La implantación de la legislación sobre protección de datos en la administración municipal: cuestionamiento teórico y estudio de caso

Alejandro Delgado Gómez*

Introducción

El presente artículo se aplica a la tarea de describir el modo en que las previsiones acerca de la protección de datos de carácter personal pueden aplicarse en el marco de la Administración Municipal y, de manera específica, en el contexto del archivar electrónico. Para ello, se hace uso de un estudio de caso, el del Archivo del Ayuntamiento de Cartagena, no porque sea un ejemplo exclusivo de buenas prácticas –creemos que es un ejemplo de buenas prácticas entre otros muchos existentes–, sino simplemente porque es el lugar en el que lleva a cabo su trabajo el autor del presente texto.

No obstante, antes de articular el estudio de caso, es preciso problematizar la noción de protección de datos de carácter personal, dado que, por una parte, sobre la misma pueden aplicarse muchas perspectivas –la jurídica, la tecnológica, la documental, la del sector privado, etc.–, y, por otra, la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal,[1] y el Real Decreto 1720/2007[2] que la desarrolla no aparecen en condiciones de aislamiento, sino en combinación con otras muchas leyes que tratan diferentes aspectos de la privacidad y el acceso, y que deben tomarse en cuenta. No podemos olvidar, en este sentido, el reciente Anteproyecto de Ley de Transparencia,[3] ampliamente publicitado, duramente cuestionado

*Ayuntamiento de Cartagena-Archivo Municipal.

1 España. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Disponible en: http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf (consulta: 14 de mayo de 2012). En lo sucesivo LOPD.

2 España. REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Disponible en: http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf (consulta: 14 de mayo de 2012). En lo sucesivo RDLPOD.

3 España. Anteproyecto de ley de Transparencia, Acceso a la Información Pública y Buen

por instituciones públicas y asociaciones profesionales, pero cuya inevitable aprobación –aunque difícilmente pueda tomarse en serio siquiera sea porque ni en un solo punto del articulado se piden responsabilidades reales ni se establecen procedimientos serios de auditoría– no es posible ignorar.

En el marco del presente artículo, orientado como se ha dicho por el archivar electrónico, se prioriza la perspectiva documental, de tal modo que la primera parte del mismo plantea más problemas que soluciones, o, en sentido estricto, analiza algunos de los matices conflictivos que desde el punto de vista del archivar puede tener la legislación vigente, tanto en las interrelaciones entre diferentes leyes, como en las interrelaciones entre la propia legislación y la realidad tecnológica y archivística. En la segunda parte del artículo, el estudio de caso, esperamos poder despejar algunos de estos conflictos.

La problematización de la noción de datos de carácter personal

La Ley Orgánica de Protección de Datos de Carácter Personal (en lo sucesivo LOPD) define "datos de carácter personal" como "cualquier información concerniente a personas físicas identificadas o identificables". Desde el punto de vista documental, esta definición ya comienza a ser problemática, en la medida en que identifica datos e información, dos conceptos diferentes y susceptibles de tratamiento también diferenciado. "Datos" son "unidades mínimas de información con significado",[4] mientras que "información" es "un ensamblaje de datos de los que se pretende su comunicación a lo largo del espacio y el tiempo".[5] Parecería, pues, que aquello que se protege no son solamente datos, sino particularmente información, en la medida en que, si bien los primeros tienen significado, es en su reunirse en una pieza de información que, además, se mueve en el tiempo y el espacio, donde este significado adquiere valor más pleno, puesto que se pone en un contexto determinado y es en este contexto en el que el significado proporciona evidencia.

Gobierno. Disponible en: http://www.leydetransparencia.gob.es/anteproyecto/ (consulta: 14 de mayo de 2012).

4 InterPARES 2 Terminology Database. Disponible en: http://www.interpares.org/ip2/ip2_terminology_db.cfm (consulta: 14 de mayo de 2012).

5 *Idem*.

