

La gestión de los documentos electrónicos

Normalización y ordenamiento jurídico





N
O
R
M
S

ALL DAY
STEAK SPECIALS
\$5.99

BURRITOS
\$5.99

ONE WAY
←

La gestión de los documentos electrónicos

Normalización
y ordenamiento jurídico

The management
of electronic records
Standardization
and legal system

Vicent Giménez-Chornet

Luis Hernández Olivera

TABULA

ESTUDIOS ARCHIVÍSTICOS DE CASTILLA Y LEÓN

ISBN: 978-84-941454-7-6

ISSN: 1132-6506 = TABULA (Salamanca)

Depósito Legal: S. 671-1992

Edita

Asociación de Archiveros de Castilla y León
Armuña, 14. 37439 San Cristóbal
de la Cuesta. Salamanca
Teléfono 606 435 736
publicaciones.acal.es
www.acal.es
administracion@acal.es

Director

Luis Hernández Olivera

Editores de este volumen

Vicent Giménez-Chornet (Universidad
Politécnica de Valencia, Valencia) y Luis
Hernández Olivera (Universidad de
Salamanca)

Política editorial

Tábula publica artículos originales sobre
trabajos de investigación y de difusión de
experiencias profesionales, previamente
sujetos a un proceso de selección y
evaluación por pares. Cada número aborda
monográficamente un tema de interés
archivístico.

La publicación tiene el objetivo de
contribuir al desarrollo de una Archivística
en la que se integren el tratamiento de la
documentación histórica y la gestión de los
documentos administrativos, una
Archivística abierta a las aportaciones de
otras disciplinas, una Archivística
autónoma y con un corpus propio de
principios y métodos que pueda hacer
frente a los problemas de los archivos.

Tábula es la revista de estudios de la
Asociación de Archiveros de Castilla y León
(ACAL). Se dirige a la comunidad profesio-
nal y científica que trabaja en el ámbito
de la gestión de los archivos y documentos.
Tábula se publica en castellano y los
títulos, resúmenes y palabras-clave de los
artículos se difunden también en inglés.

Suscripciones y compras

La suscripción a la revista se realiza por
años naturales completos. Edición
impresa: suscripción conjunta de las
revistas Tábula y Archivos (1 número
de Tábula y 4 números de Archivos)
y acceso online, 75 eur.
Edición online: suscripción de acceso
a la edición online de Tábula
(período 2005-2018), 170 eur.

Ejemplar edición impresa, 30 eur.
Ejemplar edición online, 15 eur.
Artículo edición online, 5 eur.

La suscripción o compra de la revista
se puede realizar online en
www.acal.es/tienda-online-acal
o contactando con Administración Acal:
tel. 650 336 756; administracion@acal.es
La adquisición de un pdf con un número
completo de la revista o de un artículo se
puede realizar en: publicaciones.acal.es

La publicación se distribuye de forma
gratuita a los miembros de la Asociación.

Nota de copyright

Algunos contenidos de Tábula están
protegidos por copyright:
© de los textos, los autores
© de las traducciones y edición, la
Asociación de Archiveros de Castilla y León
© de las fotografías, los autores

La Asociación de Archiveros de Castilla
y León está trabajando para ir ofreciendo
de forma gradual los contenidos
de la revista con acceso abierto.

La Asociación de Archiveros de Castilla
y León no asume ninguna responsabilidad
por las opiniones o juicios vertidos en los
artículos por sus autores.

Consejo Editorial

Alicia Barnard (Consultoría en Servicios de Información, Ciudad de México, México); Javier Barbadillo Alonso (Archivo, Ayuntamiento de Guadalajara, Guadalajara, España); Julio Cerdá Díaz (Archivo, Ayuntamiento de Arganda del Rey, Arganda del Rey, Madrid, España); Adrian Cunningham (Queensland State Archives, Department of Science, Information Technology and Innovation, Australia); Alejandro Delgado Gómez (Archivo, Ayuntamiento de Cartagena, Cartagena, España); Alfonso Díaz Rodríguez (Archivo, Gobierno del Principado de Asturias, Oviedo, España); Miguel Ángel Esteban Navarro (Universidad de Zaragoza, Zaragoza, España); Luis Esteve Casellas i Serra (Sección de Gestión Documental y Archivo (GDA), Ayuntamiento de Girona, Girona, España); Antonio González Quintana (Grupo de Trabajo sobre Archivos y Derechos Humanos del Consejo Internacional de Archivo, Madrid, España); Antonia Heredia Herrera (Archivera, Doctora en Historia de América, Sevilla, España); José María Jardim (Departamento de Documentación de la Universidad Federal Fluminense, Rio de Janeiro, Brasil); Vicent Giménez-Chornet (Departamento de Comunicación Audiovisual, Documentación e Historia del Arte, Universidad Politécnica de Valencia, Valencia, España); Joaquim Llansó Sanjuan (Archivero, Archivo General de Navarra, Pamplona, España); M. Paz Martín Pozuelo (Departamento de Biblioteconomía y Documentación, Universidad Carlos III, Getafe, Madrid, España); Abelardo Santamaría Gallo (ACAL, Valladolid, España)

Comité de evaluadores

Henar Alonso Rodríguez (Técnica Superior de Archivos, Archivo General Militar de Ávila, Ávila, España); Alicia Barnard (Consultoría en Servicios de Información, Ciudad de México, México); Pedro Cabrera Hernández (Gestión Documental y Archivo, Ayuntamiento de Tinajo, Las Palmas, España); Alfonso Díaz Rodríguez (Archivo, Gobierno del Principado de Asturias, Oviedo, España); José Luis Domínguez Álvarez (Facultad de Derecho, Universidad de Salamanca, Salamanca, España); Joan Carles Faus Mascarell (Archivero, Archivo Municipal Administrativo, Ayuntamiento de Gandía, Gandía, Valencia, España); Francisco Fernández Cuesta (Consejero Técnico, Ayuntamiento de Madrid, Madrid, España); Juan José Generelo Lanaspá (Archivo Histórico Provincial de Zaragoza, Zaragoza, España); Antonia Heredia Herrera (Archivera, Doctora en Historia de América, Sevilla, España); José María Jardim (Departamento de Documentación, Universidad Federal Fluminense, Rio de Janeiro, Brasil); Joaquim Llansó Sanjuan (Archivero, Archivo General de Navarra, Pamplona, España); Rosa López Alonso (Facultad de Traducción y Documentación, Universidad de Salamanca, Salamanca, España); Ana Belén Ríos Hilarío (Facultad de Traducción y Documentación, Universidad de Salamanca, Salamanca, España); M^a del Carmen Rodríguez López (Departamento de Patrimonio Artístico y Documental, Universidad de León, León, España) y Ana de la Rosa Castro (Máster en Evaluación y Gestión del Patrimonio Cultural)

Traducciones

Verónica Fernández de Cabo

Revisión de textos

Paz Hernández Sánchez

Diseño y maquetación

Helvética edición y diseño

Publicidad

Teléfono 606 435 736
administracion@acal.es

Fotografías

Cubierta: Norm's Coffee Shop | Ashok Sinha
Pág. 18: Construction Signs / Flickr | Jphillipg
Pág. 36: Information Sign / Flickr | speedpropertybuyers.co.uk
Pág. 51: Follow the sign / Unsplash | Cendrine Marrouat
Pág. 52: Multilingual road sign / Flickr | Alanah Heffez
Pág. 71: kuznetzov.4n
Pág. 72: NSA / Foursquare | Michael Colvin
Pág. 93: Not so secret bunker / Flickr | Ross Younger
Pág. 94: Security Cameras / Flickr | Mike Mozart
Pág. 113: Private / Flickr | Oatsy40
Pág. 114: Les Grands Voisins Project / Medium | Anat Meruk
Pág. 139: Open Range / Pxhere
Pág. 140: A los voluntarios de las Brigadas Internacionales / Wikimedia | Emilio J. Rodríguez Posada
Contracubierta: Digitaline Nativelle / Todocolectión

Normas para los autores

Los originales que se presenten deben ser inéditos y deben cumplir las directrices de presentación de textos indicadas a continuación.

Presentación de los textos

1. Formato

Los manuscritos deben entregarse en forma de fichero electrónico, preferentemente en formato Word

2. Datos de identificación del artículo

En la primera página se indicarán los siguientes datos del artículo:

a) Título y subtítulo, si lo hubiere, del artículo en castellano e inglés con un tipo de letra Arial en negrita y un tamaño de 16 puntos.

b) Nombre del autor o de los autores, centro de trabajo, y dirección de correo electrónico de cada uno de ellos, con un tipo de letra Arial en cursiva y un tamaño de 12 puntos.

Ejemplo:

*Julio Cerda Díaz
Archivo Municipal de Arganda
email: julio.cerda@uah.es*

c) Resumen del trabajo en castellano e inglés. En el resumen, con una extensión aproximada de 100 palabras, se recomienda indicar los objetivos, metodología y resultados. Para el texto del resumen se utilizará el tipo de letra Arial con un cuerpo de 12 puntos y un interlineado sencillo.

d) Palabras clave en castellano e inglés. Se recomienda presentar entre 5 y 10 palabras clave para indizar el texto y facilitar su recuperación. Se redactarán en letra Arial con un cuerpo de 12 puntos, en mayúsculas, separándolas por una barra precedida y seguida de espacio y un interlineado sencillo.

3. Extensión

El tamaño recomendado de un artículo está entre las 5.000 y 6.000 palabras. En aquellos casos que se justifiquen se podrán publicar artículos de mayor extensión.

4. Diseño del texto

El texto debe estar justificado. Para la redacción se utilizará el tipo de letra Arial con un cuerpo de 12 puntos y un interlineado sencillo.

5. Párrafos

No se efectuará ninguna sangría ni tabulado al inicio de párrafo. El último párrafo de cada epígrafe irá seguido de dos líneas en blanco que precederán al título del nuevo epígrafe.

6. Títulos de apartados

Los títulos de los diferentes epígrafes se numerarán y se presentarán con la siguiente jerarquía tipográfica según su nivel:

a) Título de epígrafe de primer nivel: se redactará en Arial de 14 puntos y negrita.

b) Título de epígrafe de segundo nivel: se redactará en Arial de 12 puntos y negrita.

c) Título de epígrafe de tercer nivel: se redactará en Arial de 12 puntos y cursiva.

Ejemplos:

2. MoReq

2.3. ¿Qué es MoReq2?

2.3.1. ¿Es MoReq2 una norma?

7. Ilustraciones

Los trabajos que incorporen tablas y figuras se entregarán en ficheros separados. Se deberá indicar de forma precisa el lugar en que se deberá ubicar cada tabla o figura. Al pie de cada una de ellas se deberá indicar, en Arial de 10 puntos, el número de orden que le corresponda y el título descriptivo de la ilustración.

Ejemplo:

Tabla 1. Grupos de problemas para la investigación Archivística
Fig. 2. Del antiguo al nuevo paradigma disciplinar en la ciencia archivística

8. Bibliografía

Para la citación bibliográfica se utilizará el sistema autor-fecha. Cada referencia que se incluya en el texto se realizará indicando el apellido del autor seguido de coma y la fecha de publicación, y si es necesario se añade la página, todo ello entre paréntesis. Cuando un autor cuente con varios títulos publicados en un mismo año se especificarán estos añadiendo en las distintas referencias al año una letra minúscula (a, b, c, etc.).
Ejemplos:

(Cox, 2003, p. 19)

(Cox, 2002a, p. 8)

Al final del artículo se indicará la bibliografía con todas las referencias bibliográficas completas ordenadas alfabéticamente por el apellido del primer autor o del primer elemento de la referencia y el año de publicación. Las referencias irán precedidas de la palabra "Bibliografía" en negrita con un tipo Arial de 14 puntos y se realizarán según los siguientes modelos y cumpliendo los estilos de fuentes prescritos para cada elemento:

Ejemplos:

Referencia de monografía:

SHELLENBERG, Theodore R. (1987). *Archivos modernos: principios y técnicas*. México: Archivo General de la Nación.

Referencia de artículo de revista:

DURANTI, Luciana. (2003). "Autenticidad y valoración: la teoría de la valoración enfrentada a los documentos electrónicos2. *Tábula: revista de Archivos de Castilla y León*. n. 6, p. 13-21.

Referencia de capítulo de libro:

Gómez González, Pedro José (2008). "La organización de archivos musicales". En: Gómez González, Pedro José et al (eds.). *El archivo de los sonidos: la gestión de fondos musicales*. Salamanca: Acal, p. 125-154.

Referencia de recurso electrónico:

Cook, Terry (2011). "Archives as Media of Communication". En: *Old Messengers, New Media: The Legacy of Innis and McLuhan*. <<http://www.collectionscanada.gc.ca/innis-mcluhan/030003-4040-e.html>>. [Consulta: 18/06/2012].

9. Notas

Las notas se colocarán al final del texto con un tamaño de letra de 10 puntos del mismo tipo de letra Arial. Irán precedidas de la palabra "Notas" en negrita con un tipo Arial de 14 puntos.

Las notas en el cuerpo del texto irán colocadas en superíndice numérico (1, 2, 3, ...).

10. Apéndices

Si el artículo tiene apéndices, éstos se añadirán al final del texto, después de las notas, introducidos por la palabra "Apéndice" en negrita cuerpo 14, y el texto en cuerpo 10.

La gestión de los documentos electrónicos. Normalización y ordenamiento jurídico

- 11 Introducción
El ordenamiento de la gestión de los documentos electrónicos
- 19 Cinco reflexiones sobre normativa para gestión documental
Enriqueta Sesmero Cutanda
- 37 Los metadatos en el ordenamiento jurídico español y europeo
Vicent Giménez-Chornet
- 53 La terminología internacional de gestión de documentos
y archivos según las normas ISO e IEC
Liudmila Varlamova
- 73 Secretos empresariales en documentos
y ficheros electrónicos y la protección de datos personales
y garantía de los derechos digitales
Francisca Ramón Fernández
- 95 Interoperabilidad administrativa y protección de datos personales:
claves para garantizar el derecho a una buena Administración
José Luis Domínguez Álvarez
- 115 Documentos electrónicos en el Gobierno Abierto de la República
Argentina: hacia un sistema de gestión con tutela constitucional,
convencional y procesal de la protección de datos personales
y acceso a la información pública
Diego Robledo
- 141 La Sección Histórica de las Brigadas Internacionales:
los archivos al servicio de la propaganda y la memoria histórica
Francisco Javier Fito Manteca

The management of electronic records. Standardization and legal system

- 15 Introduction
The legal order of electronic records management
- 19 Five reflections on records management regulation
Enriqueta Sesmero Cutanda
- 37 Metadata in the Spanish and European legal system
Vicent Giménez-Chornet
- 53 International terminology standardized by ISO and IEC
used in records and archives management
Liudmila Varlamova
- 73 Business secrets in electronic records and files and
the personal data protection and guarantee of digital rights
Francisca Ramón Fernández
- 95 Administrative Interoperability and personal data protection:
keys to guarantee the right to good Administration
José Luis Domínguez Álvarez
- 115 E-files in the Open Government of the Republic Argentina:
looking forward to a management system with constitutional,
covenant and procedural warrants of personal data's
protection and access to public information
Diego Robledo
- 141 The Historical Section of the International Brigades:
the archives at the service of propaganda and historical memory
Francisco Javier Fito Manteca

El ordenamiento de la gestión de los documentos electrónicos

Nos encontramos en un periodo de transición de una administración basada en los documentos en papel a una administración cuyos documentos han sido producidos en formato electrónico. La revolución digital en la que nos encontramos repercute no sólo en los soportes y formatos sino también, y de manera relevante, en nuevos modelos de procesos y de gestión, que demandan otros conocimientos y competencias del personal que realiza un trabajo técnico más complejo. La interdisciplinaridad en el aprendizaje es cada vez más necesaria para la resolución de los retos de nuestra era. El marco normativo también se debe adecuar en regular un nuevo modelo de administración, y en dar validez a los documentos electrónicos. Sin papel, u otros soportes tradicionales, no se hubieran registrado las evidencias de la sociedad y de las administraciones, y ahora, sin electricidad, no hay documento digital.

Las Tecnologías de la Información y la Comunicación (TIC) han cambiado la administración pública, y su incorporación la solemos denominar como modernización de la administración, repercutiendo en la cultura organizacional. La producción y recepción de la información requiere de un uso de la tecnología que las administraciones canalizarán mediante servicios para satisfacer a su comunidad de ciudadanos, que demandan menos restricciones en el acceso a la información. Las disposiciones legales y la jurisprudencia se deben adecuar a las sociedades democráticas, donde las evidencias de los actos administrativos y de gobierno deben ser accesibles, con eficacia. Para ello la gestión de la información,

la gestión de los documentos de archivo, la gestión de datos, requiere del uso de las TIC para satisfacer a las necesidades de unos ciudadanos que demandan más transparencia en la gobernanza. Los archiveros no sólo deben conocer el nuevo marco normativo, sino que deben estar involucrados en el trabajo legislativo, que incidirá en la planificación y gestión de la información. Los archiveros son conscientes de los nuevos riesgos que supone la gestión de los documentos electrónicos, por ello las normas jurídicas y las normas de buenas prácticas ayudan a canalizar soluciones para minimizar esos riesgos, en aspectos tan importantes como a preservación digital, la autenticidad e integridad de los documentos, la interoperabilidad, la descripción, la recuperación de la información, la protección de datos, la reutilización de la información, la transparencia, las responsabilidades o el gobierno abierto.

Las Tecnologías de la Información y la Comunicación (TIC) han cambiado la administración pública, y su incorporación la solemos denominar como modernización de la administración, repercutiendo en la cultura organizacional. La producción y recepción de la información requiere de un uso de la tecnología que las administraciones canalizarán mediante servicios para satisfacer a su comunidad de ciudadanos, que demandan menos restricciones en el acceso a la información. Las disposiciones legales y la jurisprudencia se deben adecuar a las sociedades democráticas, donde las evidencias de los actos administrativos y de gobierno deben ser accesibles, con eficacia. Para ello la gestión de la información, la gestión de los documentos de archivo, la gestión de datos, requiere del uso de las TIC para satisfacer a las necesidades de unos ciudadanos que demandan más transparencia en la gobernanza. Los archiveros no sólo deben conocer el nuevo marco normativo, sino que deben estar involucrados en el trabajo legislativo, que incidirá en la planificación y gestión de la información. Los archiveros son conscientes de los nuevos riesgos que supone la gestión de los documentos electrónicos, por ello las normas jurídicas y las normas de buenas prácticas ayudan a canalizar soluciones para minimizar esos riesgos, en aspectos tan importantes como a preservación digital, la autenticidad e integridad de los documentos, la interoperabilidad, la descripción, la recuperación de la información, la protección de datos, la reutilización de la información, la transparencia, las responsabilidades o el gobierno abierto.

Como afirman A. Dikopoulou y A. Mihiotis (2012) “el documento se define como la declaración de voluntad de cualquier persona o entidad corporativa, pública o privada, que ha sido registrada, firmada y emitida de acuerdo con los procedimientos administrativos y legislativos establecidos y bajo la jurisdicción establecida de la persona u entidad corporativa”. Los aspectos legales inciden desde la misma generación de los documentos. Los gobiernos locales, más cercanos a los ciudadanos, deben de dar signos de transparencia y accesibilidad para alentar un diálogo entre gobernantes y gobernados, mediante una administración más cercana

y rápida en la capacidad de respuesta. Es un diálogo bidireccional que aumenta la confianza de los ciudadanos en sus gobiernos. El Reglamento Europeo n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (denominado eIDAS), es un incentivo legislativo para que los servicios de nuestras administraciones sean confiables a los ciudadanos, entre ellos deben estar los servicios archivísticos y los servicios de información de las administraciones públicas. Para disponer de un “servicio de confianza cualificado” los prestadores del servicio deben ser auditados, para confirmar que prestan correctamente los servicios establecidos. Si bien el reglamento indica que los auditores deben ser externos a la organización, las inspecciones y auditorías internas de archivos han estado contemplados en el ordenamiento jurídico español, como un medio de evaluar el servicio prestado y funcionamiento de nuestras instituciones archivísticas.

En el presente número de *Tabula* encontramos análisis de algunos de los aspectos tan amplios que las normas están contemplado, poniendo de relieve su importancia en la labor archivística, en la eficiencia de las administraciones y, en definitiva, en un gobierno democrático confiable. Enriqueta Sesmero señala algunas insuficiencias en el marco jurídico vigente, y remarca que en la gestión documental electrónica se desaprovechan las ventajas que ofrecen las TIC para custodiar la información de manera distribuida. Vicent Giménez analiza en qué aspectos la normativa europea y española regulan los metadatos, especialmente en la reutilización, la interoperabilidad y la descripción. Liudmila Varlamova aborda el debate de la terminología en la gestión de los documentos de archivos repasando las normas ISO e IEC, normas de buenas prácticas, donde advierte que el sistema terminológico no está bien armonizado. Francisca Ramón se adentra en el análisis de los documentos de las empresas, en el marco jurídico de la protección de los secretos empresariales y la protección de datos de carácter personal. José Luis Domínguez resalta la importancia de la interoperabilidad administrativa en la implementación de la administración electrónica, donde se debe dedicar especial atención en garantizar la seguridad de la información que contenga datos de carácter personal, consecuencia de un proceso de digitalización y datificación de nuestra sociedad. Diego Robledo analiza el marco jurídico que se está desarrollando en Argentina en base a cinco ejes, el gobierno digital, la modernización administrativa, el gobierno abierto, los recursos humanos y el país digital, y señala como la tecnología blockchain puede ser una alternativa eficaz para la validez probatoria de los documentos digitales. Finalmente, en el apartado *Varia*, Francisco Javier Fito realiza un estudio sobre la importancia que tuvo la creación en 1937 de la Sección Histórica de las Brigadas Internacionales para la creación de un servicio de documentación que apoyase al comisariado de guerra.

Referencias

- DIKOPOULOU, A.; MIHIOTIS, A. (2012), “The contribution of records management to good governance”, *The TQM Journal*, vol. 24 n° 2, p. 123-141. <<https://doi.org/10.1108/17542731211215071>> [Consulta: 18/11/2019].
- UNIÓN EUROPEA (2014). Reglamento (UE) n° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. *Diario Oficial de la Unión Europea*, L 257, 28.8.2014, p. 73-114 <<http://data.europa.eu/eli/reg/2014/910/oj>>; [Consulta: 18/11/2019].

Vicent Giménez-Chornet
Luis Hernández Olivera

The legal order of electronic records management

We are in a period of transition from a paper-based administration to an electronic format one. We are undergoing a digital revolution that has an impact not only on the media and formats but also, and in a relevant way, on new models of process and management, demanding other skills and competencies of the staff performing more complex technical tasks. Interdisciplinarity in learning is becoming more and more necessary for the resolution of the challenges of our time. The legislative framework should also be adapted to regulating a new management model and validating electronic documents. Without paper or other traditional media, the evidence of society and administrations would not have been recorded, and now, without electricity, there is no digital document.

Information and Communication Technologies (ICTs) have changed public administration and its incorporation is often referred to as a modernization of the administration, affecting the organizational culture. The production and receipt of information requires the use of technology that administrations will channel through services in order to satisfy their community of citizens, who demand fewer restrictions on access to information. Legal provisions and jurisprudence should be adapted to democratic societies, where evidence of administrative and governance acts must be effectively available. To do this, ICTs are required in information, records and data management in order to meet the needs of citizens demanding more transparency in governance. Archivists must not only know the new regulatory framework, but must also be involved in legislative work, which will have an impact on information planning and management. Archivists are aware of the new risks involved in managing electronic documents,

so legal norms and good practice standards help channel solutions so as to minimize those risks in such important aspects as digital preservation, document authenticity and integrity, interoperability, description, retrieval of information, data protection, reuse of information, transparency, responsibilities or open government.

As stated by A. Dikopoulou and A. Mihiotis (2012) “the document is defined as the statement of intent of any person or corporate entity, public or private, that has been registered, signed and issued in accordance with administrative and legislative procedures established under the jurisdiction of the corporate person or entity.” The legal aspects exist from the very generation of the documents. Local governments, closer to citizens, must give signs of transparency and accessibility to encourage dialogue between rulers and governed, through an administration closer and faster in its responsiveness. It is a two-way dialogue that increases citizens’ confidence in their governments.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (called eIDAS) is an incentive for the services of our administrations to be reliable to citizens and archival and information services of public administrations must be among them.

In order to have a “qualified trust service”, service providers must be audited to confirm that they provide the correct services. While the regulation states that auditors should be external to the organization, internal inspections and audits of records have been provided for by the Spanish legislation as a means of assessing the service provided and the way our archival institutions work.

In this issue of *Tabula* we find analyses of some of the broad aspects provided for by standards, highlighting their importance in the archival work, in the efficiency of administrations and, ultimately, in a reliable democratic government. Enriqueta Sesmero points out some weaknesses in the current legislative framework, and highlights that electronic records management misses the advantages offered by ICTs to preserve information in a distributed manner. Vicent Giménez analyses where European and Spanish legislations regulate metadata, especially in reuse, interoperability and description. Liudmila Varlamova addresses the discussion of terminology in the records management by reviewing ISO and IEC standards, good practice standards where she warns that the terminology system is not well harmonized. Francisca Ramón delves into the analysis of business records in the legislative framework for the protection of trade secrets and personal information. José Luis Domínguez emphasizes administrative interoperability in the implementation of electronic administration, where special attention should be devoted to ensuring the security of personal information, result of a process of digitization and datification of our society. Diego Robledo analyses the legislative framework being developed in Argentina based on five axes, the Digital

Government, Administrative Modernization, Open Government, Human Resources and the Digital Country, and points out how Blockchain technology can be an effective alternative for the evidential validity of digital documents. Finally, in the Varia section, Francisco Javier Fito studies how the creation in 1937 of the Historical Department in the International Brigades was important for the creation of a documentation service that supported the war commissionerhip.

References

- DIKOPOULOU, A.; MIHIOTIS, A. (2012), "The contribution of records management to good governance", *The TQM Journal*, vol. 24 no 2, pp.123-141. <<https://doi.org/10.1108/17542731211215071>> [Accessed: Nov 18, 2019].
- EUROPEAN UNION (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ, L 257, 28.8.2014, p. 73-114 <<http://data.europa.eu/eli/reg/2014/910/oj>> [Accessed: Nov 18, 2019].

Vicent Giménez-Chornet
Luis Hernández Olivera





ENRIQUETA SESMERO CUTANDA

Cinco reflexiones sobre normativa para gestión documental

Five reflections on records
management regulation

Enriqueta Sesmero Cutanda
Enriqueta.SESMERO@bizkaia.eus
Diputación Foral de Bizkaia

Citación: Sesmero Cutanda, Enriqueta (2019). "Cinco reflexiones sobre normativa para gestión documental". *Tábula*, n. 22, pp. 19-35

Recibido: 22-7-2019. *Aceptado:* 4-9-2019

Resumen analítico / Analytic summary

Este ensayo trata cinco campos concretos de la gestión documental en que, a juicio de la autora, la normativa vigente es insuficiente o requiere una mejor interpretación: los sistemas basados en documentación distribuida, la validez jurídica de las trazas de tramitación, las transferencias en entornos digitales, la documentación de cargos públicos y la archivística colaborativa. Tras analizar los problemas desde una perspectiva empírica, se proponen vías de actuación. Según los casos, se indican las bases teóricas, cuestiones colaterales e implicaciones sociales y éticas de lo expuesto .

GESTIÓN DOCUMENTAL | NORMATIVA | ARQUITECTURA DE SISTEMAS | TRAZAS INFORMÁTICAS | DOCUMENTACIÓN DISTRIBUIDA | TRANSFERENCIA | DOCUMENTACIÓN | PRESERVACIÓN | CARGOS PÚBLICOS | ARCHIVÍSTICA COLABORATIVA

This essay deals with five specific areas of records management in which, according to the author, current regulation is insufficient or require a better interpretation: systems based on distributed records, legal validity of administrative processing traces, document transfers in digital environments, records of public offices and collaborative archiving. Firstly, problems are analysed from an empirical point of view; then, some ways of intervention are suggested. Depending on the case, either theoretical basis, collateral issues and/or social and ethic consequences are indicated.

RECORDS MANAGEMENT | REGULATION | SYSTEMS ARCHITECTURE | COMPUTER TRACES | DISTRIBUTED RECORDS | TRANSFER | RECORDS | PRESERVATION | PUBLIC OFFICES | COMMUNITY ARCHIVES

Las tecnologías de la información y la comunicación permiten a quienes nos ocupamos en la gestión documental [GD] una ligereza que contrasta con parte del acervo normativo superior que afecta a la administración pública [AP], lastrado por la tradición conceptual y la praxis en soporte analógico. Como es de obligado cumplimiento, y dada la rigidez procedimental del Derecho imperante, su interpretación restringe el de menor rango e incluso afecta al técnico. Subyace un problema de fondo: la falta de atención a nuestra profesión por “el legislador” (figura impersonal a la que debería ser preceptivo poner nombre y apellidos, para fijar responsabilidades) cuando redacta disposiciones que afectan a nuestro campo, aun de modo tangencial. Dejémoslo ahí, aunque habría que comenzar por variar la legislación con respecto a eso.

Este ensayo es de contenido heterogéneo, pues deriva del cotejo de problemas prácticos con el cuadro normativo que los rige. Las tres primeras versan sobre arquitectura de un sistema de GD. Proceden de haber constatado que en ciertas Administraciones se está remedando el funcionamiento en soporte papel. Aparte del coste en recursos de todo tipo, eso tiene el agravante de que puede dificultar lo que se está configurando como una tendencia imparable: implantar el datacentrismo, sea cual sea su alcance.

Siguen otras dos sobre preservación; dimanen de la consciencia que nuestro colectivo profesional tiene sobre su papel activo en la protección de la democracia y el cumplimiento de la transparencia, pese a que tal intervención pocas veces haya logrado reconocimiento explícito en las normas¹. Las cinco son reflexiones personales, simplificadas por limitación de espacio; tratan de la Administración en abstracto y no detallan modelo alguno.

Toda referencia a documentación presupone que es electrónica, con indicación expresa para lo analógico, como en parte hace la Ley 39/2015, de

Procedimiento Administrativo Común (PACAP) y ya debería ser habitual en la regulación. Aunque comprenda todo tipo de objetos, al tratar de sistemas de GD hablaremos de expedientes y documentos porque así es habitual en las normas generales. Dicha gestión se concibe como integral, sin cesuras desde la fase de diseño hasta la aplicación de las decisiones de disposición y los usos tras el archivado, como convendría fijar en la norma.

Quiero pensar que ninguna AP necesita ya regular que su proyecto de GD sea multidisciplinar, incluya lo archivístico desde el principio y considere de continuo a la ciudadanía usuaria, derechohabiente y cotizante. Como profesional y como simple persona cuento con él. Lo que haya de bueno en estas líneas es un reconocimiento a quienes lo están llevando a cabo en mi institución; todas ellas, sólo responsabilidad de quien las firma.

Arquitectura del sistema

Documentación distribuida

Reflexión de partida: en general, la normativa existente basa la GD en objetos digitales, lo que propicia sobrecargar innecesariamente los sistemas.

O al menos así se interpreta, aunque ni el expediente ni el documento existan de entrada como objetos. Son una construcción conceptual y funcional que tecnológicamente se conforma a la carta a partir de elementos de origen y localización a menudo dispares, cuyo tratamiento y configuración va variando a lo largo su ciclo de vida. En la PACAP (art. 70) se consideraron entidades “cerradas”, en el sentido administrativo clásico, porque se pretendía asegurar que la producción documental se ajustase al cumplimiento de las funciones públicas. Que esa ley sea uno de nuestros marcos de referencia no implica que adoptemos su perspectiva. Renunciaríamos a una de las grandes ventajas de la GD electrónica, la de funcionar en base a entornos distribuidos de almacenamiento de la información. Su elegancia consiste en que permite cumplir dos principios. Uno, el famoso –por incumplido– *once only* de presentación única de documentos ante la Administración. Otro, el de economía: que gestionar más no implique producir documentación en proporción directa, ni tampoco conservarla. Especificarlo y desarrollarlo normativamente es, pues, una necesidad.

Quizá sea hoy más fácil ver desde esa óptica el documento simple². Está de luna de miel con la datificación, y no es para menos. Lo ha convertido en una interfaz para que la ciudadanía nos proporcione y actualice información reutilizable más allá del procedimiento para el que se presenta, con lo cual somos capaces de automatizar, de manera proactiva, la propia conformación de la unidad documental. Sin embargo, en bastantes sistemas se pretende generar un fichero fijo, habitualmente en PDF. Resulta la mejor opción actual de visualización, cierto, lo

que no implica que lo sea para el archivado. Así lo entiende el proyecto de reglamento (2018) que desarrollará la PACAP: establece que *la conservación de los documentos electrónicos se hará de forma unitaria*, a la vez que admite que se guarde su información en bases, a condición de que la acompañen los formularios o modelos de los documentos y que se puedan comprobar su identificación o firma; imbricados, pero no obligatoriamente encapsulados. Si existe un estándar para preservar bases de datos relacionales³, ¿qué nos obliga a quedarnos con todos sus pesadísimos productos?

Por su parte, el expediente parece condenado a una pesadez dinosauria, por una interpretación restrictiva del Esquema Nacional de Interoperabilidad [ENI]. Se entiende que desde el principio de la tramitación hay que ir conformando entes unitarios, por más que sean modificables antes del cierre definitivo; y se olvida que el ENI los exige sólo para el intercambio. En tramitación no hay por qué mantenerlos así. Cumpliremos si cuando se nos solicite uno completo, porque no baste que quien lo pida verifique su existencia o por otro motivo, lo enviemos como ENI impecable. Mientras, sus componentes (documentos, trazas, validaciones) podrán almacenarse por separado y en realidad manejaremos los que se ha dado en llamar expedientes ENI-compatibles. No es un problema de metadato, por la facilidad de implementar el mínimo exigido por la Norma Técnica de Interoperabilidad de expediente electrónico⁴. Lo que aligera el sistema, incluso si su grado de docucentrismo es todavía alto, es construirlo distribuido. Permite la utilización múltiple de un solo documento; después, discriminar los activos de información dignos de vida permanente, blindarlos y eliminar el resto.

Al final, eso nos lleva a lo que debe ir primero. En toda buena arquitectura de GD hay dos pilares indispensables: la reingeniería de procesos y la valoración. Si en aquella intervienen todas las partes implicadas en cada procedimiento, comenzando por los servicios jurídicos, evitaremos seguir clonando la normativa papelerística; en consecuencia, no pediremos lo que ya tengamos o podamos conseguir de otras AP por nuestros propios medios, sabremos si quien tramita necesita todo el documento o sólo tal o cual dato, y diseñaremos unos flujos de tramitación claros y ligeros fáciles de automatizar. La figura de técnica/o de organización nos resulta un miembro de proyecto indispensable.

Pensar en cómo conformaremos los objetos destinados a preservación a largo plazo es un punto clave. Trabajar en un entorno distribuido y con componente datacéntrico permite aligera los descomunales montos de documentación que producen nuestras organizaciones, si reutilizamos los elementos básicos que la conforman y eliminamos los superfluos. Una línea de gestión bien diseñada habrá permitido ir cumpliendo etapas secuenciales concatenadas y estará contextualizado al detalle. Partiendo siempre de la macrovaloración de base funcional que formulara hace casi treinta años Terry Cook (2003), al evaluar en detalle los

documentos y los datos detectaremos mejor los activos de información relevantes para otros usos o como legado de futuro, y se los dejaremos disponibles libres de todo ruido.

Trazas de actuación

Reflexión de partida: reconocer validez jurídica a ciertas trazas de los sistemas de tramitación.

La simplificación de los procedimientos administrativos resultante de aplicarles reingeniería de procesos, interoperabilidad, el principio de presentación única y sentido común topa a veces con las reticencias de algún servicio jurídico muy garantista, que ve la administración electrónica como un trasunto de su antecesora en papel. No se trata de brecha digital; personas recién graduadas entienden como necesario un PDF firmado para validar una consulta a bases de datos externas o una mera ejecución en la línea de tramitación. Tal prevención es hasta cierto punto comprensible: el mundo de la ley es rígido y formalista a la par que sinuoso e interpretable, y es inhabitual que se haya (in)formado a sus especialistas en los fundamentos de la GD actual y sus altísimas exigencias de control, validación y verificación. Las unidades administrativas no siempre se atreven a contradecir a quien tiene gran peso en la institución, no vayan a pillarse los dedos con algún retruécano legal, y acaban cediendo.

La visualización amigable de una traza es conveniente para quien tramita, incluso indispensable. En cambio, convertirla en documento resulta superfluo, y aún más validarla con firma o sello (los que sean). Los sistemas de gestión reglados y los instrumentos de interoperabilidad cuentan con bases bien desarrolladas y seguras; las administraciones, con políticas de gestión documental y de seguridad de la información, y sendos mecanismos de auditoría. El proyecto de Real Decreto de desarrollo de las leyes 39 y 40/2015 (2018, art. 26) considera las transmisiones de datos efectuadas mediante redes corporativas entre administraciones públicas como certificados administrativos probatorios. Además, en bastantes ocasiones quien tramita sólo necesita verificar la existencia o corrección del dato que ya posee. Como dijimos, en un sistema preciso un expediente con cierre definitivo habrá recorrido apropiadamente su camino, por lo que de cara a preservarlo las trazas habrán quedado implícitas, carecerán de la más mínima utilidad y la valoración nos permitirá eliminarlas con absoluta tranquilidad.

Transferencias

Reflexión de partida: la necesidad de una normativa dúctil sobre transferencias, para escenarios diversos de GD.

Las Normas Técnicas de Interoperabilidad están conformando un corpus modélico, entre otros motivos, por su precisión y su estabilidad al tratar de los requisitos de GD, pues son independientes de los detalles tecnológicos. Adaptar

nuestras construcciones a ellas es tan ventajoso, que en la práctica extendemos su alcance más allá de preparar nuestros sistemas para la interacción y son bases organizativas. De ahí que nos planteemos cómo será la futura NTI de Transferencia, cuyo borrador no se ha difundido en el momento en que se escriben estas líneas⁵. Este procedimiento, esencial para los archivos, está establecido desde hace largo tiempo. Ahora bien, si con los soportes analógicos hay que asegurarse de que la documentación se traslade completa y se legitimize expresamente el traspaso de custodia entre su órgano u organismo productor y el archivo, en un entorno electrónico ambas facetas se diluyen sin que se pierda un ápice de esas garantías.

Situémonos en el repositorio documental de una administración pública. Es único para todas las entidades que la conforman, y de máxima seguridad en todas sus prestaciones de almacenamiento y uso, por lo que nuestros documentos reposan ahí tranquilos. Por encima se han construido las aplicaciones de gestión administrativa, que apuntan hacia ellos para llamarlos o bien los generan según parámetros, reglas y plantillas concretos y los van incorporando al repositorio; en cada caso, tal y como se ha preestablecido al diseñar el flujo de tramitación. Para simplificar, pensemos sólo que manejan expedientes, porque suelen ser el grueso de la producción en aquel contexto, y olvidemos las cuestiones de propiedad de los documentos o de la información que vehiculan. El sistema es autocontrolado y auditable de modo férreo, y garantiza la completitud y corrección de cuanto en él exista. Cuando las tareas con ellos en las aplicaciones han terminado por completo, hay dos opciones conceptuales. Una, separar el trabajo administrativo del archivístico y preparar una transferencia de tipo habitual; la otra, concebir el archivado, por numerosas que sus implicaciones sean, como un “trámite” que desencadena un cambio de estado y el cómputo de plazos para las ulteriores de disposición. La gestión documental integral no sólo consiste en incluir al archivo como agente desde el diseño de la documentación para prever la realización de las tareas archivísticas, lo cual está muy bien; implica que uno y otras sean parte integrante del flujo de tramitación e integrada conceptualmente por completo en él. El expediente distribuido y el funcionamiento multientidad nos lo permiten por fin en el entorno digital, como a otras instancias (contabilidad, auditoría, etc.). ¿Por qué renunciar a semejante ventaja?

Volvamos a la transferencia. Con independencia de cómo se haya concebido su conformación en cuanto a objetos, los expedientes no van a moverse; cambiarán los permisos y vías para acceder a ellos, lo cual es otro asunto. Entonces, la primera faceta de la transferencia es innecesaria. ¿Qué pasa con la custodia? Entendámosla como en el glosario del proyecto de investigación sobre confianza de documentos y datos en entornos digitales InterPARES Trust (ITRUST, 2018, voz *Custody*): *the basic responsibility for guardianship of records/archives based upon their physical possession but not necessarily implying legal title.*

Atención a esto último. Hay expedientes que inician su vida administrativa en una unidad, la terminan en otra y recorren varias en el trayecto; la línea secuencial se lo permite con fluidez porque se ha previsto y admitido una actuación compartida. Bien, pues de inmediato al cierre el Archivo se introduce de manera automatizada (con validación humana, por supuesto) como un agente, constituido en servicio de confianza. De hecho, esta última característica debería ser admitida por norma, lo que otorgaría validez jurídica al ingreso de documentación en él –o al paso a ese estadio, según la arquitectura de la GD– y solventaría varias cuestiones de preservación⁶. ¿Objetará quien tramita? Bastante carga lleva con sus asuntos abiertos; en cuanto los haya cerrado definitivamente, agradecerá descargarse de intervenir sobre ellos, visto que la seguridad está garantizada. En efecto, la responsabilidad de custodia recae en última instancia sobre el propio sistema, en cuanto que integra los agentes en el proceso de modo holístico y absolutamente controlado. Entendiéndolo así, cabe prescindir de un acta específica firmada (con la validación que sea); el acto administrativo de cierre embebe el acto jurídico de transferir, y ni las unidades más estrictas con la protección de su documentación objetan⁷. Se ha agilizado el funcionamiento gracias a una interpretación muy sui generis del postcustodialismo⁸.

¿Y los niveles de archivo? Sin llegar al extremo de no hablar más de los propios archivos⁹, tampoco se necesitan los clásicos de oficina, intermedio e histórico. Normativamente, lo permite un renovado concepto de ciclo de vida de los documentos, el que ofrece la Guía de aplicación de la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos (2016, p. 14). Es hijo del debate anglosajón entre esa noción y la de continuo documental, y en puridad nada tiene ya que ver con la linealidad estanca que en francés se llamó, expresivamente, “teoría de las tres edades”¹⁰. Las fases de captura, mantenimiento y disposición –conservación y selección, en la NTI– están en manos de diversos agentes; no obstante, cabe implementarlas sobre un mismo sistema con arquitectura independiente de la distribución orgánica de la institución si es, como dijimos, autoprotegido, organizado según un flujo de eventos predeterminado y cimentado en relaciones de confianza. Los requerimientos para sistemas de tratamiento de documentación establecidos por MoReq2010 (DLM FORUM FOUNDATION, 2011, p. 19-20) se aúnan y cumplen sin solución de continuidad¹¹.

