economía, sociedad y cultura. Volumen I. La sociedad red*. Madrid: Alianza Editorial.
- Castells, M. 2003. "La interacció entre les tecnologies de la informació i la comunicació i la societat xarxa: un procés de canvi històric", *Coneixement i Societat. Revista d'Universitats, Recerca i Societat de la Informació. Generalitat de Catalunya*, 01: 8-21.
- Chacón, L., y Cortés, C. 2002. *Manual de Procedimientos y Formularios de Organización Municipal, Potestad Reglamentaria y Régimen Jurídico*. Barcelona: Editorial Bayer Hnos.
- Cobo Olvera, T. 2002. *Régimen Jurídico de las Administraciones Públicas*. 2.ª edición. Madrid: El Consultor de los Ayuntamientos.
- Comisión Europea, 1994. *Los archivos de la Unión Europea. Informe del grupo de expertos sobre los problemas de coordinación en materia de archivos*. Luxemburgo: Oficina de Publicaciones Oficiales de las Comunidades Europeas (OPOCE).
- Cremades, J. 2000. *Telecomunicaciones: 1000 Conceptos Básicos*. Madrid: La Ley.
- Davara, M. A. 2000. "Los principios de la protección de datos y los derechos de las personas en la nueva Ley Orgánica de Protección de Datos de carácter persona". *Actividad Informática Aranzadi*, enero.
- Del Caño Gil, M. C. y Turmo Blanco, C. 2002. "El registro telemático en el Ministerio de Ciencia y Tecnología". *Ponencia presentada en VII jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas. A Coruña*.
- Del Peso, E y Ramos, M. A. 1994. *Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas*. Madrid: Díaz de Santos.
- Diputació de Barcelona, 2003. *Guia de serveis*. Barcelona.
- "E-España 2002. Informe anual sobre el desarrollo de la Sociedad de la Información en España". 2002. Madrid: Ed. Fundación Auna