Las definiciones aportadas por el Reglamento que desarrolla la LOPD no contribuyen a mejorar las cosas. El Reglamento refina la definición de "datos de carácter personal" del siguiente modo: "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables", es decir, tipifica la información a la que se aplica la protección, y por ende los soportes en los que esta información se inscribe, y deja la puerta abierta a ampliar esta tipificación a un "cualquier otro tipo" que, en el entorno digital, como veremos, resulta particularmente conflictivo.

Además, el Reglamento introduce el concepto de "documento", en gran medida ausente de la LOPD, al que define como "todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada". Esta definición no coincide con la definición archivística de documento, que es "una unidad indivisible de información constituida por un mensaje fijado en un soporte (registrado) de manera sintácticamente estable. Un documento tiene forma fija y contenido estable".[6] Tampoco coincide con la definición de documento de archivo, que es "un documento realizado o recibido en el curso de una actividad práctica como instrumento o resultado de tal actividad, y guardado para acción o referencia".[7] Es decir, de la conceptualización elaborada por el cuerpo regulador acerca de la protección de datos están ausentes, en primer lugar, las características de forma fija y contenido estable de los documentos, adoptando una perspectiva datacéntrica, más que docucéntrica, que no nos preocuparía demasiado, dada la tendencia de los universos archivísticos hacia el datacentrismo, de no ser porque, por una parte, ese propio cuerpo regulador reconoce que la información puede ser "de cualquier otro tipo", lo cual incluye al documento con una forma fija y un soporte estable; y, por otra parte, otros cuerpos legales como la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos[8] y sus derivados, sí parecen adoptar una aproximación docucéntrica susceptible de entrar en conflicto con la percepción de la LOPD y su Reglamento de

6 *Idem*.
7 *Idem*.
8 España. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Disponible en: http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf (consulta: 14 de mayo de 2012).

desarrollo, si bien este docucentrismo se va diluyendo a medida que tales derivados afianzan su redacción.[9]

En segundo lugar, nos preocupa que del cuerpo regulador acerca de la protección de datos esté ausente la noción de evidencia, que desde el punto de vista archivístico es más amplia que el convencional "valor probatorio" o valor ante los tribunales, en la medida en que afecta a todos los agentes sociales, y no sólo por motivos jurídicos, sino también, por ejemplo, éticos, testimoniales, cívicos o científicos.[10] Además, en tanto reflejo de acciones, y como vendría a sugerir la reciente eclosión de la disciplina de la ciencia forense digital, la evidencia puede estar contenida tanto en datos, como en información o en documentos.

Para colmo, tanto la LOPD como su reglamento afirman explícitamente que los datos están contenidos en cualquier tipo de soporte físico. Así, dice la Ley en su artículo 2, "la presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado"; y el Reglamento, también en su artículo 2, "el presente reglamento será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado". Aunque se suele pensar de la LOPD y de su Reglamento en términos informáticos, lo cierto es que las precedentes afirmaciones vienen a significar que un documento analógico también contiene datos que deben ser protegidos.

Algunas de las consecuencias de esta falta de rigor terminológico, o, en sentido estricto, de esta percepción unilateral de las definiciones aportadas por la LOPD y su Reglamento de desarrollo son, por ejemplo, que los documentos analógicos que contienen datos de carácter personal están sujetos también a otras regulaciones y no se pueden "cancelar" ni por supuesto destruir,[11] sino más bien tratar su confidencialidad de otras

---

9 A este respecto, confróntese, por ejemplo, el conjunto de normas técnicas de interoperabilidad. Disponible en:
http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=P60215901274203521811&langPae=es (consulta: 14 de mayo de 2012).