Para que ese proceder no se ejecute en detrimento de la preservación, incluiremos las intervenciones archivísticas desde el principio, cuando se diseñe el flujo documental. De ese modo, aplicaremos el modelo OAIS de inmediato al cierre definitivo en tramitación, generando paquetes para duración a largo plazo según estándar interoperable europeo¹², pero sólo con la documentación admitida para ello. Un motivo más para dar importancia capital a la valoración. Sin entrar ni en esta ni en la cuestión de la preservación patrimonialista, dos apuntes:

que el análisis previo de valores y contextualización contemple las reutilizaciones de datos fuera de su serie original (en algún caso, algo no tan obvio), y que la norma no limite la presencia de especialistas en las comisiones evaluadoras al habitual profesorado de Historia o Derecho Administrativo, e incluso facilite la presencia de instancias ciudadanas cuando lo recomiende el análisis funcional¹³.

Acotación al margen, tan evidente como a veces necesaria: en las instituciones que mantengan sistemas de archivo tradicionales, es indispensable acordar y regular los aspectos organizativos, con el fin de que los subsistemas (electrónico y físico, administrativo e histórico) se articulen sin cesura y sirvan con agilidad a las funciones internas y a la ciudadanía. Ni a una ni a otra les importan dónde se encuentra la información que necesitan o su grado de dispersión o disgregación, sino obtenerla completa, con rapidez y facilidad. No perdamos de vista ese objetivo primordial.

Cuestiones sobre preservación

Documentación de cargohabientes

Reflexión de partida: la generalizada desprotección legal de la documentación de cargohabientes, en especial de puestos políticos.

La escasa simpatía de nuestra profesión hacia cómo gestionan su documentación oficial las personas con destinos de rango superior es injusta en muchísimos casos. Ahora bien, aquellos en que lo hacen habiendo echado a la cuneta la ética alcanzan tal calibre, que no se comprende (o demasiado bien, según cómo y a dónde se mire) que no haya aún una regulación estricta para impedirlos. El cargo no es de nadie; lo *ejerce* alguien, y en un sistema democrático hay que impedir que lo detente. Sin seguir por ahí y aun limitándonos a la GD¹⁴, la solución es difícil por lo mucho que requiere. Para empezar, establecer flujos reglados de actuación y, sobre todo, decisiones de alto nivel que impidan el “síndrome de los archivos vacíos”. La paradoja consiste en que justamente porque una institución cumple a rajatabla sus obligaciones de transparencia, por temor a la rendición de cuentas ciertas cuestiones se tratan y aun deciden en persona por teléfono, mensajería u otras vías no controladas por el sistema de GD y quedan indocumentadas¹⁵. No menos importante es un deslinde claro entre lo público, lo privado y lo personal en cada acto y, por ende, en los elementos de información que se generan.

Esto se agrava en las redes sociales. Ahora nos preocupa su manejo para obtener datos que influyen en las decisiones de gobierno sin estar regulado, o no a fondo, por la gobernanza institucional de la información. Su uso hacia fuera de la institución está desbancando a otros recursos web menos dinámicos (blogs, foros) en la interrelación con la ciudadanía. Son instrumentos muy poderosos porque

permiten una inmediatez vertiginosa para transmitir información, visibilizar personas y hechos, generar y pulsar opinión pública y expandirse indefinidamente en ramificaciones no jerarquizadas¹⁶. Aun en el mejor de los casos –cuentas bien deslindadas, usos preestablecidos– la gestión de esos materiales es compleja. Problema de la volatilidad aparte, plantean el de la propiedad de las entradas, en dos sentidos. Uno, el de su venalidad. El utilizadísimo Twitter, por ejemplo, cobra –y no poco– por proporcionar los tuits. Triste gracia es que una administración haya de pagar por obtener una información que ha generado y de la que es dueña. ¿O no lo es? Porque si el límite entre lo público y lo privado en las redes sociales es confuso, en las de alcance político se ha difuminado hasta convertirlas en espacios complejos, a menudo deliberadamente, de nuevo con la del pajarito a la cabeza. ¿Es legítimo hacer una declaración cuasi-institucional desde una cuenta particular? Visto del revés: las cuentas “privadas” de altos cargos, ¿lo son de veras? ¿Quién lo discierne, y cómo se controla y audita su (ab)uso? Los tuiteos de Donald Trump, capaces de causar un vahído a las Bolsas de medio mundo, son un ejemplo perfecto¹⁷.

En este vidrioso campo, lo indispensable no es archivístico, sino ético: que no tumbe el proyecto de norma un órgano legislativo controlado por gente afín a quienes ejercitan desde sus sillones la opacidad de la transparencia.

Archivística colaborativa

Reflexión de partida: apoyar la interacción de los archivos con la ciudadanía para la gestión documental.

Quienes investigan en Historia anterior a la más reciente contemporaneidad lamentan la frecuente imposibilidad de conseguir testimonios directos procedentes de las clases subalternas. Es imposible. Lo documentado se amoldaba a los parámetros del poder (causas judiciales, por ejemplo) o era reinterpretado por intermediarios sociales –típico: el notariado– que comprendían la realidad popular, pero que la expresaban mediante un utillaje mental en parte ajeno. Óptica monodireccional + fuentes indirectas = pérdida de datos + sesgo de la información conservada.

Hoy no tiene por qué ser así. Desde el último tercio del XX, muchos archivos y centros de conocimiento se esfuerzan por concienciar a la gente sobre la valía de sus fuentes de información, incluida su propia memoria, y recaban así fondos¹⁸. Aunque sea una opción importante, sigue vías ya reguladas, por lo que no la trataremos¹⁹. Pese a ella, salvo notorias excepciones²⁰, la mayoría de los movimientos e iniciativas gestados por la ciudadanía se sigue documentando en vertical y a través de medios ajenos; una mínima parte de la información llega a archivos constituidos como tales, y menos aún a los públicos. Los motivos son varios: visión administrativista y/o reduccionismo intelectualista por parte del centro de archivo, algún corporativismo archivero mal entendido, falta de medios

técnicos aun cuando nada de lo anterior suceda y, el que nos interesa aquí, la carencia de amparo a la participación de la ciudadanía como sujeto agente en los procesos archivísticos que atañen a su actuación autónoma.

No por casualidad, en países anglosajones que en su día innovaron en GD, con Australia a la cabeza, se está desarrollando la comunidad de archivo (*community archives*). Se ha definido (Ruiz, 2016) como *el marco social de reapropiación del poder político por parte de la ciudadanía a través de su relación con la información pública*, lo que supone *considerar a la ciudadanía como coproductora de la información pública* y que el sistema de gestión documental sea un *mecanismo de buen gobierno*. Es un campo de extensas implicaciones éticas y metodológicas, imposibles de detallar en estas páginas. Sólo en parte son novedosas. Hace tiempo ya que nuestro colectivo criticó la falacia de la neutralidad en el archivado, la parcialidad en la conservación de documentos o el limitarse a servir a las demandas administrativas y académicas por más que estuviesen orientadas hacia mejoras sociales. Lo renovador es el modo de entender el “multiverso archivístico”²¹.

Comienza por recoger evidencias de todo tipo de fuentes y presentarlas de forma directa, no condicionada por las “élites de la información” (gobiernos, gran empresa etc.), pero va mucho más allá. Propugna dar desde el inicio voz activa a la comunidad que produce los documentos, para que los gestione y decida sobre su uso y su destino final por sí misma; la intervención archivera se limita a un asesoramiento no dirigista. A la par, reformula el principio de procedencia y plantea una valoración documental participativa. Ante las dificultades materiales para que un centro establecido recopile la documentación o la negativa de quienes la producen a que eso suceda, o por cuestión de principios, propone un sistema de archivado distribuido entre los agentes ciudadanos²², con base teórica en el postcustodialismo.

Aplicar todo eso es mucho menos fácil que decirlo. Nos encontramos con una realidad que cambia con rapidez, y que es capaz de construir circuitos y prácticas autorreguladas sin contar con lo oficial. Por congruencia ante lo lícito de esa opción y por sus propias características, en tal entorno sólo cabe una regulación mínima. Desde la óptica institucional, supone incluir la archivística colaborativa entre los principios de misión y visión del archivo, asignar a éste un mandato en consecuencia, y dotarlo de flexibilidad para interactuar y establecer sinergias fuera de los cauces todavía habituales. Para que sirva de veras hace falta un debate previo sobre su alcance y sus límites profesionales y sociales. Aunque en las circunstancias actuales se demande el grueso de nuestros esfuerzos para montar una Administración-e impecable, no olvidemos que hay otras formas de atender a la ciudadanía, y pidamos vías para valernos de su inmenso potencial de colaboración.

Para terminar...

...una petición a quienes redacten las normas: que cuiden su legibilidad. Que expresen las disposiciones de manera unívoca, evitando los riesgos de las interpretaciones; que las acerquen al lenguaje actual, sin nominalizaciones innecesarias, modismos desfasados y frases interminables. Quienes trabajamos con documentación necesitamos que cualquier persona pueda comprender los derechos y las garantías que una GD bien regulada le ofrece, exigirla a su AP como una prestación de primer orden y, cuando se tercie, intervenir activa y conscientemente en su construcción.

Conclusiones

El conjunto normativo estatal de obligado cumplimiento sobre gestión documental integral, modélico en muchos aspectos, adolece en ocasiones de una ligazón excesiva con la tramitación de procedimientos en soporte papel. Debido a ello, existe el riesgo de que se construyan sistemas de gestión documental que desaprovechen varias de las grandes ventajas que ofrece la tecnología actual para almacenar información de manera distribuida.

La conformación de documentos y expedientes como objetos digitales unitarios ENI-compatibles no debería entenderse como obligatoria desde el principio de la tramitación, ni ser el objetivo pasarlos todos al nivel de archivo como objetos OAIS. Una correcta valoración funcional puede sustituir los primeros por bases de datos, y dejar de los segundos los activos relevantes de información, lo cual facilitaría su reutilización en ambos casos.

Otro motivo para esa visión quizá sea el garantismo, que ha aumentado para la documentación electrónica y lastra el uso de recursos tan ágiles como la interoperabilidad. Se necesita resolver la indefinición jurídica sobre la validez de sus trazas cuando el sistema consumidor de ese servicio consulte pero no almacene el dato, algo que suele ser innecesario a efectos de tramitación y las Administraciones públicas efectúan además mediante transacciones entre sistemas de confianza en entornos tecnológicos de máxima seguridad.

En digital, y contando con repositorios de ese tipo, los niveles de archivo son innecesarios. El archivado se convierte en un paso más de la tramitación, cierto que no administrativa, pero sin solución de continuidad con ella. La futura NTI de transferencia debería prever soluciones de ese tipo, basadas en un funcionamiento multiagente y de continuo documental; también, evitar las exigencias garantistas sobre la custodia.

Al hilo de la preservación, se evidencian dos vacíos legales. Uno, inconcebible en una sociedad democrática, el desamparo en que está la documentación

pública de las personas cargohabientes. Urge regular de modo estricto sobre su conservación, con graves penas para las infracciones, a la par que promover un estudio multidisciplinar para solventar los problemas de gestión y valoración que conlleva.

Otro, contemplar a la ciudadanía como agente capaz de gestionar por sí misma documentación, entendida ésta en sentido extenso. La llamada archivística colaborativa no es del todo regulable por definición, pues incluye alternativas “fuera de sistema”. Sin embargo, hay que reflexionar sobre cómo favorecerla mediante un mínimo marco normativo, para que no se desaproveche su gran potencial de servicio a la colectividad.

El colectivo archivero-gestor documental está llamado a ser agente activo desde el comienzo para preparar esas y otras disposiciones de su ámbito, sea cual sea su rango, y procurar que sean precisas en su formulación y comprensibles por la ciudadanía. Aparte de su cualificación técnica, si algo lo caracteriza hoy es su voluntad de servir no sólo a las Administraciones, por supuesto, sino a quienes son la verdadera razón de que estas existan: las personas.

Bibliografía

- 15 M (2011). Página “Archivo”, en #15Mpedia. *Todo el conocimiento del 15M*. <<https://15mpedia.org/wiki/Archivo>>. [Consulta: 10/10/2019].
- ALAMILLO, Nacho (2019). “A voltes amb la conservació de la signatura i el segell electrònic dels documents”. En *La DaDa*, 154. <<https://arxiv.org/abs/1905.00001>>. [Consulta: 10/10/2019].
- ANDRÉS DÍAZ, Rosana de (2018). “Sistemas de gestión de documentos y archivos para la transparencia y contra la corrupción”. En ANDRÉS DÍAZ, Rosana de; SIERRA RODRÍGUEZ, Javier (coords.): *La función de archivo y la transparencia en España*. Madrid: Universidad Complutense de Madrid. Centro Superior de Estudios de Gestión, p. 31-40. <<https://books.google.es/books?id=sYNyDwAAQBAJ&pg=PA37&lpg=PA37&dq=sindrome+archivos+vac%C3%ADos&source=bl&ots=wkWNcjTvyR&sig=ACfU3U1VxRMnD6FBGoIn-D9uUZGmshLWvQ&hl=es&sa=X&ved=2ahUKEwjA7qfemMDiAhUL-hQKHRzkBIQQ6AEwBnoECAkQAQ#v=onepage&q=sindrome%20archivos%20vac%C3%ADos&f=false>>. [Consulta: 10/10/2019].
- AMOEDO SOUTO, Carlos A. (2016). “Os límites da transparencia administrativa como política pública en España”. En *Actas das I Xornadas Olga Gallego de Arquivos. Transparencia “versus” corrupción: os arquivos e a democracia*. A Coruña: Fundación Olga Gallego, p. 17-25. <http://fundacionolgagallego.gal/upload/recursos/cat_2/44/transparencia_1_olgagallego_def.pdf>. [Consulta: 10/10/2019].
- ANDERSON, Janet (2019). “Herramientas disponibles en el eArchiving Building Block” [en ponencia compartida con José BORBINHA]. En *Jornadas eArchiving Building*

- Block. *¿Cómo aplicar las herramientas de la Unión Europea en el modelo español de administración electrónica y archivo electrónico? 4 y 5 de abril 2019*. Madrid: Ministerio de Cultura y Deporte. <<http://www.culturaydeporte.gob.es/cultura-mecd/areas-cultura/archivos/novedades/2019/e-archiving.html>>. [Consulta: 10/10/2019].
- ARCHIVO 15M (2015-1). “¡Importante! No basura. Carteles, pancartas. ¡Archivo!”. En *Tabula*, 18, p. 137-147.
- ARCHIVO 15M (2015-2). *Archivo 15M*. <<https://archivosol15m.wordpress.com/>>. [Consulta: 10/10/2019].
- BIBLIOTECA DE CATALUNYA (2013). *Transcriu-me!!* <<http://transcriu.bnc.cat/>>. [Consulta: 10/10/2019].
- CAYA, Marcel (2004). “La théorie des trois âges en archivistique. En avons-nous toujours besoin?” En *Élec. Éditions en ligne de l'École des Chartes*. <elec-enc.sorbonne.fr/conferences/caya>. [Consulta: 10/10/2019].
- CEF DIGITAL (2019-1). *eArchiving*. <<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eArchiving>>. [Consulta: 10/10/2019].
- CEF DIGITAL (2019-2). *Publication of the eArchiving Building Block technical specifications*. En *News*. <<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/06/04/Publication+of+the+eArchiving+Building+Block+technical+specifications>>. [Consulta: 10/10/2019].
- CONVERY, Nicole (2014). “From reactive to proactive appraisal”. En *Recordkeeping Roundtable. Reinventing archival methods: Continuing the conversation*. <<https://rkroundtable.org/2014/06/30/from-reactive-to-proactive-appraisal/>>. [Consulta: 10/10/2019].
- COOK, Terry (2003). “Macrovaloración y análisis funcional. La preeminencia de la interacción político-social sobre el gobierno”. En *Tabula*, 6, p. 87-104.
- CUNNINGHAM, Adrian (2015). Voz “Postcustodialism”. En DURANTI, Luciana (coord.); FRANKS, Patricia C. (coord.): *Encyclopedia on archival science*. Lanham (MD): Rowman & Littlefield, p. 274-278.
- DLM Forum Foundation (2011). *MoReq2010®: Modular Requirements for Records Systems - Volume 1: Core Services & Plug-in Modules*. <<http://moreq2010.eu/>>, <http://moreq.info/files/moreq2010_vol1_v1_1_en.pdf>. [Consulta: 10/10/2019].
- E-ARK4ALL (2019). <<http://e-ark4all.eu/>>. [Consulta: 10/10/2019].
- EVANS, Joanne; McKEMMISH, Sue; y ROLAN, Greg (2017). “Critical Archiving and Recordkeeping Research and Practice in the Continuum”. En *Journal of Critical Library and Information Studies. Critical Archival Studies. Special Issue.*, 1-2, DOI: 10.24242/jclis.v1i2.35. <<https://journals.litwinbooks.com/index.php/jclis/article/view/35/29>>. [Consulta: 10/10/2019].
- FLINN, Andrew; JONES, Harriet (eds.) (2009). *Freedom of Information. Open Access, Empty Archives?* London y New York: Routledge.
- GAIP (2019). “Qui som?”. En *Comissió de Garantia del Dret d'Accés a la Informació Pública*. <<http://www.gaip.cat/ca/qui-som/que-es-la-gaip/equip/>>. [Consulta: 10/10/2019].
- GARCÍA RUIPÉREZ, Mariano (2018). “El metadato Tipo documental de la NTIDE y las propuestas de desarrollo de su esquema de valores”. En *Boletín ANABAD, LXVIII-2*. <file:///C:/Users/SC58/Documents/BFIA_Tipos%20Doc%20NTIDoc-e_2018.pdf>. [Consulta: 10/10/2019].

- GILILAND, Anne J.; McKEMMISH, Sue; y LAU, Andrew J. (eds): *Research in the Archival Multiverse*. Clayton, Victoria: Monash University Publishing. <<https://opaen.org/download?Type=document&docid=628143>>. [Consulta: 10/10/2019].
- GRUPO ANTIMILITARISTA TORTUGA (2018). *Se constituye el archivo histórico del pacifismo y el antimilitarismo en el País Valencià*. <<https://www.grupotortuga.com/Se-constituye-un-archivo-historico>>. [Consulta: 10/10/2019].
- GRUPO DE TRABAJO DE PGD-e (2019). *Política de gestión de documentos electrónicos (3ª edición)*. 8. *Guía de aplicación de transferencia*. Madrid: Ministerio de Hacienda-Secretaría General Técnica-Subdirección General de Información, Documentación y Publicaciones. <[https://www.hacienda.gob.es/Documentacion/Publico/SGT/CATALOGO_SEFP/281_8.Guia%20de%20aplicacion%20de%20transferencia%20\(acc\).pdf](https://www.hacienda.gob.es/Documentacion/Publico/SGT/CATALOGO_SEFP/281_8.Guia%20de%20aplicacion%20de%20transferencia%20(acc).pdf)>. [Consulta: 10/10/2019].
- ITRUST (2018). *Voz "Post-custodialism"*. En *Terminology*. <<https://interparestrust.org/terminology/term/post-custodialism>>. [Consulta: 10/10/2019].
- LEY 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno. En *Diari Oficial de la Generalitat de Catalunya*, n° 6780 (31/12/2014), ref. CVE-DOGC-A-14364076-2014. <https://portaljuridic.gencat.cat/ca/pjur_ocults/pjur_resultats_fitxa/?action=fitxa&documentId=680124&language=ca_ES&searchId=4712977&mode=single>. [Consulta: 10/10/2019].
- LEY 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En *Boletín Oficial del Estado*, n° 236, 02/10/2015, ref. BOE-A-2015-10565. <<https://www.boe.es/eli/es/l/2015/10/01/39/con>>. [Consulta: 10/10/2019].
- MARTÍN REY, Rosa; HERNÁNDEZ DÍEZ, Javier (2018). "El archivo electrónico: principios funcionales y técnicos para su diseño". En BUSTOS PRETEL, Gerardo (coord.): *La gestión del documento electrónico*, Madrid: Wolters Kluwer, 2018, p. 585-617.
- NOVA CIENCIA (2018). *El Archivo de la Democracia de la UA gestionará el fondo del Movimiento de Objeción de Conciencia*. <<http://novaciencia.es/el-archivo-de-la-democracia-de-la-ua-gestionara-el-fondo-del-movimiento-de-objecion-de-conciencia/>>. [Consulta: 10/10/2019].
- POLÍTICA de gestión de documentos electrónicos. *Guía de aplicación de la Norma Técnica de Interoperabilidad*. 2ª edición electrónica (2016). Madrid: Ministerio de Hacienda. <https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Archivo_electronico/pae_Politica-de-gestion-de-documentos-electronicos.html>. [Consulta: 10/10/2019].
- POLÍTICA de gestión de documentos electrónicos MINHAP. (2ª edición) (2016). Madrid: Ministerio de Hacienda y Administraciones Públicas. <<http://www.hacienda.gob.es/Documentacion/Publico/SGT/POLITICA%20DE%20GESTION%20DE%20DOCUMENTOS%20MINHAP/politica%20de%20gestion%20de%20documentos%20electronicos%20MINHAP.pdf>>. [Consulta: 10/10/2019].
- PROYECTO de Real Decreto por el que se desarrollan la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en materia de actuación y funcionamiento del sector público por medios electrónicos (2018). <http://www.hacienda.gob.es/Documentacion/Publico/NormativaDoctrina/Proyectos/RD_Adm_Electr%C3%B3nica_20180516.pdf>. [Consulta: 10/10/2019].

- ROCA I MARQUÈS, Eva (2018). “Conservación y preservación”. En BUSTOS PRETEL, Gerardo (coord.): *La gestión del documento electrónico*. Madrid: Wolters Kluwer, 2018, p. 495-504.
- RUIZ GÓMEZ, Vicenç (2016). “Gobierno abierto: ¿smart cities o comunidades de archivo?”. En *Empowering archives. From metadata to social change*. <<https://empoweringarchives.wordpress.com/>>. [Consulta: 10/10/2019].
- SIARD (2015). “Specification for SIARD Format v.2”. En *eARK-Resources-Specifications*. < <https://www.eark-project.com/resources/specificationdocs/32-specification-for-siard-format-v20>>. [Consulta: 10/10/2019].
- ZASTROW, Jan (2014). “Crowdsourcing Cultural Heritage: ‘Citizen Archivists’ for the Future”. En *The Digital Archivist*, 34-8 (2014). <<http://www.infotoday.com/cilmag/oct14/Zastrow—Crowdsourcing-Cultural-Heritage.shtml>>. [Consulta: 10/10/2019].

Notas

¹ Como excepción, el peso compartido del personal jurista y técnico de archivo o GD en la Comisión de Garantía del Derecho de Acceso a la Información Pública (GAIP, 2019) de Cataluña, reconocido por el art. 40 de la ley catalana de transparencia (LEY 19/2014).

² Cfr. ROCA I MARQUÈS (2018, 496), quien lo relaciona con la plataforma de custodia de evidencias electrónicas de las universidades de Cataluña.

³ El software libre suizo SIARD (2015), parte ya del proyecto eArchiving (v. nota 12). Traslada los datos a tablas XML con metadatos sobre la estructura de la base y sus relaciones de negocio. Documentar y reproducir adecuadamente estas últimas son el problema más grave para interpretar las BBDD en el futuro. También causan problemas la heterogeneidad de objetos conservados en ellas y los formatos propietarios. Sobre todo ello se sigue trabajando.

⁴ En contraste, la insuficiente tipología documental propuesta por norma ENI. Basada en el mundo del papel, ha generado desarrollos heterogéneos en diversas AP y sigue necesitando remodelación. Entre las críticas, v. GARCÍA RUIPÉREZ (2018).

⁵ La Guía de aplicación de transferencia del Grupo de trabajo de PGD-e (2019) parte de la situación predominante en la Administración General del Estado, por lo que describe el procedimiento en un entorno “clásico”.

⁶ Por ejemplo, el problema de mantener a largo plazo las validaciones. Cfr. ALAMILLO (2019).

⁷ El trasunto de la transferencia analógica que describen MARTÍN y HERNÁNDEZ (2018, 601-602) se entendería a lo sumo en una organización donde el repositorio de archivo estuviese disgregado con respecto a las aplicaciones de tramitación y/o fuese distribuido; exigir acta con firma electrónica (¿por qué se elimine lo transferido en la aplicación remitente?) resulta más garantista que la propia PACAP. Remitir a la aplicación de origen quizá apunte al productor y no a su herramienta, pues en una de negocio no encaja; la constancia probatoria corresponde a la de archivo.

⁸ Definición y alcance, en CUNNINGHAM (2015). Los principios son distintos con respecto a la idea de sistemas y repositorios distintos (cfr. ITrust, 2018, voz *Post-custodialism*).

⁹ Propuesta de Janet ANDERSON (2019), por considerarlos una anticuada idea conservacionista. En cuanto al todavía fuerte desequilibrio en favor de la preservación al diseñar gestiones archivísticas no le falta razón.

¹⁰ Definición, en CRUZ MUNDET (2011, p. 153-154). Una crítica tardía en relación con contextos electrónicos, lo que prueba la fuerza de la idea, en CAYA (2004).

¹¹ La política de gestión de documentos del MINHAP (2015, p. 15), considerada modélica y premio ACAL 2016 al mejor proyecto archivístico, expone las características de un Sistema de Gestión de Documentos Electrónicos-SGDE y del consecuente SGDEA, de Archivo; el problema de delimitarlos con nitidez al que se refiere no es exclusivo de esa institución. Cita MoReq-2, de 2008; MoReq2010 (DLM Forum Foundation, 2011, p. 19-20) contempla una integración mucho más flexible de ambos.

¹² En base al proyecto eArchiving (CEF Digital, 2019-1), de la Comisión Europea. Sobre su desarrollo, v. e-ARK4ALL (2019). Uno de sus méritos es la relevancia que concede a la interoperabilidad semántica. El 14/06/2019 se publicaron en abierto las especificaciones técnicas del bloque de construcción eArchiving Building Block (CEF Digital, 2019-2).

¹³ Esto remite a la archivística colaborativa, de la que trataremos después. Cf. CONVERY (2014).

¹⁴ Sobre la relación entre control de la información administrativa e intereses políticos, v. AMOE-DO (2015), en una publicación con muchos otros aportes interesantes.

¹⁵ Cfr. ANDRÉS DÍAZ (2018), p. 37. Remite a FLINN y JONES (2009), volumen que estudia la compleja relación entre archivos y transparencia en Gran Bretaña, Canadá, Estados Unidos, Países Bajos y Suecia.

¹⁶ Cuestión distinta es su uso en la comunicación interior. Por su instantaneidad, escalabilidad y baratura, incluso para discusión y toma de decisiones va imponiéndose al correo electrónico en las empresas, mucho más inmediatistas que las AAPP. Si bien en estas el deslinde entre los instrumentos y espacios colaborativos y la tramitación reglada es claro, no hay que descuidarse al normativizar los circuitos, también al más alto nivel. En expedientes físicos, ¿nadie se ha encontrado nunca información relevante en un post-it?

¹⁷ Por asociación de ideas: ante el desarrollo de *fake news* (información intencionalmente falsa) cada vez más difíciles de detectar, nuestro colectivo debería actualizar su código deontológico al respecto, con formulaciones explícitas; en lo operativo, se impone elaborar políticas para la cooperación interdisciplinar con agentes tecnológicos. El problema aún se percibe como periodístico, pero es de temer que llegue a ser archivístico.

¹⁸ Solo un ejemplo: el depósito de los fondos del movimiento de objeción de conciencia del País Valencià al Archivo de la Democracia de la Universidad de Alicante, vía Archivo Municipal de Gandía. Cfr. las percepciones ciudadana e institucional en Grup Antimilitarista Tortuga (2018) y Nova Ciència (2018).

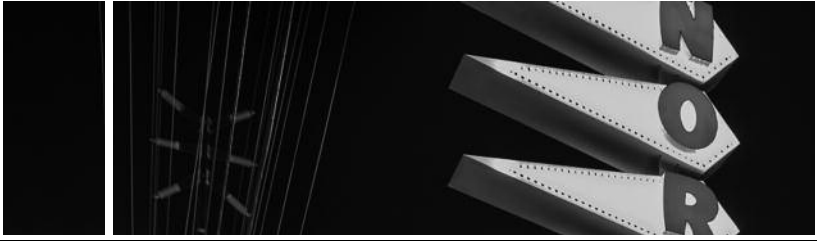
¹⁹ También necesita marco específico el crowdsourcing archivístico, colaboración o delegación de tareas abierta y distribuida vía web para transcripción de textos, identificación de fotografías, etc., arraigada en los países anglosajones, donde el voluntariado cultural suple una concepción de los servicios públicos más restringida que la europea. Cfr. ZASTROW (2014). En nuestro entorno hay reticencias por la externalización: implican cierta complejidad en la propiedad intelectual y, sobre todo, figuras contractuales no remuneradas inhabituales en la AP, que teme ser acusada de conculcar los derechos laborales o recurrir al empleo encubierto. Buena iniciativa con larga andadura: *Transcriu-me!!* (¡¡*Transcribeme!*!!), de la Biblioteca de Catalunya (2013).

²⁰ Destaca el del Movimiento 15 M (2011), protesta iniciada por la sociedad civil en Madrid contra la clase política, por su temprana autoconsciencia sobre la importancia de documentarse y, para minimizar los inherentes problemas de logística y perdurabilidad, por el diálogo con profesionales (actuación modélica, la del Arxiu Municipal de Terrassa).

²¹ Para una visión de conjunto, casos concretos incluidos, v. GILILAND, McKEMMISH y LAU (2017). Resumen metodológico en EVANS, McKEMMISH y ROLAN (2017); debo la referencia a Vicenç Ruiz.

²² Cfr. la autopercepción del Archivo 15M (2015-1 y 2): *somos un archivo un poco especial y el resto de archivos no nos representan*. Su metodología merece atención.





VICENT GIMÉNEZ-CHORNET

Los metadatos en el ordenamiento jurídico español y europeo

Metadata in the Spanish and European legal system

Vicent Giménez-Chornet
vigicho@har.upv.es
Universitat Politècnica de València

Citación: Giménez-Chornet, Vicent (2019). "Los metadatos en el ordenamiento jurídico español y europeo". *Tábula*, n. 22, pp. 37-50

Recibido: 17-9-2019. *Aceptado:* 1-10-2019

Resumen analítico / Analytic summary

El tema de los metadatos está presente en las normas técnicas internacionales, pero también se debe incorporar a la normativa jurídica para regular los asuntos que las autoridades crean más pertinentes. El presente estudio tiene como objetivo analizar en qué asuntos la normativa jurídica europea y española han necesitado incorporar el concepto de metadatos. Para ello se han analizado reglamentos, directivas, leyes y decretos publicados en las bases de datos europea y española. Tres aspectos relevantes han sido tratados por estas normativas: la reutilización de la información, la descripción de los documentos digitales y la interoperabilidad de datos e información entre las administraciones públicas.

METADATOS | NORMATIVA JURÍDICA | REUTILIZACIÓN DE LA INFORMACIÓN | DESCRIPCIÓN DOCUMENTAL | INTEROPERABILIDAD

The issue of metadata is present in international technical standards, but also should incorporate the legal rules to regulate matters that authorities create more relevant. This study aims to analyze what matters European and Spanish legal regulations have needed to incorporate the concept of metadata. To that end, we have analyzed regulations, directives, laws and decrees issued on the basis of European and Spanish data. Three important aspects have been addressed by these regulations: the reuse of information, the description of digital documents and data interoperability and information between public administrations.

METADATA | LEGAL REGULATIONS | INFORMATION REUSE | DOCUMENTARY DESCRIPTION | INTEROPERABILITY

El concepto de metadatos

se ha generalizado desde la automatización en la gestión de los documentos. Han aparecido distintos esquemas de metadatos, como conjunto de descriptores disponibles para abordar la gestión de la información. Estos esquemas de metadatos, normalizados como estándares, han surgido de las necesidades de distintos grupos de interés para normalizar la descripción de la información y, posteriormente, para abordar la interoperabilidad entre las administraciones o los organismos. Se están desarrollando muchos esquemas diferentes de metadatos como estándares en diferentes disciplinas, como biblioteconomía, educación, archivo, comercio electrónico y artes (Anil Hirwade, 2011). En los archivos, los esquemas de metadatos para la descripción más usados son la ISAD (G), la ISAAR-CPF, la EAD y la EAC-CPF, estos dos últimos con el lenguaje legible por máquina XML. Se han definido los estándares de metadatos como un conjunto de elementos con una estructura semántica especial, desarrollada para describir, identificar, descubrir, preservar y administrar objetos de contenido en los sistemas de información (Mahdi Taheri, *et al.*, 2014). La organización y descripción del contenido de la web se realiza en base a metadatos de descripción. El formato de metadatos MARC, la iniciativa de metadatos Dublin Core (DCMI) y el esquema de descripción de objetos de metadatos (MODS) se consideran los estándares de metadatos descriptivos más importantes y comunes para los contenidos Web. Según Mahdi Taheri (2014), es adecuado crear un método de isla de datos XML como un método para incrustar un documento XML en un documento HTML, y poder describir el contenido web.

En el ámbito de los archivos, y especialmente de los que contienen documentos electrónicos como consecuencia de la tramitación telemática, los metadatos capturados sistemáticamente durante la vida de un documento, y transferidos

finalmente a un archivo definitivo, pueden simplificar el proceso de descripción y evitar la pérdida de información del contexto en que se han producido. Todo ello se puede llevar a cabo siguiendo la norma ISO 15489, que dispone de elementos de metadatos esenciales para la interoperabilidad (Shepherd, West, 2003). Ya han pasado dos décadas desde las primeras iniciativas de un esquema de metadatos para la gestión de los documentos de archivo. En 1999, Australia elaboró el esquema de metadatos para la gestión de documentos (RKMS) con el Proyecto de Metadatos de Mantenimiento de Documentos denominado SPIRT, que definía y estandarizaba la estructura de los metadatos para la gestión de los documentos electrónicos (McKemmish, *et al.*, 1999).

La preservación digital en la era de *Big Data* necesita de nuevos modelos en los que la información o los metadatos de los recursos digitales podrían ser tan valiosos como la información de los propios objetos, ya que dichos datos serán usados, tanto de entrada como de salida, en sofisticados conjuntos producidos por distintas herramientas analíticas (Gerrard, *et al.*, 2018). En la preservación del documento digital el fichero tiene que contener metadatos que se deberían conservar en las conversiones a otros formatos, pues los metadatos técnicos y descriptivos son esenciales para la preservación (Moro Cabero, 2018). Con el gobierno abierto y el acceso a la información del sector público, la gestión de los datos es un reto para los profesionales de la gestión de la información y los documentos, con el objetivo de conseguir que las autoridades públicas entreguen datos abiertos a los ciudadanos. Hay estudios que han detectado una falta de estándares de metadatos comunes para la gestión de los datos abiertos, o problemas de redundancia de datos, así como inconsistencia e integridad de los datos (Shepherd, *et al.*, 2019).

El interés por regular la seguridad, integridad y autenticidad de los documentos digitales o electrónicos, desde diferentes ámbitos, se ha plasmado en distintas normativas del Estado español y de la Unión Europea, que pretendemos analizar para conocer qué aspectos jurídicos relacionados con los metadatos han sido de interés para estos legisladores.

Marco jurídico de los metadatos

Con el desarrollo de la administración electrónica la implementación de metadatos para disponer de una información estructurada o semiestructurada ha sido esencial para controlar los documentos que esta produce (Giménez-Chornet, 2017). Diferentes grupos de trabajo dedicados a avanzar en una administración electrónica interoperable en la Unión Europea han hecho posible que dispongamos de normativa, además de algunos estándares, como el MoReq, que aborden la gestión de los datos en distintos niveles del documento digital.

1. Metadatos para la reutilización

La reutilización de la información del sector público, que es financiada con fondos públicos en toda la Unión Europea, ha sido una de las políticas públicas más destacadas para avanzar en la comunicación de la información y su uso por la sociedad para impulsar nuevas líneas de negocio, pudiendo «contribuir a mejorar el mercado único y al desarrollo de nuevas aplicaciones para los consumidores y las personas jurídicas. El empleo inteligente de los datos, incluido su tratamiento a través de aplicaciones de inteligencia artificial, puede tener un efecto transformador en todos los sectores de la economía», como señala la reciente actualizada directiva de 2019, la primera fue de 2003, donde se refunden aspectos que posteriores directivas y reglamentos de la Unión han introducido en sus contenidos. Esta Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público (Unión Europea, 2019) opina que:

«El sector público de los Estados miembros recoge, produce, reproduce y difunde una amplia gama de información en numerosos ámbitos de actividad, como el social, político, económico, jurídico, geográfico, medioambiental, meteorológico, sísmico, turístico, empresarial, educativo y de las patentes. Los documentos elaborados por los organismos del sector público de carácter ejecutivo, legislativo o judicial constituyen un conjunto amplio, diverso y valioso de recursos que pueden beneficiar a la sociedad. Ofrecer esta información, que incluye los datos dinámicos, en un formato electrónico de uso habitual permite que los ciudadanos y las personas jurídicas hallen nuevas formas de utilizarla y creen productos y servicios nuevos e innovadores.» (Considerando 8)

La Directiva menciona distintos tipos de datos que pueden ser tratados de forma automatizada, como los datos de investigación recopilados de actividades y publicaciones científicas, los datos «dinámicos» de documentos en formato digital con rápida obsolescencia, como los de los sensores, o los que denomina «conjuntos de datos de alto valor», ligados a una reutilización que producirá considerables beneficios para la sociedad, el medio ambiente y la economía, que podrá repercutir en la creación de servicios de valor añadido.

Esta Directiva obliga a que las administraciones utilicen formatos de archivo electrónico que contengan metadatos, preferiblemente de formatos abiertos:

«Sin perjuicio del capítulo V, los organismos del sector público y las empresas públicas facilitarán sus documentos en cualquier formato o lengua en que existan previamente y, siempre que sea posible y apropiado, por medios electrónicos, en formas o formatos que sean abiertos, legibles por máquina, accesibles, fáciles de localizar y reutilizables, conjuntamente con

sus metadatos. Tanto el formato como los metadatos cumplirán, cuando sea posible, normas formales abiertas.» (Art. 5.1)

Estos metadatos, cuando se trate de conjunto de datos de alto valor, deberán ponerse a disposición de la sociedad para su reutilización a través de las API pertinentes pues, al ser un formato legible por máquina, los usuarios podrán realizar descargas masivas (Art. 5.8, y art. 14). La Directiva también reconoce la importancia de los metadatos para la recuperación de la información, determinando su uso, y aconsejando el multilingüismo para facilitar la búsqueda a escala de la Unión (Art. 9.1).

En España, la Directiva Europea de reutilización de 2003 se traspuso con la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, que posteriormente fue modificada por la Ley 18/2015, de 9 de julio (España, 2015), en la que también se insiste en que las administraciones públicas «facilitarán herramientas informáticas que permitan la búsqueda de los documentos disponibles para su reutilización, con los metadatos pertinentes de conformidad con lo establecido en las normas técnicas de interoperabilidad, accesibles, siempre que sea posible y apropiado, en línea y en formato legible por máquina» (artículo único, dos). Un ejemplo español de la importancia de los metadatos que servirán para localizar documentos depositados en Europeana (<https://www.europeana.eu>) es la Resolución de 20 de octubre de 2017, de la Secretaría General Técnica, por la que se publica el Convenio con Provincia de Hermanos Menores Capuchinos de España, para regular el suministro de metadatos y previsualizaciones por parte de Provincia de Hermanos Menores Capuchinos de España al Ministerio de Educación, Cultura y Deporte y, a través de este, a Europeana¹ (España, 2017) que «tiene por objeto regular el suministro de metadatos y previsualizaciones por parte de Provincia de Hermanos Menores Capuchinos de España al Ministerio de Educación, Cultura y Deporte y, a través de este, a Europeana».

2. Metadatos para la descripción

Las normas de descripción archivística más implementadas a nivel europeo son las ISAD (G) (*International Standard Archival Description, General*), para las unidades archivísticas, y las ISAAR-CPF (*International Standard Archival Authority Record for Corporate Bodies, Persons, and Families*), para la descripción de las autoridades productoras de los documentos, que por tanto se deben utilizar en la misma base de datos tecnológica que describe las unidades, enlazadas al campo del Nombre del productor de la ISAD (G). Estas dos normas internacionales, así como distintas normas ISO, tratan a nivel técnico cómo se deben gestionar y describir los documentos, especialmente los electrónicos (Giménez-Chornet, 2015). Las normas tienen definidos los campos de metadatos por áreas, con la finalidad

de describir su contenido y su contexto. Para la recuperación de la información se aconseja la indización con un lenguaje documental, especialmente por la elaboración de tesauros. Todos esos campos, los de descripción e indización, formarían el conjunto de metadatos para la identificación de las unidades archivísticas. La Unión Europea se interesó por el uso de la ISAD (G) y la ISAAR-CPF en la *Convocatoria de propuestas relativa al tratamiento del patrimonio archivístico de los diputados europeos, formado en el ejercicio de su mandato y entregado a título de donaciones o de legados legales*, de 2004, donde se exigía junto al establecimiento de un plan de clasificación que el tratamiento archivístico siguiese las normas ISAD(G) e ISAAR(CPF) (Parlamento Europeo, 2004).

En España pronto hubo interés en aplicar este esquema de metadatos de descripción. En la convocatoria de las pruebas selectivas para ingreso en el Cuerpo Facultativo de Archiveros, Bibliotecarios y Arqueólogos de 2001 se añadió el tema «La normalización en la descripción archivística: Normas ISAD (G) e ISAAR (CPF)» (España, 2001), que ya sería una de las exigencias en las sucesivas convocatorias. Pero no será hasta el 2011 cuando, con la Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior, se obligue a que la descripción de los datos cumpla con una estructura conforme a la Norma Internacional de Descripción Archivística ISAD (G), señalando que puede incluir todas o algunas de las áreas y de los campos indicados en dicha norma (España, 2011a). En el 2012 la Secretaría de Estado de Administraciones Públicas señala algunas normas, en un catálogo de estándares, donde se pueden contemplar metadatos para la gestión archivística y documental con fines de interoperabilidad: la ISAD (G), la ISAAR-CPF, la ISDF (Norma internacional para la descripción de funciones), y la NEDA (Modelo conceptual de descripción archivística y requisitos de datos básicos de las descripciones de documentos de archivo, agentes y funciones – Parte 1: Tipos de entidad) (España, 2012a).