- Escobar, L. 2001. *Derecho de la Información*. Madrid: Dykinson.
- Fernández López, J.M. 2000. "La nueva Ley de Protección de Datos. Su porqué y sus novedades principales". *Actividad Informática Aranzadi*, enero.
- Freixas, G. 2001. *La Protección de Datos de Carácter Personal en el Derecho Español*. Barcelona: Bosch.
- García de Entrerriá, E., y Fernández, T. 2002. *Curso de Derecho Administrativo I*. 11ª edición. Madrid: Cívitas.
- González Pérez, J., y González Navarro, F. 1999. *Comentarios a la Ley de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo (Ley 30/1999, de 26 de noviembre)*. Volumen I y II. Madrid: Cívitas.
- Guasch Marimón, J., J. L. Martínez-Alonso Camps, y A. Ortiz Villuendas. 2002. "*Marc Legal del Document Electrònic*". Ponencia presentada en la preconferencia del DLM fórum 2002. Barcelona.
- Herdero, M. 1996. *La Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal. Comentarios y textos*. Barcelona: Tecnos.
- Hernández González, F. L. 2002. "*Consideraciones jurídicas sobre la informatización de los procedimientos administrativos. La iniciación y terminación del procedimiento por vía telemática*". Ponencia presentada en VII jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas. A Coruña.
- Herrán, Al. 2002. *El Derecho a la Intimidación en la Nueva Ley Orgánica de Protección de Datos Personales*. Madrid: Dykinson
- Jordana, J., y D. Sancho. (Editores). 1999. *Políticas de telecomunicaciones en España*. Madrid: Tecnos.
- Kuhn, T. 1977. *La estructura de las revoluciones científicas*. Madrid: Fondo de Cultura Económica.
- "La norma ISO 15489. Informació i documentació. Gestió documental". 2002. Escola d'Administració Pública de Catalunya. Barcelona
- Magide Herrero, M. 2000 *Límites constitucionales de las Administraciones independientes*. Madrid: Ministerio de Administraciones Públicas. INAP
- Martínez-Alonso, J. L. 1998: "L'organització territorial i els governs locals a Catalunya." En: Caminal, M. i Matas, J., eds. *El sistema polític de Catalunya*. Barcelona: Tecnos/Ed. Universitat de Barcelona/S. Publicacions Universitat Autònoma de Barcelona.
- Martínez-Alonso, J. L. 1998b. "La encomienda de la gestión informatizada de los padrones municipales de habitantes: un ejemplo de colaboración entre Administraciones públicas." *Revista de Estudios de la Administración Local y Autonómica*, 276: 151-177.
- Martínez-Alonso, J. L. 1999. "El subsistema local; una propuesta d'anàlisi amb vista al futur". *Revista de serveis personals*, núm. 11. CIFA/Patronat Flor de Maig de la Diputació de Barcelona.
- Martínez-Alonso, J. L. 2000. "La población municipal". En: Mir, Josep (Director y coordinador): *Manual de Govern Local*. Barcelona: Federació de Municipis de Catalunya.
- Martínez-Alonso, J. L. e Ysa, T. 2003. *Les personificacions instrumentals locals a Catalunya: organismes autònoms, consorcis, mancomunitats i societats públiques*. Barcelona: Generalitat de Catalunya. Escola d'Administració Pública de Catalunya. Col. Estudis, núm. 17. 2a. ed.
- Martínez-Alonso, J. L. e Ysa, T. 2003: *Las personificaciones instrumentales locales en Cataluña: organismos autónomos, consorcios, mancomunidades y sociedades públicas*. Instituto Nacional de Administración Pública (INAP) y Escola d'Administració Pública de Catalunya (EAPC). Madrid.
- Matas, Josep, 2000. *El acceso a los documentos: un derecho democrático*. (Ponencia presentada al XIV Congreso Internacional de Archivos, celebrado en Sevilla, 18-20.09.2000).
- Ministerio de Administraciones Públicas (MAP), 2003. *Propiedad intelectual de los programas de ordenador*. (medidas, recomendaciones y buenas prácticas contenidas, en fecha 31.7.2003, en la dirección <http://www.csi.map.es/csi/propiedad/>).
- Morell Ocaña, L. 1998. *Curso de Derecho Administrativo. Tomo I. El Derecho Administrativo y sus Fuentes. La Organización Administrativa y sus Medios*. 4ª edición. Pamplona: Aranzadi.
- "MoReq: Modelo de Requisitos para la gestión de registros electrónicos". 2001. CECA-CEE- CEEA. Bruselas - Luxemburgo.
- Muro i Bas, Xavier. 1998. "La Agencia de Protección de Datos". *RAP*, nº 147.
- Otero Lastres, José Manuel, 2002. "La nueva Ley de Marcas de 7 de diciembre de 2001", *Revista Jurídica de Catalunya* 3/2002, 39-62.
- Paricio Rallo, E. 2002. "L'Administració Pública i la protecció de dades". Ponencia presentada en el *Cicle de seminaris d'actualització jurídica local*, 2002. Barcelona, 28 de junio de 2002.
- Pliego de Cláusulas Administrativas Generales aplicables a los contratos de Consultoría y asistencia, de servicios y de suministros, a otros contratos administrativos y a los privados de la Diputació de Barcelona* (BOPB núm. 161 de 6.07.02, pp. 24-39).
- Sánchez, A. 2001. *Internet y la Sociedad Europea de la Información: Implicaciones para los Ciudadanos*. Sevilla: Universidad de Sevilla.
- Sanromà, M. 2002. "Una Administració Oberta" *Butlletí Informatiu de la STSI (Secretaria de Telecomunicacions i Societat de la Informació)*. Generalitat de Catalunya. núm. 4, 16.10.2002.
- Serra Serra, J. 2001. "Gestión de los documentos digitales: estrategias para su conservación". *El profesional de la información*, septiembre, V. 10, nº 9, 4-18.

Serra Serra, J. 2002. "Estrategias de Preservación de Documentos electrónicos: El National archives and Records Administration y el Public Record Office". *Ponencia presentada en V Jornadas de Archivos electrónicos, Priego de Córdoba, 14 y 15 de marzo de 2002.*

Sibina Tomás, D. 1999. "La implantació obligatòria, abans del 26 de març i 26 de juny de 2000, respectivament, de les mesures de seguretat de nivell bàsic i de nivell mitjà previstes en el reglament de mesures de seguretat dels fitxers automatitzats que continguin dades de caràcter personal, aprovat pel Reial decret 994/1999". *Quaderns de Dret Local*. Diputació de Barcelona. Barcelona, 23: 34-60.

Valero Torrijos, J. 2002. "El régimen jurídico de los registros administrativos telemáticos: algunas cuestiones problemáticas". *Ponencia presentada en VII jornadas sobre tecnologías de la información para la modernización de las Administraciones públicas*. A Coruña. 15, 16 y 17 de octubre.

Villaverde Menéndez, I. 2003. "Protección de datos personales y padrón municipal". *Cuadernos de Derecho Local*. Fundación Democracia y Gobierno Local. Barcelona, 1: 89-104.

Villaverde Menéndez, I. 2003b. "Protección de datos personales y padrón municipal (II)". *Cuadernos de Derecho Local*. Fundación Democracia y Gobierno Local. Barcelona, 3: 72-90.

Vizcaíno, M. 2001. *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*. Madrid: Civitas Ediciones. ■