10 Delgado Gómez, Alejandro, *El centro y la equis: una introducción a la descripción archivística contemporánea*.

11 España. Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. Disponible en: http://www.boe.es/boe/dias/1985/06/29/pdfs/A20342-20352.pdf (consulta: 14 de mayo de 2012).

maneras, alguna de las cuales viene apuntada por el propio Reglamento. Otra consecuencia sería el hecho de que, por ejemplo, una base de datos puede recibir, dependiendo del punto de vista que se adopte, el tratamiento simultáneo de datos, información y documento, siéndole por tanto de aplicación diferentes regulaciones, en cierto modo contradictorias entre ellas: si una base de datos es un documento, entonces no se puede alterar, de tal modo que no se podrían cancelar, bloquear, rectificar, borrar los datos que contiene. La casuística derivada de las conflictivas definiciones de la LOPD y el Reglamento de desarrollo, en combinación con otras regulaciones y textos legales, constituye sin duda un problema que quizá no existiría si el legislador hubiera consultado a un archivero, cuya especialidad son los datos, la información y los documentos; o si se hubiera previsto en el Consejo Consultivo la figura de tal especialista.

Una segunda faceta problemática, desde el punto de vista de la ciencia de los archivos, de la LOPD y regulaciones asociadas, es la del inevitable choque entre el derecho al recuerdo y el derecho al olvido, o, en otros términos, entre el derecho al acceso y el derecho a la intimidad.[12] Bien es cierto que la Constitución de 1978 recoge el derecho a la intimidad como fundamental; pero no es menos cierto que en su artículo 20.1 también recoge el derecho "a comunicar o recibir libremente información veraz por cualquier medio de difusión",[13] es decir, el derecho a lo que en otras tradiciones se conoce como libertad de información, o derecho a acceder a la misma. Indudablemente, tanto por el contexto en el que se inscribe, dentro del texto constitucional, como por el indicio de que nunca se desarrolló un documento normativo con carácter de ley orgánica acerca de libertad de información o derecho de acceso, los padres de la Constitución no estaban pensando en los archivos cuando redactaron el mencionado artículo. Resulta significativo también el hecho de que la normativa sobre acceso se encuentra dispersa en numerosos y en ocasiones contradictorios textos normativos, a diferencia, por ejemplo,

---

12 Iacovino, Livia, "Privacy as a human right in Italian data protection law and its impact on records as evidence and memory". Disponible en:
http://socialstudies.cartagena.es/images/PDF/vol2n2/iacovino_privacy.pdf (consulta: 14 de mayo de 2012)

13 España. Constitución, 1978. Disponible en:
http://www.boe.es/aeboe/consultas/enlaces/documentos/ConstitucionCASTELLANO.pdf (consulta: 14 de mayo de 2012).

de las tradiciones Westminster, que suelen contar con legislación específica a este respecto, cuando no de legislación que trata de manera conjunta ambos derechos, el de acceso y el de privacidad. En cualquier caso, aunque quizá no mencionado como derecho fundamental, el derecho de acceso está previsto en la propia Constitución, en su artículo 105, que establece la regulación del "acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas". La legislación posterior, si bien como hemos dicho de manera confusa y contradictoria, ha venido sancionando este derecho, y la realidad de los últimos treinta años ha mostrado que la transparencia y el derecho a obtener información acerca del buen hacer, o más a menudo el mal hacer, de los poderes públicos por parte de la ciudadanía, debería haber sido explícitamente desde el principio un derecho fundamental. Si no lo es, esto no lo excluye del discurso archivístico, que debe conciliar el necesario derecho a la intimidad, sobre el que se concentra la LOPD y su reglamentación asociada, con el derecho de acceso, recogido en otras leyes[14] –incluido el cuestionable Anteproyecto de Ley de Transparencia mencionado– y, en cualquier caso, un imperativo ético.