Sin especificar qué tipo de esquema de metadatos se debe aplicar para la descripción archivística, el Real Decreto 1708/2011, en el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado, obliga a «describir las fracciones de serie conforme a las normas internacionales y nacionales de descripción archivística» (art. 10.1.3), reconociendo que un metadato es:

«cualquier descripción estandarizada de las características de un conjunto de datos. En el contexto del documento electrónico cualquier tipo de información en forma electrónica asociada a los documentos electrónicos, de carácter instrumental e independiente de su contenido, destinada al conocimiento inmediato y automatizable de alguna de sus características, con la finalidad de garantizar la disponibilidad, el acceso, la conservación y la interoperabilidad del propio documento» (art. 2.2.j) (España, 2011b)

Distintas leyes autonómicas sobre archivos incluyeron la obligatoriedad de la descripción archivística según normas internacionales (Giménez-Chornet, 2017, pp. 80-82), reconociendo que este esquema de metadatos son los idóneos para la gestión de los documentos de las administraciones públicas.

3. Metadatos para la interoperabilidad

La interoperabilidad es la capacidad de dos o más sistemas, o sus componentes, para intercambiar información, y utilizar la información que han recibido como resultado de este intercambio. Para las administraciones públicas esto plantea varios problemas, entre ellos la regulación legal y tecnológica (la falta de estandarización en el desarrollo de sistemas redunde en su incompatibilidad). Para los usuarios de las administraciones, ante la falta de sistemas técnicos compatibles entre sí, se ven obligados a elegir la tecnología de un productor (Zharova, 2015). Con la administración electrónica los metadatos son esenciales para describir e integrar los recursos heterogéneos en un solo portal, y de esta forma favorecer la recuperación de la información y la interoperabilidad (Martínez-Usero, 2006). El Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea, considera que los datos electrónicos se encuentran en el centro de los sistemas económicos y de las sociedades innovadoras modernas. Estos datos «pueden generar un gran valor cuando se analizan o combinan con servicios y productos. Al mismo tiempo, el rápido desarrollo de la economía de los datos y las tecnologías emergentes, como la inteligencia artificial, productos y servicios del “internet de las cosas”, sistemas autónomos y la tecnología 5G, están planteando problemas jurídicos nuevos en torno a las cuestiones del acceso a los datos y su reutilización, la responsabilidad, la ética y la solidaridad» (Unión Europea, 2018). Este Reglamento de 2018 especifica, en cuanto a la portabilidad de los datos, que:

«1. La Comisión fomentará y facilitará la elaboración de códigos de conducta autorreguladores a escala de la Unión (en lo sucesivo, “códigos de conducta”), con el fin de contribuir a una economía de datos competitiva, basada en los principios de transparencia e interoperabilidad, que tenga debidamente en cuenta estándares abiertos y que incluya, entre otros, los siguientes aspectos:

- a) las mejores prácticas para facilitar el cambio de proveedores de servicios y la portabilidad en un formato estructurado, de uso común y de lectura automática, incluidos formatos basados en estándares abiertos cuando lo exija o solicite el proveedor de servicios que reciba los datos;
- b) los requisitos de información mínimos para garantizar que los usuarios profesionales, antes de celebrar un contrato de tratamiento de datos, reciban

información suficientemente detallada, clara y transparente relativa a los procedimientos, los requisitos técnicos, los plazos y los costes aplicables en caso de que un usuario profesional desee cambiar de proveedor de servicios o transferir sus datos a sus propios sistemas informáticos;

c) los enfoques de regímenes de certificación que faciliten la comparación de los productos y servicios de tratamiento de datos para usuarios profesionales, teniendo en cuenta las normas nacionales o internacionales establecidas, que facilitan la comparabilidad de estos productos y servicios. Dichos enfoques podrán incluir, entre otros, la gestión de la calidad, la gestión de la seguridad de la información, la gestión de la continuidad de negocio y la gestión medioambiental;

d) los planes de comunicación que adopten un enfoque multidisciplinar para concienciar a los interesados sobre el código de conducta.» (Art. 6)

A nivel europeo, uno de los usos destacable es la interoperabilidad de datos e información para el control de las fronteras. El Reglamento (UE) n° 1052/2013 del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, por el que se crea un Sistema Europeo de Vigilancia de Fronteras (Eurosur), da competencias a la Agencia Europea responsable de la gestión de la cooperación operativa en las fronteras exteriores de los Estados miembros de la Unión Europea, determinando que «la Agencia proporcionará apoyo técnico y garantizará que la red de comunicación sea interoperable con cualquier otro sistema de comunicación e información pertinente gestionado por la Agencia» (art. 7.2), reconociendo que dicha Agencia intercambiará, tratará y almacenará información sensible no clasificada e información clasificada en la red de comunicación (Unión Europea, 2013) si es para «para facilitar el intercambio con la Comisión y los Estados miembros de información pertinente para la ejecución de sus funciones», según el Reglamento (CE) n° 2007/2004 del Consejo, de 26 de octubre de 2004, por el que se crea una Agencia Europea para la gestión de la cooperación operativa en las fronteras exteriores de los Estados miembros de la Unión Europea. El Plan de Acción de Interoperabilidad de la Unión Europea de 2017 reconoce la importancia de «analizar el contenido de los datos y los sistemas de metadatos existentes en relación con la información de las administraciones públicas (incluidos los documentos) utilizados en un contexto transfronterizo o intersectorial. Identificar los obstáculos para el reconocimiento mutuo, elaborar cartografías y apoyar esfuerzos de armonización.» (Comisión Europea, 2017).

La preocupación por la gestión de los datos espaciales impulsó la Directiva 2007/2/CE del Parlamento Europeo y del Consejo, por la que se crea una Infraestructura de Información Espacial en la Comunidad Europea (Unión Europea, 2007), y el posterior Reglamento (CE) n° 1205/2008 de la Comisión de 3 de diciembre de 2008, por el que se ejecuta la Directiva 2007/2/CE del Parlamento

Europeo y del Consejo en lo que se refiere a los metadatos, que resalta la importancia de la definición de un conjunto de elementos de metadatos para poder identificar y clasificar el recurso de información, que permita determinar su localización geográfica y su referencia temporal. Este reglamento también señala la importancia de la calidad y validez de los metadatos, así como la conformidad con las normas de aplicación sobre la interoperabilidad de los servicios, o las restricciones de acceso y uso (Unión Europea, 2008).

El actual el programa ISA² de la Unión Europea para el periodo 2016-2020, regulado por la Decisión (UE) 2015/2240 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015, por la que se establece un programa relativo a las soluciones de interoperabilidad y los marcos comunes para las administraciones públicas, las empresas y los ciudadanos europeos (programa ISA²) como medio de modernización del sector público, considera que «en el ámbito de la justicia y los asuntos de interior, una mejor interoperabilidad entre las bases de datos europeas es la base del Sistema de Información de Visados, del Sistema de Información de Schengen II, del sistema europeo de huellas dactilares y del portal de e-Justicia» (Unión Europea, 2015), haciendo «hincapié en que los organismos del sector público deben, siempre que sea posible y oportuno, ofrecer los documentos en formatos abiertos y legibles por máquina, junto con sus metadatos, al mejor nivel de precisión y granularidad, en un formato que garantice la interoperabilidad, la reutilización y la accesibilidad».

En España, el Esquema Nacional de Interoperabilidad, regulado por el Real Decreto 4/2010, es el que armoniza normas técnicas para garantizar la normalización de unos metadatos que hagan posible la interoperabilidad de las administraciones públicas españolas. La Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico (España, 2011c) tiene por «objeto establecer los componentes del documento electrónico, contenido, en su caso, firma electrónica y metadatos, así como la estructura y formato para su intercambio», entendiendo por contenido el conjunto de datos o información del documento, proponiendo distintos esquemas XML para dicho intercambio y un esquema de metadatos mínimos obligatorios del propio documento electrónico, donde se exigen, entre otros, datos para su identificación única, el órgano productor, la fecha de alta del documento, el estado de elaboración (original, copia, etc.), la tipología documental (acta, diligencia, denuncia, etc.), o datos sobre la firma, pero no ha considerado como mínimo exigible registrar la información sobre el contenido de los documentos o metadatos de indexación del contenido mediante un lenguaje documental para la recuperación de la información.

El Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE) es la documentación complementaria de la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos aprobada por

resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas (España, 2012b). El campo “eEMGDE.Descripcion5” sí que contempla la necesidad de añadir información adicional en texto libre para la entidad productora y el campo o metadato “eEMGDE21.1.1 - Descripción Acción” para la descripción del tipo de acción realizada sobre una o varias entidades del sistema. Este desarrollado esquema de metadatos puede garantizar no sólo la eficaz interoperabilidad de datos e información de los documentos electrónicos, sino también su recuperación más pertinente.

Conclusiones

Además de las normas técnicas internacionales que tratan el tema de los metadatos para la gestión de la información, tanto la Unión Europea como España han incorporado en su ordenamiento jurídico el concepto de los metadatos. Los metadatos, como esquema, es relevante cuando se regulan aspectos como la reutilización de la información, la descripción de los recursos digitales o la interoperabilidad entre organizaciones, especialmente entre las administraciones públicas.

La importancia de proteger a las personas frente al tratamiento de los datos de carácter personal es otro de los aspectos, más reciente, que la Unión Europea ha regulado, especialmente cuando afecta a su portabilidad, aunque en el vocabulario utilizado en la normativa jurídica se hable más de datos que de esquema de metadatos.

Bibliografía

- Anil Hirwade, M. (2011). “A study of metadata standards”. *Library Hi Tech News*, vol. 28, n. 7, p. 18-25. <https://doi.org/10.1108/07419051111184052> [Consulta: 14/05/2019]
- Comisión Europea (2017). Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Marco Europeo de Interoperabilidad – Estrategia de Aplicación. <<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017DC0134>> [Consulta: 5/05/2019]
- España (2001). “Orden de 24 de septiembre de 2001 por la que se convocan pruebas selectivas para ingreso en el Cuerpo Facultativo de Archiveros, Bibliotecarios y Arqueólogos”. *BOE*, núm. 234, de 29 de septiembre de 2001, p. 36265-36278. <<https://www.boe.es/buscar/doc.php?id=BOE-A-2001-18268>> [Consulta: 21/05/2019]
- España (2011a). “Orden INT/1202/2011, de 4 de mayo, por la que se regulan los ficheros de datos de carácter personal del Ministerio del Interior”. *BOE*, núm. 114, de 13

- de mayo de 2011, p. 48748-48961. <<https://www.boe.es/eli/es/o/2011/05/04/int1202>> [Consulta: 5/05/2019]
- España (2011b). “Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso”. BOE, núm. 284, de 25/11/2011. <<https://www.boe.es/eli/es/rd/2011/11/18/1708/con>> [Consulta: 17/05/2019]
- España (2011c). “Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico”. BOE, núm. 182, de 30/07/2011. <[https://www.boe.es/eli/es/res/2011/07/19/\(3\)/con](https://www.boe.es/eli/es/res/2011/07/19/(3)/con)> [Consulta: 17/05/2019]
- España (2012a). “Resolución de 3 de octubre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Catálogo de estándares”. BOE, núm. 262, de 31 de octubre de 2012, p. 76713-76723. <[https://www.boe.es/eli/es/res/2012/10/03/\(3\)/](https://www.boe.es/eli/es/res/2012/10/03/(3)/)> [Consulta: 16/05/2019]
- España (2012b). “Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos”. BOE, núm. 178, de 26 de julio de 2012, p. 53776-53780. <[https://www.boe.es/eli/es/res/2012/06/28/\(3\)/](https://www.boe.es/eli/es/res/2012/06/28/(3)/)> [Consulta: 16/05/2019]
- España (2015). “Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público”. BOE, núm. 164, de 10/07/2015. <<https://www.boe.es/eli/es/l/2015/07/09/18/con>> [Consulta: 16/05/2019]
- España (2017). “Resolución de 20 de octubre de 2017, de la Secretaría General Técnica, por la que se publica el Convenio con Provincia de Hermanos Menores Capuchinos de España, para regular el suministro de metadatos y previsualizaciones por parte de Provincia de Hermanos Menores Capuchinos de España al Ministerio de Educación, Cultura y Deporte y, a través de este, a Europea, así como el uso de dichos metadatos y previsualizaciones por parte del Ministerio de Educación, Cultura y Deporte y de Europea”. BOE, núm. 267, de 3 de noviembre de 2017, p. 105572-05582. <https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-12642> [Consulta: 12/05/2019]
- Gerrard, D.; Mooney, J.; Thompson, D. (2018). “Digital preservation at Big Data scales: proposing a step-change in preservation system architectures”. *Library Hi Tech*, vol. 36, n. 3, p. 524-538. <<https://doi.org/10.1108/LHT-06-2017-0122>> [Consulta: 12/05/2019]
- Giménez-Chornet, V. (2015). “Normas ISO para la gestión de los documentos electrónicos: buenas prácticas para la gestión documental en las empresas”. *Fuentes*, vol. 9, n. 40, p.7-16. <http://www.revistasbolivianas.org.bo/pdf/fdc/v9n40/v9n40_a03.pdf> [Consulta: 4/05/2019]
- Giménez-Chornet, V. (2017). *Legislación de archivos*. Barcelona: UOC- El Profesional de la Información. ISBN 978-84-9116-989-5
- Mahdi Taheri, S.; Hariri, N.; Rahmatollah Fattahi, S. (2014). “Using data island method for creating metadata records with indexability and visibility of tag names in web

- search engines". *Library Hi Tech*, vol. 32, n. 1, p. 83-97. <<https://doi.org/10.1108/LHT-06-2013-0065>> [Consulta: 23/05/2019]
- Martínez-Usero, J. Á. (2006). "El uso de metadatos para mejorar la interoperabilidad del conocimiento en los servicios de administración electrónica". *El profesional de la información*, vol. 15, n. 2, p. 114-126. <<http://www.elprofesionaldelainformacion.com/contenidos/2006/marzo/4.pdf>> [Consulta: 23/05/2019]
- McKemmish, S.; Acland, G.; Reed, B. (1999). "Towards a framework for standardising recordkeeping metadata: the Australian recordkeeping metadata schema". *Records Management Journal*, vol. 9, n. 3, p. 173-198. <<https://doi.org/10.1108/EUM000000007249>> [Consulta: 23/05/2019]
- Moro Cabero, M. (2018). "Identificación, caracterización y selección de formatos para la preservación del recurso digital". *Métodos de Información*, vol. 9, n. 16, p. 5-46. <<http://dx.doi.org/10.5557/IIIMEI9-N16-049090>> [Consulta: 12/05/2019]
- Parlamento Europeo (2004). "Convocatoria de propuestas relativa al tratamiento del patrimonio archivístico de los diputados europeos formado en el ejercicio de su mandato y entregado a título de donaciones o de legados legales, (2004/C 88/12)". *Diario Oficial de la Unión Europea*, C 88, p. 23-33. <<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:088:0023:0033:ES:PDF>> [Consulta: 18/05/2019]
- Shepherd, E.; Bunn, J.; Flinn, A.; Lomas, E.; Sexton, A.; Brimble, S.; Chorley, K.; Harrison, E.; Lowry, J.; Page, J. (2019). "Open government data: critical information management perspectives". *Records Management Journal*, vol. 29, n. 1/2, p. 152-167. <<https://doi.org/10.1108/RMJ-08-2018-0023>> [Consulta: 21/05/2019]
- Shepherd, E.; West, V. (2003). "Are ISO 15489-1:2001 and ISAD(G) compatible? Part 1". *Records Management Journal*, vol. 13, n. 1, p. 9-23. <<https://doi.org/10.1108/09565690310465704>> [Consulta: 11/05/2019]
- Unión Europea (2007). "Directiva 2007/2/CE del Parlamento Europeo y del Consejo, de 14 de marzo de 2007, por la que se establece una infraestructura de información espacial en la Comunidad Europea (Inspire)". *Diario Oficial de la Unión Europea*, L 108 de 25.4.2007, p. 1-14. <<https://eur-lex.europa.eu/eli/dir/2007/2/2019-06-26>> [Consulta: 15/05/2019]
- Unión Europea (2008). "Reglamento (CE) n. 1205/2008 de la Comisión de 3 de diciembre de 2008 por el que se ejecuta la Directiva 2007/2/CE del Parlamento Europeo y del Consejo en lo que se refiere a los metadatos". *Diario Oficial de la Unión Europea*, L 326 de 4.12.2008, p. 12-30. <<https://eur-lex.europa.eu/eli/reg/2008/1205/oj>> [Consulta: 15/05/2019]
- Unión Europea (2013). "Reglamento (UE) n° 1052/2013 del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, por el que se crea un Sistema Europeo de Vigilancia de Fronteras (Eurosur)". *Diario Oficial de la Unión Europea*, L 295 de 6.11.2013, p. 11-26. <<http://data.europa.eu/eli/reg/2013/1052/oj>> [Consulta: 12/05/2019]
- Unión Europea (2015). "Decisión (UE) 2015/2240 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, por la que se establece un programa relativo a las soluciones de interoperabilidad y los marcos comunes para las administraciones públicas, las empresas y los ciudadanos europeos (programa ISA²) como medio de

- modernización del sector público (Texto pertinente a efectos del EEE)". *Diario Oficial de la Unión Europea*, L 318 de 4.12.2015, p. 1-16. <<http://data.europa.eu/eli/dec/2015/2240/oj>> [Consulta: 12/05/2019]
- Unión Europea (2018). "Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea". *Diario Oficial de la Unión Europea*, L 303 de 28.11.2018, p. 59-68. <<http://data.europa.eu/eli/reg/2018/1807/oj>> [Consulta: 13/05/2019]
- Unión Europea (2019). "Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público". *Diario Oficial de la Unión Europea*, L 172 de 26.6.2019, p. 56-83. <<https://eur-lex.europa.eu/eli/dir/2019/1024/oj>> [Consulta: 13/05/2019]
- Zharova, A. (2015). "Influence of the principle of interoperability on legal regulation". *International Journal of Law and Management*, vol. 57, n. 6, p. 562-572. <<https://doi.org/10.1108/IJLMA-07-2014-0044>> [Consulta: 11/05/2019]

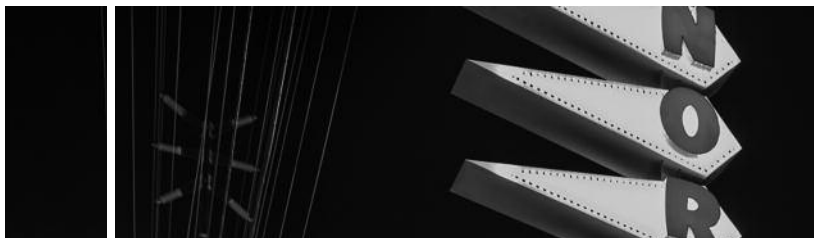
Notas

¹ En este convenio de manifiesta que "Europeana es la biblioteca digital pública de la Unión Europea. Europeana tiene como objetivo proporcionar acceso al patrimonio cultural y científico europeo. Europeana, con ese objetivo, lleva a cabo las tareas de recolectar, indizar, enriquecer y hacer accesibles los metadatos descriptivos y las previsualizaciones de los objetos que forman parte de dicho patrimonio. Europeana intenta, de ese modo, beneficiar tanto a los titulares de dichos objetos como al público en general".





ARRÊT
STOP



LIUDMILA VARLAMOVA

La terminología internacional de gestión de documentos y archivos según las normas ISO e IEC

International terminology standardized by ISO and IEC used in records and archives management

Liudmila Varlamova

lvarlam@yandex.ru

All-Russian Scientific and Research Institute for Records and Archives Management (VNIIDAD), The History and Archives College of the Russian State University for the Humanities (RSUH), Moscú, Federación Rusa

Citación: Varlamova, Liudmila (2019). "La terminología internacional de gestión de documentos y archivos según las normas ISO e IEC". *Tábula*, n. 22, pp. 53-70

Traducción: Verónica Fernández

Recibido: 1-8-2019. *Aceptado:* 10-11-2019

Resumen analítico / Analytic summary

La normalización de la terminología de la gestión documental es una ardua tarea. Por ello la estandarización de los términos fundamentales de la gestión documental la deben desarrollar los archiveros junto con expertos en seguridad de la información, gestión de calidad, de riesgos, etc. Esto plantea la cuestión de la compatibilidad entre términos y definiciones de diferentes ámbitos profesionales, especialmente términos básicos como «información documentada», «información registrada», «documento», «documento administrativo» y «datos». Hoy las distintas áreas profesionales tienden a emplear sistemas terminológicos normalizados por ISO e IEC. Sin embargo, al introducir las normas no se controla su compatibilidad con los términos y definiciones usados en otros ámbitos relacionados. Analizaremos las normas ISO 5127 y 15489, en las dos versiones, lo que facilita el rastreo de la evolución del sistema terminológico de normalización ISO. El artículo introduce en el discurso una amplia gama de términos, subtérminos y sus definiciones estandarizadas por ISO e IEC.

ESTANDARIZACIÓN | NORMAS INTERNACIONALES | NORMALIZACIÓN TERMINOLÓGICA | GESTIÓN DOCUMENTAL | ISO | IEC

Standardization of records and archives management terminology is a very challenging task. So standardization of the fundamental terms used in records and archives management must be carried out by records managers and archivists together with experts in informational security, quality management systems, risk management etc. It raises the question of the compatibility of terms and definitions used in different professional areas, especially of such basic terms as «documented information», «recorded information», «document», «record» and «data». Nowadays different professional areas reveal a tendency to use international terminological systems standardized by ISO and IEC. However, when introducing international standards the control over the compatibility of terms and definitions used in neighboring areas is not conducted. It is important to note that we analyzed the ISO 5127 and ISO 15489 in two versions which made it possible to follow the evolution of the ISO terminology system standardized for the above areas. The article introduces into discourse a wide range of the terms, sub-terms and their definitions standardized by ISO and IEC.

STANDARDIZATION | INTERNATIONAL STANDARDS | TERMINOLOGY STANDARDIZATION | RECORDS AND ARCHIVES MANAGEMENT | ISO | IEC

La normalización

de la terminología siempre ha sido una de las cuestiones más importantes en cualquier ámbito y ha precisado no sólo mucha atención sino también un enfoque equilibrado. La estandarización de la terminología de los archivos y la gestión documental no es una excepción. Sus términos básicos se utilizan en muchos campos de actividad relacionados entre sí y la comprensión mutua de los expertos depende de la exactitud de sus definiciones.

La introducción de las tecnologías de la información, acogidas con gran entusiasmo, se hace a menudo de forma espontánea y no siempre de una manera cuidada, lo que se traduce en algunos problemas como los que se refieren a la compatibilidad entre los términos utilizados en las distintas profesiones. La terminología de la gestión documental, de los archivos y de las citadas TI pueden constituir un buen ejemplo de esta afirmación. Y ello es especialmente importante cuando hablamos de términos básicos relacionados con los archivos o la gestión documental, como por ejemplo «información registrada», «documento», «documento administrativo»¹ y «datos». La elección de los términos anteriores para nuestro análisis se basa en la necesidad de desarrollar enfoques conceptuales unificados para la protección de la información contenida en ellos y, por lo tanto, es esencial entender la diferencia que existe entre las definiciones de dichos términos. Actualmente todos ellos aparecen tanto en el contexto tradicional como digital y dado que las normas ISO e IEC se utilizan en todas estas áreas, podríamos preguntarnos si la interpretación de estos términos básicos es idéntica en todas ellas. Cabe señalar que muchos científicos ya estudian la terminología de la gestión documental, pero se ha pasado por alto la cuestión de la compatibilidad entre la terminología normalizada en estos ámbitos y la de las TI (incluida la seguridad de la información). Problema aún más evidente tras la

publicación del diccionario comentado inglés-ruso de terminología normalizada utilizada en la gestión de archivos, que fue elaborado por la autora de este artículo junto con L. Bayun y K. Bastrikova.²

El objetivo de este artículo será pues determinar el grado de unificación y compatibilidad entre las definiciones de los citados términos. De hecho, los términos que se analizan en este artículo deben interpretarse de forma idéntica tanto en la gestión documental como en las TI, en la gestión de la seguridad de la información, y en la gestión de riesgos y calidad.

Los términos “información documentada” e “información registrada”

Es interesante observar que las normas ISO en el área de las humanidades (por ejemplo, ISO 15489, ISO 30300)³ se decantan por el término “información registrada”, mientras que las normas “tecnológicas” prefieren el término “información documentada”.

ISO 9000 define el término “información documentada” como “Información que una organización tiene que controlar y conservar, y el medio que la contiene”. Las notas a la entrada especifican:

- «La información documentada puede estar en cualquier formato y medio, y puede proceder de cualquier fuente.
- La información documentada puede hacer referencia a: el sistema de gestión, incluidos los procesos relacionados; la información generada para que la organización opere (documentación); la evidencia de los resultados alcanzados (documentos administrativos).
- Se trata de uno de los términos comunes y de una de las definiciones básicas de las normas del sistema de gestión ISO que figura en el anexo SL del complemento consolidado ISO de las Directivas ISO/CEI, Parte 1».⁴

Las normas ISO 27000 e ISO 14000 entienden el término “información documentada” de la misma manera, como «Información que una organización tiene que controlar y conservar, y el medio que la contiene» pero, aunque ambas normas especifican que la “información documentada” puede estar en cualquier formato y medio y puede proceder de cualquier fuente en este caso puede referirse a:

- La información producida/creada por/para que la organización haga posible el trabajo (con la documentación);
- La información que respalda los resultados obtenidos (que pueden ser definidos como “documentos”).

Por lo tanto, podemos llegar a la conclusión de que aunque los términos “información documentada” e “información registrada” podrían ser sinónimos, el primero parece tener un uso más generalizado.

ISO 5127 interpreta el término “información registrada” como la “representación de la información en un modo formalizado apto para la comunicación, interpretación y procesamiento”⁵.

Los términos “documento”, “documento administrativo” y sus subtérminos

Otro par de términos básicos que necesitamos tener en consideración son “documento de archivo” y “documento administrativo”.

En todas las normas internacionales sobre gestión documental (como ISO 15489, ISO 30300 y otras) se entiende el término “documento” como «objeto o información registrada que puede ser tratado como una unidad»⁶.

En la ISO 15489:2001 e ISO 30300:2011 el término “documento” nuevamente se describe como «información u objeto registrado que puede ser tratado como una unidad».⁷ Mientras que en ISO 15489:2016 dicho término no figura.

ISO 5127:2017 describe el término «documento» más ampliamente como «Información registrada u objeto material que puede ser tratado como una unidad en un proceso de documentación».⁸ Sin embargo, la última versión tiene varias notas explicativas:

- «Esta definición se refiere no sólo a los materiales escritos e impresos en papel o en formato microfilm (por ejemplo, libros convencionales, revistas, gráficas, mapas), sino también a medios no impresos como archivos de lectura mecánica o digitalizados, recursos de internet e intranet, películas, grabaciones sonoras, personas y organizaciones como fuentes de conocimiento, edificios, sitios, monumentos, objetos tridimensionales o bienes inmuebles; y a las colecciones de tales artículos o partes de los mismos.
- Los documentos a menudo son las manifestaciones de las obras. Pueden diferir ampliamente en forma y características.
- En algunas profesiones a los documentos a veces se les denomina “medio”, “título” o “artículo».⁹

En ISO 9000 “documento” se define como «Información y el medio en el que está contenida».¹⁰ También se especifica:

- el soporte puede ser papel, disco magnético, electrónico u óptico, fotografía o master, o una combinación de los mismos;

- denominamos “documentación” a un conjunto de documentos, como por ejemplo especificaciones y registros.

Es importante señalar que las normas anteriores sugieren una interpretación muy amplia de este término como un documento utilizado para los procesos oficiales, administrativos y de trabajo, de especificación, imagen, informe, normas, etc. Todas estas interpretaciones tan amplias están correlacionadas con las normas internacionales utilizadas en las tecnologías de la información.

Por otro lado, en ISO 25964 “documento” se describe como «Cualquier recurso que se puede clasificar o indexar con el fin de que los datos o la información contenida en él se pueda recuperar».¹¹ La nota a la entrada específica que esta definición se refiere no sólo a los materiales escritos o impresos en papel o en formato microfilm (por ejemplo, libros convencionales, revistas, diagramas, mapas), sino también a soportes no impresos como archivos de lectura mecánica o digital («Cualquier recurso que pueda ser clasificado o indexado con el fin de que los datos o información contenida en él se pueda recuperar»), recursos de internet e intranet, películas, grabaciones sonoras, personas y organizaciones como fuentes de conocimiento, edificios, sitios, monumentos, objetos tridimensionales o bienes inmuebles; y a las colecciones de tales artículos o partes de los mismos. Curiosamente, si bien la definición de este término difiere de la de ISO 5127-2017, esta última repite literalmente sus especificaciones.

ISO 10209 contiene dos definiciones del término «documento»:

- «Cantidad fija y estructurada de información destinada a la percepción humana que puede gestionarse e intercambiarse como una unidad entre usuarios y sistemas».¹²
- «Cualquier medio con información registrada sobre o en él».¹³

En IEC 82045 el término «documento» se interpreta como «cantidad fija y estructurada de información que se puede gestionar e intercambiar como una unidad entre usuarios y sistemas».¹⁴

Ya hemos observado que los términos «documento» y «documento administrativo» no son sinónimos y lo podemos ver claramente gracias a sus definiciones en ISO 5127.

Por lo tanto, es evidente que la interpretación del término “documento” es muy cercana a la de la “información documentada”. Sin embargo, en las tecnologías de la información un “documento” puede ser cualquier objeto que esté en el sistema (archivo, presentación, observación, gráfico, documento compuesto), muy similar al concepto de “datos” y aquí es donde los ámbitos de las tecnologías de la información y la gestión de documentos difieren en su enfoque a la hora de dotar de significado al término “documento”.

En las normas de las TI desarrolladas por ISO e IEC, el término «documento administrativo» puede entenderse como una forma de fijar la información

en un soporte. Vale la pena señalar que los estándares de las TI prefieren el término «documento» a «documento administrativo».

El término «documento administrativo» no está incluido en IEC 82045.

Las definiciones del término «documento administrativo» en las versiones antiguas y nuevas de ISO 15489 lo describen con la ayuda del término «información» y anulan por completo la idea de que el «documento administrativo» es un subtipo de «documento».

En la primera versión de ISO 15489 (2001) «documento administrativo» es «Información creada, recibida y mantenida como evidencia e información por una organización o persona, en cumplimiento de obligaciones legales o en las transacciones empresariales».¹⁵

En la versión reciente de ISO 15489 (2016) «documento administrativo» es «Información creada, recibida y mantenida como evidencia o como activo por una organización o persona, en cumplimiento de obligaciones legales o en las transacciones empresariales».¹⁶

Como se puede ver, las definiciones anteriores no son muy diferentes entre sí y la nueva versión ISO 15489 sólo agrega algunos detalles menores.

Por lo tanto, podemos concluir que las definiciones de los términos «documento» y «documento administrativo» no están coordinadas en las normas ISO e IEC y pueden interpretarse tanto como sinónimos como conceptos diferentes. Sus definiciones en ISO 5127 lo demuestran claramente.

En ISO 5127:2001 el término “documento administrativo” tiene 2 definiciones:

- «Conjunto de datos sobre una persona u objeto, seleccionados y presentados con un fin específico y predefinido»¹⁷.
- «Documento creado o recibido y mantenido por una agencia, organización o persona en cumplimiento de obligaciones legales o en las gestiones empresariales»¹⁸.

Por lo tanto, la norma terminológica básica ISO da 2 interpretaciones de este término:

- a) una más completa que incluye todo tipo de datos;
- b) otra más específica relacionada con todas las esferas de la actividad empresarial.

Así, mientras que en (a) “documento administrativo” se entiende como “documentación”, “información documentada” o “datos”, es decir, se utiliza con este significado general propio de la ciencia archivística y bibliotecaria, en (b) significa un documento oficial o administrativo que se utiliza en los negocios y se refiere a la gestión documental y al ámbito jurídico.

En las TI “registro” puede entenderse como una forma de fijar la información en un soporte. Es importante tener en cuenta que “registro” no se utiliza en las normas metodológicas ISO desarrolladas para expertos en TI, porque estos últimos utilizan los términos “documento” y “datos”. En cuanto a las normas ISO tecnológicas y técnicas sobre las TI, siempre se especifica el término “documento administrativo”, por ejemplo, “campo de registro” (en una base de datos).

Siguiendo con el término “documento administrativo”, vemos que no tiene el mismo significado en otras áreas profesionales. ISO 9000 define este término como “Documento que indica los resultados obtenidos o proporciona evidencia de las actividades realizadas”. En la nota a las entradas figura que “los documentos administrativos se pueden utilizar, por ejemplo, para formalizar la trazabilidad y verificar una acción preventiva o correctiva” y “generalmente los documentos administrativos no necesitan someterse a revisión”.¹⁹

En las definiciones de los subterminos de este concepto prevalece la interpretación de «registro» como «conjunto de datos». A continuación, algunos ejemplos de ISO 5127-2017:

- Registro catalográfico – «registro establecido para un artículo bibliográfico».²⁰
- Registro local – «registro bibliográfico <conjunto de datos> que contiene datos adicionales pertenecientes a una sola institución o aplicación ».²¹
- Registro electrónico, registro de lectura mecánica – «registro <conjunto de datos> almacenado en un medio de lectura mecánica».²²
- Registro audiovisual – «soporte de grabación y almacenamiento <ubicación> de sonidos e imágenes».²³
- Documentos administrativos, archivos corrientes – «registros <documentos> utilizados de forma regular para la realización de los negocios de una agencia, institución u organización ».²⁴
- Documentos semiactivos – «archivos intermedios <documentos> que se demandan con poca frecuencia para la realización de los negocios presentes».²⁵
- Documento inactivos – «registros <documentos> que ya no son necesarios para la realización de los negocios ».²⁶
- Documentos públicos:
<registros gubernamentales>- «registros <documentos> o archivos <registros> creados o recibidos, y recopilados por agencias gubernamentales en la realización de los asuntos públicos».²⁷
<término legal> - «registros públicos <documentos gubernamentales> designados como tal en la legislación ».²⁸
- Registro de autoridad – «entrada en un catálogo de autoridades».²⁹

Significativamente, ISO 5127 no contiene «documento de archivo» ni «registro de archivo» como términos individuales. Sin embargo, algunas definiciones de los subterminos de «registro» están conectadas con los archivos.

Después de haber analizado los subterminos de «documento administrativo» podríamos concluir que este término es un subtipo del término «documento». Sin embargo, las definiciones de los subterminos «documento administrativo público» y «documento público» en la ISO 5127-2017 no nos permiten esta conclusión.

ISO 5127-2017 también nos presenta una gran cantidad de subterminos. Por ejemplo:

- Documento analógico – «documento de recursos analógicos utilizable sin equipo digital».³⁰
- Documento digital - «unidad de información con un contenido definido que ha sido digitalizado o producido originalmente en formato digital». En las notas a la entrada podemos leer lo siguiente: «Esto incluye libros electrónicos, patentes electrónicas, documentos audiovisuales en red y otros documentos cuando están en formato digital, por ejemplo, informes, documentos cartográficos y musicales, preimpresiones. Se excluyen las bases de datos y las publicaciones periódicas electrónicas. Un documento digital se puede estructurar en uno o más archivos. Un documento digital consta de una o más unidades de contenido».³¹
- Documento digitalizado - «documento cuyo contenido y/o apariencia ha sido, a través de técnicas de escaneo digital, transferida/convertida a formato digital».³²
- Documento virtual – «documento que existe de forma concreta pero no gráfica, por ejemplo, en cinta o disco o en una memoria de ordenador».³³
- Documento secundario – «la documentación secundaria es una obra por derecho propio pero que se basa en el análisis, discusión o comentario de uno o más documentos, lo que resulta generalmente en una modificación parcial de la perspectiva vigente sobre el tema». En las notas a la entrada podemos ver lo siguiente: «La distinción entre documentación secundaria y primaria juega un papel muy importante en los estudios académicos y en las reglas del trabajo académico. En ocasiones, puede ser necesario un análisis más profundo para poder distinguir entre documentos primarios, derivados y secundarios».³⁴
- Documento inédito – «documento que no se ha ofrecido para su recepción al público general».³⁵
- Documento anónimo – «documento de autor desconocido o no mencionado».³⁶

- Documento público – «documento elaborado (diseñado) en su debida forma por una autoridad pública o una persona capacitada jurídicamente para su acción en nombre de la autoridad». Con ello un «documento público» puede ser un documento de notaría, por ejemplo: «Un testamento público, un contrato comercial depositado ante notario, un certificado de nacimiento, un diploma universitario, una demanda fiscal, una garantía (pagaré), papel moneda».³⁷
- Documento privado – «documento creado (diseñado) con respecto a ciertos requisitos de forma y establecido por o entre personas privadas sin necesidad de una certificación formal <declaración> ya que está aprobado por la opinión pública».³⁸ Un documento privado puede ser un contrato privado de préstamo de dinero o un contrato de compraventa común.
- Documento gubernamental – «documento publicado por el gobierno o por exigencia legal o bien publicado por un organismo internacional»³⁹. Con lo último nos referimos a las Naciones Unidas, la Unión Europea, la UNESCO, etc.-
- Documento legal – «documento por el que se establecen las decisiones de personas jurídicas, parlamentos o resoluciones judiciales redactadas conforme a determinadas normas».⁴⁰
- Documento administrativo – «documento creado en la realización de las actividades diarias de una persona jurídica o de cualquier organización en general».⁴¹
- Documento jurídico - «documento que contiene disertaciones sobre asuntos jurídicos de cualquier tipo».⁴²
- Documento técnico – «documento que trata cuestiones tecnológicas en el estudio, construcción y examen de aparatos técnicos».⁴³
- Documento comercial – «documento creado por cualquier área funcional dentro de una empresa comercial».⁴⁴
- Documento personal – «documento con implicaciones jurídicas en, o una conexión particularmente íntima con, la trayectoria vital pudiendo formar parte del patrimonio personal». En los ejemplos de este término encontramos «Certificados de nacimiento, libros de familia, pasaportes, contratos de trabajo, visados, tarjetas de membresía, etc.; diarios personales; cartas de amor <documento >».⁴⁵

Una vez analizados los términos anteriores, se puede concluir que en la mayoría de los casos su definición nos remite a ellos en calidad de subterminos de «documento» tal como se utiliza en la actividad empresarial, lo cual podría tener consecuencias jurídicas. La única excepción es la definición de «documento

digital» interpretado como una «unidad de información con un contenido definido...», que enfatiza la diferencia esencial de este concepto y que lo conecta con «datos» y en parte con «registro».

El término “datos” y sus subterminos

Ya que últimamente se tiende a utilizar el término “datos” en lugar de los términos “información registrada” e “información documentada” es interesante tener en cuenta las diferentes definiciones de este término según las normas ISO e IEC.

Esta palabra aparece en la norma terminológica especial ISO 5127-2001 que combina varios sistemas de términos: bibliotecas, publicaciones, archivos, gestión, etc. donde «datos» es definido como: «Representación de la información de manera formalizada adecuada para la comunicación, interpretación y procesamiento».⁴⁶

En ISO 5127-2017 la definición de este término cambia ligeramente: «representación reinterpretable de la información de una manera formalizada adecuada para la comunicación, interpretación o procesamiento»⁴⁷. Además, en la nota a la entrada del término leemos que «a menudo entendemos que los datos toman la forma de un conjunto de valores con variables cualitativas o cuantitativas».⁴⁸

La definición de este término puede resultar un poco vaga porque «representación reinterpretable de la información» sugiere o bien su posible transferencia o bien posibles futuras distorsiones.

ISO 5127-2017 contiene varios tipos de «datos» presentados como subterminos. Estos son:

- Datos intrínsecos: «datos que se pueden leer en un documento u objeto material directamente a través de su presencia física».⁴⁹
- Datos extrínsecos: «datos acerca un documento u objeto material que no se pueden obtener directamente de él, sino únicamente a través de su comunicación».⁵⁰
- Datos vinculados: «datos que permiten conexiones entre datos».⁵¹
- Datos sin procesar: «datos adquiridos en su forma original y directa con respecto a su fuente antes de su procesamiento posterior».⁵²
- Datos procesados: «datos que han pasado, a partir de datos sin procesar o datos procedentes de una fase anterior, a una fase más refinada gracias a la limpieza, clasificación, vinculación, y verificación de datos así como a operaciones similares».⁵³
- Datos maestros: «datos que representan las características de contenido de sus objetos de datos y que constituyen una base sólida para ciertos procesos

recurrentes, se pueden utilizar repetidamente en una variedad de operaciones y, por lo tanto, permanecen estables durante más tiempo». ⁵⁴

- Datos dinámicos: «datos cuyo contenido varía con frecuencia y en momentos asincrónicos». Al mismo tiempo, «Los datos dinámicos pueden ser de varios estilos. Pueden ser flujos de datos generados por sensores cuando los segmentos de datos aparecen de forma impredecible. Es decir, los flujos de datos tienen lagunas. También pueden ser flujos de datos que son generados por los seres humanos en escenarios de colaboración abierta distribuida donde no está claro en qué momento y qué celda de una base de datos se llenará». ⁵⁵
- Datos masivos: «grandes cantidades de datos que resultan de la aplicación de una medición o recopilación normalmente automática». ⁵⁶
- Big data o macrodatos: «conjunto de datos/colecciones/datos vinculados de gran extensión caracterizados principalmente por su gran volumen, amplia variedad, alta velocidad (creación y uso) y/o variabilidad que en conjunto precisan una arquitectura escalable para un almacenamiento de datos eficiente (1) <ubicación>, manipulación y análisis». ⁵⁷
- Datos de investigación: «datos recopilados, observados o creados, con fines de análisis de datos para producir información y resultados de investigación originales». ⁵⁸
- Datos científicos: «datos que son base o resultado de los esfuerzos de la ciencia». ⁵⁹
- Datos abiertos: «datos disponibles/visibles para otros y que pueden ser utilizados, reutilizados, republicados y redistribuidos libremente por cualquiera». ⁶⁰
- Datos personales: «datos relativos a una persona identificada o identificable». ⁶¹
- Datos anónimos: «datos personales modificados de tal manera que queda suprimida la referencia directa a los interesados». ⁶²
- Datos sensibles: «datos con efectos potencialmente dañinos en caso de su divulgación o mal uso». ⁶³
- Datos clasificados: «datos cuyo acceso está restringido por medios administrativos que varían según el grado de protección de datos o de protección de la información solicitada». ⁶⁴
- Datos confidenciales: «datos a los que sólo un número limitado de personas tienen acceso y que están destinados a un uso restringido». ⁶⁵
- Datos de referencia: «objetos de datos normalizados de dominio y comunidad que definen el conjunto de valores permitidos que se utilizarán para rellenar otros objetos de datos». ⁶⁶

- Datos registrados: «datos que han pasado por un proceso de registro y como resultado tiene un identificador y generalmente metadatos para su búsqueda y recuperación».⁶⁷
- Datos en tiempo real: «datos que se reciben, procesan y almacenan en el momento de su aparición con sólo un pequeño desfase temporal».⁶⁸
- Datos activos: «datos que denotan unidades virtuales de objetos de datos que se crean dinámicamente mediante código ejecutable».⁶⁹
- Datos referibles: «datos (digitales o no) que se almacenan de forma repetitiva y a los que hace referencia un identificador persistente».⁷⁰
- Datos citables: «datos referibles que han sido sometidos a registro y evaluación de su calidad y pueden denominarse citas en publicaciones y formar parte de objetos de investigación».⁷¹
- Datos digitales: «datos en forma de secuencia estructurada de bits/bytes que representan el contenido de la información».⁷²

Después de haber analizado las definiciones de los tipos de datos en ISO 5127-2017 podemos ver que son definiciones lógicas y bien coordinadas, aunque idealizadas. Por ejemplo, desde nuestro punto de vista, los datos de investigación y los datos científicos no deben considerarse distintos porque pueden transformarse unos en otros y otros en unos.

Además, la definición de «datos digitales» es llamativa porque no explica su significado/esencia (como otras definiciones) sino su forma.⁷³ Siguiendo esta lógica nosotros podríamos ser los creadores de los términos y definiciones de los datos en papel o película. Sería más apropiado que la definición de este término reflejara la esencia de los «datos digitales».

Ni las versiones antiguas ni las nuevas de ISO 15489 contienen el término «datos», lo que podría deberse al hecho de que este término no se utiliza demasiado en la gestión documental, ya que la situación legal de los datos no es muy clara.

La norma internacional IEC 82045, así como la ISO 15489 destinada a expertos en gestión documental definen el término «datos» como «presentación de información reinterpretable de manera formalizada y adecuada para la comunicación, interpretación o procesamiento».⁷⁴

El término «datos» también se encuentra en las normas internacionales de sistemas de gestión de calidad, por ejemplo, ISO 9000, donde aparecen como «hechos sobre un objeto».⁷⁵ Sin embargo, los datos no siempre son un hecho y las normas internacionales utilizadas en la seguridad de la información enfatizan este aspecto.

En las normas de las TI, el término «datos» se interpreta como «recopilación de valores asignados a medidas de base, medidas derivadas y/o indicadores».⁷⁶

En ISO 10209 nos encontramos tres definiciones de este término, según su uso:

- <definición de producto digital> «Información representada de manera formal y adecuada para la comunicación, interpretación o procesamiento por seres humanos u ordenadores». ⁷⁷
- <metadatos> «Representación de hechos, conceptos o instrucciones de manera formalizada y adecuada para la comunicación, interpretación o procesamiento por los seres humanos o por medios automáticos». ⁷⁸
- «Gestión de documentos» «Presentación reinterpretable de la información de manera formalizada y adecuada para la comunicación, interpretación o tratamiento». ⁷⁹

Cabe señalar que las dos últimas definiciones fueron copiadas de IEC 82045-1-2001 y se han utilizado hasta la actualidad. Así que podemos ver que el término «datos» tiene un significado específico según del área profesional. Pero al mismo tiempo tiene un significado general estandarizado por ISO 5127.

Por lo que podemos concluir que los «datos» son la información estructurada adecuada para la percepción, interpretación y transferencia, que tiene valor legal pero no validez legal. Además, los datos no tienen reglas estrictas (unificadas) para su creación, formato, registro y almacenamiento. La característica principal de este concepto es el amplísimo alcance del término «datos».

Para finalizar y a modo de resumen podemos señalar que todas estas cuestiones terminológicas siempre han sido uno de los eternos problemas a solventar. El análisis de las definiciones de los términos básicos y de sus subterminos utilizados en la gestión documental nos lleva a la conclusión de que el sistema terminológico normalizado por ISO e IEC no es homogéneo y puede incluir varias y a veces muy diferentes definiciones del mismo término. Al mismo tiempo, debemos señalar el gran valor y utilidad que la experiencia de estandarización de este término por parte de estas organizaciones de normalización tan conocidas tiene para los expertos en gestión documental de todo el mundo.

Conclusión

Podemos concluir a partir del análisis de las definiciones de los términos normalizados por ISO, que dicho sistema terminológico no está bien armonizado y además puede contener varias definiciones, en ocasiones bastante controvertidas, de un mismo término. Esta situación es patente en las normas que regulan la gestión de documentos y archivos, las TI y el sistema de gestión de calidad. Los términos “información documentada” e “información registrada”, “documento” y “documento administrativo”, así como el término “datos” son buen ejemplo de ello.

Todo esto viene a decir que las labores de unificación terminológica ni siquiera han concluido en la Organización Internacional de Normalización (ISO).

Lejos de mejorar esta situación, la introducción de la terminología internacional la ha complicado en muchas áreas profesionales, lo que incluye la gestión documental ya que esta última ha comenzado a emplear numerosos términos procedentes de las TI que no están coordinados con los sistemas terminológicos de los ámbitos profesionales relacionados. Por ejemplo, el término «documento» es a menudo sinónimo del término «datos» lo cual es básicamente erróneo desde el punto de vista de la gestión documental. La situación se ve agravada por las diferentes interpretaciones de los mismos términos que figuran en las normas ISO utilizados en áreas adyacentes. Por ejemplo, la nueva versión del estándar principal de la gestión documental internacional (ISO 15489:2016 “Información y documentación. Gestión documental. Concepto y principios”) ha coordinado su terminología con la serie ISO 30300 “Información y documentación. Sistema de gestión documental” pero seguimos sin tener una definición uniforme de los términos «documento» y «documento administrativo» en las normas para las TI y la gestión de la calidad. Aunque la norma terminológica principal ISO 5127 “Información y documentación. Vocabulario” se actualizó en 2017, el sistema de coordinación de términos idénticos empleados en diferentes áreas profesionales no se ha desarrollado con totalidad.

Todo esto incide en la complejidad y el alcance real de las tareas de compatibilidad terminológica a las que se enfrentan los expertos. La presente investigación ha demostrado la urgente necesidad de resolver este problema a nivel internacional mediante las normas ISO utilizadas en todo el mundo.

Notas

¹ NOTA DE LA TRADUCTORA: se ha optado generalmente, y según el contexto, por traducir el término “record” por documento administrativo

² Varlamova L., Bayun L., Bastrikova K. Gestión documental: diccionario comentado inglés-ruso de terminología normalizada. – Moscú, 2017. El diccionario ha recopilado los términos y definiciones de más de 20 estándares internacionales utilizados en la gestión documental, en los archivos, en la gestión de la calidad, en la gestión de la seguridad de la información, en la evaluación de riesgos etc. Este diccionario contiene aproximadamente 600 entradas y comentarios a las mismas. Muestra las diferencias de significado del mismo término por parte de los gestores documentales, archiveros y especialistas en TI.

³ ISO 9000:2015 Sistemas de gestión de calidad – Fundamentos y vocabulario; definición 3.8.6

⁴ ISO 9000:2015 Sistemas de gestión de calidad – Fundamentos y vocabulario; definición 3.8.6

⁵ ISO 5127:2001 Información y documentación – Vocabulario; definición 1.1.4.01

⁶ ISO 15489-1:2001 Información y documentación – Gestión documental – Parte 1: General; definición 3.10

ISO 30300:2011 Información y documentación – Sistemas de gestión documental – Fundamentos y vocabulario; definición 3.1.3

ISO/IEC 11179-5:2015 Tecnología de la información – Registros de metadatos (MDR) – Parte 5: Principios para la designación; definición 2.2

⁷ ISO 15489-1:2001 Información y documentación – Gestión documental – Parte 1: General; definición 3.10.

ISO 30300:2011 Información y documentación – Sistemas de gestión documental – Fundamentos y vocabulario; definición 3.1.3.

ISO/IEC 11179-5:2015 Tecnología de la información – Registros de metadatos (MDR) – Parte 5: Principios para la designación; definición 2.2.

⁸ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.1.1.38.

⁹ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.1.1.38.

¹⁰ ISO 25964-2:2013 Información y documentación – Tesoros e interoperabilidad con otros vocabularios – Parte 2: Interoperabilidad con otros vocabularios; definición 2.15

¹¹ ISO 25964-2:2013 Información y documentación – Tesoros e interoperabilidad con otros vocabularios – Parte 2: Interoperabilidad con otros vocabularios; definición 2.15

¹² ISO 10209-2012 Documentación técnica del producto – Vocabulario – Términos relacionados con el dibujo técnico, la definición de producto y documentación relacionada; definición 11.54.2.

¹³ ISO 10209-2012 Documentación técnica del producto – Vocabulario – Términos relacionados con el dibujo técnico, la definición de producto y documentación relacionada; definición 11.54.3.

¹⁴ CEI/IEC 82045-1:2001 Gestión documental. Parte 1: Principios y métodos; definición 3.2.3.

¹⁵ ISO 15489-1:2001 Información y documentación – Gestión documental – Parte 1: General; definición 3.15.

¹⁶ ISO 15489-1:2016 Información y documentación –Gestión documental –Parte 1: Conceptos y principios; definición 3.14.

¹⁷ ISO 5127:2001 Información y documentación - Vocabulario; definición 1.1.3.11.

¹⁸ ISO 5127:2001 Información y documentación - Vocabulario; definición 2.2.1.08.

¹⁹ ISO 9000:2015 Sistemas de gestión de calidad – Fundamentos y vocabulario; definición 3.8.6.

²⁰ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.1.13.17.

²¹ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.1.13.18.

²² ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.3.3.11.

²³ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.4.5.17.

²⁴ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.6.3.01.

²⁵ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.6.3.02.

²⁶ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.6.3.03.

²⁷ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.6.3.04.

²⁸ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.6.3.05.

²⁹ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.7.2.28.

³⁰ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.3.3.01.

³¹ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.3.3.02.

³² ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.3.3.04.

³³ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.3.3.12.

³⁴ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.4.1.07.

- ³⁵ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.4.1.10.
- ³⁶ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.4.1.18.
- ³⁷ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.4.4.19.
- ³⁸ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.4.4.20.
- ³⁹ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.4.6.01.
- ⁴⁰ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.4.6.02.
- ⁴¹ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.4.6.03.
- ⁴² ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.4.6.06.
- ⁴³ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.4.6.07.
- ⁴⁴ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.4.6.10.
- ⁴⁵ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.4.6.24.
- ⁴⁶ ISO 5127:2017 Información y documentación – Vocabulario; – definición 1.1.4.01.
- ⁴⁷ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.1.1.15.
- ⁴⁸ ISO 5127:2017 Información y documentación – Vocabulario; – definición 3.1.1.15.
- ⁴⁹ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.01.
- ⁵⁰ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.02.
- ⁵¹ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.03.
- ⁵² ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.04.
- ⁵³ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.05.
- ⁵⁴ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.06.
- ⁵⁵ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.07.
- ⁵⁶ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.08.
- ⁵⁷ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.09.
- ⁵⁸ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.10.
- ⁵⁹ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.11.
- ⁶⁰ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.13.
- ⁶¹ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.14.
- ⁶² ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.15.
- ⁶³ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.16.
- ⁶⁴ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.17.
- ⁶⁵ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.18.
- ⁶⁶ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.19.
- ⁶⁷ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.20.
- ⁶⁸ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.21.
- ⁶⁹ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.22.
- ⁷⁰ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.23.
- ⁷¹ ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.24.
- ⁷² ISO 5127:2017 Información y documentación – Vocabulario. – definición 3.1.10.25.

⁷³ Es necesario mencionar que en ISO 5127-2017 el término “data” (“datos”) se usa a menudo como un sustantivo singular. Sin embargo, hemos preferido entenderlo en plural siguiendo las reglas gramaticales tradicionales.

⁷⁴ IEC 82045-1:2001 Gestión documental - Parte 1: Principios y métodos. – definición 3.1.4.

⁷⁵ ISO 9000:2015 Sistemas de gestión de calidad – Fundamentos y vocabulario. – definición 3.8.1.

⁷⁶ ISO/IEC 15939:2007 Ingeniería de Software y sistemas – Proceso de medición. – definición 2.4.

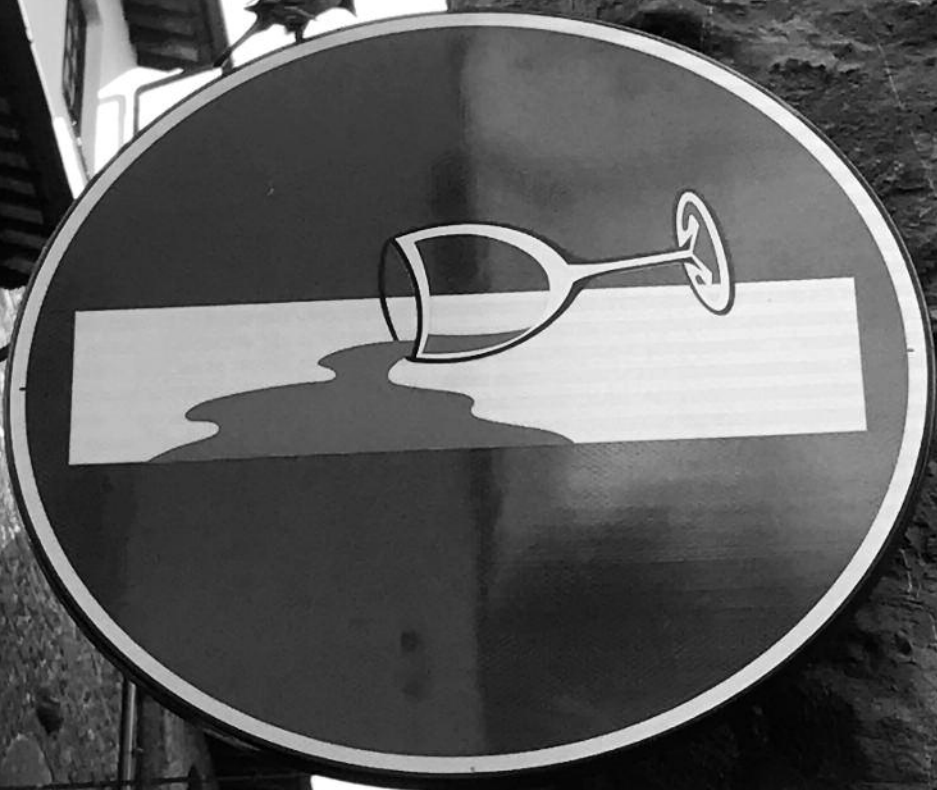
ISO/IEC 27000-2014 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Resumen y vocabulario. – definición 2.20.

⁷⁷ ISO 10209-2012 Documentación técnica del producto – Vocabulario – Términos relacionados con el dibujo técnico, la definición del producto y documentación relacionada. – definición 11.44.1.

⁷⁸ ISO 10209-2012 Documentación técnica del producto – Vocabulario – Términos relacionados con el dibujo técnico, la definición del producto y documentación relacionada. – definición 11.44.2.

⁷⁹ IEC 82045-1:2001 Gestión documental - Parte 1: Principios y métodos. – definición 3.1.4.

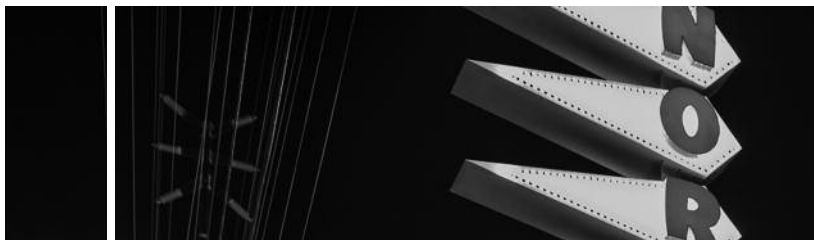
ISO 10209-2012 Documentación técnica del producto – Vocabulario – Términos relacionados con el dibujo técnico, la definición del producto y documentación relacionada. – definición 11.44.3.



NSA



**RESTRICTED
ENTRANCE**



FRANCISCA RAMÓN FERNÁNDEZ

Secretos empresariales en documentos y ficheros electrónicos y la protección de datos personales y garantía de los derechos digitales¹

Business secrets in electronic records and files and the personal data protection and guarantee of digital rights

Francisca Ramón Fernández
 frarafer@urb.upv.es
 Universitat Politècnica de València

Citación: Ramón Fernández, Francisca (2019). "Secretos empresariales en documentos y ficheros electrónicos y la protección de datos personales y garantía de los derechos digitales". *Tábula*, n. 22, pp. 73-92

Recibido: 1-4-2019. *Aceptado:* 9-9-2019

Resumen analítico / Analytic summary

Se analiza la relación existente entre los documentos y ficheros electrónicos que contienen secretos empresariales y la protección de datos de carácter personal, a través del análisis de la principal legislación aplicable como es la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Se atenderá a la casuística referente a la prestación del consentimiento, confidencialidad y derecho a la información. Los resultados nos determinarán si la legislación resulta adecuada y las lagunas e incertidumbres que la normativa no resuelve.

DOCUMENTOS | FICHEROS ELECTRÓNICOS | SECRETOS EMPRESARIALES |
PROTECCIÓN DE DATOS | DERECHO A LA INFORMACIÓN

The relationship between electronic documents and files containing business secrets and the protection of personal data is analyzed, through the analysis of the main applicable legislation such as Law 1/2019, of February 20, on Business Secrets, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, and Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights. The casuistry regarding the provision of consent, confidentiality and right to information will be addressed. The results will determine if the legislation is adequate and the gaps and uncertainties that the regulation does not resolve.

DOCUMENTS | ELECTRONIC FILES | BUSINESS SECRETS | DATA PROTECTION |
RIGHT TO INFORMATION

En el ámbito de la transferencia de conocimiento y la innovación, la protección de ésta última se enmarca tanto a través de la propiedad intelectual e industrial respecto de cada uno de los derechos que se aplican (Ramón, 2015, p. 41; Flores, 2017, p. 57). La relación con la competitividad y la protección de la información es innegable y los conocimientos abarcan no sólo el área tecnológica y científica (Rabasa, 2018, p. 5), sino también los datos en relación con listas de clientes, proveedores, etc. (Fernández, 2013, p. 413; Fernández, 2016, p. 260).

En el presente trabajo se analizará la repercusión que ha tenido la Ley 1/2019, de 20 de febrero, de Secretos Empresariales (BOE núm. 45, de 21 de febrero de 2019) al referirse a documentos y ficheros electrónicos como soporte de los mismos y su encaje con el derecho a la información y la protección de datos tras el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Diario Oficial de la Unión Europea L119/1, de 4 de mayo de 2016), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 6 de diciembre de 2018).

Los secretos empresariales: concepto y características

Con anterioridad a la Ley 1/2019, no se disponía de una legislación en la que se definiera lo que se entendía como secreto empresarial. El propio Tribunal Supremo, en sentencia 285/2008, de 12 de mayo (TOL1.335.978) manifestó que ello

era debido por “tratarse de un concepto lábil, dinámico, no constreñible en un «numerus clausus»”. La sentencia se inclinaba, pues, por “ir a una concepción funcional-práctica, debiendo considerar secretos de empresa los propios de la actividad empresarial, que de ser conocidos contra la voluntad de la empresa, pueden afectar a su capacidad competitiva”.

Posteriormente, la sentencia núm. 679/2018, de 20 de diciembre (TOL6.988.673), reiteró que ante la falta de un concepto legal de secreto empresarial, para determinar si existía o no el mismo, se debía acudir al art. 39 del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (Anexo 1C del Convenio por el que se crea la Organización Mundial del Comercio, Ronda de Uruguay de 1994, conocido con el nombre de ADPIC, que fue ratificado por España el 30 de diciembre de 1994 (BOE núm. 20, de 24 de enero de 1995).

En esta última sentencia del Alto Tribunal se precisaba que la información tenía que contener una serie de caracteres para que se pudiera considerar como secreto:

- a) Que sea secreta, en cuanto no sea conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza este tipo de información.
- b) Que tenga un valor comercial o competitivo por ser secreta.
- c) Que haya sido objeto de medidas razonables, en las circunstancias concurrentes, para mantenerla secreta, tomadas por la persona que legítimamente la controla.

Por lo que se refiere a sus características, se encuentran las siguientes, siguiendo lo indicado en el Acuerdo sobre los aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, Ronda, Uruguay, 1994, conocidos como Acuerdo ADPIC, en su art. 39:

- a) confidencialidad;
- b) exclusividad;
- c) valor económico, y
- d) licitud.

El fundamento reside en la lealtad de quienes deben guardar el secreto, e incluye los secretos de naturaleza técnico industrial (objeto empresarial), comercial (clientela o marketing) y organizacional (laboral, funcionamiento y planes empresariales).

Se puede materializar el secreto en cualquier tipo de soporte, tanto en papel como electrónico, y en original como copia, incluso en el caso de comunicación

verbal, y se extiende a cifras, listados, partidas contables, organigramas, planos, memorándums, entre otros. La duración de la obligación de no revelación se atenderá a la fuente del deber de reserva que se establezca por norma o contractualmente.

La jurisprudencia también se ha pronunciado respecto a un supuesto relativo a revelación de secretos empresariales mediante la utilización del correo electrónico (Cfr. Trujillo, 2014, p. 292). Así, la sentencia del Tribunal Constitucional 170/2013, de 7 de octubre de 2013 (BOE núm. 267, de 07 de noviembre de 2013) consideró que:

“En atención al carácter vinculante de esta regulación colectivamente pactada, cabe concluir que, en su relación laboral, sólo estaba permitido al trabajador el uso profesional del correo electrónico de titularidad empresarial en tanto su utilización para fines ajenos al contenido de la prestación laboral se encontraba tipificada como infracción sancionable por el empresario, regía pues en la empresa una prohibición expresa de uso extralaboral, no constando que dicha prohibición hubiera sido atenuada por la entidad. Siendo este el régimen aplicable, el poder de control de la empresa sobre las herramientas informáticas de titularidad empresarial puestas a disposición de los trabajadores podía legítimamente ejercerse, *ex art. 20.3 LET*, tanto a efectos de vigilar el cumplimiento de la prestación laboral realizada a través del uso profesional de estos instrumentos, como para fiscalizar que su utilización no se destinaba a fines personales o ajenos al contenido propio de su prestación de trabajo.

En tales circunstancias, de acuerdo con la doctrina constitucional expuesta, cabe entender también en el presente supuesto que no podía existir una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de la cuenta de correo proporcionada por la empresa y que habían quedado registradas en el ordenador de propiedad empresarial. La expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, incluida la adecuación de su prestación a las exigencias de la buena fe [arts. 5 a) y 20.2 y 3 LET]. En el supuesto analizado la remisión de mensajes enjuiciada se llevó a cabo a través de un canal de comunicación que, conforme a las previsiones legales y convencionales indicadas, se hallaba abierto al ejercicio del poder de inspección reconocido al empresario, sometido en consecuencia a su posible fiscalización, con lo que, de acuerdo con nuestra doctrina, quedaba fuera de la protección constitucional del art. 18.3 CE.

En el contexto descrito, debemos concluir que la conducta empresarial denunciada, realizada además cuando el proceso de comunicación podía entenderse ya finalizado, no ha supuesto una interceptación o conocimiento antijurídico de comunicaciones ajenas realizadas en canal cerrado, en definitiva, debe descartarse la invocada lesión del derecho al secreto de las comunicaciones”.

La futura regulación contemplaba una definición, así como la incorporación de la Directiva comunitaria. De esta forma, el informe del Anteproyecto de la actual Ley 1/2019, de 20 de febrero, de Secretos Empresariales (BOE núm. 45, de 21 de febrero de 2019) (en adelante, Ley 1/2019), que emitió el Consejo General del Poder Judicial, mediante acuerdo del 22 de marzo de 2018, señaló:

“La norma europea trata de paliar la falta de armonización existente en los ordenamientos de los Estados miembros de la Unión Europea en la definición y protección de los secretos empresariales, identificados con los conocimientos técnicos (*know how*) y la información empresarial, articulando las medidas, remedios y procedimientos a través de los que se ha de dispensar tal protección. (...)

Se concibe, por tanto, como una norma de contenido netamente tuitivo de tal derecho y de aquellos intereses legítimos que tiene como finalidad establecer un marco procesal de tutela que comprende no sólo la delimitación de las acciones y subsiguientes pretensiones de que dispone el titular del secreto para obtener la protección del capital intelectual y de la información empresarial que constituyen su objeto (...).”

El texto actual, Ley 1/2019, recoge las anteriores precisiones del Tribunal Supremo, y formula el concepto de secreto empresarial como cualquier información o conocimiento, entre los que se incluye el tecnológico, científico, industrial, comercial, organizativo o financiero, pero que debe reunir unas condiciones específicas que determina el art. 1 de la Ley 1/2019. En este sentido, debe ser secreto, entendido como no conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento, ni sea fácilmente accesible; debe tener un valor empresarial, que puede ser real o potencial; y debe haber sido objeto de medidas razonables por parte de su titular para que no sea conocido (más ampliamente, véase, Sainz de Aja y Peinado, 2018, p. 32; Saldarriaga, 2018, p. 9).

Queda, por tanto, excluida la información de escasa importancia, así como la experiencia y competencias adquiridas por el personal durante el transcurso de su trayectoria, así como la información que sea de conocimiento general o considerada como fácilmente accesible en los círculos en los que se utilice (Cfr. Félix y Díaz, 2018; Lissén y Guillén, 2019; Massaguer, 2018a, p. 7 y 2018b, p. 3; Fernández de Córdoba, 2019, p. 16).

Por último, se encuentra tipificado el secreto de empresa dentro de los delitos relativos al mercado y a los consumidores, recogidos en los arts. 278 y 279 del Código Penal.

El art. 278 se entiende tanto por parte de personas que trabajan dentro de la empresa, como también por parte de terceros (Fernández, 2017; Domingo, 2018). Los instrumentos que señala el art. 197.1 del Código penal son los siguientes: papeles, cartas, mensajes de correo electrónico o cualquiera otros documentos o efectos personales, interceptación de telecomunicaciones, o utilización de artificios técnicos de escucha, transmisión, grabación o reproducción de sonido e imagen, o cualquier otra señal de comunicación.

Esta nueva norma se incluye, de conformidad con lo indicado en la Ley 50/1997, de 27 de noviembre, del Gobierno (BOE núm. 285, de 28 de noviembre de 1997), en su art. 25, dentro del Plan Anual Normativo de 2018, con la finalidad, como hemos indicado, de transposición de la Directiva, mejora la eficacia de la protección jurídica de los secretos empresariales contra la apropiación indebida y como complemento de lo indicado en la Ley 3/1991, de 10 de enero, de Competencia Desleal (BOE núm. 10, de 11 de enero de 1991), (véase, Suñol, 2009), en su art. 13, que se modifica por la disposición final segunda de la Ley 1/2019, quedando con la siguiente redacción que establece:

“1. Se considera desleal la violación de secretos empresariales, que se regirá por lo dispuesto en la legislación de secretos empresariales”.

Documento, ficheros electrónicos y secreto empresarial: la Ley 1/2019, de 20 de febrero, de secretos empresariales

Se entiende por documento como establece el art. 49.1 de la Ley 16/1985, de 25 de junio, de Patrimonio Histórico Español (BOE núm. 155, de 29 de junio de 1985), “toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos”.

La doctrina indica que esta definición de documento no se aplica para la generalidad de documentos de archivo producidos por organizaciones o personas (Giménez, 2017, p. 65).

La Ley 1/2019 traspone la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas (DOUE núm. 157, de 15 de junio de 2016). La citada norma nacional contempla, en su art. 3, el documento en relación con la obtención de secretos empresariales y su violación

cuando, sin consentimiento de su titular, y de manera no autorizada, se accede, copia o apropia de documentos, objetos, materiales, sustancias, ficheros electrónicos u otros soportes que contengan el secreto empresarial o a partir de los cuales se pueda deducir el mismo.

Se indica que en el caso de violación de secretos empresariales se podrá solicitar, como precisa el art. 9, la remoción que comprenderá la entrega al demandante de todos o parte de los documentos y ficheros electrónicos, y en su caso su destrucción total o parcial.

Hay que tener en cuenta la relación entre documento y secreto empresarial, ya que los primeros pueden ser el soporte del secreto, y por ello hay que realizar una adecuada gestión de los documentos con la finalidad de garantizar un tratamiento lícito de los mismos. Esta adecuada gestión documental se traduciría en una serie de medidas: clasificación de los documentos y archivo correspondiente; determinar la forma de acceso al documento (establecimiento de claves, restricciones a determinadas personas); indicar cuáles serán los criterios para la gestión del soporte (copias de seguridad, cifrado, medidas informáticas ante posibles ataques); acuerdos de confidencialidad con cláusulas referentes a la revelación de los secretos; establecimiento de los procedimientos de transmisión de la información contenida en los documentos (físicos o electrónicos), y la utilización de correo electrónico y firma electrónica.

Respecto a la gestión de los documentos se debe tener en cuenta lo indicado en el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso (BOE núm. 284, de 25 de noviembre de 2011), por lo que se tendrá que tener en cuenta el establecimiento de repositorios de estos documentos, estableciendo los metadatos, y con la clasificación adecuada para la reutilización y el intercambio, teniendo en cuenta de adoptar las medidas adecuadas en los casos de contener un secreto empresarial. También se adoptarán las medidas adecuadas para proteger la información con el fin de asegurar su acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos.

Respecto a la información que se contiene en un documento o fichero electrónico en relación con el secreto empresarial, es contemplado por la Ley 1/2019, en su art. 15, con la adopción de una serie de medidas específicas:

- a) Los operadores jurídicos, partes y peritos que intervienen en un procedimiento que resuelva una controversia sobre violación de secreto empresarial, o bien tengan acceso a documentos obrantes en el procedimiento, no pueden hacer uso ni revelar la información constitutiva de secreto empresarial, y que los órganos judiciales (de oficio o a instancia de parte) hayan declarado confidencial y que hayan tenido conocimiento por intervenir en el procedimiento o acceder a la documentación.

La prohibición se extenderá no sólo durante el proceso, sino también después, salvo que por sentencia firme se indique que la información no es constitutiva de secreto empresarial, o bien con el paso del tiempo pase a ser de conocimiento general o fácilmente accesible en los círculos en los que se utilice.

b) Los órganos judiciales (de oficio o a instancia de parte) podrán adoptar medidas para la preservación de la confidencialidad de la información.

Estas medidas pueden ser las siguientes, no excluyéndose otras que se consideren adecuadas y proporcionadas:

1. Restricción a un número limitado de personas el acceso a los documentos o ficheros electrónicos que contengan información que pueda constituir total o parcialmente secreto empresarial.
2. Restricción a un número limitado de personas el acceso a las vistas, grabaciones o transcripciones de ellas cuando se pueda revelar información total o parcial que pueda constituir secreto empresarial.

La prestación del consentimiento y confidencialidad en relación con los secretos empresariales

Como hemos indicado, el art. 3 de la Ley 1/2019 se refiere al consentimiento y la obtención de secretos sin él como ilícita. Así como el incumplimiento del acuerdo de confidencialidad.

Respecto al consentimiento la norma no indica qué tipo de consentimiento debe prestarse para que sea lícita la obtención de secretos, si debe ser expreso o por escrito o tácito. Junto a ello, el consentimiento no deberá adolecer de ningún vicio (error, violencia, intimidación o dolo) (Ramón, 2014, p. 21). Es por ello, que debemos acudir a la normativa de protección de datos para documentar el consentimiento de un tratamiento de datos personales por parte de la persona interesada o afectada. Así, respecto a la prestación del consentimiento y la confidencialidad, debemos mencionar el Reglamento (UE) 2016/679, y la Ley Orgánica 3/2018 que se erige en complemento de la normativa comunitaria, al que se remite de forma constante, sin que, en ningún caso sustituya al citado Reglamento (UE) 2016/679, sino que lo desarrolla en los aspectos que se dejan a la interpretación discrecional de los Estados miembros.

El Reglamento (UE) 2016/679 indica que el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado. Consideramos que su aplicación en relación con los secretos empresariales excluiría un consentimiento de tipo tácito, y que debería ser prestado por escrito, ya que como dice el mencionado Reglamento (UE) 2016/679, puede ser marcar una casilla de un sitio web

en internet, utilizar parámetros técnicos para la utilización de servicios de la sociedad de la información, u cualquier otra declaración o conducta que se considere que el interesado acepta. No debe constituir consentimiento el silencio, las casillas ya marcadas o la inacción. Debe ser el consentimiento claro y conciso, y no perturbar de forma innecesaria el uso del servicio para el que se presta.

El acuerdo de confidencialidad debemos tener en cuenta que se precisará el valor de la tecnología, marcas, así como los extremos a los que se atenderá el citado acuerdo (Acea, 2016, p. 145).

Ello también lo aplicamos, desde luego, al tratamiento de datos personales en relación con los secretos empresariales por referencia a dicha legislación del art. 15 de la Ley 1/2019.

El Reglamento (UE) 2016/679 indica que se deberá de proporcionar un modelo de declaración de consentimiento elaborado de forma previa por el responsable del tratamiento con un lenguaje inteligible, accesible, claro y sencillo, sin cláusulas abusivas. Debe informarse de la identidad del responsable del tratamiento y los fines a los que se van a destinar los datos.

El art. 4 del Reglamento (UE) 2016/679 precisa que por consentimiento del interesado se entiende: “toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen”.

El art. 6 de la Ley Orgánica 3/2018, referente al tratamiento basado en el consentimiento del afectado, se remite al art. 4 del Reglamento (UE) 2016/679 referido anteriormente, y excluye, consideramos el consentimiento tácito, ya que indica que se entenderá como consentimiento “toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen”. Es por ello que el consentimiento debe proceder de una declaración o de una acción clara afirmativa del afectado, excluyendo el consentimiento tácito, que no se admite. Importante insistir en que el Reglamento (UE) 2016/679 prohíbe de forma tajante el consentimiento tácito como presupuesto para el tratamiento de datos.

También señala el art. 6 de la Ley Orgánica 3/2018, que cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para distintas finalidades, deberá constar de forma específica e inequívoca que el consentimiento se presta para todas ellas.

No se puede supeditar la ejecución contractual a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

No obstante, es preciso indicar que el consentimiento no es la única base legitimadora para poder realizar el tratamiento de datos personales. Así, el

Reglamento (UE) 2016/679, en su art. 6.4, establece que en los casos en que el tratamiento para otro fin diferente de aquel para el que se recogieron los datos no esté basado en el consentimiento, el responsable del tratamiento para poder determinar si el tratamiento con otro fin es compatible con el inicial, tendrá en cuenta las siguientes circunstancias:

- a) Cualquier relación entre los fines para los que se han recogido los datos y los fines del tratamiento posterior previsto.
- b) El contexto en que se hayan recogido los datos personales.
- c) La naturaleza de los datos personales, particularmente si son categorías especiales de datos.
- d) Las posibles consecuencias para los interesados del tratamiento ulterior.
- e) La existencia de garantías adecuadas, que podrá ser cifrar los datos o bien la seudonimización

En cuanto al deber de confidencialidad, el art. 5 de la Ley Orgánica 3/2018, precisa que se sujetarán los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase al deber de responsabilidad que establece el art. 5.1.f) del Reglamento (UE) 2016/679, que determina lo siguiente, que los mismos serán tratados “de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)”.

Derecho a la información en el caso de documentos y ficheros electrónicos que contienen secretos empresariales: análisis de la casuística

El art. 2 de la Ley 1/2019 trata de la obtención, utilización y revelación lícita de secretos empresariales. De tal forma, que la información obtenida que sea constitutiva de secreto empresarial será lícita cuando sea realizada por alguno de los medios que señala. Se indica que no proceden las acciones y medidas de la Ley 1/2019 en los casos de obtención, utilización y revelación que se haya producido en ejercicio del derecho a la libertad de expresión e información que se contempla en el art. 11 de la Carta de los Derechos Fundamentales de la Unión Europea (2016/C 202/02) (DOUE C 202/389, de 7 de junio de 2016) que comprende la libertad de opinión y la libertad de recibir o comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.

Hay que tener en cuenta que en relación con los secretos empresariales se encuentra la transmisión de conocimiento dentro de la empresa y que se conecta con la innovación y la creación (Canós, Ramón y Mauri, 2008, p. 57). Es por ello, que la transmisión de dicho activo deberá atender a estándares de seguridad y privacidad (Ramón, 2011, p. 102) en relación con los datos que se puedan contener (Canós, Ramón y Mauri, 2007, p. 3).

Otra cuestión a tener en cuenta es la distinción que se debe establecer, como ha indicado la doctrina (Martín, 2019) con lo que se refiere a las bases de datos de clientes como datos protegidos en relación con el secreto empresarial. Para ello, hay que tener en cuenta varias premisas: su consideración como secreto según lo indicado en la Ley 1/2019; que tenga valor comercial y las medidas de protección aplicables.

En el ámbito internacional la cuestión no es pacífica (Sosa, 2015, p.251). Así, podemos señalar que el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) de Perú, en la Resolución 1069-2012/SC1, de 7 de mayo de 2012, se remite a la Resolución 006-2012/SC1-INDECOPI del 12 de enero de 2012, la Sala dijo a propósito de las listas de clientes lo siguiente:

“Si bien las bases de datos poseen un valor comercial efectivo derivado de los costos de búsqueda invertidos para recabar dicha información; ello no resulta suficiente para calificarlos como secreto empresarial y, por tanto, otorgarle la protección que dispone la Ley. Así, en anteriores pronunciamientos, la Sala ha considerado que la relación o listado de clientes de una empresa puede llegar a constituir un secreto comercial o empresarial, en la medida que dicha información se encuentra directamente vinculada a la situación comercial y posición en el mercado de un competidor.
(...)

De lo anterior se desprende claramente que la relación o lista de clientes no califica por sí misma como secreto comercial, siendo que debe existir una justificación que sustente tal afirmación. (...)

Sobre el particular, de la revisión de la información obrante en el expediente se aprecia que la base de datos a la que hace referencia la denunciante se encuentra limitada a un listado de clientes y proveedores que no contiene mayor detalle (descuentos aplicados, beneficios ofrecidos, flujo de transacciones celebradas, etc.) y que es susceptible de ser conocida por cualquier tercero. En efecto, las referidas bases de datos contienen nombres de empresas y personas de contacto, lo cual se encuentra también en otras fuentes públicas de información (páginas web, guía telefónica, etc.).”

El art. 1 de la Ley 1/2019 hace alusión a medidas razonables para mantenerlo en secreto el secreto empresarial, valga la redundancia. Pero no nos indica qué medidas razonables hay que adoptar, ni cuáles se consideran como medidas razonables. El Preámbulo de la Ley 1/2019 nos indica al respecto solamente que «esta definición de secreto empresarial no abarca la información de escasa importancia, como tampoco la experiencia y las competencias adquiridas por los trabajadores durante el normal transcurso de su carrera profesional ni la información que es de conocimiento general o fácilmente accesible en los círculos en que normalmente se utilice el tipo de información en cuestión», pero no realiza una enumeración de medidas en ningún precepto de la legislación.

El derecho de acceso a la información, el secreto empresarial y el derecho a la protección de datos de carácter personal deben de ser considerados de forma que no constituya éste último un freno al primero, teniendo en cuenta el respeto a los derechos fundamentales. Es por ello, que la normativa de protección de datos que hemos indicado contempla medidas para garantizar los derechos fundamentales, y el acceso a la información contenida en los documentos que contienen secretos empresariales no puede ser ilimitada, sino precisamente limitada por la regulación de los mismos, y con el límite de los derechos de los sujetos intervinientes, principalmente el derecho a la intimidad y al honor de conformidad con lo establecido en la Ley Orgánica 17/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (BOE núm. 115, de 14 de mayo de 1982).

Si acudimos a la normativa aplicable en protección de datos de carácter personal, mencionada anteriormente, podemos entender que no se va a considerar como secreto por el simple hecho de que digamos que lo es. Es más, según la Ley 1/2019, tiene que reunir las condiciones indicadas. Es por ello, que consideramos (siguiendo a Martín, 2019) que habrá que tener en cuenta:

1. Que se tendrá que realizar una clasificación de la información; que no sea accesible, sino restringida en su acceso.
2. La gestión del soporte y transferencia de la información; la utilización de herramientas informáticas y el uso de las mismas; la protección y seguridad de la información, proveedores y acceso por lo que habrá que tenerse en cuenta lo indicado en la Decisión del Consejo, de 31 de marzo de 1992, relativa a la seguridad de los sistemas de información (DOCE núm. 123, de 8 de mayo de 1992), Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (BOE núm. 218, de 8 de septiembre de 2018), que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DOCE L194/1, de 19 de julio de 2016).

No hay que olvidar que el art. 1 del Real Decreto-ley 12/2018 excluye de su ámbito de aplicación a:

- a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril.
 - b) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas».
3. Los acuerdos de confidencialidad que se hayan adoptado. Aquí es importante indicar siguiendo a Oliva (2019), que se indique en el mismo que la información, datos, objetivos de futuro, no se hagan públicos. Dicha obligación de confidencialidad resulta esencial en cualquier transferencia de conocimiento que se vaya a realizar. Habrá que atender también a los límites de las cláusulas contractuales para determinar la naturaleza jurídica de la información que se contiene a efectos de protección de los secretos empresariales (Remolina y Tafur, 2017, p. 145).
4. Política referente a las copias de seguridad, transmisión de información, controles y auditorias.
5. Las indicaciones sobre ello contenidas en los esquemas de seguridad de la información. Así, habrá de tenerse en cuenta las siguientes normas, en el caso de que sean aplicables teniendo en cuenta las características de la información, y de conformidad con lo indicado en la Guía de Seguridad de las TIC CCN-STIC 821. Esquema Nacional de Seguridad. Normas de Seguridad (2018):
- a) Ley 40/2015, de 1 de octubre, de Régimen jurídico del Sector Público (BOE núm. 236, de 2 de octubre de 2015).
 - b) Reglamento (UE) 2015/703 de la Comisión, de 30 de abril de 2015, por el que se establece un código de red sobre las normas de interoperabilidad y de intercambio de datos (Texto pertinente a efectos del EEE) (DOUE núm. 113, de 1 de mayo de 2015).
 - c) Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 de septiembre de 2015, sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) n° 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (DOUE núm. 235, de 9 de septiembre de 2015).

- d) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (BOE núm. 25, de 29 de enero de 2010), modificado por Real Decreto 951/2015, de 23 de octubre (BOE núm. 264, de 4 de noviembre de 2015).
- e) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (BOE núm. 25, de 29 de enero de 2010).
- f) Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (BOE núm. 150, de 23 de junio de 2007), que ha sido desarrollada parcialmente por Real Decreto 1671/2009, de 6 de noviembre (BOE núm. 278, de 18 de noviembre de 2009), y modificado éste por Real Decreto 668/2015, de 17 de julio (BOE núm. 171, de 18 de julio de 2015).

Respecto a las bases de datos de clientes y los requisitos que se deben de cumplir para que su cesión sea lícita, debemos remitirnos a la normativa de protección de casos, que, como ya hemos indicado se encuentra en el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018.