Además, y como no puede ser menos en un entorno tecnológico permanentemente cambiante y en evolución, la legislación sobre protección de datos ya se ha quedado por detrás de los más recientes desarrollos tecnológicos. Éste parece ser un mal inevitable, habida cuenta de que no resulta previsible el que la tecnología se detenga, o al menos se estabilice, en algún momento, mientras que una ley ha de tener cierto grado de estabilidad, no puede cambiarse todos los días. El argumento de que la ley adopta una forma concreta en la jurisprudencia no resulta de mucho recibo, dado que, en el *perpetuum mobile* de las actuales tecnologías de la información y de las comunicaciones, por ejemplo, un acto delictivo cometido haciendo uso de unas determinadas tecnologías puede ser objeto de un tratamiento jurídico dado y, en otro lugar o momento, otro acto de iguales características, pero que se realiza utilizando unas tecnologías más avanzadas, puede ser objeto de un tratamiento jurídico diferente, puesto que el tratamiento anterior no

14 España. Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Disponible en: http://www.boe.es/boe/dias/1992/11/27/pdfs/A40300-40319.pdf (consulta: 14 de mayo de 2012).

puede servir de precedente, en la medida en que los medios utilizados no existían cuando el acto delictivo se llevó a cabo por primera vez.

En este sentido, nos preocupan particularmente una propiedad y un fenómeno emergente en el actual entorno de las tecnologías de la información y las comunicaciones. La propiedad a la que nos referimos es la proliferación, o la extrema sencillez con la que pueden multiplicarse las copias de datos, información o documentos. Esto no es por naturaleza malo; antes al contrario, la realización de copias redundantes para optimizar la posibilidad de que los datos sobrevivan es una buena práctica frecuentemente recomendada. Sin embargo, y aunque nuestras regulaciones sobre protección de datos prevén el tratamiento que se debe dar a las copias o a los datos comunicados, en un entorno en el que hacer una copia es cuestión de segundos y en el que, dependiendo de la calidad de los procedimientos, varias copias, con sus correspondientes copias de seguridad, pueden encontrarse en diferentes manos y comunicarse por diversos medios, no podemos dejar de preguntarnos si realmente tenemos el control de nuestros datos. A la misma pregunta nos conduce el análisis del fenómeno emergente que mencionábamos, el llamado *Cloud Computing*. Partimos de la base de que, en efecto, el trabajar en la nube es económico, ecológico, eficaz, eficiente y, sobre todo, extremadamente barato. Puesto que atravesamos una de las peores crisis financieras globales jamás conocidas, el uso de la nube, en algunas de sus variantes, parece una apuesta de futuro. Pero, y aunque la LOPD y sobre todo el Reglamento tratan figuras como las del responsable del fichero, el encargado del tratamiento o los posibles sub-contratistas a emplear, así como los requisitos, condiciones y responsabilidades que deben satisfacer cada uno de ellos, en un entorno tan extremadamente difuso como el de la nube, tampoco podemos dejar de preguntarnos en qué momento el control sobre nuestros datos puede llegar a perderse. En este sentido, dos líneas de exploración adicional son necesarias a nuestro juicio: en primer lugar, el modo en que la proliferación de copias o las medidas de seguridad sobre la producción de las mismas podría ponerse bajo control; y, en segundo, la inexistencia de un derecho digital internacional que trate de manera conjunta aspectos tales como la privacidad, la vigilancia, la transparencia, el derecho de acceso y el derecho de olvido.

Por último, en esta primera parte, dedicada como hemos dicho a la

problematización de la noción de protección de datos en el marco del archivar electrónico, debemos examinar el tratamiento que reglamentariamente se da precisamente a este archivar. Lo primero que llama la atención, por supuesto, es que el Reglamento contenido en el Real Decreto 1720/2007 no considere el archivar como una medida de seguridad para los ficheros y tratamientos automatizados, a ningunos de los niveles básico, medio y alto, y que sólo mencione el archivo como medida de nivel básico para ficheros y tratamientos no automatizados. Es decir, con respecto al archivar, el Reglamento sólo aplica un artículo, el 106, en el que se dice que:

> […] el archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.[15]

Sin embargo, los capítulos III y IV del título VIII, dedicados a las medidas de seguridad aplicables a los ficheros y tratamientos de distinto nivel, se encuentran plagados de procesos de seguridad que cualquier archivero consideraría de su competencia y a los que por tanto debe prestar la debida atención.