El art. 8 de la Ley Orgánica 3/2018 contempla el tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos, que sólo se podrá considerar fundado en el cumplimiento de una obligación legal exigible al responsable, remitiéndose a lo indicado en el art. 6. 1. c) del Reglamento (UE) 2016/679, en los casos que lo prevea una norma del Derecho de la UE o una norma que tenga rango de ley, que podrá determinar las condiciones del tratamiento y los tipos de datos, así como las cesiones que puedan realizarse en cumplimiento de la norma legal. Se podrán imponer medidas adicionales de seguridad, de conformidad con el capítulo IV del Reglamento (UE) 2016/679. Un ejemplo de ello, son las bases de datos reguladas por ley y gestionadas por autoridades públicas para control y solvencia.

El tratamiento de los datos, según lo que dispone el Reglamento (UE) 2016/679, en su art. 6.1, sólo será lícito si se cumple alguna de las siguientes condiciones:

- a) Que el interesado preste su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.
- b) Que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado sea parte o bien para la aplicación de medidas precontractuales.
- c) El tratamiento sea preciso para cumplir una obligación legal aplicable al responsable de aquél.

- d) El tratamiento sea necesario para proteger intereses vitales del interesado o de un tercero.
- e) El tratamiento se requiera para cumplir una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del mismo.
- f) Se precise el tratamiento para satisfacer intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre los intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que precisan la protección de los datos.

Ponderación entre la legislación en materia de secretos empresariales y la nueva regulación de los derechos digitales

El Título X de la Ley Orgánica 3/2018, en los arts. 79 a 97, regula los denominados derechos digitales y sus garantías, en sintonía con lo indicado en el art. 18.4 de la Constitución Española. Se contiene derechos del entorno digital, en la era internet, como es el caso de la neutralidad en la Red, y el acceso universal a la misma, y también derechos a la seguridad y educación digital, así como el derecho al olvido, a la portabilidad y al testamento digital, y la protección de los menores en internet. Sin embargo, en el ámbito de la empresa y los secretos empresariales nos interesa destacar, aunque sea brevemente, el derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral, así como la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digital.

En el ámbito empresarial, se plantea algún problema en relación con los secretos empresariales y la utilización de dispositivos electrónicos, respecto a su control por parte de la empresa. Se trataría de determinar si la monitorización por parte de la empresa de los dispositivos electrónicos puede interferir con los derechos digitales del trabajador, en concreto, con su intimidad y privacidad (Brands, 2019; Ramón, 2019).

Así, el art. 88 de la Ley Orgánica 3/2018 debe entenderse en sintonía con el artículo 20 bis del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (BOE núm. 255, de 24 de octubre de 2015), introducido por la Ley Orgánica 3/2018, que regula el derecho de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión. De tal forma, que tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, así como a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización según la normativa de protección de datos personales y garantía de los derechos digitales.

La recopilación de datos debe atender a su necesidad, es decir, que sean imprescindibles, y no la utilización de datos masivos. Se deben conocer qué datos se van a tratar, así como la finalidad de los mismos, y la proporcionalidad en su recopilación (Brands, 2019).

Bien, todo ello aplicado a los secretos empresariales se discute cómo establecer su protección en un mundo hiperdigitalizado, en el que el secreto empresarial va mucho más allá de la presencia física en una empresa, ya que puede estar en riesgo al implicarse los dispositivos electrónicos. Se trata de ver cómo evitar y prevenir una fuga de información. Se deben establecer medidas de precaución o cautelares que no vayan en contra de los derechos digitales contemplados en la Ley Orgánica 3/2018, es decir, que permitan el derecho a la desconexión digital, así como el derecho a la intimidad del trabajador.

Esta protección puede realizarse a través de distintas medidas, como por ejemplo de tipo tecnológico, en el que podría implantarse la denominada “cadena de bloques” o blockchain, o bien también de tipo contractual, estableciendo cláusulas para el trabajador y su acceso a los secretos empresariales, como los acuerdos de confidencialidad.

Este argumento lo podemos sostener interpretando el art.3 de la Ley 1/2019, referente a la violación de secretos empresariales, al referirse al incumplimiento de los acuerdos de confidencialidad o el incumplimiento de las obligaciones contractuales.

Conclusiones

La regulación de los secretos empresariales plantea distintos problemas en relación con los documentos y ficheros electrónicos que pueden contener dicha información. No podemos obviar la íntima relación que tiene dicha información protegida con la normativa actual de protección de datos personales, así como con los acuerdos de confidencialidad respecto al tratamiento de los secretos empresariales y los sujetos en las relaciones contractuales.

La legislación principal, la Ley 1/2019, adolece de algunas carencias que hubiera sido deseable que se hubieran indicando, como, por ejemplo, la falta de precisión de las medidas razonables para el mantenimiento del secreto. Ello en el caso de los documentos y ficheros electrónicos plantea problemas de determinación y operabilidad.

La Ley 1/2019 se remite a la normativa de protección de datos de carácter personal que se regula por el Reglamento (UE) 2016/679 y por la Ley Orgánica 3/2018, siendo ésta última una norma que se remite de forma constante al Reglamento (UE) 2016/679, y que no lo sustituye, sino que lo complementa y desarrolla.

La información referente al secreto empresarial puede estar en un soporte físico o electrónico, y la gestión del documento es de especial relevancia, no sólo para la conservación del mismo, sino también para evitar filtraciones de la información. Es por ello que se deben articular medidas adecuadas de gestión, como la utilización de cifrados y el acceso al correo electrónico por parte de los sujetos titulares del secreto empresarial.

La normativa de protección de datos personales, tanto el Reglamento (UE) 2016/679, como la Ley Orgánica 3/2018, contiene una serie de requisitos para el tratamiento de los datos y su transferencia a terceros, siendo especialmente relevante la necesidad de un consentimiento expreso, no admitiéndose el consentimiento de forma tácita.

Es preciso establecer una ponderación entre la normativa de secretos empresariales y la regulación de los derechos digitales de la Ley Orgánica 3/2018, en el caso de la desconexión digital y también en la utilización de dispositivos electrónicos que contengan secretos empresariales por parte del trabajador y sujetos al control del empresario, para evitar una invasión en el derecho a la intimidad del primero. Se deben articular medidas de control no invasivas, así como fomentar las cláusulas de confianza o la cadenas de bloques, o blockchain.

Bibliografía

- ACEA VALDÉS, Yeney (2016). “La transferencia de tecnología en Cuba”. *Dereito: Revista xuridica da Universidade de Santiago de Compostela*, vol. 25, n. 2, p. 139-149. <<http://www.usc.es/revistas/index.php/dereito/article/view/3474/4122>>. [Consulta: 01/03/2019].
- BRANDS, E.C. (2019). “Control vs privacidad: ¿qué pueden hacer las empresas con los datos de sus empleados?”. *El Confidencial*. <https://www.elconfidencial.com/empresas/2019-06-03/empresas-empleados-datos-secreto-empresarial-bra_1973894/>. [Consulta: 05/10/2019].
- CANÓS DARÓS, Lourdes, RAMÓN FERNÁNDEZ, Francisca y MAURI CASTELLÓ, Jordi (2007). “La protección de datos personales y la información para la gestión del conocimiento en las empresas”. *Revista General Informática de Derecho*, p. 1-13.
- (2008). “Aspectos jurídicos y económicos de la propiedad industrial de la empresa”. *Novática*, n. 193, p. 56-58.
- CONSEJO GENERAL DEL PODER JUDICIAL (2018). *Informe sobre el Anteproyecto de Ley de Secretos Empresariales*. <http://www.poderjudicial.es/portal/site/cgpj/menuitem.65d2c4456b6ddb628e635fc1dc432ea0/?vgnextoid=d32caea63c162610VgnVCM1000006f48ac0aRCRD&vgnnextchannel=a64e3da6cbe0a210VgnVCM100000cb34e20aRCRD&vgnnextfmt=default&vgnnextlocale=es_ES>. [Consulta: 31/03/2019].
- DOMINGO MONFORTE, José (2018). “El secreto empresarial. Revelación. Tipicidad penal”. *Diario La Ley*, n. 9144.

- FERNÁNDEZ CARBALLO-CALERO, Pablo (2013). “La configuración del listado de clientes como un secreto empresarial en el derecho contra la competencia desleal”. En: Tobío Rivas, Ana María (coord.), Fernández Albor Baltar, Ángel, Tato Plaza, Anxo (ed.), *Estudios de derecho mercantil: Libro homenaje al Prof. Dr. h. c. José Antonio Gómez Segade*. Madrid: Marcial Pons, p. 411-436.
- FERNÁNDEZ DE CÓRDOVA, Álvaro (2019). “Ley 1/2019, de 20 de febrero, de Secretos Empresariales: aproximación a los elementos sustantivos de esa «nueva» propiedad intelectual”. *Economist & Jurist*, n. 228, p. 16-27.
- FERNÁNDEZ DÍAZ, Carmen Rocío (2016). “La lista de clientes como objeto del secreto empresarial”. *Revista Aranzadi Doctrinal*, n. 7, p. 251-274.
- FÉLIX PARRONDO, Esther DE y DÍAZ BAÑOS, Manuel (2018). “El Anteproyecto de Ley de Secretos Empresariales, a debate”. *Diario La Ley*, n. 9201.
- FERNÁNDEZ DÍAZ, Carmen Rocío (2017). *La violación de secretos empresariales por persona ajena a la empresa: un estudio del artículo 278 del código penal*, García Pérez, Octavio y Díez Ripollés, José Luis (dir.). Málaga: Universidad de Málaga.
- FLORES SÁNCHEZ, José Alejandro (2017). “La protección de los derechos de propiedad industrial en el ámbito empresarial. ¿proteger o no proteger?. *Olimpia: Publicación científica de la facultad de cultura física de la Universidad de Granma*, vol. 14, n. 14, p. 55-68.
- GIMÉNEZ-CHORNET, Vicent (2017). *Legislación de archivos*. Barcelona: UOC.
- Guía de Seguridad de las TIC CCN-STIC 821. Esquema Nacional de Seguridad. Normas de Seguridad* (2018). <<https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/529-ccn-stic-821-normas-de-seguridad-en-el-ens/file.html>>. [Consulta: 31/03/2019].
- LISSEN ARBEOLA, José Miguel y GUILLÉN MONJE, Patricia (2019). “Características, alcance de la protección conferida e implicaciones para las empresas en la nueva Ley de Secretos Empresariales”. *Diario La Ley*, n. 9363.
- MARTÍN, Paz (2019). “La nueva ley de secretos empresariales y la protección de datos ¿algo en común?”. *Blog Legal Things Abogados*, 21 de febrero. <<https://legalthings.es/la-nueva-ley-de-secretos-empresariales-y-la-proteccion-de-datos-algo-en-comun/>>. [Consulta: 31/03/2019].
- MASSAGUER FUENTES, José (2018a). “El Anteproyecto de Ley sobre Protección de los Secretos Empresariales”. *Actualidad jurídica Aranzadi*, n. 941, p. 7.
- (2018b). “El incumplimiento de los contratos de licencia de patente y de licencia de secretos empresariales: concurrencia entre acciones contractuales y acciones por infracción”. *Revista de Derecho mercantil*, n. 309, p. 3.
- OLIVA LEÓN, Ricardo (2019). “Acuerdo de confidencialidad y protección de secretos empresariales”. *Blog Algoritmo Legal*, 3 de febrero. <<https://www.algoritmolegal.com/propiedad-intelectual/acuerdo-de-confidencialidad-y-proteccion-de-secretos-empresariales/>>. [Consulta: 31/03/2019].
- RABASA MARTÍNEZ, Ignacio (2018). “El anteproyecto de Ley de Secretos Empresariales y la Directiva 2016/943 relativa a los conocimientos técnicos e información empresarial no divulgados”. *La Ley mercantil*, n. 47, p. 5.
- RAMÓN FERNÁNDEZ, Francisca (2011). “Transmisión del conocimiento en la empresa y la influencia de las redes sociales y TICs”. *Revista da micro e pequena empresa*,

- v. 5, n. 3, p. 99-113. <<http://revistas.uexternado.edu.co/index.php/propin/article/view/4347/4931>>. [Consulta: 02/02/2019].
- (2015). “La ingeniería y la propiedad industrial en el ámbito universitario: marco legal y algunas dudas habituales”. *Revista La Propiedad Inmaterial*, n. 20, p. 39-56. <<http://www.cc.faccamp.br/ojs-2.4.8-2/index.php/RMPE/article/view/232/174>>. [Consulta: 03/02/2019].
- (2014). “La mediación electrónica, la confidencialidad y la protección de datos de carácter personal”. *InDret. Revista para el análisis del Derecho*, n. 3, p. 1-28. <http://www.indret.com/pdf/1069_es.pdf>. [Consulta: 05/02/2019].
- (2019). “La normativa de protección de datos y derechos digitales en el ámbito de los recursos humanos: un reto para la sociedad y la legislación”. En: *¿Se puede crear capital social? Innovación y tecnología: retos para los recursos humanos de las organizaciones*. Valencia: Tirant lo Blanch, p. 203-227.
- REMOLINA ANGARITA, Nelson y TAFUR NÁDER, Gabriela (2017). “Limitaciones de las cláusulas contractuales para determinar la naturaleza jurídica de la información y para proteger los secretos empresariales”. *Revista La Propiedad Inmaterial*, n. 24, p. 145-165. <<https://revistas.uexternado.edu.co/index.php/propin/article/view/5201/6268>>. [Consulta: 01/03/2019].
- SAINZ DE AJA TIRAPU, Borja y PEINADO IRIBAR, Estíbaliz (2018). “Secretos empresariales. Cuestiones relevantes de la Directiva y del Proyecto de Ley”. *Comunicaciones en propiedad industrial y derecho de la competencia*, n. 84, p. 31-45.
- SALDARRIAGA, José Ignacio (2018). “La protección del secreto empresarial a la luz de la nueva regulación”. *Actualidad jurídica Aranzadi*, n. 945, p. 9.
- SOSA HUAPAYA, Alex (2015). “Competencia desleal y resguardo de los secretos empresariales”. *THEMIS: Revista de Derecho*, n. 68, p. 245-259. <<http://revistas.pucp.edu.pe/index.php/themis/article/view/15597/16046>>. [Consulta: 25/02/2019].
- SUÑOL LUCEA, Aurea (2009). *La protección jurídica del secreto empresarial en el artículo 13 de la Ley de competencia desleal*. Madrid: Civitas.
- TRUJILLO PONS, Francisco (2014). “Revelación de secretos empresariales a terceros por medio del correo electrónico. Posición del Tribunal Constitucional ante una supuesta vulneración a los derechos a la intimidad y al secreto de comunicaciones. Sentencia del Tribunal Constitucional 170/2013, de 7 de octubre de 2013”. *Revista General de Derecho del Trabajo y de la Seguridad Social*, n. 36, p. 292-320.

Notas

¹ Agradecimientos: Trabajo realizado en el marco del Proyecto I+D+i «Retos investigación» del Programa estatal de I+D+i orientado a los Retos de la Sociedad del Ministerio de Ciencia, Innovación y Universidades: RTI2018-097354-B-I00.

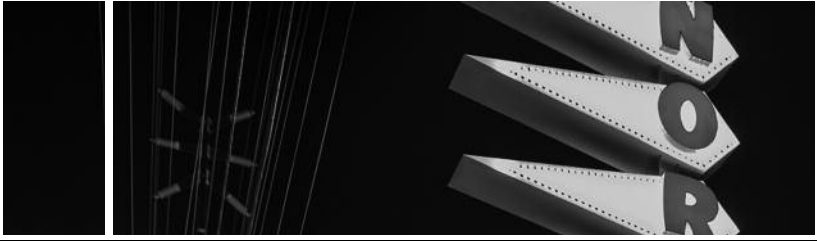


Scotland's
Secret Bunker



**SECURITY
CAMERAS
IN USE**

© 2008



JOSÉ LUIS DOMÍNGUEZ ÁLVAREZ

Interoperabilidad administrativa y protección de datos personales: claves para garantizar el derecho a una buena Administración

Administrative
interoperability and personal
data protection:
keys to guarantee the right
to good Administration

José Luis Domínguez Álvarez¹
jldoa@usal.es
Universidad de Salamanca

*Citación: Domínguez Álvarez, José Luis (2019). "Interoperabilidad administrativa y protección de datos personales: claves para garantizar el derecho a una buena administración". *Tábula*, n. 22, pp. 95-112*

Recibido: 23-9-2019. Aceptado: 13-11-2019

Resumen analítico / Analytic summary

El estudio sistemático de la implementación de la administración electrónica lleva aparejado de forma inherente el análisis exhaustivo de una serie de elementos imprescindibles para conseguir potenciar, de forma efectiva, la digitalización de las estructuras y procedimientos administrativos. En este sentido, la interoperabilidad administrativa se plantea como uno de los principales retos de la gestión administrativa del siglo XXI, en tanto en cuanto constituye el motor de la administración electrónica y una herramienta esencial para reducir el flujo de datos personales de la ciudadanía en manos de las Administraciones públicas, presupuesto indispensable no sólo para el cumplimiento escrupuloso de la nueva regulación en materia de datos personales, sino también para el despliegue de la administración automatizada, presidida por el empoderamiento de los algoritmos y el crecimiento exponencial del tratamiento de datos de carácter personal.

INTEROPERABILIDAD ADMINISTRATIVA | PROTECCIÓN DE DATOS PERSONALES | BUENA ADMINISTRACIÓN | SEGURIDAD | DIGITALIZACIÓN

The systematic study of the implementation of electronic administration inherently entails the exhaustive analysis of a series of essential elements to effectively enhance the digitalization of administrative structures and procedures. In this sense, administrative interoperability is considered as one of the main challenges of the administrative management of the 21st century, insofar as it constitutes the engine of electronic administration and an essential tool to reduce the flow of personal data of citizenship in the hands of the Public Administrations, indispensable budget not only for scrupulous compliance with the new regulation on personal data, but also for the deployment of automated administration, chaired by the empowerment of algorithms and the exponential growth of the treatment of Personal data.

ADMINISTRATIVE INTEROPERABILITY | PERSONAL DATA PROTECTION | GOOD ADMINISTRATION | SECURITY | DIGITALIZATION

La proclamación

de la Carta de los Derechos Fundamentales de la Unión Europea, y con ello del derecho a la buena administración, pretendía traer consigo una transformación sin precedentes tanto de las categorías tradicionales del Derecho administrativo como de la propia concepción de las Administraciones públicas. La novedosa regulación en materia de protección de datos de carácter personal, fruto de la preocupación del legislador europeo por limitar los efectos perniciosos que el proceso de digitalización y datificación de la sociedad puede representar para la dignidad y libertad de la ciudadanía, exige hoy realizar una nueva lectura de ese derecho a la buena administración a la luz de estos profundos cambios normativos.

En este sentido, se hace necesario que las Administraciones públicas redoblen los esfuerzos destinados a maximizar los estándares de seguridad de la información que obra en su poder, y especialmente en aquellos casos en los que dicha información pública contenga datos personales, ya que la protección de datos de carácter personal debe constituir, sin lugar a dudas, uno de los presupuestos indispensables para alcanzar el derecho a la buena administración.

Sin embargo, esta tarea de maximización de los estándares de protección de los datos personales, lejos de presentarse como un quehacer sencillo, puede convertirse en un auténtico quebradero de cabeza para buena parte de las Administraciones públicas españolas. En las siguientes líneas, se pretende hacer una pequeña incursión en las estribaciones de esta difícil problemática, planteando algunas respuestas que pueden contribuir a mejorar la seguridad de la información, el correcto tratamiento de los datos personales y la eficacia administrativa, soluciones entre las que destaca por su extraordinaria importancia, el impulso decidido de la interoperabilidad administrativa.

Una revisión del derecho a la buena administración a la luz de la nueva regulación en materia de protección de datos de carácter personal

El 7 de diciembre del año 2000 tiene lugar la proclamación de la Carta de los Derechos Fundamentales de la Unión Europea, Carta que está llamada a ser la positivación de los principios generales del derecho comunitario (RODRÍGUEZ DÍAZ, 2001).

Proclamada en el Consejo Europeo de Niza, la Carta es un texto atípico (MARTÍN-RETORTILLO BAQUER, 2008) al que el Tratado de Lisboa otorga el mismo valor jurídico que los Tratados. Dicho texto consta de un Preámbulo y 54 artículos comprendidos en siete Capítulos estructurados en siete grandes rúbricas: Dignidad, Capítulo I –artículos 1 a 5–; Libertades, Capítulo II –artículos 6 a 19–; Igualdad, Capítulo III –artículos 20 a 26–; Solidaridad, Capítulo IV –artículos 27 a 38–; Ciudadanía, Capítulo V –artículos 39 a 46–; Justicia, Capítulo VI –artículos 47 a 50–; y Disposiciones generales, Capítulo VII –artículos 51a 54–, referidas al ámbito de aplicación de la Carta, el alcance de los derechos reconocidos, el nivel de protección y la prohibición del abuso de derecho (CARRILLO SALCEDO, 2001).

Aproximándonos al objeto de nuestro estudio, la Carta de Niza supuso la positivación de un novedoso derecho, el derecho a la buena administración –artículo 41–, cuya importancia estriba en que supone de facto un replanteamiento del derecho administrativo en su conjunto. En este sentido, algunos teóricos señalan que el derecho a la buena administración viene a exigir una nueva formulación del Derecho administrativo y sus principales categorías, al objeto de convertir a la ciudadanía –y la participación activa de ésta– en el centro gravitacional de la nueva concepción del sistema del Derecho administrativo (RODRÍGUEZ-ARANA, 2013).

En efecto, tal y como señala el profesor RODRIGUEZ-ARANA, la buena administración –también conocido como el buen gobierno–, aspira a colocar en el centro del sistema a la persona y sus derechos fundamentales (RODRÍGUEZ-ARANA, 2006). Otros teóricos señalan en cambio que el principio de buena administración responde a las concepciones más recientes del Derecho administrativo, caracterizadas por el intento de superar la visión estrictamente formal que legitima la Administración para el mero cumplimiento neutral y objetivo de la norma que le otorga las potestades de actuación y, por otro lado, por la voluntad de situar al ciudadano en el centro de la preocupación de las normas que ordenan la actividad administrativa (SANZ LARRUGA, 2009).

A grandes rasgos, cuando nos referimos a la buena administración, estamos haciendo alusión a aquella que cumple con las funciones que le son otorgadas en

democracia. Es decir, una Administración pública que sirve objetivamente a la ciudadanía, que realiza su trabajo con racionalidad, justificando sus actuaciones y que se orienta continuamente al interés general. Un interés general que en el Estado social y democrático de Derecho no puede concebirse de otra forma que no sea la mejora permanente e integral de las condiciones de vida de las personas (RODRÍGUEZ-ARANA, 2013).

Pero más allá del espíritu inherente de este artículo 41 de la Carta de Niza, el cual estaba concebido con la finalidad de provocar una verdadera catarsis en el seno del Derecho administrativo europeo, el mismo posee una serie de implicaciones en la cuestión que nos ocupa, la mejora de la protección de datos de carácter personal, con la finalidad de mejorar la seguridad de la información en poder de las Administraciones públicas. Y es que, de conformidad con lo establecido en el artículo 21 del Código Europeo de Buena Conducta Administrativa de la Unión Europea –redactado por el Defensor del Pueblo Europeo y aprobado por Resolución del Parlamento Europeo de 6 de septiembre de 2001– se establece el principio del respeto a la vida privada y a la integridad de las personas, es decir a la protección de los datos personales, como corolario del derecho a la buena administración. De esta forma, se establece lo siguiente: «el funcionario que maneje datos personales referentes a un ciudadano respetará la vida privada y la integridad de la persona, de conformidad con las disposiciones del Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos».

Todo ello nos conduce a señalar la relación de causalidad y proximidad existente entre el derecho a una buena administración y el derecho a la protección de datos de carácter personal. Ciertamente, en nuestra opinión ambos derechos forman parte de un todo indisoluble –que no es otro que satisfacer los intereses generales y mejorar las condiciones de vida de la ciudadanía–, pues parece lógico que para que se cumpla la premisa de disponer de una buena administración es necesario que esta respete escrupulosamente las exigencias establecidas por la nueva regulación en materia de protección de datos, ya que en caso contrario no sólo se estará entrando en contradicción con el contenido del artículo 41 de la Carta de Niza, sino también vulnerando el derecho al honor y la intimidad personal de la ciudadanía.

Nueva regulación en materia de protección de datos de carácter personal: ¿una respuesta a la digitalización de la sociedad?

El derecho a la protección de datos personales constituye una de las grandes aportaciones de la Unión Europea a la esfera internacional en las últimas décadas y una prueba palpable del liderazgo que ha demostrado nuestro continente en la promoción de los valores de paz y tolerancia en defensa de las libertades y derechos fundamentales del individuo (TERRÓN SANTOS & DOMÍNGUEZ ÁLVAREZ, 2019).

En efecto, la protección de la vida privada ha visto transcurrir un periodo de casi tres cuartos de siglo desde su primera formulación teórica por WARREN y BRANDEIS hasta su reconocimiento jurisdiccional en Estados Unidos o su aparición en nuestro ordenamiento jurídico con la promulgación de la Constitución española de 1978. Pese a todo ello, el derecho a la protección de datos se ha asentado en nuestro ordenamiento con una rapidez inusitada teniendo en cuenta sus especiales características morfológicas y la técnica jurisprudencial que ha determinado su nacimiento (MARTÍNEZ MARTÍNEZ, 2007).

Ciertamente, el derecho a la protección de datos personales tiene un largo e intenso recorrido durante la segunda mitad del siglo XIX y la primera década del siglo XXI (ÁLVAREZ HERNANDO, 2018). Si se efectúa una primera aproximación a su evolución histórica, encontramos una serie de antecedentes que destacan con extraordinaria claridad. El primero de esos antecedentes lo encontramos en el artículo 12 de la Declaración Universal de los Derechos Humanos, adoptada y proclamada por la Asamblea General en su resolución 217 A (III), de 10 de diciembre de 1948:

«Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».

Inmediatamente después, el 4 de noviembre de 1950, tuvo lugar la aprobación del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales², más conocido como la Convención Europea de Derechos Humanos (CEDH), instrumento que tenía como finalidad prioritaria reafirmar la profunda adhesión del Consejo de Europa «a las libertades fundamentales que constituyen las bases mismas de la justicia y de la paz en el mundo, y cuyo mantenimiento reposa esencialmente, de una parte, en un régimen político verdaderamente democrático, y, de otra, en una concepción y un respeto comunes de los derechos humanos de los cuales dependen», también hizo mención

expresa en su artículo octavo al Derecho al respeto a la vida privada y familiar, en los términos que a continuación se expresan:

«Artículo 8. Derecho al respeto a la vida privada y familiar»

1. *Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*
2. *No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria.*

Esta inquietud de las organizaciones supranacionales por el respeto a los derechos de la personalidad, así como por las disfunciones sociales que los nuevos medios tecnológicos pueden producir, tuvo su plasmación por vez primera en el Convenio n° 108 del Consejo de Europa (REBOLLO DELGADO, 2018). Dicha norma constituye no sólo el primer instrumento internacional jurídicamente vinculante en materia de protección de datos, sino también, el punto de partida para afrontar los retos de la automatización desde el reconocimiento de un derecho a la protección de datos, derecho que vino a ser reforzado con posterioridad por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre en 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Sin embargo, la vertiginosa evolución tecnológica y la globalización han planteado la necesidad de acometer importantes cambios normativos, una modernización sin precedentes en aras de ofrecer un enfoque global que garantice el pleno respeto no solo del derecho fundamental a la protección de datos personales sino, también, de la dignidad humana ante los riesgos y amenazas de la realidad digital (PÉREZ LUÑO, 2012).

En este sentido, el Diario Oficial de la Unión Europea, publicaba el 4 de mayo de 2016 el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante RGPD). En esencia, la reforma pretende devolver a los ciudadanos el control de sus datos personales y garantizar en todo el territorio de la Unión Europea unos elevados estándares de protección, adaptados al entorno digital (DAVARA RODRÍGUEZ, 2016). Esta idea-fuerza, presente en todo el texto del RGPD, se establece con meridiana claridad desde sus primeros considerandos –especialmente en el considerando cuarto–:

«El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y

mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística».

En líneas generales, podemos decir, que el RGPD nace con vocación de erigirse como el instrumento normativo encargado de dar respuesta y solución al tsunami tecnológico en el que se sumerge la sociedad actual (RALLO LOMBARTE & GARCÍA MAHAMUT, 2015). En este sentido, su finalidad no es otra que la de garantizar un nivel uniforme y elevado de protección de las personas físicas, al tiempo que pretende eliminar los obstáculos a la libre circulación de datos personales dentro de la Unión Europea, apostando de forma decidida por el establecimiento de elevados y equivalentes niveles de protección de los derechos y libertades de las personas físicas –en lo que se refiere al tratamiento de dichos datos– en todos los Estados miembros.

En otras palabras, la nueva regulación trata de dar respuesta a la profunda evolución que el derecho a la libertad informática ha experimentado en el continente europeo, lo que ha propiciado el paso de considerar el *habeas data* como un instituto de protección de otros derechos, principalmente la intimidad, a entenderlo como un derecho autónomo e independiente con su propia configuración y lógica interna (FERNÁNDEZ VILLAZÓN, 2016).

Algo similar ocurre con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD), la cual, sin lugar a dudas, constituye un ejemplo palmario de la transformación provocada por la tecnología en la sociedad contemporánea (RALLO LOMBARTE, 2019). Si el derecho a la protección de datos personales sirvió durante las últimas décadas para preservar los derechos individuales frente a buena parte de los efectos generados por las tecnologías de la información y del conocimiento, la sociedad digital en la que nos hallamos completamente inmersos demanda un haz de derechos que se extienda a la práctica totalidad de los ámbitos en que el individuo se desarrolla en sociedad (RALLO LOMBARTE, 2017).

Y es que, de conformidad con lo establecido en el artículo primero de la norma objeto de estudio, observamos que el legislador español confiere un doble objetivo a la LOPDGDD: en primer lugar, adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta

al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones, y en segundo lugar garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

En definitiva, cuando hablamos del RGPD y la LOPDGDD, nos referimos a nuevos instrumentos normativos diseñados con la finalidad de hacer frente a nuevas y vertiginosas realidades, entre las que destacan especialmente la digitalización y la datificación de la sociedad en su conjunto, lo que exige articular nuevas respuestas jurídicas para salvaguardar la integridad y el ejercicio efectivo de los derechos fundamentales de la ciudadanía. El derecho a la protección de datos de carácter personal se presenta, por tanto, como el presupuesto indispensable para garantizar la dignidad humana ante los riesgos y amenazas de la realidad digital, lo que requiere no sólo el compromiso y el cumplimiento de las exigencias normativas en materia de protección de datos por parte de todos los actores –públicos y privados–, sino también la adopción de las medidas pertinentes y necesarias para garantizar en todo momento la minimización de los riesgos en la seguridad de la información, proceso que deberían abanderar de forma diligente las diferentes Administraciones públicas, y para lo cual urge, de una vez por todas, desplegar todo un haz de actuaciones y de herramientas que contribuyan de forma efectiva a lograr la tan ansiada interoperabilidad administrativa, mecanismo idóneo para reducir la proliferación excesiva de datos personales, datos que se presentan como principal activo para las diferentes unidades administrativas en los albores del nuevo paradigma de la Administración pública: la administración automatizada.

Interoperabilidad administrativa como mecanismo idóneo para reducir la proliferación de datos personales

Cuando nos referimos a los principales frenos o resistencias que presentan las Administraciones públicas a la hora de afrontar el proceso de digitalización de la acción administrativa, necesariamente debemos hacer alusión a la falta de confianza imperante entre las diferentes Administraciones públicas, algo extremadamente preocupante en un contexto de patente evolución y ampliación de los procedimientos administrativos desarrollados por medios electrónicos.

1. El impulso del principio «once only»

La cooperación entre las Administraciones públicas es esencial para proporcionar los servicios a los ciudadanos y garantizarles su derecho a relacionarse con ellas por medios electrónicos. Dicha cooperación requiere unas condiciones tales

que permitan que la misma se pueda llevar a cabo con fluidez para lo cual es necesario que haya interoperabilidad (TERRÓN SANTOS & DOMÍNGUEZ ÁLVAREZ, 2019).

La interoperabilidad³ se presenta, por tanto, como el desafío más importante que se plantea a la gestión administrativa en la primera mitad del siglo XXI. Hace posible que los datos situados en un punto de un sistema (por ejemplo, los que contenga un expediente administrativo electrónico confiado a un concreto órgano administrativo) puedan ser utilizados de manera electrónica por el conjunto de dicho sistema (es decir, por todos los órganos de una misma Administración) y cruzarse asimismo por medios electrónicos para su uso por los interesados y por otras entidades públicas y privadas (GAMERO CASADO, 2009).

En efecto, una vez superada la fase inicial de concienciación acerca de la necesidad de implantar la administración electrónica y sus beneficios, el problema principal para hacer realidad la gestión electrónica es la interoperabilidad; de ahí que sostenga CERRILLO MARTÍNEZ que la interoperabilidad es el motor de la administración electrónica (CERRILLO MARTÍNEZ, 2008).

La interoperabilidad se convierte así en la piedra angular para el impulso de la administración electrónica integral, fruto de esta importancia, el Real Decreto 4/2010, de 8 de enero, establece el Esquema Nacional de Interoperabilidad (en adelante ENI), entendido éste como el conjunto de criterios y recomendaciones en materia de seguridad, normalización y conservación de la información, que deberán ser tenidos en cuenta por las Administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad⁴.

Ahora bien, conviene señalar que el ENI se puso en marcha a la luz del estado del arte y tomando como principal referencia las actuaciones puestas en marcha previamente en los países de nuestro entorno más próximo⁵. De esta forma, el ENI se encuentra alineado con la Estrategia Europea de Interoperabilidad⁶ y el Marco Europeo de Interoperabilidad, lo que permite que tanto el ENI, como sus normas técnicas de interoperabilidad, contemplan de manera sistemática el enlace con instrumentos equivalentes del ámbito europeo.

Entre los principales objetivos perseguidos por el Esquema Nacional de Interoperabilidad podemos destacar los siguientes:

- Comprender los criterios y recomendaciones que deberán ser tenidos en cuenta por las Administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunde en beneficio de la eficacia y la eficiencia, evitando la discriminación a los ciudadanos por razón de su elección tecnológica.

- Introducir los elementos comunes que han de guiar la actuación de las Administraciones públicas en materia de interoperabilidad.
- Aportar un lenguaje común para facilitar la interacción de las Administraciones públicas, así como la comunicación de los requisitos de interoperabilidad a la industria.

No debemos olvidar que la interoperabilidad se concibe desde una perspectiva integral, de manera que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas, pero deficientemente ensambladas. Por ello, apostar por la mejora paulatina de la interoperabilidad administrativa es esencial desde el punto de vista de los procesos de impulso y desarrollo de la administración electrónica, ya que no solamente es imprescindible para la correcta extensión del proyecto de digitalización de la acción administrativa, sino también desde la perspectiva de la protección de datos. La interoperabilidad es el motor de la administración electrónica y el vehículo adecuado para reducir la proliferación de datos de carácter personal en un contexto dominado por el tratamiento masivo de datos a través de internet (TERRÓN SANTOS & DOMÍNGUEZ ÁLVAREZ, 2019).

Justamente, la Administración electrónica, en esencia, conlleva de forma intrínseca el impulso de los procesos de simplificación administrativa. Esto significa suprimir trámites redundantes o innecesarios, reducir la documentación que se exige a los ciudadanos –especialmente aquellos documentos que ya tenga la Administración y que se pueden obtener a través de la interconexión de registros administrativos–, implantar bases generales de procedimientos y plazos únicos y la instauración progresiva del silencio positivo como regla general. Todo ello permite una gestión administrativa más rápida y más clara (TRONCOSO REIGADA, 2008).

Esta idea de simplificación administrativa ligada a la supresión de trámites innecesarios y a la reducción de la documentación exigida a la ciudadanía no es novedosa. La propia Ley 30/1992, de 26 de noviembre, del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJPAC) pretendía de manera ambiciosa modernizar la gestión de la Administración pública, simplificando la necesidad de aportar documentos que se encontraran ya en poder de la Administración. Así, reconoce el derecho de los ciudadanos en sus relaciones con las Administraciones públicas «a no presentar documentos no exigidos por las normas aplicables al procedimiento de que se trate o que ya se encuentren en poder de la Administración actuante» –artículo 35.f)–.

Este mismo precepto –conocido también como principio *once only* (MARTÍN DELGADO, 2017)– se reproduce igualmente en la actual Ley 39/2015, concretamente en el artículo 28.3 LPAC –precepto modificado por la

Disposición final duodécima de la LPDGDD con la finalidad de mejorar la protección de datos de carácter personal en poder de las diferentes Administraciones públicas—, al señalar que «[...] Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario. Asimismo, las Administraciones públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación».

Esta reciente modificación normativa pone de manifiesto la relevancia que el legislador español confiere a la interoperabilidad administrativa, consciente de que el intercambio de datos entre las diferentes Administraciones públicas constituye un axioma imprescindible, no sólo desde el punto de vista de la prestación de servicios avanzados de administración electrónica a los ciudadanos, sino también como mecanismo idóneo para la reducción de los costes de transacción y la mejora de la eficiencia y la eficacia de las organizaciones.

En este sentido, la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos, aprobada mediante Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, supuso la creación de la *Plataforma de Intermediación de Datos (PID)* del Ministerio de Hacienda y Administraciones Públicas, hoy dependiente del Ministerio de Política Territorial y Función Pública, proyecto concebido en última estancia con la finalidad de facilitar el intercambio de datos entre Administraciones públicas, evitando con ello la solicitud reiterada al ciudadano de aquellos datos que ya obren en poder de la Administración (BARRERA, 2019). La PID permite verificar y consultar los datos de un ciudadano mediante el acceso a los servicios de verificación y consulta de datos (SVD), debiendo en todo momento asegurar la confidencialidad e integridad de la información intercambiada entre las diferentes organizaciones, y no almacenando, en ningún caso, la información personal de ciudadano alguno, derivada de los procesos de transacción de intercambio de datos.

De esta forma, mediante el acceso a los servicios de verificación y consulta de datos de la Plataforma de Intermediación de Datos se permite que cualquier organismo de la Administración, pueda consultar o verificar datos previamente aportados por los ciudadanos o administrados, sin necesidad de solicitar la aportación de los correspondientes documentos acreditativos, permitiendo así hacer

efectiva esta supresión y reduciendo de forma significativa la proliferación de datos personales en las relaciones Administración-administrado. Actualmente en SVD se pueden verificar los siguientes tipos de datos:

- Servicios de Verificación y Consulta de Datos de Identidad (SVDI).
- Servicio de Verificación de Datos de Residencia (SVDR).
- Servicio de Verificación de Datos de Prestación de Desempleo (SVDP).
- Servicio de Verificación de Datos de Títulos Oficiales (SVDT).
- Servicio de Verificación de Datos de la Tesorería General de la Seguridad Social (TGSS).
- Servicio de Verificación de Datos de la Agencia Estatal de Administración Tributaria (AEAT).
- Servicio de Verificación de Datos Catastrales.
- Servicio de Consulta de Nivel y Grado de Dependencia (IMSERSO).
- Servicio de Consulta de Prestaciones Públicas (INSS).
- Servicio de Consulta de Datos del Ministerio de Justicia.
- Servicio de Consulta de entidades aseguradoras y reaseguradoras de la Dirección General de Seguros y Fondos de Pensiones (DGSFP).
- Servicio de Impuesto sobre Actividades Económicas (IAE) Gobierno de Navarra.
- Servicio de Impuesto sobre Actividades Económicas (IAE) Gobierno del País Vasco.
- Servicio de Consulta de Firmas para Legalización Diplomática de Documentos Públicos Extranjeros del Ministerio de Justicia.
- Servicios de Poderes Notariales del Consejo General del Notariado.
- Servicios de MUFACE.
- Servicio del Instituto Cervantes.
- Servicio de la Conferencia de Rectores de las Universidades Españolas (CRUE).

Todos estos servicios, unidos al conjunto de previsiones en materia de seguridad, confidencialidad y privacidad de los datos establecidas en la Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, convierten a la Plataforma de Intermediación de Datos en la herramienta idónea para maximizar la protección de los datos personales de la ciudadanía en poder de las Administraciones públicas, siempre y cuando se aseguren las máximas

garantías de seguridad y confidencialidad de las consultas, preservando la privacidad de los datos consultados tanto en el propio intercambio como en el tratamiento posterior de la información obtenida. Para ello, la normativa vigente prevé el establecimiento de controles de autorización, acceso y uso por parte de los usuarios en aras de potenciar el correcto funcionamiento de la interoperabilidad administrativa en nuestro país.

Esta herramienta representa a grandes rasgos el posicionamiento mayoritario de la doctrina administrativista, la cual ha señalado desde un primer momento, la necesidad de establecer una base de datos general radicada, por ejemplo, en la Administración General del Estado (o Comunidad Autónoma en su caso), a la que pudiesen acceder los aplicativos del resto de Administraciones gracias a la debida interoperabilidad; hasta su consecución debería garantizarse, al menos, para dar cumplimiento al principio «*once only*», que todos los datos obrantes en una determinada Administración sean retroalimentados al realizar trámites en un procedimiento posterior al primero (MARTÍN DELGADO, 2017). Esta idea, vista con recelo por quienes enarbolan un férreo discurso en favor de la –malentendida– autonomía de las Comunidades Autónomas, ha supuesto de facto el principal escollo para el establecimiento de un sistema interoperable que propiciara el despliegue efectivo de la administración electrónica en nuestro país, lo que se ha traducido en última instancia en numerosos desvelos para quienes se han visto obligados a relacionarse por medios telemáticos con las Administraciones públicas. Ciertamente, la pluralidad de sistemas y productos informáticos implementados por las diferentes instituciones –especialmente las Comunidades Autónomas– al objeto de desplegar la administración electrónica en sus respectivos territorios, unido al desconocimiento de los elementos indispensables –tanto en términos de eficacia como en términos legales– para garantizar la interoperabilidad administrativa por parte de quienes se erigieron como expertos en el diseño de herramientas y plataformas para el avance de la administración digital, dificulta extraordinariamente la adopción de un modelo eficaz de administra electrónica, algo carente de toda lógica.

Por todo ello, y a pesar de los avances alcanzados en el campo de la interoperabilidad administrativa, la efectividad de ese principio que apuntábamos con anterioridad conocido como «*once only*» sigue pareciendo más una quimera que una realidad tangible próxima a nuestros días. Su puesta en marcha decidida contribuiría de manera significativa a la mejora de la seguridad de la información, al tiempo que reduciría el grado de vulnerabilidad de los datos personales de la ciudadanía en poder de las Administraciones públicas. No podemos más que reafirmarnos en esta tesis, pues parece lógico que una reducción de la documentación exigida por parte de las Administraciones públicas –y ya aportada previamente por el administrado–, llevaría aparejada la consiguiente disminución del riesgo y la vulnerabilidad de los datos personales de la ciudadanía, lo que

redundaría en la realización efectiva del contenido establecido en el artículo 18.4 CE, según el cual, la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Esta aspiración loable exige un replanteamiento de las herramientas concebidas por la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios públicos con la finalidad de impulsar la administración electrónica: el Esquema Nacional de Interoperabilidad (ENI) y el Esquema Nacional de Seguridad (ENS); renovación necesaria tanto para afrontar la transformación digital que ha experimentado la sociedad española en la última década, como para preparar el próximo salto cualitativo que se está fraguando ya en el seno de la Administración pública, cuando nos encontramos en los albores de la administración automatizada. Con todo ello, ¿será necesario replantear la estrategia de interoperabilidad y seguridad de las Administraciones públicas?