Además, la LOPD declara, y el Reglamento desarrolla, un tratamiento especial cuando los datos sean susceptibles de ser utilizados a efectos estadísticos, históricos o científicos, remitiendo a la legislación sectorial específica y añadiendo además el Reglamento un breve procedimiento en la sección segunda del capítulo VII del título IX. Tal procedimiento se limita a obligar acerca de informar y documentar la petición de exención del tratamiento general por parte del responsable del fichero, así como a indicar el plazo de resolución. No obstante, y como sucediera en el párrafo anterior, puesto que una de las obligaciones del archivo es precisamente la conservación a lo largo del tiempo de información con fines estadísticos,

15 RDLPOD. Disponible en: http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf (consulta: 14 de mayo de 2012).

históricos y científicos, entre otros, el archivo debe prestar atención especial a este implícito procedimiento de exención.

Es decir, las obligaciones del archivo se multiplican, con respecto a la protección de datos, y en relación con otras áreas organizativas, en la medida en que debe atender a los datos resultantes de: a) su actuar cotidiano, b) sus relaciones con otras áreas organizativas, y c) sus relaciones con agentes externos orientados por la investigación. Además, debe atender al tratamiento de datos, información y documentos, y no sólo en soporte digital, sino también en soporte analógico. Por último, como adelantamos, debe gestionar no sólo el derecho a la intimidad, sino también el derecho al acceso, no sólo por parte del afectado, sino también por parte de otros agentes, recogido en legislación dispersa. Una tarea cualquier cosa menos sencilla, y, como se ha visto, mal reconocida, si es que en algún momento se reconoce en absoluto.

No obstante, imaginamos que tal tarea es posible, y en lo que sigue exponemos, mediante un estudio de caso, el modo en que el Archivo Municipal de Cartagena ha intentado cumplir con sus obligaciones legales.

Estudio de caso: la protección de datos en el Archivo del Ayuntamiento de Cartagena

Como es natural, el proceder del Archivo Municipal en lo que concierne a la protección de datos no se produce en condiciones de aislamiento, sino en el marco de la política general del ayuntamiento a este respecto. Aunque éste no dispone aún de un código tipo, sí cuenta con una política y varios instrumentos que se concretan en:

- Directrices generales de seguridad.
- Recomendaciones para la creación de documentos relativos a la protección de datos.
- Planes formativos, y
- Auditoría de cada uno de los ficheros existentes en el Ayuntamiento, en la que se detallan las características de todos ellos, así como su nivel de seguridad de acuerdo con la LOPD.

Por otra parte, y sobre todo en lo que hace a documentos digitales, el Archivo parte del consolidado principio de que, en digital, la conservación comienza con la creación, e incluso antes, durante la fase de diseño del sistema, de tal modo que sus sistemas de conservación se encuentran integrados con los sistemas pertinentes de producción, a efectos de una mejor y más eficaz gestión archivística, no *post hoc*, posición inviable en entornos digitales, sino *ab initio*, es decir, desde que los datos se crean en otro sistema.

Esta concepción de los procesos archivísticos, en conjunción tanto con la política general del ayuntamiento como con la legislación vigente, obliga al Archivo a disponer de aplicaciones informáticas que operen de manera distribuida, puesto que el Archivo no se encuentra en condiciones de aislamiento, sino integrado con otros sistemas, y, en consecuencia, que permitan extremar las medidas de seguridad, tanto para preservar la privacidad de los datos recogidos acerca de terceros, que son los datos que concurren a la formación de expedientes, y que en un ayuntamiento, con pequeñas excepciones, contienen de manera casi constante información de carácter personal; como para preservar la privacidad de los datos de los propios usuarios del sistema. Puesto que, por otra parte, la legislación obliga a recabar datos únicamente para los fines para los que han sido concebidos y, como se adelantó, deja la puerta abierta para que cualquier soporte incluidas las bases de datos pueda ser considerado documento, soluciones técnicamente económicas como la mera transferencia de responsabilidad sobre un solo servidor, de producción y de conservación, no es viable: habida cuenta de que cabe la posibilidad de que el Archivo conserve datos para la recuperación de documentos, en términos legales, o de la posibilidad de que conserve datos con fines estadísticos, históricos o científicos; y habida cuenta de que en el entorno de producción los datos se cancelan, modifican o borran, circunstancias que no tienen lugar en el entorno de conservación, la transferencia física tanto de datos en cuanto datos, datos en cuanto documentos, y datos en cuanto relativos a documentos, es necesaria, y a su vez está necesitada de particulares niveles de seguridad.