Conclusiones

El vertiginoso proceso de digitalización y datificación experimentado por la sociedad de su conjunto en los últimos años ha traído consigo la necesidad de acometer importantes y profundas transformaciones del sistema jurídico, todo ello con la finalidad de limitar y minimizar el alcance lesivo que el avance de la tecnología puede suponer para el disfrute efectivo de los derechos fundamentales de la ciudadanía. Consciente de ello, el legislador europeo ha llevado a cabo un ambicioso proceso de modernización y mejora de la regulación en materia de protección de datos de carácter personal, cuyo mayor hito ha sido la adopción del RGPD, o lo que es lo mismo, un auténtico cambio de paradigma en la normativa sobre la materia hasta la fecha. Nuevas obligaciones y exigencias con un horizonte común, crear las condiciones necesarias que garanticen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Exigencias y obligaciones a las que, por otro lado, no son ajenas las diferentes Administraciones públicas, las cuales deberían adoptar una posición de liderazgo en la defensa del derecho a la protección de datos de carácter personal, para lo cual resulta indispensable la mejora tanto de las herramientas como de la estrategia de interoperabilidad administrativa –así como la plena eficacia de principios tan manidos como el de «once only»–, cuestión clave para evitar la proliferación innecesaria de datos personales en la relación Administración-ciudadano.

En este sentido, conviene poner en marcha no solo los procedimientos pertinentes de mejora y perfeccionamiento continuado de las herramientas articuladas para promover la interoperabilidad administrativa, sino también implementar la difusión y conocimiento de los mecanismos articulados por la

Administración pública a tal fin, algo para lo que es imprescindible mejorar la formación de los empleados públicos –como principales usuarios de estos instrumentos–, ardua tarea en la que los archiveros están llamados a ser los auténticos protagonistas.

Urge, en definitiva, la puesta en marcha de medidas concretas en el campo de la interoperabilidad que contribuyan de manera significativa a la mejora de la seguridad de la información y a reducir notoriamente el grado de vulnerabilidad de los datos personales de la ciudadanía en poder de las Administraciones públicas, sólo así podrá darse cumplimiento a las previsiones realizadas por la Unión Europea en lo referente al derecho a una buena administración: *el buen gobierno implica necesariamente un tratamiento eficaz de los datos personales de la ciudadanía, principal activo para el correcto funcionamiento de la acción administrativa.*

Bibliografía

- Álvarez Hernando, Javier (2018). “Practicum de protección de datos 2018”. Pamplona, Thomson Reuters-Aranzadi, pág. 48.
- Barrera, Jorge (2019). “La plataforma de intermediación de datos”. *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, núm. 4, págs. 87-104.
- Carrillo Salcedo, Juan Antonio (2001). “Notas sobre el significado político y jurídico de la Carta de Derechos Fundamentales de la Unión Europea”. *Revista de Derecho Comunitario Europeo*, núm. 9, pág. 12.
- Cerrillo Martínez, Agustí (2008). “Cooperación entre Administraciones públicas para el impulso de la administración electrónica”, en Gamero Casado y Valero Torrijos (coord.), *La Ley de administración electrónica. Comentario sistemático a la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos*. Thomson Reuters-Aranzadi, Navarra, pág. 497.
- Davara Rodríguez, Miguel Ángel (2016). “Reglamento Europeo sobre protección de datos”. *Actualidad administrativa*, núm. 7, pág. 10.
- Fernández Villazón, Luis Antonio (2016). “El nuevo Reglamento Europeo de Protección de Datos”. *Nueva época*, vol. 19, núm. 1, pp. 395-411.
- Gamero Casado, Eduardo (2009) “Interoperabilidad y Administración electrónica: concéntense, por favor”. En: *Revista de Administración Pública*, núm. 179, Madrid, págs. 291–332.
- Martín Delgado, Isaac (2017). “La reforma de la Administración electrónica: Una oportunidad para la innovación desde el Derecho”. Madrid, Instituto Nacional de Administraciones Públicas.
- Martínez Martínez, Ricard (2007). “El derecho fundamental a la protección de datos: perspectivas”. *IDP: revista de Internet, derecho y política= revista d’Internet, dret i política*, núm. 5, pág. 4.

- Martín-Retortillo Baquer, Lorenzo (2008). “Los Derechos Fundamentales en el ámbito de la Unión Europea y su incidencia en España (con especial referencia a la Ley Orgánica 1/2008, de 30 de julio, por la que se autoriza la ratificación del Tratado de Lisboa, de 13 de diciembre de 2007)”. *Revista Aragonesa de Administración Pública*, núm. 33, pág. 35.
- Pérez Luño, Antonio Enrique (2012). “Los derechos humanos en la sociedad tecnológica”. Madrid, Universitas.
- Rallo Lombarte, Artemi & García Mahamut, Rosario (2015). “Hacia un nuevo derecho europeo de protección de datos. Towards a new European Data Protection Regime”. Valencia, Tirant lo Blanch.
- Rallo Lombarte, Artemi (2017). “De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)”. *Revista de Derecho Político*, núm. 100, págs. 637-667.
- Rallo Lombarte, Artemi (2019). “Del derecho a la protección de datos a la garantía de nuevos derechos digitales”. En: Rallo Lombarte, Artemi et al. *Tratado de Protección de Datos*. Valencia: Tirant lo Blanch, págs. 23-52.
- Rebollo Delgado, Lucrecio (2018). “Protección de datos en Europa. Origen, evolución y regulación actual”. Madrid, Editorial Dykinson, pág. 83.
- Rodríguez-Arana Muñoz, Jaime. (2006). “El buen gobierno y la buena Administración de las Instituciones Públicas (adaptado a la Ley 5/2006, de 10 de abril)”. Cizur Menor, Thomson-Aranzadi.
- Rodríguez-Arana Muñoz, Jaime. (2014). “La buena Administración como principio y como derecho fundamental en Europa”. *Misión Jurídica, Revista de Derecho y Ciencias Sociales*. núm. 6, págs. 23-56.
- Rodríguez Díaz, Alonso (2001). “Sobre la naturaleza jurídica de la Carta de Derechos Fundamentales de la Unión Europea”. *Revista de Derecho Político*, núm. 51.
- Samuel D. Warren & Louis D. Brandeis (1890). “The right to privacy”. *Harvard Law Review*. Vol. IV, n.º 5.
- Sanz Larruga, J. (2009). El ordenamiento europeo, el derecho administrativo español y el derecho a una buena administración. *Anuario da Facultade de Dereito da Universidade da Coruña*, núm. 13, págs. 729-751.
- Terrón Santos, Daniel & Domínguez Álvarez, José Luis (2019). “Nueva regulación de la protección de datos y su perspectiva digital”. Granada, Editorial Comares.
- Troncoso Reigada, Antonio (2008). “La administración electrónica y la protección de datos personales”. *Revista jurídica de Castilla y León*, núm. 16, págs. 31-112.

Notas

¹ Personal Investigador en Formación del Área de Derecho Administrativo de la Universidad de Salamanca | FPU 17/01088 Ministerio de Ciencia, Innovación y Universidades.

² El texto del Convenio ha sido modificado tras su aprobación por las disposiciones del Protocolo n.º 14 (STCE n.º 194) a partir de su entrada en vigor el 1 de junio de 2010. El texto del Convenio fue anteriormente modificado por las disposiciones del Protocolo n.º 3 (STE n.º 45), que entró en vigor el 21 de septiembre de 1970, del Protocolo n.º 5 (STE n.º 55), que entró en vigor el 20 de diciembre

de 1971 y del Protocolo n° 8 (STE n° 118), que entró en vigor el 1 de enero de 1990. Incluía asimismo el texto del Protocolo n° 2 (STE n° 4) que, de conformidad con su artículo 5 párrafo 3, formaba parte integrante del Convenio desde su entrada en vigor el 21 de septiembre de 1970. Todas las disposiciones modificadas o añadidas por dichos Protocolos fueron sustituidas por el Protocolo n° 11 (STE n° 155), a partir de la fecha de su entrada en vigor el 1 de noviembre de 1998. Desde esa fecha, el Protocolo n° 9 (STE n° 140), que entró en vigor el 1 de octubre de 1994, quedó derogado y el Protocolo n° 10 (STE n° 146) quedó sin objeto.

³ El enchufe es un ejemplo rudimentario de interoperabilidad en procesos puramente industriales: la clavija de que disponga un aparato debe ser compatible con la clavija de suministro de corriente a la que vamos a conectarlo, porque en caso contrario no podríamos enchufar el equipo, cosa que no es tan fácil de lograr cuando son muchos los fabricantes y la distribución del producto abarca grandes áreas.

⁴ El Esquema Nacional de Interoperabilidad se establece en el artículo 156.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que sustituye al apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

⁵ Decisión 2004/387/CE de la Comisión, de 28 de abril de 2004; Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos.

⁶ Mediante la Decisión (UE) 2015/2240 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 por la que se establece un programa relativo a las soluciones de interoperabilidad y los marcos comunes para las administraciones públicas, las empresas y los ciudadanos europeos (programa ISA2) como medio de modernización del sector público la Comisión persigue continuar el esfuerzo del Programa ISA (Soluciones de interoperabilidad para las administraciones públicas europeas) extendiendo la proyección a los ciudadanos y las empresas, con el objetivo de desarrollar, mantener y promover un enfoque holístico hacia la interoperabilidad en la Unión para eliminar la fragmentación en el panorama de la interoperabilidad en la Unión; facilitando una interacción electrónica transfronteriza o intersectorial eficiente y eficaz tanto entre las administraciones públicas europeas como entre ellas y las empresas y los ciudadanos, y contribuir al desarrollo de una administración electrónica más eficaz, simplificada y orientada a los usuarios en los niveles nacional, regional y local de la administración pública; y promoviendo la reutilización de las soluciones de interoperabilidad por parte de las administraciones públicas europeas.



**PRIVATE
NATURE
RESERVE**

CIRCULEZ
Y'A TOUT
À VOIR





DIEGO ROBLEDO

Documentos electrónicos en el Gobierno Abierto de la República Argentina:

hacia un sistema de gestión con tutela constitucional, convencional y procesal de la protección de datos personales y acceso a la información pública

E-files in the Open Government of the Republic Argentina:

looking forward to a management system with constitutional, covenant and procedural warrants of personal data's protection and access to public information

Diego Robledo

drobledoavilapaz@gmail.com

Universidad Nacional de La Rioja

y Universidad Nacional de Córdoba, Argentina

Citación: Robledo, Diego (2019). "Documentos electrónicos en el Gobierno Abierto de la República Argentina: hacia un sistema de gestión con tutela constitucional, convencional y procesal de la protección de datos personales y acceso a la información pública". *Tábula*, n. 22, pp. 115-138

Recibido: 26-7-2019. *Aceptado:* 22-11-2019

Resumen analítico / Analytic summary

El presente artículo explora el Documento Electrónico a partir de su regulación en la República Argentina. Desde una perspectiva jurídica, abierta a la interdisciplina, se procura comprender la relación con el Gobierno Abierto que atraviesa Argentina como parte de la modernización del Estado a la luz de los derechos y garantías constitucionales y convencionales como lo es por excelencia el proceso constitucional denominado Habeas Data. En nuestra propuesta presentamos tres desafíos, conceptual, tecnológico y jurídico teniendo en cuenta los avances de la Inteligencia Artificial, Blockchain, Big Data y Data Science.

SISTEMA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS | GOBIERNO ABIERTO | HABEAS DATA

In this article we analyze the Electronic File from the normative system of Republic Argentina. From a juridical and interdisciplinary point of view we reflex about the Open Government that the Republic Argentina is on the plan of modernization of the State. Our argumentation takes in special consideration human rights and warrants of the Constitution and Human Rights Conventions about data protection – personal, private, sensitive, public, open data– with the Habeas Data. Our proposal explore three challenges: conceptual, technological and juridical taking in consideration Artificial Intelligence, Blockchain, Big Data and Data Science.

SYSTEM OF MANAGEMENT OF ELECTRONIC FILES | OPEN GOVERNMENT | HABEAS DATA

Presentamos

un enfoque desde Argentina acerca del Documento Electrónico en el Gobierno Abierto de nuestra República.

Una particularidad de Argentina es que adopta el sistema de federalismo (ROBLEDO, Federico Justiniano 2002, 2003, 2006), por lo que tenemos Nación y Provincias y nuestra Capital es la Ciudad Autónoma de Buenos Aires, todos los cuales se relacionan como parte de un sistema. Por esta razón, tenemos un ordenamiento nacional y a su vez cada provincia tiene legislación provincial autónoma. Asimismo, en las Provincias existen Municipios con legislación local. Esta aclaración la hacemos en función que al referirnos a Ley Nacional y Ley Provincial lo hacemos con este alcance.

Nuestro análisis va de lo general a lo específico, por cuanto señalamos que el Gobierno Abierto sirve de marco para el sistema de Gestión de Documentación Electrónica en el cual fluyen los documentos electrónicos.

El proceso constitucional de habeas data es una herramienta de tutela y garantía de los derechos fundamentales de las personas en relación a la información que oscila entre el límite público o privado.

Nuestra investigación parte de una perspectiva jurídica y se vale de la interdisciplina. Aplicamos metodológicamente la Dogmática Jurídica, la Filosofía del Derecho, la Teoría General del Proceso, el Derecho Procesal Constitucional, Derecho Constitucional, Derecho Administrativo, Derecho de la Información y Legislación de Archivos.

Por esta razón a los efectos expositivos, presentamos estos tres elementos: Gobierno Abierto, Sistema de Gestión de Documentación Electrónica y proceso constitucional de Habeas Data. Presentamos las bases de un sistema de gestión de documentación electrónica sostenible junto a nuestras reflexiones finales.

Gobierno Abierto Electrónico

Los grandes y continuos avances tecnológicos e informáticos, introducen cambios copernicanos en materia de comunicación, teniendo en cuenta que, a través de Internet, es posible comunicarse en tiempo real a cualquier lugar del mundo. En esta línea, Rosa Avila Paz nos enseña que *“Internet es una revolución tecnológica de las comunicaciones, en la cual se combinan una variedad de inventos en cada vez menos aparatos. Tecnología, Información y Comunicación (TICs) fundan un trionfismo en esta nueva era. El uso de la computadora ha cambiado el mundo, como un prisma a partir del cual se puede observar al mundo (... y como herramienta) permite a las personas expresarse”* entre redes (“inter” “net”) (Avila Paz de Robledo, Rosa A. 2012:194). Desde 1994, se ha producido un crecimiento exponencial de páginas web (conocido como fenómeno “.com”), al que ya en 2004 ingresamos a la “Web 2.0” –refiriéndonos a la *“web como plataforma”* para envolver una segunda generación de sitios webs que posibilitan nuevas maneras de interacción en la red, lo que ha dado lugar a una nueva *cultura virtual o civilización en la red en la que vivimos conectados*, o como también se dijo *“Internet es el imperio donde nunca se pone el sol”* (Avila Paz de Robledo, Rosa A. 2012:204). Luis María Bunge Campos sostiene que *“la irrupción de las redes sociales en nuestra vida cotidiana ha causado tantos cambios como los que representó la aparición de la imprenta en el siglo XV”* (2015:6).

Mauricio Devoto (2001:60) explica que Internet es *“una red”* y acceder a ella es de interés nacional (Dec. 554/97). En segundo lugar, el Decreto del Poder Ejecutivo de la Nación Argentina N°1279/97 lo declara comprendido dentro de la garantía constitucional que ampara la libertad de expresión al *“servicio”* de Internet. En tercer lugar, *“es una autopista”* (Res. 1018/98 de la Secretaría de Comunicaciones de la Nación Argentina). La Ley Nacional N° 26032 (B.O. 17-06-2005) en su artículo 1° dice *“La búsqueda, recepción y difusión de información e ideas de toda índole, a través del servicio de Internet, se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión”*. Además, puede leerse entre los considerandos del Decreto 378/2005 (B.O. 28/04/2005) –*Plan Nacional de Gobierno Electrónico y planes sectoriales del Gobierno Electrónico*: *“Que el empleo de las Tecnologías de la Información y las Comunicaciones, y especialmente Internet, está transformando las relaciones entre las personas y las organizaciones públicas y privadas, resultando un instrumento idóneo para facilitar el acceso a la información y a los servicios del Estado, integrar los distintos niveles de la Administración Pública Nacional, dotar de transparencia a la actividad del Estado, digitalizar con validez legal la documentación pública y permitir el intercambio de información entre el Estado y los particulares mediante canales alternativos al papel”*.

En la actualidad, el Gobierno Abierto Electrónico es una manifestación constitucional del principio republicano de gobierno de publicidad de los actos

de gobierno y de transparencia (art. 1° de la Constitución Nacional de la República Argentina).

Este Gobierno Abierto lo observamos en el plano del Poder Ejecutivo, Poder Legislativo y Judicial.

En el ámbito del Poder Ejecutivo se viene desarrollando una agenda de cinco ejes de gestión: “*Gobierno Digital, Modernización Administrativa, Gobierno Abierto, Recursos Humanos y País Digital*” (Borrman, Rudi 2017:6). De ello, se ha derivado como marco jurídico:

- a) *Plan Nacional de Apertura de Datos* reglamentado a través del Decreto 117/2016 se establecen plazos para publicar los primeros conjuntos de datos del portal <https://datos.gob.ar/> y establece un cronograma de publicación;
- b) *Sistema Nacional de Datos Públicos*, que surge a partir de la Resolución 538/2013 que reglamenta la creación del *Sistema Nacional de Datos Públicos* (SINDAP);
- c) el *Régimen de Acceso a la Información Pública* de acuerdo a la Ley Nacional N° 27275 de Derecho de Acceso a la Información Pública.

En el plano legislativo, a través de la Ley N° 27.275 se crea la Agencia de Acceso a la Información Pública, que es a su vez quien se desempeña como Autoridad de Aplicación de la Ley de Protección de Datos Personales N° 25.326 y tiene la competencia de controlar la protección integral de los datos personales asentados en archivos, registros, banco de datos, y todos los demás modos técnicos de tratamiento de datos –ya sean públicos, o privados destinados a dar informes– en aras de garantizar el derecho al honor y a la intimidad de las personas (cc. art. 19 de la Constitución Nacional), y el acceso a la información que sobre las mismas se registre.

El artículo 1° de la Ley Nacional N° 27.275 establece que “*la inscripción, modificación y baja de las bases de datos personales de carácter privado, público estatal y público no estatal, que habrán de cumplimentar los responsables de su tratamiento, ante el REGISTRO NACIONAL DE BASES DE DATOS de la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES, deberán tramitarse exclusivamente a través de la plataforma “Trámites a Distancia” (TAD) o sistema de Gestión Documental Electrónica (GDE): 1. Registro del Titular o Responsable de Base de Datos, Privada o Pública; 2. Registro de Base de Datos Privada o Pública –estatal o no estatal–*”.

Resulta importante tomar en consideración que la modernización ha implementado un lenguaje técnico como el que surge de las voces de este glosario del portal <https://datos.gob.ar/>

Cómo género se identifica la voz “Datos” que se presentan definidos como “*un elemento descontextualizado que puede dar origen a la generación de información. Son símbolos que describen hechos, condiciones, valores o situaciones. Un dato puede*

ser una letra, un número o cualquier símbolo que representa una cantidad, una medida, una palabra o una descripción. Los datos son la verdadera materia prima para generar información con valor agregado”. Asimismo, se distinguen dos especies, Dato público y Dato abierto. El primero es conceptualizado como “cualquier dato generado en el ámbito gubernamental, o que se encuentra bajo su guarda”, mientras que el dato abierto es presentado como “un dato de origen público o no, al que cualquier persona puede acceder, usar y compartir libremente. Sólo deben atribuirse y compararse con la misma licencia con la que fueron publicados. Son, a su vez, datos públicos disponibilizados en un medio digital, bajo una licencia abierta y usando para ello un formato estándar abierto”.

A este glosario se le añaden voces como:

- “Activo de datos”, definido como “cualquier recurso de datos con valor para el desarrollo de las funciones de una organización, que puede ser comprendido y tratado como una única unidad a efectos de gestión, uso, protección e intercambio”.
- La voz “Información”, se presenta como “un dato dotado de relevancia, utilidad e interpretación. Para obtener información es necesario aplicar algún tipo de transformación o procesamiento sobre los datos”.
- Mientras que “Metadatos” es entendido como “Ciertas características o atributos de los datos son definidos para facilitar su comprensión. Estas características se conocen como “metadatos”. Suele decirse, por esa razón, que “los metadatos son datos sobre los datos”. Los metadatos pueden describir cómo un dato es representado, cuáles son los rangos de valores aceptables, su relación con otros datos y cómo estos deben ser etiquetados. También pueden proporcionar otra información pertinente, como el administrador responsable, leyes y reglamentos asociados, y la política de gestión de acceso”.
- La voz “Catálogo de datos” se explica como “el sistema de información que recopila y organiza metadatos descriptivos sobre los distintos conjuntos de datos abiertos por una organización, dando un acceso único a los mismos. Un portal de datos es un catálogo”.
- Y los “Datasets o conjuntos de datos” son presentados como “la pieza principal en todo el catálogo de datos. Éstos agrupan uno o más recursos de datos y son el eje sobre el que se documentan los metadatos de la información”.
- Las “Distribuciones” o “Recursos” se presentan como “la pieza de información más pequeña del catálogo y son los verdaderos activos de datos del portal”.

Es importante apreciar que la ley y política pública de información y gobierno abierto requiere un lenguaje adecuado a los fines que proyecta, y ello nos interpela hacia una redefinición conceptual y nuevos paradigmas.

En el plano judicial, observamos que la Corte Suprema de Justicia de la Nación es un Gobierno Judicial Abierto (Avila Paz de Robledo, Rosa A. 2016). Como política de estado, el Gobierno Abierto Judicial promueve la transparencia, el acceso a la información y la participación ciudadana. Representa una reforma integral con el acento puesto en la accesibilidad de la justicia tanto institucional como de la manera de desenvolverse y comunicar en forma de datos abiertos más asequibles y más disponibles a la ciudadanía. “*Gobierno Abierto Judicial es un proceso dinámico, que se construye día a día, como respuesta concreta al derecho que tiene el ciudadano de acceder a la información que producen los poderes públicos*” (BOURDIN, María 2015). En la faz procesal se utiliza notificación electrónica, oficio judicial electrónico (Avila Paz de Robledo, Rosa A. y ROBLEDOS, Diego 2019), registro multimedia de audiencias orales y expediente electrónico.

Esta política de estado es una aplicación al campo judicial del “Gobierno Abierto”, como un movimiento de escala mundial que iniciara Barack Obama con su directiva de Gobierno Abierto y transparencia y que muchos países vienen implementando en sus gobiernos.

Esta política implicó además de implementar nuevas tecnologías en el proceso judicial, una contribución al fortalecimiento de la “eficacia” y “calidad” en la prestación del servicio de justicia, particularmente, no sólo en la reducción de tiempos y costos, para el Tribunal y las partes, sino también en el impacto ambiental para la sociedad.

El gobierno abierto sigue un modelo de transparencia activa, en el cual como advierte Vicent Giménez-Chornet “*conseguir que los documentos sean identificados y localizados implica, al igual que en las bibliotecas, que sean descritos e indizados adecuadamente para que en los distintos sistemas de búsqueda los usuarios puedan obtener resultados pertinentes y rápidos*”, en dicho proceso explica, son esenciales los archivistas para describir e indizar e informáticos para crear bases de datos accesibles e interoperables (2017:44).

Gestión de documentación electrónica

En Argentina, a nivel nacional resultó un hito la sanción de la Ley N°25.506 de Firma Digital (Sancionada 14/11/2001, promulgada de hecho: 11/12/2001) y su Decreto Reglamentario 2628/2002. Luego la Ley N°26.685 (B.O.07/07/2011) sobre expedientes electrónicos. Este escenario se robusteció con la entrada en vigor del Código Civil y Comercial de la Nación (Ley 26.994, B.O. 01/10/2014, vigente desde el 01/08/2015). A los efectos aclaramos que de acuerdo al Código Civil y Comercial de la Nación en su art. 287 se legisla sobre los instrumentos privados no firmados y dentro de ellos da cabida a los documentos generados por medios electrónicos que los que denominamos documentos electrónicos porque

constituyen una nueva forma de manifestación de la voluntad de las personas humanas y de las personas jurídicas privadas o públicas nacionales, provinciales o municipales.

El Decreto N° 561 (06/04/2016) aprobó la implementación del Sistema de Gestión Documental Electrónica (GDE) como sistema integrado de caratulación, numeración, seguimiento y registración de los movimientos de todos los actos y expedientes del Sector Público Nacional, operando como plataforma para la implementación de gestión de expedientes electrónicos. Surge como una estrategia del Plan de modernización del Estado (aprobado por Dec. 434/2016) con miras a simplificar a través de la incorporación de las *“nuevas plataformas tecnológicas que facilitan la vinculación y las transformaciones entre los distintos organismos que la componen, pero principalmente con los ciudadanos. Que los trámites existentes, con la implementación del expediente electrónico y el proceso de digitalización, deben reflejarse en términos de menores costos y plazos y, en consecuencia, en una mejor atención del ciudadano y en una mejora en la productividad de las empresas y de la economía”*.

Desde un punto de vista técnico, la utilización del sistema de Gestión Documental Electrónica –GDE–, permite dar certeza del origen, de la firma, de la integridad y de la autoría del documento, por lo que goza de pleno valor probatorio en los términos del inciso e) del artículo 15 del Reglamento de Procedimientos Administrativos Decreto 1759/72 T.O. 2017, haciendo innecesaria la legalización de dichos documentos electrónicos, toda vez que la misma se realiza automáticamente en el mencionado sistema informático. Asimismo, el sistema de Gestión Documental Electrónica –GDE– fue distribuido para su utilización en provincias, municipios, otros poderes, entes públicos no estatales, sociedades del Estado, Banco Central, entre otros, y que por lo tanto cuentan con sistemas de gestión documental electrónica interoperables con el sistema de Gestión Documental Electrónica –GDE– del Sector Público Nacional, generando documentos electrónicos oficiales firmados digitalmente que gozan de pleno valor probatorio.

Siguiendo a Avila Paz de Robledo enseña que *“la firma digital, en sentido amplio: es un medio tecnológico, que la ley reconoce para conferir seguridad virtual y jurídica a un documento digital. Y, en sentido estricto: es –a la simple lectura– un bloque de caracteres digitales ilegibles que se acompaña a un documento digital para acreditar quién es su autor y, que los datos del mismo no fueron objeto de una posterior modificación”* y consiste en *“una herramienta tecnológica que se manifiesta en un documento con características técnicas y normativas, dado que requiere del procedimiento técnico conocido como el sistema de las dos claves o llaves (privada y pública) para la creación y verificación de la firma digital, y del certificado de clave pública que respalda el valor legal que dicha firma posee”* (2009:17).

El Código Civil y Comercial de la Nación (en adelante CCyC) en la regulación de los actos jurídicos admite cualquier soporte (cfr. art. 286 CCyC); y

establece que *“la firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo. En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital, que asegure indubitablemente la autoría e integridad del instrumento”* (art. 288 CCyC).

El Decreto Nacional 27/2018 también tiene consecuencias en materia de prueba por cuanto establece la presunción *“Cuando un documento electrónico sea firmado por un certificado de aplicación, se presumirá, salvo prueba en contrario, que el documento firmado proviene de la persona titular del certificado”* (art. 10 Ley N°25506 modif. Dec. 27/2018). En este proceso ya el Decreto Nacional 182/2019 reglamentó la firma digital en Argentina.

Se establece que *“los documentos oficiales electrónicos firmados digitalmente, expedientes electrónicos, comunicaciones oficiales, notificaciones electrónicas y domicilio especial constituido electrónico de la plataforma de trámites a distancia y de los sistemas de gestión documental electrónica que utilizan el Sector Público Nacional, las provincias, el Gobierno de la Ciudad Autónoma de Buenos Aires, municipios, Poderes Judiciales, entes públicos no estatales, sociedades del Estado, entes tripartitos, entes binacionales, Banco Central de la República Argentina, en procedimientos administrativos y procesos judiciales, tienen para el Sector Público Nacional idéntica eficacia y valor probatorio que sus equivalentes en soporte papel o cualquier otro soporte que se utilice a la fecha de entrada en vigencia de la presente medida, debido a su interoperabilidad que produce su reconocimiento automático en los sistemas de gestión documental electrónica, por lo que no se requerirá su legalización”* (Art. 30 b) de la Ley 25506 modif. por art. 128 Dec. 27/2018).

Desde el punto de vista archivístico, Andrés Pak Linares (2016) reflexiona: *“La implementación de GDE ha traído para los archivistas las (quizás) típicas prevenciones, por no decir críticas, respecto de cuestiones tales como la falta de perspectiva archivística para la identificación, clasificación, registro y descripción de los documentos simples y compuestos que son tramitados en los distintos módulos del GDE”*. Afirma que es necesario *“incorporar una mirada archivística al proceso, especialmente en lo que hace al establecimiento de plazos de guarda y efectivizar la disposición final de las series con anterioridad al proceso de digitalización”*.

En este sentido Vicent Giménez-Chornet explica que *“[en] el proceso de modernización de los archivos uno de los aspectos menos tratados es la implantación de un sistema de innovación, unido al de investigación y desarrollo (I+D+i), que permita la adecuación de la gestión documental a los nuevos retos que las organizaciones y la sociedad de la información tienen planteados”* (2010:132).

La innovación tecno-informática nos demanda comprender el flujo con criterios de evaluación desde el inicio del ciclo vital de los documentos electrónicos con criterios archivísticos. Ello requiere trabajar desde el inicio con los metadatos en la inscripción, clasificación, registro, garantizando una cadena de

preservación documental sostenible. A partir de esta cadena de preservación documental sostenible se hace posible recuperar documentos electrónicos auténticos, confiables, íntegros. Por ello, Pak Linares (2016) reflexiona que *“esta vocación por intervenir en la implementación conflictiva de GDE que se traduzca en una legislación en donde la perspectiva archivística contemporánea esté presente incluye cambiar en la diversa normativa el concepto de “valor histórico”, local y coyunturalmente ligado discursivamente al interés de los historiadores por “sus fuentes”, por el de “valor secundario”, que refleja la posición del [Archivo General de la Nación] respecto de la triple función social de los Archivos en el largo plazo”*.

En materia de Legislación Archivística en relación al GDE se ha legislado en Argentina –a nivel nacional–

- Decreto 1131/2016 (28/10/2016): que otorga valor legal del original de los documentos y expedientes generados electrónicamente, y de los digitalizados de originales en cualquier otro soporte de acuerdo al procedimiento aprobado por Resolución SMA 44/16, los cuales pierden su condición jurídica de original y pueden destruirse previa evaluación de su valor histórico. Asimismo, se ha aprobado el Repositorio Único de Documentos Oficiales (RUDO) para conservar todos los documentos electrónicos obrantes en GDE, siendo el órgano de competencia el Archivo General de la Nación para definir los documentos y expedientes digitalizados que deberán conservarse en soporte original debido a su valor histórico.
- Resolución SMA 7/2016 (02/6/2016) en la que se establece el archivo de documentos en el RUDO.
- Resolución SMA 44/2016 (30/12/2016) establece la Tabla de Plazos Mínimos de Conservación y Guarda de Actuaciones Administrativas de cuarenta y seis trámites para expedientes en soporte papel y electrónicos; asimismo regula la guarda automática de documentos generados en Módulo GEDO en Repositorio Único de Documentos Oficiales (RUDO) de GDE así como también regula el Procedimiento de digitalización de documentos originales en soporte papel y el Procedimiento de guarda temporal, archivo y recuperación de expedientes electrónicos.
- Resolución SMA 32/2017 (28/3/2017) regula el procedimiento de depuración de actuaciones administrativas con vencidos plazos de guarda y evaluación de valor histórico de documentos o expedientes digitalizados.
- Resolución SMA 48/2017 (07/6/2017) designa funcionarios responsables de los organismos de rehabilitar los expedientes electrónicos con guarda temporal en el sistema de Gestión Documental Electrónica.
- Resolución SMA 7/2018 (6/2/2018) establece la Tabla de Plazos Mínimos de Conservación y Guarda de Actuaciones Administrativas de veinticuatro trámites, para expedientes en soporte papel y electrónico

- Resolución SMA 9/2018 (16/2/2018) regula la Tabla de Plazos Mínimos de Conservación y Guarda de Actuaciones Administrativas de nueve trámites, para expedientes en soporte papel y electrónico.
- Resolución SMA 18/2018 (26/2/2018) establece el qué y el cómo del Procedimiento de Digitalización de Documentación Administrativa por Lotes en soporte papel para su archivo electrónico en RUDO.
- Resolución SMA 47/2018 (7/5/2018) establece la “Tabla de Plazos Mínimos de Conservación y Guarda de Actuaciones Administrativas de veintiocho trámites de la Agencia de Administración de Bienes del Estado” - Decreto 1131/2016, para expedientes en soporte papel y electrónico”.

La gestión de documentación electrónica GDE junto al portal de Trámites a Distancia (TAD) –Decreto 1063/2016– vienen transformando el modo de relación entre la ciudadanía y el Estado, por cuanto, simplifican trámites que ahora pueden hacerse online, acortando tiempos y distancias.

La normativa de la Legislación Archivística descrita completa digesto de legislación archivística argentina que adolecía de una regulación completa en materia archivística; no obstante, como la implementación viene desarrollándose de forma dinámica, la legislación archivística también queda incompleta a medida que se van implementando nuevas fases del proceso de modernización del Estado.

Protección del Patrimonio Cultural Documental en la Legislación de Archivos

En la Constitución Nacional encontramos en su artículo 41 la preservación y protección del patrimonio ambiental y cultural, dentro del cual interpretamos incluido al patrimonio cultural documental. Este artículo fue incorporado en la Reforma Constitucional de 1994. Hacemos nuestras las enseñanzas de Federico Justiniano Robledo quien explicaba que *“la cultura, en su perfil específico de tutela del patrimonio cultural, recién cuenta con una preceptiva constitucional expresa a partir de la segunda mitad del siglo XX, como un singular aporte del derecho constitucional occidental, que viene produciéndose desde la segunda posguerra”* (Robledo, Federico J. 1998:711). Identificar al patrimonio documental en este artículo tiene una gran importancia práctica, la supremacía constitucional a la vez que su reconocimiento como derecho y su consecuente protección y garantía.

La preservación y protección del patrimonio cultural documental tiene principios jurídicos, el principio de precaución y el principio de prevención que actúan en forma previa a la producción o no de un daño. La protección cultural documental también es una expresión de la soberanía cultural de cada Nación que abarca todos sus soportes (Robledo, Diego 2007).

Luego, en la legislación infraconstitucional encontramos la Ley Nacional N°15.930 junto a una serie de decretos reglamentarios y resoluciones establecen el marco normativo de nuestro Archivo General de la Nación.

El Archivo General de la Nación tiene por finalidad “reunir, ordenar y conservar la documentación que la ley le confía, para difundir el conocimiento de las fuentes de la historia argentina” (art. 1). Y entre sus funciones

- a) Mantener y organizar la documentación pública y el acervo geográfico y sónico, perteneciente al Estado Nacional, y que integren el patrimonio del Archivo, o la documentación privada que le fuera entregada para su custodia, distribuyéndola en las secciones que se estimen más adecuadas para su mejor ordenamiento técnico.
- b) Ordenar y clasificar con criterio histórico dicha documentación y facilitar la consulta de sus colecciones.
- c) Inventariar, catalogar y divulgar los documentos que están bajo su custodia.
- d) Publicar repertorios y series documentales para la difusión de los documentos que poseen reconocido valor.
- e) Difundir por cualquier otro medio el conocimiento del material existente en el Archivo.
- f) Preparar un inventario de los fondos documentales que se refieran a la historia de la República.
- g) Obtener copias del documental conservado en los archivos oficiales de las provincias o del extranjero, en cuanto interese para el estudio de la historia nacional y entregarles a su vez, copia del material que conserve y reúna” (art.2).

Y asimismo, esta ley nacional crea con autonomía una Comisión Nacional de Archivos en relación a los archivos históricos.

Esta Ley Nacional establece en su artículo 16 el concepto de documento histórico estableciendo que son:

- a) “Los de cualquier naturaleza relacionados con asuntos públicos, expedidos por autoridades civiles, militares o eclesiásticas, ya sean firmados o no, originales, borradores o copias, como así también sellos, libros y registros y, en general, todos los que hayan pertenecido a oficinas públicas o auxiliares del Estado y tengan una antigüedad no menor de treinta años.
- b) Los mapas, planos, cartas geográficas y marítimas con antigüedad de por lo menos cincuenta años.
- c) Las cartas privadas, diarios, memorias, autobiografías, comunicaciones y otros actos particulares y utilizables para el conocimiento de la historia patria.
- d) Los dibujos, pinturas y fotografías referentes a aspectos o personalidades del país.

- e) *Los impresos cuya conservación sea indispensable para el conocimiento de la historia argentina.*
- f) *Los de procedencia extranjera relacionados con la Argentina o hechos de su historia, similares a los enumerados en los incisos anteriores”.*

Y en consecuencia, establece que los “documentos de carácter históricos son de interés público y no podrán extraerse del territorio nacional sin previo dictamen favorable del Archivo General de la Nación”.

Asimismo, entre la legislación nacional de archivos se encuentra entre otras (Casareto, Laura y Pene, L 2017):

- a) *Normas que regulan archivos en relación a la vida política* como son la Ley Nacional N° 24.905 crea el Museo, Biblioteca y Archivo del Trabajo y del Movimiento Obrero Argentino, como también el Sistema Nacional de Museos y Archivos Presidenciales por Decreto Nacional N°209/1999 con información referida a presidentes a partir de 1983. También el Archivo Nacional de la Memoria instituido por Decreto Nacional 1259/2003.
- b) *Normas que regulan documentos audiovisuales* como por ejemplo, la Ley 23820 que establece el régimen legal de toda la documentación audiovisual emitida por los canales de televisión del país, cuyo art. 1 encarga al Archivo General de la Nación la recuperación de la memoria audiovisual del pueblo argentino con el deber de conservación de la documentación fílmica y televisa y la Ley Nacional 25.119 –reglamentada por Decreto Nacional N° 1.209/2010 establece la Cinemateca y archivo de la imagen nacional (CINAIN), con la función de reunir, registrar y difundir el patrimonio fílmico nacional.
- c) A este marco jurídico se integran *normas de preservación y protección cultural* como la Ley Nacional 25.197 en relación al Registro Nacional de Bienes Culturales que en su artículo 2° incluye a los documentos de archivo y la Ley Nacional N° 25.750 sobre preservación de bienes y patrimonios culturales fijando como política pública la preservación del patrimonio antropológico, histórico, artístico, y cultural.
- d) *En relación a la educación*, ubicamos la Ley Nacional 26.917 que crea el Sistema Nacional de Bibliotecas Escolares y Unidades de Información Educativas, por cuanto establece condiciones de los archivos escolares. También la Ley de Educación Superior, referida a las Universidades que con su autonomía universitaria deben tener archivo adecuado. Vale señalar que entre las Universidades argentinas encontramos algunas con más de 400 años como es la Universidad Nacional de Córdoba, declarada Patrimonio Cultural de la Humanidad por UNESCO.

- e) Especial consideración merecen las *Historias Clínicas e Historias Clínicas Electrónicas*, diferenciadas en base a su soporte, ya sea físico (en papel, escrito a mano) o bien electrónico o informático, que regula la Ley Nacional N° 26529/2009 (Cap. IV. Arts. 12-21). Como advierte Rosa Avila Paz de Robledo, en el caso de la historia clínica digital, requiere firma digital, conforme la Ley 25.506 y art. 288 del Código Civil y Comercial de la Nación (2019:53-80).
- f) *Normas en relación al registro de documento electrónico, digitalización y microfilmación*: además de las que hemos desarrollado en los apartados anteriores, agregamos que a partir del Decreto Nacional N° 1131/2016 se crea el Registro Único de Documentos Oficiales con el propósito de centralizar, contener y conservar todos los documentos electrónicos del Sistema de Gestión de Documentación Electrónica. En este punto, nos remitimos a lo expuesto en el apartado anterior.

Aquí respecto a la digitalización conviene tener presente como en la Microfilmación de documentos –Ley Nacional 18.569/1970 reglamentada por Decreto 385/1970– que deben tener igual valor probatorio cuando sigue las pautas de validez de microfilmación. Asimismo, como advierte Vicent Giménez-Chorner “*el proceso de digitalización requiere de un proyecto mucho más complejo que no se trata en la norma jurídica, pero que la norma ISO 13028 desarrolla con más detalle en las Directrices para la implementación de la digitalización de documentos*” (2017:27).

Todos estos conforme a su tutela constitucional como patrimonio cultural requieren pensar –como apunta Anna Slejcher– en una estrategia de preservación de los documentos digitales a partir de la “*existencia de un sistema de evaluación y selección de documentos administrativos, en el contexto de un sistema integral de gestión documental, que permita identificar los documentos de conservación permanente y establecer las características de su creación, utilización y disposición*” (2016:96).

En la *legislación provincial*, encontramos algunas provincias con normativa específica de Archivos:

- San Juan, Ley N°5307/1984
- Chaco, Ley N°3123/1985.
- Neuquén, Ley N°1732/1987.
- Santa Fe, Ley N°10870/1992.
- Salta, Ley N°7092/2000.
- Tierra del Fuego e Islas del Atlántico Sur, Ley N°714/2006.
- La Rioja, Ley N°10080/2018.

Entre ellas, la ley riojana establece la digitalización como uno de los objetivos del Sistema Provincial de Archivo. Entre la legislación de Córdoba destacamos la creación del Registro de Comunidades de los Pueblos Indígenas de la Provincia, como una innovación provincial por Ley Provincial 10316 del año 2015. Asimismo, todas las provincias tienen un archivo histórico.

Una característica común es que el avance en materia de legislación archivística nacional debe reflejarse en forma jurídica y tecnológicamente interoperable.

En un balance general aún no hay un sistema nacional de archivo (SWIDERSKI, Graciela 2014:219), lo que ha dado lugar a una mayor autonomía provincial respecto de su regulación que han instituido innovadores sistemas provinciales de archivo antes que la Nación; sin embargo, a través de la implementación del Sistema de Gestión de Documentación Electrónica se están generando puentes para hacerlo interoperable y accesible.