Por estos motivos, el Archivo decidió la utilización de un producto propietario que presentaba dos características técnicas críticas y una característica organizativa que garantizaba seguridad adicional. Esta característica organizativa era el hecho de que la compañía responsable del

desarrollo del *software* contaba con certificación ISO 27001 en varios aspectos concernientes a seguridad. Por supuesto, las garantías, en entornos digitales, son siempre asunto de grado, y nada está nunca seguro al cien por cien; pero el reconocimiento de que se están cumpliendo ciertos procedimientos normativos consolidados siempre contribuye a incrementar ese grado de confiabilidad. En lo que se refiere a las características técnicas, por una parte, el *software* seleccionado funciona enteramente sobre tecnologías *web*, lo que permite operar de manera distribuida e integrada con otras aplicaciones; por otra, dicho *software* se adecúa a estándares técnicos en los que la seguridad constituye un foco de interés primordial, por ejemplo, ISO 15489, ISO 23081, ISO 16175, ISO 30300 o, desde otra perspectiva, MoReq2010, lo cual tiene como consecuencia el desarrollo de funcionalidades muy estrictas para gestionar tanto el control sobre los datos como el control sobre los usuarios de los mismos, y por parte de dos agentes: el servicio de informática, que gestiona tales controles desde el punto de vista tecnológico; y el propio Archivo, que gestiona tales controles desde el punto de vista documental, lo cual permite incrementar la seguridad, en la medida en que se aplican dos criterios no coincidentes pero complementarios, que, en su conjunto, dan cumplimiento a los requisitos de seguridad establecidos en la LOPD y, particularmente, en su Reglamento de desarrollo. Otras características del *software* en cuestión quedan al margen del asunto del presente artículo, de modo que, en lo que sigue, describimos sólo las funcionalidades de seguridad en uso en el Archivo Municipal de Cartagena. Por supuesto, como se dijo al inicio, la que se describe es una implantación específica, y otras muchas implantaciones son posibles. La descripción siguiente es extremadamente somera por motivos de espacio, pero debería servir al menos para obtener una idea general del modelo de implantación propuesto.

El *software* citado cuenta con tablas de perfiles de usuario y de grupos de usuario. Desde la primera se definen los privilegios de obtención de documentos para los distintos niveles de uso común en el entorno archivístico, o para niveles definidos *ad hoc*; y desde la segunda aquellos archivos, o contenedores de registros, a los que se tendrá acceso. Cada usuario individual tiene asignado un perfil y un grupo, a partir de los cuales se regulan las condiciones de acceso y uso en los módulos de consulta y de circulación.

De igual modo, el *software* mencionado define por defecto perfiles

administrador, supervisor y usuario, cada uno de ellos refinable en función de diferentes criterios, disponiendo el administrador de todos los privilegios para definir condiciones de acceso, tanto sobre los usuarios como sobre los registros y partes del mismo, y pudiendo, por lo demás, definir tantas condiciones de acceso como grupos de usuarios diferenciados existan.

La aplicación permite la restricción de la visibilidad de los datos, tanto a nivel de registro, como de campo (entendido en el contexto del *software* de referencia como contenedor de campos) y subcampo (campos en sentido convencional), permitiendo además la definición de diferentes ficheros de indización, de tal manera que no se pueda acceder a información a la que no se tiene derecho navegando por los índices.