Proceso constitucional Habeas Data

El Habeas Data es un proceso constitucional cuyo objeto de tutela es la autodeterminación informativa (Avila Paz de Robledo, Rosa A. 2002:24), *“el objeto tutelado coincide globalmente con la intimidad o privacidad de la persona, ya que todos los datos a ella referidos que no tienen por destino la publicidad, o la información a terceros, necesitan preservarse”* como explica Germán Bidart Campos (2001:387-389). Como garantía constitucional y convencional se encuentra reconocida en nuestra Carta Magna (art. 43). Vale señalar que por su naturaleza de garantía de derechos humanos fundamentales su tutela es evolutiva e irradia su proyección en todas las manifestaciones vitales como persona. Por ello, se ha reconocido el derecho a la intimidad, a la protección de datos personales y sensibles, a la privacidad, a acceder, suprimir, rectificar, agregar datos, a ser informado y oponerse al tratamiento de los datos, entre otras manifestaciones (BAZAN, Víctor 2005). En algunos horizontes jurisprudenciales se advierte también comprende el derecho a la verdad y el derecho al olvido (Vgr. Tribunal Europeo de Derechos Humanos, *“Costeja vs Google”* <https://www.abogacia.es/wp-content/uploads/2014/05/Sentencia-131-12-TJUE-derecho-al-olvido.pdf>).

Asimismo, el Habeas Data puede ser interpuesto en forma individual o colectiva, puede asumir una finalidad preventiva o reparadora (Puccinelli, Oscar 2019:1).

En nuestra opinión, a partir de la era digital consideramos que debe incluir el control sobre el algoritmo computacional que se genera a partir de nuestra información.

Inteligencia Artificial, Blockchain, Big Data y Data Science

En este proceso advertimos cuatro conceptos necesarios para repensar la teoría y praxis de la gestión documental electrónica sostenible.

1. Inteligencia artificial

La inteligencia artificial es un campo de la ciencia, que permite desarrollar una meta en la menor cantidad de acciones posible. También se ha dicho que es *“una rama de las ciencias de la computación que se ocupa de la comprensión, desde el punto de vista informático, de lo que se denomina comúnmente comportamiento inteligente”* (Rainer Granados, José J. y Rodríguez Baena, Luis 2019:16) y que *“trabaja en diferentes campos como la representación del conocimiento, búsqueda heurística, procesamiento de lenguaje natural, aprendizaje automático y, en sus comienzos, en el desarrollo de sistemas expertos”* (Ibidem, 2019:24).

En Argentina ya se ha introducido softwares que reemplazan algunas tareas o empleos. Por ejemplo, en junio de 2019, *“Laura empezó a trabajar en el Ministerio de Finanzas de la Provincia de Córdoba. Tiene casilla de correo electrónico, nombre de usuario y clave para hacer trámites, pero no es una persona sino un robot virtual. En rigor, se trata de un software que incorporó el organismo hace un par de meses y que se programa por única vez para hacer una determinada tarea. En general, son procesos rutinarios y repetitivos, de bajo valor agregado para una persona. Ya comenzó a ser usado en un trámite y, en un par de meses, se sumarán otros 67. Pero la potencialidad es mucho mayor”* (<https://www.lavoz.com.ar/politica/robot-laura-ya-trabaja-en-ministerio-de-finanzas>). De ello, se puede pensar en los modelos organizacionales del ámbito público y privado y su transformación que experimenta en nuestra época, “Estado Digital”, “E-Commerce”, por citar algunos ejemplos. Una de sus potencialidades estriba en la reducción de tiempos y costos.

Al respecto, Romina Cabrera advierte que *“la relación entre la Inteligencia Artificial y el Derecho es antigua. Desde el punto de vista de su uso, el derecho mismo (sus categorizaciones, sus procedimientos, sus prácticas), constituyen una tecnología cognitiva, un modo de aproximarse a la realidad social, para controlarla, dirigirla, y hacer efectivos en ella determinados planes y modelos sociales, económicos y políticos”* (2018:85-94). En este sentido, el sistema jurídico puede perfeccionarse a partir de sus operadores.

2. Blockchain

Blockchain es una tecnología de bases de datos descentralizada, es decir que, *“los registros allí almacenados no están sujetos a una autoridad central que pueda decidir sobre la eliminación o modificación de ningún registro. Blockchain distribuye registros (que pueden representar transacciones o datos de muy variadas temáticas) entre muchos*

equipos pertenecientes a diferentes personas. Mientras más variadas son las manos que poseen esos equipos más confiable es una red de computadoras almacenando una cadena de bloques (blockchain) (...) Debido a que con la tecnología de hoy no es posible adulterar una cadena de bloques estas pueden ser muy útiles para grabar registros que persistan en el tiempo y no sean modificables. Blockchain se presenta como una buena opción para certificar la inmutabilidad de registros” (Cfr. <https://gobiernoabierto.cordoba.gov.ar/blockchain/>).

Melo explica que “Blockchain opera como un libro público de transacciones que depende sustancialmente de los usuarios para el envío de contenido, verificación y actualización de la información. Se trata de un sistema descentralizado de verificación de transacciones, sin un órgano que sirva de autoridad central. El sistema se utiliza para grabar todas las operaciones realizadas, garantizando que no sean duplicadas, tampoco borradas, por no ser de propiedad de un determinado órgano. Así, la invención de Blockchain representa un sistema completamente nuevo, que permitirá un ecosistema tan amplio y diverso como la propia Internet” (Ibidem).

De esta manera en la República Argentina el Boletín Oficial ya publica los registros de cada edición, al igual que lo hace la Provincia de Córdoba con su Boletín Oficial, la Municipalidad de Córdoba con su Boletín Municipal, o la Comisión Nacional de Energía de Chile.

Blockchain se presenta como una alternativa eficaz y de acceso abierto, que permite una gestión documental electrónica con validez probatoria. Es menos costosa que la firma digital y permite la integridad y recuperación del documento con validez probatoria.

3. Big data y Data Science

Se ha previsto que para el año “2025 cada habitante del planeta produciría 62 gigabytes (GB) de información, por lo que, si se utilizaran discos versátiles digitales (DVDs) para almacenar los datos de un día de la humanidad, se requeriría una pila de 100 mil kilómetros de altura. Esta dinámica, ha conducido a que las compañías cambien la forma de cómo guardan la información. Por ejemplo, Amazon ha diseñado una especie de camiones que pueden almacenar hasta 10 terabytes (TB) de información y les lleva 10 días llenar dicha capacidad; por lo que, con 30 camiones se podrían haber almacenado los datos que se generaban en 2012 en un día en todo el mundo” (KO-SINSKI, Michael 2017).

Un sistema Big Data se caracteriza por “su capacidad relacionada con el volumen de la cantidad de datos para almacenar y procesar; la velocidad de transformación de los datos en información útil en el menor tiempo posible; la variedad de datos que un sistema de Big Data procesa y la heterogeneidad de sus formatos (bases de datos, HTML, XML, texto plano, imágenes, video, audio, código fuente, etc.); la veracidad de los datos y el valor del sistema Big Data en sí mismo, esto es, su capacidad para obtener valor de todos los datos disponibles a través de un almacenamiento y

procesamiento eficiente y al menor coste posible” (<http://oiprodat.com/declaracion-de-mexico-d-f/>).

Entre el Big Data y el Acceso Abierto la gestión de documentos electrónicos y repositorios facilitan *“a la implementación de la accesibilidad y a la información contenida en los documentos públicos. La única restricción sobre la distribución y reproducción es dar al autor el control sobre la integridad de su trabajo y el derecho a ser adecuadamente reconocido y citado, esto a partir de Budapest Open Access Initiative”* (Andrada, Roberto L. 2016:64).

Las huellas digitales que dejamos en internet (HUESO, Lorenzo 2017:131-150) y en los artefactos tecnológicos pueden ser empleados para desarrollar algoritmos computacionales que pueden poner en jaque la autonomía informativa de cada persona así como los modelos de seguridad de protección de datos que se genera en las plataformas de documentación electrónica.

Reflexiones y conclusiones

En este artículo hemos abordado el Documento Electrónico en el Gobierno Abierto de la República Argentina y nos hemos planteado las bases hacia un sistema de gestión sostenible con tutela constitucional, convencional y procesal de la protección de datos personales y acceso a la información pública. Hemos trabajado con un diseño exploratorio, procurando sistematizar un plexo normativo disperso y difuso, sobre la base de un nuevo fenómeno jurídico y archivístico que viene de mano de las nuevas tecnologías y en las que hemos identificado su tutela constitucional y convencional.

Consideramos que en un Estado de Derecho Constitucional y Convencional que avanza hacia el Gobierno Abierto es necesario que se garantice la protección de los datos públicos, privados y sensibles. Vale señalar que en aras de la construcción de un Gobierno Abierto en el que se publican datos debe resguardarse la tutela de los datos personales, privados y sensibles. La política pública de comunicación debe observar el standard de la intimidad y privacidad. Los profesionales que administran documentos y archivos tienen en ello un deber normativo y deontológico como garantía de la información que custodian. Más aún velar también por la preservación y conservación de la documentación que asegure su recuperación con calidad e integridad.

Las dimensiones pública y privada, cuya frontera limítrofe pareciera haberse desdibujado con la globalización, hoy se erige en categorías relevantes respecto a qué dato publicar para evitar que sean vulnerados los derechos humanos. Sin duda el impacto de las tecnologías, nuevas formas de información y comunicación impactan en el proceso de gestión de los archivos, así como nos atraviesan como sociedad y nos interpelan.

Se nos plantean tres desafíos. Un *desafío conceptual* sobre el cual es importante apreciar que la ley y política pública de información y gobierno abierto requiere un lenguaje adecuado a los fines que proyecta, y ello nos interpela hacia una redefinición conceptual y nuevos paradigmas. Como se estableció en el *Congreso Internacional de la Lengua Española* organizado por la Real Academia Española en Argentina en 2019, debemos procurar un lenguaje jurídico claro y para ello consideramos oportuno trabajar sobre el vocabulario que permita un punto de encuentro entre las disciplinas que intervienen en el proceso. La modernización requiere replantear muchos de los conceptos clásicos ante los nuevos desafíos. No sólo surgen una nueva manera de comprender la Archivística, un paradigma que supera la mirada acerca del soporte, es un nuevo modo de ser y hacer, en el que documentos electrónicos son generados en un sistema y requieren ser pensados y desarrollados de un modo fiel a su naturaleza ontológica.

Un *desafío tecnológico*, a través del cual advertimos que el Sistema de Gestión de Documentación Electrónica y la plataforma de Trámites a Distancia vienen transformando el modo de relación entre la ciudadanía y el Estado, por cuanto, simplifican trámites que ahora pueden hacerse online, acortando tiempos y distancias. Se vienen incorporando las inteligencias artificiales, el blockchain, el *big data* y la *data science*. A través del diseño de estrategias inteligentes la tecnología debe contribuir a reducir los costos y los impactos ambientales, preservando y protegiendo el patrimonio documental electrónico, contribuyendo a un sistema de gestión documental sostenible. También es un nuevo desafío la administración de documentos y archivos de nuevos usuarios y operadores del sistema como son los que vienen a través de la inteligencia artificial, como hemos referenciado, empleados robots y softwares con un legajo propio dentro de la Administración Pública. Para ello, es necesario contar con herramientas adecuadas pero también con la continua capacitación de los profesionales.

Un *desafío jurídico*, que además del lenguaje jurídico claro, también se debe legislar normas integrales y ejecutar políticas públicas con la participación de las distintas disciplinas para diseñar un sistema de gestión documental electrónico sostenible, accesible, interoperable, inclusivo y garantista. Hoy más que nunca en un proceso de gobierno abierto es necesario pensar en voz alta las garantías de derechos humanos tan vitales como son la intimidad, la autodeterminación informativa.

El Habeas Data es un proceso constitucional que puede ser interpuesto en forma individual o colectiva y en forma preventiva o reparadora. Apuntamos a fortalecer las garantías fundamentales de las personas en estos procesos. Creemos que es necesario fortalecer las garantías de los más vulnerables de este proceso. Para que el gobierno abierto electrónico cumpla su cometido de multiplicar la participación ciudadana es necesario (re)pensar en accesos inclusivos y sostenibles, teniendo en cuenta entre otros los derechos de los pueblos indígenas y los

derechos de las personas con discapacidad, los derechos de niños, niñas y adolescentes, pacientes, entre muchos otros. En nuestra cultura jurídica el archivo se relaciona con el valor seguridad jurídica.

Entre las rupturas que plantea Internet surge un nuevo fenómeno jurídico archivístico, el metadato. Cuya regulación CKAN (dublin core <http://dublincore.org/> y dcat <http://www.w3.org/TR/2013/WD-vocab-dcat-20130312/>) debe permanecer en construcción. Sin duda esta es una realidad que impacta en el Archivo, en tanto, forma parte de un sistema de gestión de documentación electrónica interoperable y conectado en red con todos los todos del todo social.

Abogamos por una gestión humanista de los archivos que tutele en forma integral las garantías y derechos humanos fundamentales.

Bibliografía

- ANDRADA, Roberto L. (2016) “Accesibilidad a la información registrada en los documentos de la Administración Pública de la provincia de Córdoba” en *Ágora*, Universidad Nacional de La Rioja, Argentina, Vol. 1 N°1, pp. 63-79. Accedido en <https://revistaelectronica.unlar.edu.ar/index.php/agoraunlar/article/view/258/249>.
- ANDRADA, Roberto L. (2018) “Los archivos no están actuando como un sistema de información coordinado en pos de un objetivo común” en *Archivos*, España, accedido en <https://www.archivos.es/entrevista-a-roberto-lucas-andrada/>
- AVILA PAZ DE ROBLEDO, Rosa A. (2002) “Amparos especiales, Habeas Data, Amparo Electoral, Amparo Fiscal, y Amparo por Mora de la Administración” *Revista de Direito Processual Civil- Genesis*, Brasil, Año VII, N°24.
- AVILA PAZ DE ROBLEDO, Rosa A. (2009) “La Firma Digital en la Justicia de Argentina” en *Revista de Derecho Procesal*, España, N° 1, 2009 [Ejemplar dedicado a: Homenaje al profesor Pedro Aragoneses Alonso], pp. 17-55.
- AVILA PAZ de ROBLEDO, Rosa A. (2012) “La Persona Humana y el Bien Común en el Siglo XXI. La tutela jurídica de Internet y las nuevas tecnologías desde el humanismo de Jacques Maritain” en Jorge H. Gentile (Director) *La Persona humana y el Bien común*, Ed. Alveroni, Córdoba.
- AVILA PAZ DE ROBLEDO, Rosa A. (2016) “Gobierno Judicial Abierto” en “*Simposio Internacional Gobierno Judicial Abierto y la Opinión Pública en la Era Digital*”, celebrado en la Facultad de Derecho de la Universidad Nacional de Córdoba, 14 de junio de 2016, declarado de interés académico por Res. Dec.755/2016 y declarado directora a la Prof. Dra. Rosa A. Avila Paz de Robledo y Res.Dec. 786/2016 declarando huésped de honor al Prof. Dr. Robert Yale Shapiro (Universidad de Columbia, Estados Unidos).
- AVILA PAZ DE ROBLEDO, Rosa A. (2019) “Los derechos de los usuarios de salud y la historia clínica – con particular referencia a la historia clínica informatizada” en *Anuario XVII*, Centro de Investigaciones Jurídicas y Sociales de la Facultad de Derecho de la Universidad Nacional de Córdoba, Ed. Advocatus, Córdoba, Argentina.

- AVILA PAZ DE ROBLEDO, Rosa A. y ROBLEDO, Federico Justiniano (2002) “La Región en nuestra Organización Federal” *Cuaderno de Federalismo*, Instituto de Federalismo de la Academia Nacional de Derecho y Ciencias Sociales de Córdoba, Editorial Advocatus, Córdoba, Argentina, Vol. XV, pp. 99-106
- AVILA PAZ DE ROBLEDO, Rosa Angélica del Valle; ROBLEDO, Diego (2019) “Oficio Judicial Electrónico: su valor probatorio informativo en el Gobierno Abierto Judicial” en Lorenzo Bujosa-Vadell (director) *En torno a la Prueba y al Proceso*, Ed. Comares, España.
- BAZÁN, Víctor (2005) “El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado” *Estudios Constitucionales*, Chile, vol. 3, N° 2.
- BELLIX, Laila; GUIMARÃES, Caroline Burle S.; MACHADO, Jorge (2017) “Qual conceito de Governo Aberto? Uma aproximação aos seus princípios” *GIGAPP Estudos Working Papers*, vol. 4, no 55-59, p. 78-91.
- BIDART CAMPOS, German (2001) *Manual de la Constitución Reformada*, Ediar, Buenos Aires, Argentina.
- BORRMAN, Rudi (2017) “Un Estado abierto para el Siglo XXI” en *III Plan Nacional de Gobierno Abierto en la República Argentina 2017-2019*, Ministerio de Modernización de la Nación, Buenos Aires, Argentina.
- BOURDIN, María (2016) “Qué es el Gobierno Abierto Judicial” en sitio oficial de la Corte Suprema de Justicia de la Nación <https://www.csjn.gov.ar/> (consulta 14/03/2016).
- BUNGE CAMPOS, Luis María (2015) “Jueces y redes sociales: perspectiva desde la ética judicial” en *ÉTICA JUDICIAL Cuaderno 7*, Costa Rica, Vol. 4, N° 2, octubre de 2015, p. 6 accedido en el sitio del Poder Judicial de Costa Rica <http://www.poder-judicial.go.cr/eticayvalores/> (consulta 14/03/2019).
- CABRERA, Romina Florencia (2018) “Inteligencia artificial y su impacto en la justicia” en *Informática y Derecho: Revista Iberoamericana de Derecho Informático* (segunda época), N° 5, España, pp. 85-94.
- CASARETO, Laura; PENE, L. (2017) “Legislación archivística nacional, provincial y universitaria. Las consecuencias del decreto de modernización del Estado” en II Encuentro de Archivos Universitarios, 22 al 24 de mayo de 2017, La Plata, Argentina. En Memoria Académica, Argentina, en http://www.memoria.fahce.unlp.edu.ar/trab_eventos/ev.8746/ev.8746.pdf
- CKAN (dublin core <http://dublincore.org/> y dcat <http://www.w3.org/TR/2013/WD-vocab-dcat-20130312/>)
- DEVOTO, Mauricio (2001) *Comercio electrónico y Firma Digital. La regulación del Ciberespacio y las estrategias globales*, Ed. La Ley, Buenos Aires, Argentina.
- GIMENEZ-CHORNET, Vicent (2010) La innovación en los archivos. VIII Congreso de Archivología de Mercosur. Montevideo (Uruguay), 17-20 de noviembre de 2009. Publicado en Revista de ANABAD (LX, 2010) CD anexo, pp. 132-144 accedido en <http://www.vicentgimenez.net/curri/innovacion.pdf> (10-07-2019)
- GIMENEZ-CHORNET, Vicent (2017) *Legislación de Archivos*, Ed. UOC, España, 2017.
- HUESO, Lorenzo Cotino (2017) “Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales” *Dilemata*, 2017, N°24, p. 131-150.

- KOSINSKI, Michael (2017) “Big data, inteligencia artificial y el futuro de la democracia” en Senado de la República de México, 2017 accedido en <http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/3499/1%20Publicacion%20Aportes%20al%20debat%20e%20parlamentario%204%20Big%20data.pdf?sequence=35&isAllowed=y>
- OTERO, J. Manuel (2017) *Investigación jurídica. El arte de escribir una investigación jurídica*. Editorial: Ministerio de Justicia y Derechos Humanos de la Nación, Id SAIJ: LB000225, Argentina.
- PAK LINARES, Andrés “El Sistema de Gestión Documental Electrónica (GDE) y la Evaluación documental. El rol y las acciones del Archivo General de la Nación de Argentina” en https://www.uned.ac.cr/actividades/images/sellar/memoria/Andr/C3/A9s_Pak_-_Argentina.pdf Fecha de acceso: 20/09/2018
- PUCCINELLI, Oscar R. “Tipos y subtipos de hábeas data en América Latina” Cuaderno de Derecho Público, 2019, N° 1.
- RAINER GRANADOS, José J. RODRÍGUEZ BAENA, Luis “Perspectiva histórica y evolución de la inteligencia artificial” (2019) en Instituto Español de Estudios Estratégicos *La inteligencia artificial aplicada a la defensa*, Ministerio de Defensa, España.
- ROBLEDO, Diego (2007) “La Protección de la Cultura en las Relaciones Internacionales” Primer Premio Concurso de Monografías 2007, convocado por el INSTITUTO DE FEDERALISMO y el INSTITUTO DE DERECHO INTERNACIONAL PÚBLICO Y DERECHO DE LA INTEGRACIÓN de la Academia Nacional de Derecho y Ciencias Sociales de Córdoba, y las Filiales Córdoba del CONSEJO ARGENTINO PARA LAS RELACIONES INTERNACIONALES (CARI) y del INSTITUTO ARGENTINO CHILENO DE CULTURA y de la ACADEMIA DEL PLATA, sobre: “La Cultura en las Relaciones Internacionales”.
- ROBLEDO, Diego et.al. (2009) “La inclusión de los Fondos Bibliográficos Antiguos en la Difusión del Patrimonio Cultural. Su marco jurídico” en I Jornadas La Universidad en la Sociedad, Aportes de la investigación de la Universidad Nacional de Córdoba para el diseño de Políticas Públicas, [Sección 11, Políticas Culturales], Compiladoras: María C. Mata y Nora Aquin, CD editado por la Universidad Nacional de Córdoba, Argentina.
- ROBLEDO, Federico Justiniano (1998) “Educación y cultura en la Constitución Nacional y en la Constitución de la Provincia de Córdoba”, *Semanario Jurídico, Fallos y Doctrina*, Ed. Comercio y Justicia S.A., Córdoba, 1998-A, 1998, T.78
- ROBLEDO, Federico Justiniano (2003) “La necesaria revitalización del federalismo argentino” en *Homenaje al sesquicentenario de la Constitución Nacional: 1853-2003*, Academia Nacional de Derecho y Ciencias Sociales de Córdoba, Ed. Advocatus, Córdoba, Argentina.
- ROBLEDO, Federico Justiniano (2006) “El Sistema Federal Argentino” *Revista del Instituto de Ciencia Política y Derecho Constitucional “Reforma y Procesos Constitucionales”*, año XII, N° 7, Huancayo, Perú, Ed. Gráfica Palomino, pp. 154-172
- SLEJCHER, Anna (2016) *Protección del Patrimonio documental argentino. La incidencia de la legislación sobre los documentos digitales*, Ed. Corintios, Córdoba, Argentina.
- SWIDERSKI, Graciela (2015) *Las huellas de mnemosyne. La construcción del Patrimonio Documental en la Argentina*, Ed. Biblos, Buenos Aires, Argentina.

Constitución Nacional de la República Argentina
Código Civil y Comercial de la Nación
Ley Nacional N° 15.930.
Ley Nacional N° 19.546 de Procedimiento Administrativo. Decreto 378/2005 (B.O. 28/04/2005).
Ley Nacional N° 23.820.
Ley Nacional N° 24.905.
Ley Nacional N° 25.119.
Ley Nacional N° 25.197.
Ley Nacional N° 25.506.
Ley Nacional N° 25.750.
Ley Nacional N° 25.326 de Protección de datos personales, Habeas Data.
Ley Nacional N° 26.032.
Ley Nacional N° 26.529/2009.
Ley Nacional N° 26.685.
Ley Nacional N° 26.917.
Ley Nacional N° 27.275 de Derecho de Acceso a la Información Pública; Decreto N° 561 (06/04/2016).
Plan Nacional de Gobierno Electrónico y planes sectoriales del Gobierno Electrónico; Decreto 117/2016;
Reglamento de Procedimientos Administrativos Decreto 1759/72 T.O. 2017; Decreto Nacional N° 209/1999.
Decreto Nacional N° 1259/2003.
Decreto Nacional N° 1.209/2010.
Decreto Nacional N° 434/2016.
Decreto Nacional N° 1131/2016.
Decreto Nacional N° 27/2018.
Res. E. 44/2016.
Res. E. 32/2017.
Resolución 538/2013 Sistema Nacional de Datos Públicos;
Decreto 1131/2016.
Resolución SMA 7/201.
Resolución SMA 44/2016
Resolución SMA 32/2017
Resolución SMA 48/2017
Resolución SMA 7/2018
Resolución SMA 9/2018
Resolución SMA 18/2018
Resolución SMA 47/2018
Ley Provincial de San Juan N°5307/1984.
Ley Provincial de Chaco N°3123/1985.
Ley Provincial de Neuquén N°1732/1987.
Ley Provincial de Santa Fe N°10870/1992.
Ley Provincial de Salta N°7092/2000.
Ley Provincial de Tierra del Fuego e Islas del Atlántico Sur, Ley N°714/2006.

Ley Provincial de Córdoba Ley N°10316/2015.

Ley Provincial de La Rioja, Ley N°10080/2018.

Otras fuentes

<http://oiprodat.com/declaracion-de-mexico-d-f/>

<https://datos.gob.ar/acerca/seccion/Glosario>

<https://gobiernoabierto.cordoba.gob.ar/blockchain/>


<https://www.lavoz.com.ar/politica/robot-laura-ya-trabaja-en-ministerio-de-finanzas>

<https://datos.gob.ar/acerca/seccion/Glosario>

Tribunal Europeo de Derechos Humanos, “Costeja vs Google” <https://www.abogacia.es/wp-content/uploads/2014/05/Sentencia-131-12-TJUE-derecho-al-olvido.pdf>

**OPEN
RANGE**





**A LOS VOLUNTARIOS DE LAS
BRIGADAS INTERNACIONALES
22-X-2011**

*Sois la historia, sois la leyenda,
sois el ejemplo heroico de la solidaridad
y de la universalidad de la democracia*

Dolores Ibaruri (1-XI-1938)



FRANCISCO JAVIER FITO MANTECA

La Sección Histórica de las Brigadas Internacionales

los archivos al servicio de la
propaganda y la memoria histórica

The Historical Section of
the International Brigades:

the archives at the service of propaganda
and historical memory

Francisco Javier Fito Manteca
fjavier.fito@cultura.gob.es
Centro Documental de la Memoria Histórica

Citación: Fito Manteca, Francisco Javier (2019). "La Sección Histórica de las Brigadas Internacionales: los archivos al servicio de la propaganda y la memoria histórica". *Tábula*, n. 22, pp. 141-162

Recibido: 13-10-2019. *Aceptado:* 17-11-2019

Resumen analítico / Analytic summary

La creación en 1937 de la Sección Histórica dentro de la estructura organizativa de las Brigadas Internacionales supuso la puesta en marcha de un servicio de documentación para apoyar la actividad de agit-prop del comisariado de guerra. Diferentes planes ideados por algunos de sus colaboradores, como *Schindler* y *Anger*, intentaron mejorar su capacidad de archivo de documentos, hasta llegar a proponer la creación de un Archivo Histórico.

BRIGADAS INTERNACIONALES | SECCIÓN HISTÓRICA | HISTORIA ARCHIVÍSTICA | PROPAGANDA | MEMORIA

The creation in 1937 of the Historical Section within the organizational structure of the International Brigades involved the launching of a documentation service to support the agit-prop activity of the political commissariat. Different plans devised by some of their collaborators, such as *Schindler* and *Anger*, tried to improve their document archiving capacity, until they came to propose the creation of a Historical Archive.

INTERNATIONAL BRIGADES | HISTORICAL SECTION | HISTORY OF ARCHIVES | PROPAGANDA | MEMORY

Cuando el intento

de golpe de Estado ocurrido en España en julio de 1936 derivó en una guerra civil de resultado incierto, la Komintern y los partidos comunistas de los diferentes países se comprometieron a alistar a voluntarios dispuestos a luchar a favor de la República Española y el antifascismo. La estructura de esa fuerza internacional comienza así a organizarse en octubre de 1936 con la llegada a España de los primeros reclutas, eligiéndose la ciudad de Albacete como lugar para concentrar y preparar a estas unidades militares de nueva creación.

El reto desde el punto de vista organizativo era enorme puesto que sus promotores debían gestionar una tropa babelizada y necesitada de instrucción, procedente de más de 50 países, de diferentes lenguas y culturas, y en un ambiente de desorden y precipitación a causa de las urgencias de la guerra –Madrid estaba en esos momentos amenazado y su caída en manos de las tropas franquistas parecía inminente–. En la Base de Albacete, al mismo tiempo que se van conformando las brigadas que se desplazarán a Madrid y al resto de frentes, se ponen en pie toda una serie de servicios administrativos (intendencia, sanidad, correo, tesorería, etc.) y se ocupan varios edificios en la ciudad (cuartel de la Guardia Nacional, Banco de España...) y en localidades cercanas (Mahora, Madrigueras, Tarazona...), estableciéndose además delegaciones en Valencia, Alicante, Barcelona y Madrid.

El 14 de febrero de 1937, cuando llevaban ya varios meses en acción, se reunió en Albacete el Consejo Militar de las Brigadas Internacionales, con la presencia de los principales jefes de los servicios y departamentos que se habían ido conformando en la Base Militar de la ciudad manchega. En la reunión mencionada se analizó la situación y la evolución que había seguido desde su creación el contingente internacional. Se abordaron muchos temas, no tanto asuntos militares, como sí aspectos políticos y de gestión, debatiendo cuestiones como la

incorporación de soldados y cuadros españoles, la creación de una comisión de control administrativo o el salario que debían recibir los voluntarios. Se puso énfasis en potenciar la publicación de prensa periódica por parte de los diferentes batallones y brigadas, indicándose que ésta tendría que ajustarse a la línea política del Frente Popular y ofrecer material educativo a los camaradas comunistas; y se insistió además en la difusión de folletos y material de propaganda escrita *que hiciera de cada voluntario internacional un militante consciente del problema español*¹.

Llegados a este punto, Vidal, comandante de la Base –alias bajo el que se escondía el francés Vital Gayman– propuso que se incluyera en estas publicaciones contenidos atractivos: las pequeñas historias protagonizadas por los brigadistas, artículos sobre actos de heroísmo, etc. El Comisario Delegado Gallo incidió en el componente nacional, insistiendo en que cada nacionalidad debería recoger sus memorias y enfocarlas como ejemplo de la contribución de su pueblo a la lucha. En ese momento Vidal defendió la necesidad de narrar la historia y cuidar los archivos generales de las Brigadas Internacionales. Frans² propuso entonces la creación de una sección histórica encargada de recoger todos los periódicos y toda la documentación relacionada con las Brigadas Internacionales y de recabar de los comisarios políticos los documentos relevantes, debiendo destinarse a esa sección a voluntarios cualificados para la misión. Vidal propuso como archiveros a Nemov y a De Boeck e indicó que esa comisión histórica debería trabajar en colaboración con la Sección Política, bajo el control del jefe del Estado Mayor.

Antes de finalizar marzo, el belga Henri de Boeck sería asignado a la Sección Política de la Base con las tareas de editar diferentes boletines de información de prensa tanto española como extranjera y de confeccionar el diario de la Base, haciendo referencia a los documentos oficiales existentes en los archivos de la misma, con el permiso para extraer toda la información necesaria³.

El 2 de marzo Gallo, alias del dirigente del Partido Comunista Italiano Luigi Longo, desde su decisivo cargo de Comisario Delegado de Guerra-Inspector de las Brigadas Internacionales, comunicó en sendas circulares dirigidas a los diferentes comisarios políticos dependientes de él algunas de las decisiones tomadas en el Consejo Militar. En la primera les insistió en el deber de asegurar la edición regular y de calidad de los periódicos de las brigadas y los batallones por su gran importancia en el trabajo de orientación de los voluntarios. En la segunda les informó de la constitución en la Base de Albacete de la Sección Histórica⁴. La tarea de dicho servicio, en palabras de Gallo, sería la de recoger todo el material que pudiera servir a la historia de las Brigadas y en una segunda fase proceder al tratamiento y difusión de ese material. El contenido de la circular es toda una carta de fundación, en la que Gallo, tras exponer los motivos de su creación y justificar la aparición de la Sección Histórica como una labor *urgente y más que necesaria* para dar a conocer al mundo la experiencia sin precedentes de las Brigadas Internacionales, establece las pautas de su funcionamiento.

Según las instrucciones de Gallo, los comisarios políticos de cada brigada debían crear también una sección semejante en cada unidad que tendría que trabajar en la historia de la brigada respectiva y enviar a la Sección Histórica de Albacete copia de todo el material que pudiera interesar. El trabajo de estas diferentes secciones históricas en cada brigada –que podían estar compuestas en inicio por un solo camarada– debería comenzar con la recolección o copia de todos los documentos relevantes para confeccionar su historia: órdenes del día, diarios, periódicos, fotografías, etc. Tras el acopio de documentación, Gallo solicitaba a los comisarios la iniciativa de editar folletos que narrasen brevemente y de forma viva y atractiva la lucha llevada a cabo por cada brigada.

Al igual que ocurrió en el consejo mencionado celebrado en el mes anterior, Gallo volvió a insistir en esta circular sobre el tema nacional. Venía así de nuevo a afirmar que *era de la mayor importancia que cada nacionalidad, cada país, pudiera tener la historia de sus propios hijos que de forma tan alta estaban representados en la lucha en España*. Por ello instaba a sus comisarios políticos a prestar atención a las pequeñas nacionalidades que corrían el riesgo de ser ignoradas, algo que según sus palabras sería nocivo para el desarrollo del movimiento antifascista y popular en esos países.

Esta política no cayó en saco roto y desde entonces se prodigaron, perfeccionaron y regularizaron una serie de publicaciones periódicas, algunas de las cuales habían surgido ya en 1936, de forma que cada brigada y batallón comenzó a contar con su cabecera propia, como medio vehicular que hacía llegar a los voluntarios la información deseada en la lengua más frecuente según el componente nacional de las diferentes unidades. Cada brigada contaba con su órgano de expresión: *Pasaremos* (XI Brigada), *Il Garibaldino* (XII Brigada), *Venceremos* (XIII Brigada), *Le Soldat de la République* (XIV Brigada), *Our fight* (XV Brigada). También algunas unidades menores: *Vers la Liberté* (Batallón “A. Marty”), *El Fuego* (Batallón “Henri Barbusse”)... Por otra parte, *El Volontaire de la Liberté* se configuró como el órgano oficial de las Brigadas Internacionales en su conjunto, dirigido y controlado por el Comisariado de Guerra, encargado de dar las indicaciones políticas y militares generales⁵. A partir de marzo se editó en cinco lenguas: italiano, alemán, francés, inglés y polaco –*Dąbrowszczak*–; incluso llegó a publicarse, ya en noviembre, un número en albanés, *Vullnetari i Lirisë*, editado por Petro Marko y Skënder Luarasi.

Esta prensa escrita por los mismos protagonistas, reforzada con la elaboración de periódicos murales y la celebración de charlas políticas coordinadas por el comisario, se convirtió en instrumento eficaz para fomentar la camaradería y la empatía con los mandos, emular heroicidades, difundir una línea interpretativa de los hechos bélicos y políticos que se iban sucediendo, ofrecer textos comprensibles en sus idiomas vernáculos, así como para divulgar una serie de enseñanzas y consejos prácticos, tanto para la lucha como para la retaguardia, incluyendo

también en ocasiones secciones que ofrecían a los extranjeros algunas nociones del idioma español.

Además de estas tareas de edición periódica, las Brigadas Internacionales pusieron en marcha un servicio de distribución de prensa, capaz de hacer llegar las propias publicaciones interbrigadistas pero también libros y prensa extranjera a las diferentes unidades teniendo en cuenta su componente nacional y lingüístico. Para ello contaron con la implantación de un servicio central de correos y censura, dirigido por el esloveno Dragotin Gustinčič.

La labor editora no acababa con las publicaciones periódicas, sino que, tal y como recogían las órdenes del Comisario Delegado Gallo, debían confeccionarse también monografías que ensalzasen y sintetizasen las hazañas de las brigadas y las diesen a conocer al mundo. En este sentido, la XV Brigada se mostró como una de las más activas, siendo pionera en la puesta en marcha de estas iniciativas. Siguiendo la línea marcada por su jefe en las circulares mencionadas, el comisario de la XV Brigada Barthel –alias del francés Jean Chaintron– organizó ya en abril un servicio documental con el objetivo de realizar “*Le livre de combat de la XV^e Brigade*”. Dicho servicio, encargado de reunir todas las informaciones concernientes a esa Brigada, estuvo formado por el inglés Oliver Green y el francés Etienne Sacco, y contó además con la creación de un laboratorio fotográfico capaz de proporcionar una mayor vistosidad a las publicaciones⁶.

En los meses centrales de 1937⁷ aparecería finalmente en francés la edición de *Nos combats contre le fascisme : le livre de la 15^{ème} Brigade Internationale*, con sus más de 300 páginas, profusamente ilustradas con fotografías y con narraciones de los propios voluntarios. Para François Billoux⁸, responsable político de la Base de Albacete y también presente en la mencionada reunión del Consejo Militar de febrero, la presentación del libro en Francia y en otros países fue un gran éxito, y dio a conocer las hazañas de los “pequeños héroes” –más de 200 voluntarios, según él, participaron en su redacción– y sus ilustraciones se convirtieron en *un conmovedor desfile de imágenes, cada una de las cuales representaba un momento en la gigantesca batalla contra el fascismo internacional*. El libro, por tanto, más que un afán memorialístico procuraba la propaganda y quería ser ante todo acicate para el activismo de sus compatriotas en sus respectivos países. Billoux lo calificaba de publicación pionera que debían imitar el resto de las brigadas. Efectivamente, *Nos combats contre le fascisme* no sería sino uno de los títulos de una amplia serie de publicaciones dedicadas a promocionar a las Brigadas Internacionales, como lo fue *Garibaldi in Ispagna*. Algo más tarde apareció *La quatorzième*, que narra las experiencias de la 14 Brigada Mixta, encargo que le correspondió al doctor Theodor Balk y que redactó en alemán, aunque finalmente el libro se editó en francés con la traducción de Emmanuel Sedillo y Jean Bastien. Para su confección, Balk recurrió a los archivos administrativos de la Base de Albacete, consultando los ficheros del Servicio de Efectivos, para recopilar datos de muertos

y heridos⁹. Por otra parte, Alfred Kantorowicz nos relata en sus memorias las peripecias que llevó a cabo para confeccionar su “*Tschapaiew*”, *das Bataillon der 21 Nationen*. El batallón había sido disuelto y tuvo que localizar a los brigadistas supervivientes en diferentes unidades y hospitales, obligándole con frecuencia, como afirma el propio autor, a visitar la sede de la calle Velázquez de Madrid, donde se encontraba entonces el archivo de la antigua XIII Brigada (Kantorowicz, 2016, p. 457).

Detrás de esta actividad editora había una importante labor de documentación. El 7 de mayo de 1937, el Comandante de la Base de Albacete Vidal se dirige a Gallo, por aquel entonces ya instalado en la calle Velázquez de Madrid, recordándole que según lo acordado se encontraban en un proceso de recolección de todos los documentos necesarios para elaborar la historia de las Brigadas. En primer lugar querían recopilar todas las publicaciones (periódicos, revistas, folletos, etc.) elaboradas por las brigadas y batallones, todas las editadas hasta ese momento y las por editar. Por ello conminaba a Gallo, máximo responsable de la labor editora brigadista desde su puesto de Comisario Delegado de Guerra, a que le remitiese en breve plazo ese material. Ese mismo día, Vidal se dirigió también al *Comité International d'Aide au Peuple Espagnol*, en París, solicitándole una larga lista de periódicos (*Pravda, Izvestia, L'Humanité, Daily Worker*, etc.) desde el 1 de julio de 1936, para los trabajos de la Comisión Histórica. Y un día más tarde interpelló al Comité Central del Partido Comunista en Valencia, para solicitarle prensa española (*Mundo Obrero, Frente Rojo, Vanguardia, Claridad, El Socialista, C.N.T.*) en vista, según sus palabras, *de la constitución del archivo de nuestras brigadas internacionales*¹⁰.

Conviene remarcar que a pesar de recopilar material publicado eligieron el término de archivo y no el de biblioteca, que por otra parte también estuvo presente en las Brigadas Internacionales, que configuraron una red de bibliotecas para sustentar la lectura y la alfabetización de los soldados. El interés por este material, editado a veces en el mismo frente de batalla, y el deseo de reunir todas las referencias al fenómeno de la participación internacional, así como la voluntad de conservarlo de forma imperecedera, para servir a la historia de los interbrigadistas, motivarían el archivo de este material editado, junto con otra variada y diversa documentación, como diarios, manuscritos, entrevistas, etc.

En este sentido hay que recordar que por esas mismas fechas tuvo lugar también en la zona republicana la creación del denominado Archivo de la Guerra, que se presentaba en unos términos muy similares a ese archivo que surge en torno a la Sección Histórica de las Brigadas Internacionales. El Archivo de la Guerra nace por orden de 9 de agosto de 1937 (Gaceta n. 229 de 17 de agosto), dependiente de la Dirección General de Bellas Artes y vinculado al Cuerpo facultativo de Archiveros, Bibliotecarios y Arqueólogos. Su misión, tal y como se recoge literalmente en la orden firmada por delegación de Wenceslao Roces,

consistía en recoger y catalogar, para su estudio futuro, toda la información documental y bibliográfica que hiciera conocer la trascendental transformación que se estaba operando en la sociedad española. La orden obligaba a todos los editores e impresores a entregar un ejemplar de cada uno de los libros, revistas, boletines, colecciones de dibujos, folletos o cualquier clase de publicaciones creadas desde el 18 de julio de 1936 en adelante, así como dos ejemplares de todos los carteles, manifiestos, hojas volantes o cualquier otro material de propaganda aparecidos desde la citada fecha.