Las restricciones de acceso a los usuarios vienen dadas por la asignación de niveles a los grupos de usuarios, de tal manera que un usuario que no tenga derecho a ello jamás verá información que no corresponda a su nivel, ni siquiera tendrá constancia de la existencia de la misma.

Además, el *software* que nos ocupa dispone de pista de auditoría inalterable en la que quedan reflejadas todas las acciones realizadas por los usuarios, así como el usuario que la realizó, la fecha y la hora, la dirección IP, y, si procede, detalles acerca de la acción. Los registros de esta pista de auditoría nunca se borran, y sólo el administrador tiene acceso a ellos. De igual modo, el administrador puede configurar la pista de auditoría para determinar cuáles son las acciones relevantes a dejar consignadas, quedando esta misma acción del administrador reflejada en la pista.

El uso de herramientas flexibles permite que todas las opciones de la aplicación puedan configurarse y reconfigurarse por parte de usuarios autorizados, por regla general aquel perfil definido como administrador por el sistema, desde el *front-end* y sin especiales destrezas en informática. Esto incluye la configuración de parámetros generales, consultas, vistas, permisos de usuarios, pantallas de interrogación y vista de resultados, etcétera.

El procedimiento de derechos de acceso a los registros en el *software* que nos ocupa es igual para usuarios externos e internos. Deben configurarse, también para usuarios externos o grupos de usuarios, tantos archivos como resulten necesarios. Los datos mínimos de estos archivos, que se crean desde el formulario "Archivos", son un código identificador y un nombre para cada uno de ellos, así como los índices a los que irán a parar los

términos de indización que cada uno de ellos genere, a efectos de restringir el acceso mediante navegación a datos no permitidos y mantener la limpieza del sistema de indización. Además, mediante el formulario "Grupos de usuarios" deben crearse tantos como resulten necesarios, asignándoles un código y una identificación textual. En el formulario "Alta de usuarios" se crearán también los usuarios individuales pertenecientes a cada grupo, indicando, junto a los datos personales que se consideren necesarios, una palabra de paso y una contraseña, así como el archivo al que pertenece, el o los grupos a los que está asignado, los formularios de consulta previamente configurados de los que podrá hacer uso, el idioma por defecto y las fechas de alta y baja. En el formulario "Restricciones de menú" se indicarán las opciones de menú a que tendrá derecho cada grupo de usuarios. Además, en el momento de configurar las plantillas de introducción de datos y las vistas de usuario pueden determinarse, en primer lugar, los campos que permanecerán ocultos y, en segundo, simplemente los campos que no se mostrarán en pantalla. Por último, las unidades productoras y usuarios que dependen de ellas deben describirse como entidades en el *software*, a efectos de establecer, mediante aplicación del principio de herencia, sus derechos y restricciones de consulta, uso de plantillas y petición de documentos. En la descripción, los usuarios individuales heredan los privilegios de la unidad de la que dependen.

El *software* objeto del presente estudio de caso, con el fin de asegurar la coherencia de los datos, funciona mediante el procedimiento de creación de plantillas de introducción de datos para distintos tipos de usuarios. Estas plantillas permiten que el usuario con privilegios de administrador defina desde el comienzo y sin posibilidad de alteración por parte de usuarios no autorizados, las características que deben tener los datos a introducir: valores por defecto (por ejemplo, un literal, la fecha del sistema, el identificador del usuario, un contador), campos ocultos, campos obligatorios/opcionales, repetibilidad de campo, nivel superior al que se asociarán por defecto los registros, formato de los datos (fecha en sus distintas variantes, texto, etc.), posibilidad de asociar funciones a determinados campos (por ejemplo, rellenar con ceros por la izquierda, copiar o mover el contenido de un campo a otro campo, sustituir el contenido de un campo). De este modo, la coherencia queda maximizada, y minimizado el paralelo riesgo de cometer

errores. En cualquier caso, la aplicación permite definir "archivos ficticios", con el objeto de validar los datos antes de cambiarlos al archivo real correspondiente.