En cualquier caso, ninguno de los dos archivos, ni el de las Brigadas Internacionales ni el de la Guerra, se limitó a recoger sólo fondos editados y acabaron incorporando también documentación propia de archivo. En el caso del Archivo de la Guerra, la orden de 18 de mayo de 1938, que lo reorganizaba y requería a todos los maestros nacionales su colaboración en la recogida de datos, incluía además del material indicado en 1937, *documentos manuscritos o impresos, como actas de constitución de Ayuntamientos, Frente Popular, Comités, Tribunales populares, colectivizaciones, manifiestos, proclamas, carnets, emisión de papel moneda, hojas de reclutamiento de voluntarios y en general todo cuanto tienda a ilustrar sobre los episodios vividos en el pueblo.*

Fiala-Voros: recopilación de documentos

El trabajo histórico de las Brigadas Internacionales se relanzó durante el verano de 1937, con intensos planes de trabajo, entre los que destacaba la elaboración de un álbum fotográfico de las brigadas. Mientras De Boeck seguía como responsable del Servicio de Prensa, enfocado principalmente a la elaboración de boletines de información, confeccionados diariamente y en varias lenguas, el Comandante Vidal conformó un *Bureau Historique*, con un profesor de historia polaco, Emerich Fiala, como jefe¹¹, y al que fueron asignados un número de voluntarios de distintas nacionalidades y con distintos cometidos, que les obligaban a desplazarse por la geografía de la República española. Así, por ejemplo, un salvoconducto de 22 de julio autorizaba a Karl Preissner, escritor alemán y miembro de la Comisión Histórica de la Base de las Brigadas Internacionales a una misión especial que le llevaría a Valencia, Benicasim, Castellón de la Plana, Murcia, Orihuela, Denia, Benisa y Alicante¹², mientras que un mes más tarde el montenegrino Vucashin Radunovich, fue enviado también como miembro de la sección histórica a la 150 Brigada Mixta para recoger todos los documentos, archivos, fotografías, periódicos, etc. para la historia del batallón Dimitrov¹³. También la sección angloamericana se mostró especialmente activa, sobre todo con la incorporación de Sandor Voros a la Comisión Histórica, quien efectuó un viaje a Tarazona durante la primera quincena de julio, con el objetivo de recabar datos

sobre la formación y organización del primer batallón norteamericano (Abraham Lincoln), realizando entrevistas a su comandante Merriman y a otros voluntarios estadounidenses. Esta visita sirvió para dejar constituido allí, con el apoyo del comisario político José Dallet, un comité histórico que debía trabajar junto con los editores de los periódicos murales y enviar a Albacete todo aquel material que tuviera un valor histórico. Voros además solicitaba el envío de un fotógrafo a Tarragona para que realizara copias fotoestáticas de algunos documentos valiosos y tomara fotografías de Merriman y otros voluntarios, así como un cartógrafo que reprodujera mapas de las operaciones¹⁴.

Con estas actividades, el acopio de documentos iba en aumento. En un informe fechado el 1 de agosto, la Comisión Histórica, además de establecer las informaciones que debían obtenerse de las entrevistas a los voluntarios, fijó el tipo de documentos que necesitaban, incluyendo tanto documentos oficiales –originales o copias– (movimientos de tropas, operaciones militares, mapas, correspondencia oficial, órdenes sobre el trabajo político) como documentos de carácter personal (diarios, cartas, artículos, fotografías, dibujos...). El informe terminaba intentando incentivar el celo en estas actuaciones de recopilación, advirtiendo que algunas cosas que podían parecer triviales en el presente podrían alcanzar sin embargo un gran valor histórico en el futuro¹⁵. A mediados de agosto el Jefe del Estado Mayor de la Base de Albacete solicitó a la Comisión Histórica que enviara un delegado al edificio de la Tesorería General (antiguo Banco de España), donde se encontraban los archivos de la disuelta XIII Brigada Internacional para que recopilara aquellos documentos que pudieran serle de utilidad¹⁶. No siempre conseguían documentos originales; *Peter Kast* llegó a reunirse en Brihuega con el comandante Hans Kahle, jefe de la XI Brigada, donde le informó que disponía de un gran volumen de documentación militar de valor histórico, pero sólo le permitió realizar copias¹⁷. Todo esto obligó a establecer unas normas de seguridad que rigieran el uso y el acceso a estos documentos; la orden de la Comisión Histórica de 20 de agosto de 1937 prohibía que se dejaran documentos sobre las mesas o en armarios y cajones que no estuvieran bajo llave. Una vez que terminase la jornada laboral, el local debía quedar cerrado y con el material perfectamente recogido. Ningún colaborador de la Comisión Histórica podría sacar sin permiso fuera del lugar de trabajo ningún documento ni fotografía¹⁸.

Paralelamente a esta acumulación de documentos, la Sección Histórica seguía ejerciendo simultáneamente labores de predicción y reelaboración de ese material, desarrollando proyectos en los que se quería implicar a todas las unidades y nacionalidades. *Peter Kast* llegó a plantear la creación de una sección literaria encargada de promover la colaboración de literatos antifascistas en el trabajo histórico, recurriendo a escritores que estaban enrolados en las brigadas como Ludwig Renn, Gustav Regler, Marchwitza o Kantorowitz, a corresponsales extranjeros o a aquellos artistas que llegaron a España bajo la llamada del Congreso

Internacional de Escritores para la Defensa de la Cultura, como Egon Erwin Kisch¹⁹. Ya hemos visto que desde agosto asignaron a Kantorowitz la tarea de redactar la historia del batallón Tschapaiew; Kisch, además de colaborar en *Le Volontaire de la Liberté*, vio cómo el Comisariado de las Brigadas Internacionales le editaba su obra *Die drei Kühe*, cuento que redactó a partir de la historia de un campesino austriaco que vendió sus tres únicas vacas para venir a luchar a España²⁰.

Para el mundo anglosajón se decidió sacar una nueva edición sobre la XV Brigada, pero redactada esta vez en inglés, cuya redacción corrió ahora a cargo del irlandés Frank Ryan, y que contó para el soporte documental con la colaboración de Sandor Voros, húngaro americano y miembro de la Sección Histórica. Voros presenta una personalidad compleja, muy activo, enérgico, con una iniciativa desbordante, a veces rayana en la arbitrariedad. Él mismo cuenta en sus memorias cómo frente al comportamiento de sus compañeros, que esperaban *dócilmente* a que los documentos llegaran desde las unidades militares, él no dudó en ir a buscarlos allá donde se encontrasen –ya hemos aludido a su viaje a Tараzona–, granjeándose un salvoconducto firmado por él mismo y autodenominándose Jefe de la Sección Anglo-Americana (Voros, 1961, p. 335). Su camarada John Tisa, redactor de *Le Volontaire de la Liberté*, no escatima en calificativos negativos hacia él –*imperialist, authoritarian, arrogant*– y además le acusa de apropiarse de fotos y documentos para su interés personal (Tisa, 1985). Varios americanos estuvieron implicados en la Comisión Histórica, como Peter Wendorf, Leonard Grumet o, como traductor, John Cookson; con frecuencia eran oriundos de otras naciones, como el húngaro Voros, lo que les permitía moverse con mayor facilidad por el abigarrado magma interbrigadista. De esta forma, el abogado Leon Ente, residente en Estados Unidos desde 1922 se dedicó a documentar la participación de sus compatriotas polacos²¹.

La idea, según apunta Voros, era que el libro de recuerdos de la XV Brigada estuviera listo para poder ser distribuido entre los voluntarios como regalo de esas navidades, pero su publicación se retrasó hasta finales de febrero o principios de marzo del año siguiente²².

El plan Schindler: planificación de los trabajos y clasificación de la documentación

Muchos fueron los proyectos iniciados desde la Sección Histórica; a veces se atacaban en el último paso, en las instancias políticas que debían decidir la publicación del trabajo. Sin embargo, además de la divulgación propagandística, dentro de los planes de actuación también se pensaba en lo archivístico; en este sentido, en la planificación de las tareas que debía acometer la Sección de Historia para septiembre de 1937 figuraba la catalogación y descripción del fondo de

la extinta XIII Brigada, tarea que continuó en octubre, junto con la clasificación del resto de documentación que iba ingresando (de la XI y XV Brigada, de la nueva XIII Brigada, etc)²³.

La Sección Histórica se conformó, como ya hemos dicho, según el principio nacional, intentando que en sus trabajos estuvieran representadas todas las nacionalidades, aunque su presencia numérica fuera menor. Además de los colaboradores de distintas procedencias con los que se contaba en las diferentes unidades militares de los frentes, la Sección Histórica Central llegó a disponer de casi dos decenas de trabajadores, aunque su cifra y nómina varió, de orígenes y conocimientos lingüísticos diferentes, con los que se intentaba abarcar el mayor espectro posible de lenguas y pueblos, también con la ayuda de traductores. En una reunión mantenida entre sus miembros a finales de septiembre, cada uno expuso la situación de sus trabajos; Anger preparaba la crónica de la XI Brigada, Voros había reunido documentos de los batallones Lincoln y Washington y del Servicio Sanitario, Pichennik había trabajado con los austriacos y Guttman con los checos, Ente había entrevistado a voluntarios de la Dombrowsky, Gast había logrado textos sobre la primera Centuria Thälmann. Su jefe, Fiala, consideró sin embargo que el trabajo se desarrollaba carente de una perspectiva común. Había que centrarse en los archivos, ver qué es lo que se tenía ya para realizar una selección y analizar qué documentos más había que conseguir²⁴.

En este proceso de replanteamiento, autocrítica y mejora de la actividad de la Sección Histórica se sitúa el informe de A. Schindler, fechado en Albacete el 28 de septiembre de 1937, un informe, como veremos, cargado de consideraciones archivísticas²⁵. Schindler era el nombre en clave que había elegido Albert Schreiner, historiador en la futura República Democrática Alemana, presente en España desde agosto de 1936, uno de los fundadores junto con Hans Beimler de la Centuria Thälmann y Jefe del Estado Mayor de la XIII Brigada. Con anterioridad, en su exilio francés, ya había realizado labores de documentación para denunciar a la Alemania de Hitler, en publicaciones bajo diferentes pseudónimos. Sus denuncias sobre el rearme alemán iban acompañadas de documentos sobre las operaciones industriales relacionadas con el armamento, con un volumen tal de información que es difícil de entender cómo pudo caer en manos de la emigración alemana (Palmier, 2006, p. 327)²⁶. Tal y como señala su biógrafo Mario Keßler, las fuentes principales que utilizó en estas publicaciones fueron informes de la prensa alemana y memorandos de la administración, así como documentos internos del partido nazi, que provenían según sospechaba la Gestapo de un alto oficial del Reich (Keßler, 2014, p. 42).

El informe que presentó Schindler en Albacete fijaba como cometido de la Sección Histórica la recopilación de las enriquecedoras experiencias vividas en las diferentes formaciones de voluntarios durante la guerra española y su procesamiento y análisis para poner a disposición del público sus valores militares, políticos y

literarios en una presentación de base histórica. Tenía en cuenta para ello la necesaria recopilación de materiales, en unos términos similares a los que hemos visto hasta ahora, insistiendo en que los colaboradores debían desplazarse a las diferentes sedes brigadistas, cuarteles, hospitales, lugares de reposo, etc. Pero en su informe ponía de relieve sobre todo la necesidad de archivar de forma correcta y científica todo ese material que se iba recuperando e indicaba unas pautas para su clasificación. Consideraba en ese sentido que debía realizarse una clasificación desde distintos puntos de vista, siendo la fundamental la basada en las diferentes unidades militares, que debía completarse con un fichero de materias y otro de grupos nacionales.

Schindler enumeraba además las necesidades de personal y de instalaciones que requeriría la Sección Histórica. En el primer aspecto, además de la dirección y los diferentes jefes de sección establecidos en base a los grupos de lengua, traductores, cartógrafos, fotógrafos y mecanógrafos, pedía la presencia de un archivero dentro de la plantilla. En lo que se refiere al diseño espacial, consideraba necesario mantener el archivo, el laboratorio fotográfico, la sección cartográfica y una biblioteca auxiliar especializada en bibliografía militar. Finalmente, remarcaba la necesidad de desarrollar las tareas de forma metódica, con un plan de trabajo mensual y bajo el control del Estado Mayor de la Base.

Las recomendaciones de *Schindler* se proyectaron en la orden de 11 de octubre de 1937 que emitió la jefatura de la Base de Albacete²⁷. El comandante de la misma, *Belov*, que desde agosto había sustituido a *Vidal*, situaba orgánicamente a la Sección Histórica bajo la dependencia directa del Estado Mayor de la Base, configurándola como una sección del mismo, y establecía su estructura según la representación nacional existente en las brigadas internacionales, de forma que además del Jefe de la Sección Histórica –en ese momento *Fiala*, aunque en unas semanas sería llamado al frente– y del Jefe de la Sección de Operaciones –*Schindler*–, la orden establecía nueve responsables de las diferentes secciones nacionales: española, francesa, alemana, anglo-americana, polaca, italiana, balcánica, checa y húngara. Y además establecía un responsable de la sección de archivos. En la misma norma se establecía la existencia de un laboratorio fotográfico y una sección cartográfica, además de esa sección de archivos. Por otra parte, se concretaban las obligaciones a tener en cuenta en cuanto a la recopilación, clasificación y tratamiento de los materiales que se seleccionaran en las diferentes unidades y servicios militares, o de aquellos que los propios voluntarios entregaran individualmente.

La orden establecía la concentración de todo el trabajo histórico en la Sección de Albacete, para lo que el jefe de la misma debía tomar las medidas oportunas, junto con el Inspector General de las Brigadas Internacionales, y evitar así que otros servicios desarrollaran labores parecidas. En todas las unidades interbrigadistas (desde el nivel de compañía hasta el de división) se debía nombrar

un cronista encargado de llevar un diario en el que se registraran todos los acontecimientos ocurridos en la respectiva unidad o servicio. Este cronista sería además el enlace encargado de remitir a la Sección Histórica de la Base todos los materiales que considerara interesantes. Diez días más tarde, se redactó un reglamento de desarrollo de las tareas del cronista²⁸.

El desarrollo normativo y estos intentos de regularizar las actividades de la Sección Histórica se encontraron sin embargo con una serie de trabas. A principios de noviembre casi la mitad de los miembros de la sección estaban ausentes; el propio jefe de Sección Histórica, Fiala, había abandonado Albacete para incorporarse a la XIII Brigada. Su marcha precipitada podría estar relacionada con el hecho de que Fiala no había estado aún en el frente, lo que contravenía la norma de que en la Base sólo hubiera personal recluta o no apto para luchar (por edad, convalecencia, etc.). En esas circunstancias tuvo que hacer las veces de jefe el croata *Karl Anger*, que contaba con 41 años y que desde julio colaboraba con la sección histórica, después de haber estado varios meses en el frente. Por otra parte, *Peter Kast*, responsable de la sección alemana, y el fotógrafo *Desider Lederer* se encontraban en comisión de servicio en Madrid para elaborar el álbum de las brigadas internacionales; el húngaro *Laci Gyáros* y *Rosalie Lehouste*, asignada al archivo, se encontraban enfermos; *Leon Ente*, colaborador de la sección polaca, y *Paul Wendorf* tuvieron que acudir a sendas comisiones de servicios en Murcia y Tarazona; *Félix Navarro*, también del archivo de periódicos, disfrutaba de permiso en Madrid. Por otra parte, a mediados del mes de noviembre se produjo la sustitución de *Belov* como comandante de la Base por el *general Gómez*.

El laboratorio fotográfico

En aquellas fechas, la mayor parte de las energías de la propaganda se concentraban en la publicación de un álbum fotográfico que ofreciera un panorama completo y abigarrado de las brigadas internacionales en sus aspectos más diversos: su origen, la épica de la lucha, la solidaridad de los pueblos, el trabajo y el descanso en la retaguardia, la educación, la cultura. *Gallo* quería que estuviera publicado para noviembre, cuando se cumplía el primer aniversario de la llegada de los internacionales, pero las circunstancias no lo permitieron; *Un año de las Brigadas Internacionales* no se distribuiría hasta 1938 y el Comisariado de Guerra se preocupó entonces de hacerlo llegar a las más diversas personalidades, tanto españolas (*Azaña*, *Pasionaria*, *Carrillo*, *Miaja*, *Companyns*, *Martínez Barrio*...) como extranjeras (*Stalin*, *Roosevelt*, *Attlee*, *Thorez*, *Upton Sinclair*...).

En el comité de redacción del libro, además de *Szyfra Lipszyc* "*Juanita*", viuda de *Nino Nanetti* y colaboradora en el Comisariado que *Gallo* había organizado en Madrid, figuraban dos miembros de la Comisión Histórica, *Peter Kast*

y *Desider Lederer Turay*. *Kast* era el nombre de guerra del escritor y periodista, miembro del KPD y redactor de *Rote Fahne* Karl Preissner, encargado de la sección histórica alemana. *Lederer* era el nombre que adoptó el fotógrafo húngaro Dezvo Revai. No fue el único fotógrafo vinculado a la Comisión Histórica, que contó también con la colaboración del checoslovaco Franz Adorian. Las imágenes constituyeron una importante baza no sólo en este álbum sino en general en todas las publicaciones interbrigadistas y el laboratorio fotográfico de la Sección Histórica se convirtió en un centro capaz de responder a esa demanda, archivando fotografías tomadas por sus propios fotógrafos o en otros medios. En las diferentes unidades militares también existían departamentos fotográficos, como el que dirigía Harry Randall en la XV Brigada. El objetivo era reunir todo el material fotográfico relevante para las Brigadas Internacionales, independientemente de su origen. En un informe sin firmar ni datar, seguramente de finales de 1937, se da la cifra de 4.000 fotografías, la mitad de las cuales habían sido tomadas por los propios fotógrafos de la Sección Histórica y la otra mitad en las unidades militares, recopiladas a veces en negativo y otras en positivo²⁹.

Entre las consideraciones de estos reporteros gráficos no sólo estaban las capacidades técnicas sino también las habilidades para transmitir un mensaje. El propio *Lederer* plasmó en un informe estos fundamentos, afirmando que el fotógrafo debía captar la esencia del acontecimiento desde un punto de vista político e ideológico. Concretó la orientación del trabajo fotográfico interbrigadista en 9 puntos principales, que incluían la consideración de la guerra civil española como resultado de una provocación del fascismo internacional y la presencia de los voluntarios como una muestra de la solidaridad mundial, teniendo que estar representadas todas las razas y naciones, frente a la ayuda fascista que debía presentarse como una intervención bélica en toda regla. Cada voluntario debía ser consciente de que el conflicto español era sólo una batalla parcial en la lucha mundial total contra el fascismo. Se debía mostrar también fotográficamente el nacimiento y el desarrollo de las Brigadas Internacionales, que también habrían superado la fase de las milicias para integrarse en el naciente Ejército Popular de la República y enseñar las diferentes fases de la revolución española, así como – siguiendo la retórica comunista tras los hechos de mayo del 37– prevenir y denunciar las intromisiones de trotskistas y agentes fascistas³⁰.

Lederer propuso configurar ese laboratorio fotográfico central a partir del que existía en la Oficina de Efectivos, ubicado en el edificio del antiguo Banco de España. Se encargaría así de recopilar todo el material, sistematizando y coordinando los trabajos fotográficos en las diferentes unidades militares y seleccionando material adecuado para difundir en las publicaciones, también en la prensa extranjera. A ese archivo fotográfico se dirigirán desde distintas instancias; así por ejemplo, responderán a una petición del Socorro Rojo Internacional, que solicitaba fotografías de milicianos en la nieve para una campaña de recogida de ropa invernal³¹.

El plan Anger. Creación de los archivos históricos y traslado a Barcelona

La Sección Histórica de Albacete siguió completando sus archivos. Uno de sus miembros, como responsable del grupo francés, Laci Gyáros, escribió el 25 de noviembre al comisario de la XIV Brigada, acusándole recibo de los tres primeros envíos de material para el *Archive Centrale de la Commission Historique*. Le solicitaba además una relación de los nombres y números de cada batallón, y el nombre de sus comandantes y comisarios para facilitar las labores de clasificación de fotos y documentos. Por otra parte, le recordaba que todo ese material relacionado con la XIV Brigada quedaba cuidadosamente clasificado y guardado en los Archivos de la Sección Histórica, como los documentos del resto de las unidades, permaneciendo a disposición de la Brigada en cualquier ocasión que fuera necesario³². En este sentido, encontramos casos de respuestas de la Sección Histórica a demandas de información por parte de las oficinas brigadistas; así, por ejemplo, se da respuesta a la Oficina de Efectivos sobre un camarada de la XIII Brigada, recurriendo a la información que aparece en sus archivos³³.

A mediados de diciembre, sin embargo, la Sección Histórica eleva una serie de quejas al nuevo comandante de la Base, el General Gómez, presentándole una situación negativa que habría que reconducir. Se insiste en que todas las fuerzas y tiempo están concentrados en la elaboración del álbum sobre las Brigadas Internacionales que dirige el Comisariado de Gallo, mientras se adolece de una falta de personal, careciéndose de trabajadores para algunos importantes grupos de lengua; además se critica la falta de reconocimiento y el hecho de que sus miembros no reciban un grado militar y un salario en consonancia con su trabajo cualificado. Por otra parte y contraviniendo la orden de 11 de octubre, la Sección Histórica sigue dependiendo del Servicio de Prensa y no directamente del Estado Mayor, careciendo además de un administrador para la gestión diaria, permaneciendo la sección en una indefinición administrativa y financiera. Encargan entonces a Karl Anger que plantee soluciones a todos estos problemas y es en ese momento cuando el croata propone una reorganización de la Sección Histórica, reconvirtiéndola en un Archivo Central o Archivo Histórico de las Brigadas Internacionales, que debería ampliar sus objetivos y reunir junto al archivo de la Sección Histórica, el archivo de la propia Base –exceptuando los expedientes de oficina abiertos–, todos los archivos de las diferentes Brigadas y unidades militares, que deberían transferir periódicamente sus documentos siguiendo unos plazos, así como todo aquel material que fuera entregado voluntariamente, estructurándose este archivo como una sección de la Base, subordinado directamente al Jefe de la misma, al jefe del Estado Mayor o al Comisario de Guerra. Anger propone como jefe de este nuevo archivo a Paul Wendorf, un neoyorkino de 26 años especializado en historia, que había llegado a la Sección propuesto por

Sandor Voros para ser su asistente (Voros, 1961, p. 367). Además, Anger insiste en convertir el laboratorio fotográfico en una unidad independiente, separada del archivo, proponiendo a *Lederer*, todavía desplazado en Madrid y enfrascado en la elaboración del álbum de las brigadas, como responsable del mismo.

Wendorf rehusará el cargo de jefe del servicio de archivos pero sí redactará, ya en enero de 1938, el plan de transformación de la Sección Histórica en los Archivos Históricos³⁴, para los que propone que siga siendo Anger el responsable de los mismos. El principal reto que debían acometer estos archivos era el de la clasificación y catalogación, para lo que obligatoriamente se tenía que tener muy presente la variedad de lenguas en las que estaban redactados los documentos, por lo que debía buscarse personal versado en conocimiento de idiomas. Wendorf señala como principales lenguas de los documentos el español, el francés, el alemán, el inglés, el polaco y el eslovaco, señalando a Leon Ente como idóneo responsable para la documentación inglesa y polaca; a Franz Lehousse como responsable para la documentación francesa y española, así como para los trabajos gráficos (topografía, esquemas...); a Marija Habulin para la documentación alemana y eslava, junto con los trabajos de mecanografía; y a Félix Navarro para la documentación española y el archivo de prensa, así como traductor de las lenguas alemana, francesa e inglesa. Félix Navarro compondrá junto con Francisco Maestro la representación española en la sección de Archivos. En ambos casos se trata de jóvenes menores de edad, de 16 y 15 años respectivamente, que no habrían intervenido en ninguna toma de decisión, aunque sorprende la responsabilidad que recayó en Navarro, de tan corta edad, y encargado de la traducción en tres lenguas.

Dentro de esta reorganización se pensará también en cambiar sus instalaciones. A principios de febrero de 1938, los archivos se trasladaron al Círculo Mercantil, despachos número 9 y 10. Sin embargo la dotación de personal siguió presentando muchos problemas, de forma que la nómina de los trabajadores adscritos a la sección histórica quedó reducida a la mínima expresión. Desde principios de año, *Gallo* y el Comisariado de Guerra se habían trasladado a Barcelona, lugar que además de ser la sede del gobierno republicano ofrecía una mayor cercanía a la frontera con Francia. En la Ciudad Condal se encontraban ya *Peter Kast*, trabajando precisamente para el Comisariado de Guerra, y *Theodor Gutmann*, que estaba elaborando un libro sobre la participación checa. *Lederer* y *Adorjan*, como trabajadores del laboratorio fotográfico, habían quedado fuera de la sección, al igual que otros miembros como el belga Franz Lehousse, trasladado a la Escuela de Oficiales de Pozo Rubio, o Leon Ente, incorporado a la XIII Brigada. Otros casos eran baja por enfermedad, como Wendorf y Rosalía Lehosse.

Ante estas perspectivas, hay un intercambio de cartas entre *Karl Anger* y el Comisario Delegado de las Brigadas Internacionales, Luigi Longo *Gallo*, ya en su nueva sede del Paseo Méndez Vigo de Barcelona, en las que el primero, tras

informarle de la reorganización efectuada, le transmite su opinión de llevar el archivo allí, donde existe una sección de *agitprop* y se dirigen todos los trabajos de propaganda, mientras que de mantenerse en Albacete el archivo podría quedar sin utilidad alguna.

El 26 de febrero de 1938, *Anger* informa a *Gallo* por carta que la comandancia de la Base, con la aquiescencia de André Marty, ha apoyado su propuesta de remitir a Barcelona el archivo histórico. Considera que no es excesivamente voluminoso y podría ocupar una única sala, ofreciéndose él mismo para quedarse al cuidado del archivo en su nueva ubicación, solicitando únicamente al Comisario poder traerse de Albacete a su compatriota la mecanógrafa y traductora Marija Habulin. *Gallo* le responderá a los pocos días reafirmando la conveniencia del traslado del archivo cerca del Comisariado de Guerra de Barcelona, pero advierte a *Anger* de que su tarea allí no será la conservación del archivo sino el *trabajo general de Agit-Prensa*, no viendo necesidad de mantener personal especial encargado de su cuidado y rechaza igualmente su petición de adscribir a Habulin al Comisariado. Significativamente, *Anger* firma su carta como Responsable del Archivo Histórico y *Gallo*, pareciendo no reconocer tal cargo, redacta la suya remitiéndola simplemente a la Comisión Histórica de la Base de las Brigadas Internacionales³⁵.

De esta manera finalizaba la labor de la Sección Histórica de Albacete y se truncaba igualmente su reorganización en una Sección de Archivos Históricos. Poco más tarde, con el territorio de la República cortado en dos tras llegar las tropas franquistas a Vinaroz, sería clausurada también toda la Base de Albacete, meses antes incluso de que los internacionales abandonaran España. Desde finales de mayo sería la Administración Central de las Brigadas Internacionales, con sede en el Paseo Maragall de Barcelona, la que se haría cargo de todos los servicios de organización, mientras el Comisariado de *Gallo* continuaba también desde esa ciudad su labor de propaganda y control político. Los archivos reunidos por la Sección Histórica se integrarían con el resto de documentación producida por las Brigadas Internacionales y saldrían, bajo control de la Komintern, hacia Moscú.

Los jefes de las Brigadas Internacionales se mostraron muy celosos por controlar todos sus documentos. En sus archivos se conserva un telefonograma de André Marty fechado a finales de marzo de 1938 en el que, además de solicitar, como estaba convenido, el traslado de los hombres de la Comisión Histórica con sus fondos documentales a Barcelona, pide que se remita también todos los archivos de la Base y de los Cuadros, en especial lo concerniente a los estados de personal, de efectivos y de unidades, tarea que debería ser coordinada por *Edo*, uno de los agentes del Komintern³⁶. En septiembre, *Gallo* anuncia en una circular remitida a todos sus comisarios que se han comenzado a organizar todos los archivos de los comisariados de las diversas unidades y Brigadas Internacionales

con la intención de fotografiar el material más importante³⁷. La Administración Central de Barcelona, por su parte, intentó reunir todos los documentos relacionados con los voluntarios conservados en los archivos de las divisiones, brigadas, batallones y grupos de artillería, con el objetivo de gestionar el retorno a sus países, una vez que se decidió su retirada en octubre de 1938³⁸. Con las tropas franquistas ganando terreno aceleradamente sobre Cataluña y el fantasma de la inminente derrota sobre sus cabezas, se tomó la decisión de salvar esos archivos de las manos del enemigo, en una maniobra orquestada desde la Komintern, a cuyo archivo fue a parar este fondo documental.

En las memorias de los protagonistas podemos encontrar varias referencias a estos momentos. El brigadista norteamericano Arthur Landis afirma haber ayudado a cargar los archivos de la XV Brigada en un barco ruso con destino a Moscú (Celada, 2006, p. 154) y su compatriota John Tisa relata cómo llevó los archivos del cuartel general de las brigadas internacionales hasta Figueras (TISA, 1985, p. 205). A esta ciudad llegan también los recuerdos de Emilio Gómez Nadal, marido de la bibliotecaria Teresa Andrés, quien relata cómo *Gallo*, a finales de enero de 1939, en medio de los preparativos de la evacuación de Barcelona, les confió los archivos de las brigadas internacionales y un camión con destino a Figueras, donde los entregaron a *Pedro*, pseudónimo de Erno Gëro, delegado de la Komintern (Gómez Andrés, 2013, p. 98).

Los archivos de las Brigadas Internacionales quedarían así incorporados a los fondos documentales de la Internacional Comunista y, tras la disolución de ésta, al sistema de archivos soviéticos, quedando fuera de la consulta pública y de la investigación histórica hasta la desaparición de la URSS.

Conclusiones

La experiencia de la Sección Histórica creada en el seno de la Brigadas Internacionales durante la guerra civil española puede ser analizada desde múltiples puntos de vista: el estudio de la propaganda, la historiografía, el trabajo intercultural..., también desde su dimensión documental. Entre sus objetivos estaba presentar al mundo el relato de unos hechos que estaban sucediendo en ese momento e influir así en la opinión pública, pero también en la propia moral y concienciación de los voluntarios. Se trataba de forjar una historia que no buscaba la objetividad, pero sí una subjetividad sustentada en una convincente base documental; ya hemos visto cómo el fotógrafo *Lederer* no quería el disparo espontáneo y descriptivo de un momento, sino que abogaba por aportar la imagen persuasiva de un modo de relatar la historia.

Pero era también el compromiso y la convicción de los protagonistas de estar haciendo algo “grande”, “histórico”, lo que les llevaba a participar en múltiples

manifestaciones: dibujos, diarios personales, publicaciones, prensa mural, fotografías, un variado material tutelado, fomentado y controlado desde el comisariado de guerra, que debía ser conservado para la posteridad, como arsenal para construir la memoria histórica.

Ese impulso emocional a guardar los recuerdos de unos hechos memorables, así como las estrategias y tácticas políticas a la hora de presentar y difundir unos sucesos, fueron los promotores de la creación de un archivo híbrido, formado por materiales diversos (revistas, folletos, documentos, fotografías...), conseguidos de aquí y de allá, en un proceso de recopilación en el que el documento propiamente de archivo va ganando importancia, sobre todo desde la desaparición de la XIII Brigada y, por lo tanto, la custodia de un fondo documental cerrado. Desde una fase inicial, de archivo de prensa, en el que se quieren reunir todas las manifestaciones divulgativas de las diferentes unidades militares, se llega a la propuesta de constituir un archivo histórico o central, como una solución archivísticamente más correcta, al tratar toda la documentación producida por las Brigadas Internacionales como un todo, sin necesidad de desgajar la documentación de su contexto.

En esta evolución tienen una especial relevancia los planes diseñados por algunos de los miembros de la Sección Histórica, en especial el de Albert Schindler, completado más tarde por *Karl Anger*, aunque se encontraron con las limitaciones propias de una situación de guerra a la hora de ponerlos en práctica.

Aunque la orden de 23 de septiembre de 1937 consideraba a las Brigadas Internacionales parte integrante del Ejército Popular de la República Española, de modo que dependían tácticamente de los mandos militares correspondientes, y constituían unidades administrativas de modo análogo a las restantes Brigadas Mixtas del Ejército, finalmente fueron las redes de la Internacional Comunista las que permitieron reunir la mayor parte de los archivos de las Brigadas Internacionales y sacarlos fuera de España, conservándose actualmente en el Archivo Estatal Ruso de Historia Sociopolítica (RGASPI). Los servicios de Recuperación de Documentos franquistas sólo consiguieron hacerse con parte de esa documentación, que actualmente se custodia en el Centro Documental de la Memoria Histórica y en el Archivo General Militar de Ávila.

Bibliografía

- BAIGORRI JALÓN, Jesús (2019). *Lenguas entre dos fuegos: intérpretes en la Guerra Civil española (1936-1939)*. Granada: Editorial Comares.
- CASTELLS, Andreu (1974). *Las Brigadas Internacionales de la Guerra de España*. Esplugues de Llobregat: Ariel.
- CELADA, Antonio R. (2006). *Los brigadistas de habla inglesa y la Guerra Civil Española*. Salamanca: Ambos Mundos.

- DUROUX, Rose (2006). "Françoise Brauner por sí misma (1911-2000)". *Arenal: Revista de historia de mujeres*. v. 13, n. 2, p. 379-397.
- GÓMEZ ANDRES, Antonio (2013). *Teresa Andrés: biografía*. Valencia: Publicacions de la Universitat de València.
- KANTOROWICZ, Alfred (2016). *Spanisches Kriegstagebuch*. Frankfurt: Fischer.
- KEBLER, Mario (2014). *Albert Schreiner, Kommunist mit Lebensbrüchen*. Berlín: Trafo.
- NÚÑEZ DÍAZ-BALART, Mirta (1992). *La prensa de guerra en la zona republicana durante la guerra civil española (1936-1939)*. Madrid : Ediciones de la Torre.
- NÚÑEZ DÍAZ-BALART, Mirta (2006). *La disciplina de la conciencia: las Brigadas Internacionales y su artillería de papel*. Barcelona : Flor del Viento.
- PALMIER, Jean-Michel (2006). *Weimar in exile: the antifascist emigration in Europe and America*. London: Verso.
- RYAN, Frank (2019). *El libro de la XV Brigada: relatos y testimonios de la Guerra Civil española*. Salamanca: Ediciones Amarú.
- TISA, John (1985). *Recalling the good fight: an autobiography of the Spanish Civil War*. South Hadley, Massachusetts: Bergin & Garvey.
- SCHREINER, Albert (1956). "Zwei Dokumente über die historische Sektion im Stab der Internationalen Brigaden in Albacete". *Zeitschrift für Geschichtswissenschaft*. n. 3, p. 587-594.
- VOROS, Sandor (1961). *American commissar*. Philadelphia: Chilton Company.

Notas

¹ El acta con las diferentes intervenciones de los participantes se conserva con el resto de la documentación procedente de las Brigadas Internacionales en el Archivo Estatal de Historia Socio-Política de Rusia (RGASPI 545/2/46). En la relación de asistentes a este Consejo constan: Gallo, Vidal, Platone, Karbov, Aparicio, Frans, Max Hornung, Billoux, Fein, Winckler y Telge.

² Probablemente Frans haga referencia a Franek, uno de los dirigentes de los servicios sanitarios y colaborador del doctor Telge, también presente en la reunión y búlgaro como él; Castells habla de él como Franciszek Krieger, hijo del secretario del PC búlgaro Korolov (Castells, 1974, p. 151).

³ Note de Service n° JS-1629, del 24 de marzo de 1937 (RGASPI 545/2/47)

⁴ RGASPI 545/1/36

⁵ "Le journal de Valence (du Commissariat de Guerre) qui donnera des indications politiques et militaires générales" (Réunion du Conseil Militaire du 14-2-37. RGASPI 545/2/46)

⁶ RGASPI 545/3/435

⁷ Peter Kast afirma en un informe sobre el trabajo histórico de las brigadas que la obra se publicó el 12 de julio de 1937 (RGASPI 545/2/162). Para financiar su confección, se había solicitado ya en abril una suscripción a los propios brigadistas (RGASPI 545/3/514).

⁸ François Billoux era miembro del partido comunista francés y llegaría a ser ministro del gobierno, en la inmediata posguerra tras la liberación de Francia. Sus opiniones sobre la publicación *Nos combats contre le fascisme están reflejadas en: Episodes de la bataille gigantesque d'Espagne contre le fascisme international* (RGASPI 545/3/171)

⁹ Balk era el alias de Fodor Dragutin, médico y escritor, miembro del Partido Comunista Alemán cuyo archivo personal se custodia en el Literaturarchiv der Akademie der Künste, de Berlín. Sobre sus

pesquisas en los archivos de la Base: “*Le Camarade Docteur Balk est chargé d’écrire l’histoire de la 14e Brigade Internationales. Il se rend a Albacete pour ramasser dans les archives du Service des effectifs les données nécessaires sur les morts et blessés de la 14e Brigade*”: Oficio de Gallo al Comandante y al Comisario Político de la Base de Albacete, 6-8-1937 (RGASPI 545/1/46))

¹⁰ Note de Service n° JS-3103 (RGASPI 545/2/43), JS/n° 3107 (RGASPI 545/2/40). Gallo cumpliría enseguida los deseos de Vidal, remitiendo una circular a todos los comisarios de guerra de las Brigadas Internacionales solicitándoles dos ejemplares de todas sus publicaciones (14-05-1937, RGASPI 545/3/56). También desde el exterior se obtuvo respuesta; así por ejemplo, a principios de junio La Sociedad Española de Librería aseguraba a la Comisión Histórica el servicio de dos ejemplares de *La Dépêche de Toulouse*, cuya representación ostentaba (RGASPI 545/2/162)

¹¹ Voros dedica en sus memorias algunos comentarios sobre su jefe: *Comrade Fiala, Chief of the Historical Commission –a tall, broad-shouldered, close-mouthed Pole... Fiala was a highly intelligent person, a member of the Polish Bureau of the Comintern, in civilian life a Communist professor of history* (Voros, 1961, p. 329)

¹² Salvoconducto n. 2709 (RGASPI 545/2/52):

¹³ Note de service n° 7775-HR, de 22 de agosto de 1937 (RGASPI 545/2/56)

¹⁴ Report on trip to Tarazona, 14 de julio de 1937 (RGASPI 545/2/164). El comité quedó formado por Edwin Rolfé, trabajador del Daily Worker, Blaine Owen y Abramovitz, miembro de la Canadian Writers Association.

¹⁵ List of material needed for Historical Commission (versión en inglés) y Liste von Material das die Historische Kommission braucht (version en alemán). 1 de agosto de 1937 (RGASPI 545/2/162).

¹⁶ Note de Service n° 7541-HR, de 16 de agosto de 1937 (RGASPI 545/2/55).

¹⁷ Bericht über den Stand der bisher geleisteten historischen Arbeiten in den Brigaden (RGASPI 545/2/162).

¹⁸ *Dienstordnung der Historischen Sektion*, de 20 de agosto de 1937 (RGASPI 545/2/162).

¹⁹ Exposer Zentrale-Historische-Kommission (Literarische Abteilung), sin fecha (RGASPI 545/2/162)

²⁰ Anécdota recogida en Duroux (2006).

²¹ List with characterizations, of the Americans working at the Historical Commission (RGASPI 545/3/453)

²² Recientemente se ha publicado la versión española de esta obra, gracias al grupo de investigación de la Universidad de Salamanca dirigido por Antonio R. Celada, con una traducción precedida de un profundo estudio crítico (RYAN, 2019)

²³ *Arbeitsplan fuer die Zeit bis zum 30. September 1937 y Arbeitsplan der Historische Sektion fuer den Monat Oktober 1937* (RGASPI 545/2/162)

²⁴ Meeting of Historical Commission, Wednesday 9/23/37 (RGASPI 545/2/164). Tal y como figura en las actas, la reunión se desarrolló en ruso y alemán, con traducción simultánea por Adorjan. La importancia de las lenguas y el uso de intérpretes en el abigarrado conjunto interbrigadista ya ha sido puesto de manifiesto por el profesor Baigorri (2019).

²⁵ *Vorschlaege fuer die Taetigkeit der Section Historique* (RGASPI 545/2/162)

²⁶ Albert Schreiner está detrás de varias obras publicadas por la editorial dirigida desde el exilio francés por Willi Münzenberg, Editions du Carrefour. En 1934 apareció en varios idiomas *Au seuil de la guerre: “Hitler rearms”*: *documents sur le réarmement de l’Allemagne hitlérienne*, cuya autoría se atribuía únicamente a la periodista Dorothy Woodman, secretaria de la Unión de Control Democrático; y en 1936, firmando como A. Müller, *Hitlers motorisierte Stoßarmee*.

- ²⁷ Ordre du jour n° 114, de 11 de octubre de 1937 (RGASPI 545/2/59)
- ²⁸ Ausführungsbestimmungen der Section Historique zum Befehl Nr. 114 vom 11.X.1937 des Chefs der Base der Inter. Brigaden (RGASPI 545/2/162)
- ²⁹ *Zur Arbeit der Historischen Sektion* (RGASPI 545/2/162). En ese mismo expediente se puede encontrar otro informe, en esta ocasión de Peter Kast, (*Bericht über den Stand der bisher geleisteten historischen Arbeiten in den Brigaden*) en el que menciona como posible fuente fotográfica el archivo de Walter Reuter, representante del Ministerio de Guerra, con fotografías de todas las fases y frentes, en la Plaza de Nules 2 de Valencia.
- ³⁰ *Arbeitsentwurf zur Reportersarbeit im Komission Historique* (RGASPI 545/2/162)
- ³¹ Note de Service n° 9772-HR a la Section Historique de la Base (RGASPI 545/2/60)
- ³² Carta de la Comisión Histórica de las B.I., Section Française, al Cde. Vittori, Commissaire de Guerre de la XIV Br., 25/11/1937 (RGASPI 545/2/162)
- ³³ Carta del Chef der Hist. Sektion al Effectif-bureau der Base, 1-12-1937
- ³⁴ Proposition pour la reorganisation de la Section Historique en la Section des Archives Historiques, 16 de enero de 1938 (RGASPI 545/2/164)
- ³⁵ Carta de K. Anger a Gallo de 26 de febrero de 1938 (RGASPI 545/2/162) y Carta de Gallo a Anger, de 3 de marzo de 1938 (RGASPI 545/1/47)
- ³⁶ Telephonogramme à Albacete-General Gómez de la part deu Camarade André, 29-3-1938 (RGASPI 545/1/47). Marty indicaba que los documentos serían copiados en Barcelona y los originales devueltos. Edo Romano -Eduardo d'Onofrio- formaba parte de la Comisión de Cuadros Extranjeros que había creado la dirección del PCE en enero de 1938.
- ³⁷ Carta de Gallo a los Comisarios y Comandantes de las Unidades Internacionales, de 1 de septiembre de 1938 (RGASPI 545/1/47). Gallo los intenta concienciar, argumentando que “la importancia de este trabajo para la elaboración de la historia de su unidad y la de las Brigadas Internacionales era evidente”.
- ³⁸ Carta de la Sección Administrativa de las Brigadas Internacionales al Jefe del 4º Grupo de Artillería pesada, de 30 de octubre de 1938 (RGASPI 545/2/287).



ACADEMIE DE MEDECINE DE PARIS
PRIX ORFILA PRIX DESPORTES

6 Ampoules de 1 c.c.
au DIXIEME de milligramme
DE

DIGITALINE NATIVELLE
CRISTALLISEE

POUR INJECTIONS INTRAMUSCULAIRES

LABORATOIRE NATIVELLE: 49, B^d de Port-Royal, PARIS

FORMULE
pour 6 ampoules Digitaline Nativelle au 1/10 de mil. l.
Digitaline Nativelle crist.
0 gr. 0006
6 centi. cubes



ISBN 978-84-941454-7-6



9 788494 145476