Por último el *software* en uso en el Archivo Municipal del Ayuntamiento de Cartagena permite el tratamiento homogéneo de documentos analógicos y digitales, y se ha integrado de manera exitosa tanto con procesos de gestión de otras áreas organizativas, como con aplicaciones de seguridad desarrolladas por el propio Ayuntamiento, de tal manera que el grado en que los datos, la información y los documentos quedan protegidos frente a accesos no autorizados en el sistema de conservación puede considerarse óptimo, dentro de las limitaciones, como se ha indicado y la propia legislación reconoce, inevitables en los entornos digitales.

Conclusiones

En el presente artículo se ha pretendido explicar, y argumentar a partir de circunstancias reales y no abstractas, que la protección de datos de carácter personal no es en modo alguno una alegre y positivista tarea, para realizar la cual sólo es necesario aplicar procedimientos bien definidos. Antes al contrario, se ha argumentado que se trata de un proceso lleno de indefiniciones y contradicciones legales, técnicas y tecnológicas, y se ha intentado explorar, desde el punto de vista del archivo, el modo en que estas indefiniciones y contradicciones convierten el proceso en uno de los más complejos del contemporáneo quehacer archivístico, particularmente en entornos digitales.

No obstante, también se ha pretendido mostrar que estos problemas pueden solventarse, aplicando tanto unos mecanismos de reflexión detallados como unas tecnologías que aborden de frente los aspectos negativos o conflictivos, más que la mera aseveración del éxito no contrastado. Para ello, se ha descrito de manera muy somera una implantación práctica que hasta el momento no ha devuelto fracasos, lo cual no implica, por supuesto, que no pueda devolverlos en algún punto del futuro, dado el actual estado del arte, en permanente evolución y escasamente reglado, de las tecnologías de la información y de las comunicaciones.

En cualquier caso, esperamos haber dejado claro que los procesos de

protección de datos, como cualquier otro proceso de creación, gestión y uso de los mismos, tanto en los sistemas de producción como en los de conservación, son cualquier cosa menos sencillos, requieren un cuidadoso cuestionamiento de la legislación, que no por serlo es infalible, y una aportación en condiciones de igualdad de diferentes disciplinas, incluida la archivística o gestión de documentos. Finalmente, habida cuenta de la naturaleza invisible, invasiva, inestable, distribuida, multipropósito y evolutiva de las actuales tecnologías de la información y de las comunicaciones, ninguna implantación tecnológica de los requisitos legales puede tener éxito sin un permanente esfuerzo de investigación y desarrollo transdisciplinares.

Bibliografía

Delgado Gómez, Alejandro, *El centro y la equis: una introducción a la descripción archivística contemporánea*, Cartagena (España) Ayuntamiento: 3000 Informática, 2007.

España. Anteproyecto de ley de Transparencia, Acceso a la Información Pública y Buen Gobierno. Disponible en: http://www.leydetransparencia.gob.es/anteproyecto/

España. Constitución, 1978. Disponible en: http://www.boe.es/aeboe/consultas/enlaces/documentos/ConstitucionCASTELLANO.pdf

España. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Disponible en: http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf .

España. Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. Disponible en: http://www.boe.es/boe/dias/1985/06/29/pdfs/A20342-20352.pdf .

España. Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. URL: http://www.boe.es/boe/dias/1992/11/27/pdfs/A40300-40319.pdf

España. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Disponible en:
http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf .

España. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Disponible en: http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf .

Iacovino, Livia, "Privacy as a human right in Italian data protection law and its impact on records as evidence and memory", en: *Archives & Social Studies: A Journal of Interdisciplinary Research*, vol. 2, núm. 2 (september 2008). pp. 363-388. Disponible en: http://socialstudies.cartagena.es/images/PDF/vol2n2/iacovino_privacy.pdf

InterPARES 2 Terminology Database. Disponible en: http://www.interpares.org/ip2/ip2_terminology_db.cfm.