ARTÍCULOS

Revista General de **Información y Documentación**
ISSN: 1132-1873

http://dx.doi.org/10.5209/RGID.60805

EDICIONES COMPLUTENSE

La protección de datos personales en las bibliotecas universitarias españolas en el entorno digital

Concha Varela-Orol[1]; Rocío Ameneiros Rodríguez[2]

Recibido: 10 de julio 2018 / Aceptado: 14 de diciembre de 2018

Resumen. El objeto de este trabajo es analizar distintos aspectos relacionados con la protección de datos personales en las sedes web de las bibliotecas de las Universidades públicas españolas. Aunque con las limitaciones inherentes a la fuente de la investigación, se encuentran numerosas debilidades en el tratamiento de los datos personales en el entorno digital que deberían ser abordadas con objeto de cumplir el Reglamento de Protección de Datos de la Unión Europea. Se recomiendan distintas actuaciones a las bibliotecas, que afectan tanto a acciones propias como al análisis de servicios prestados por proveedores.
Palabras clave: Protección de datos personales; Bibliotecas universitarias; Confidencialidad en bibliotecas; Privacidad en bibliotecas; Gestión de identidades en bibliotecas.

[en] The protection of personal data in the spanish university libraries in the digital environment

Abstract: The aim of this work is to analyse different aspects related to the protection of personal data in the websites of the libraries of the spanish public universities. Albeit with the inherent limitations of the research source, there are many weaknesses in the treatment of personal data in the digital environment that should be addressed in order to comply with the European Union's Data Protection Regulation. A number of actions are recommended for libraries, which affect both their own actions and the analysis of services provided by suppliers.
Keywords: Personal data protection; University libraries; Library confidentiality; Library privacy; Library identity management.

[1] Universidade da Coruña. Departamento de Humanidades
E-mail: concepcion.varela@udc.gal
[2] Universidade da Coruña. Departamento de Humanidades
E-mail: rocio.ameneiros@udc.es

Cómo citar: Varela-Orol, C., Ameneiros Rodríguez, R. (2018). La protección de datos personales en las bibliotecas universitarias españolas en el entorno digital, en *Revista General de Información y Documentación* 28 (2), 685-702.

1. Introducción

Las bibliotecas han necesitado siempre un buen número de datos personales de sus usuarios para prestarles sus servicios. El tratamiento de estos datos ha sido objeto de atención desde, al menos, 1939, año en el que se redacta el primer código ético de la profesión por parte de la ALA (American Library Association, 1939), cuyo artículo 11 señalaba la necesidad de tratar como confidencial y privada la información obtenida de los usuarios.

La aplicación de las tecnologías de la información y la comunicación han modificado sustancialmente los servicios proporcionados por las bibliotecas. En primer lugar, han hecho nacer nuevos servicios que facilitan el acceso a ordenadores y otros dispositivos electrónicos, así como acceso a Internet. También han desarrollado los servicios existentes y otros nuevos en la red mediante sedes web y aplicaciones móviles, a las que con frecuencia se implementan herramientas de analítica web. Además, han modificado su papel de proveedores de recursos informativos in situ, ofreciendo servicios de terceras partes a través de sus sedes web, como sistemas de gestión que almacenan en empresas externas su catálogo o el acceso a bases de datos, revistas y libros electrónicos. Todas estas prestaciones implican el tratamiento de datos personales, que permiten desarrollar sistemas de recomendación a partir de los historiales de búsqueda.

Pero ya a partir de los años 60, cuando las bibliotecas comienzan la automatización de la gestión de sus procesos, se incrementa la elaboración de códigos éticos por parte de las asociaciones de profesionales de la información en muchos países y, en ellos, el derecho a la privacidad y confidencialidad ha estado y está presente, como lo están otros derechos incluidos en la Declaración Universal de los Derechos Humanos (libertad intelectual, propiedad intelectual, etc.). La aplicación de los principios recogidos en los códigos éticos ocasionó diversas controversias y conflictos de los bibliotecarios con el Gobierno en Estados Unidos (Starr, 2004), siendo el más conocido la impugnación en 2005 por parte de los bibliotecarios de Connecticut de una cláusula de la Patriot Act, que exigía informar al Gobierno sobre los registros de préstamos y de búsquedas de los usuarios de las bibliotecas.

La problemática derivada del marco tecnológico ha hecho patente la necesidad de desarrollar nuevos documentos de autorregulación que, más allá de los compromisos éticos, proporcionen a las bibliotecas pautas en relación a cada uno de los aspectos concretos donde puede estar en riesgo la protección de los datos personales en el uso de los servicios. El Manifiesto de la IFLA sobre Internet de 2002, actualizado en 2014 (Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas, 2014), hacía ya mención a la importancia de que las bibliotecas respetasen la privacidad de sus usuarios y la confidencialidad de los recursos que usan. La Declaración de la IFLA sobre la Privacidad en el Entorno Bibliotecario (Federación Internacional de Asociaciones de Bibliotecarios y

Bibliotecas, 2015) ha señalado los nuevos retos planteados por la deriva tecnológica actual, alertando a las bibliotecas en relación a los servicios contratados con proveedores de contenidos y servicios comerciales, los sistemas bibliotecarios basados en la nube y los servicios que ofrecen prestaciones para los dispositivos móviles. Por su parte, la ALA ha elaborado un cuerpo de directrices en relación a la privacidad en los sistemas integrados de gestión de las bibliotecas (American Library Association, 2016); para la relación con los proveedores de contenidos digitales (American Library Association, 2015); para el intercambio de datos entre dispositivos y servicios en red (American Library Association, 2016); para computadores y redes de acceso público (American Library Association, 2016); para sedes web de bibliotecas, OPAC y plataformas de descubrimiento (American Library Association, 2016), etc. Esta relación ya proporciona una idea de hasta qué punto los datos personales pueden estar comprometidos en los servicios bibliotecarios.

El objeto de esta investigación es analizar la protección de datos puesta en marcha en los servicios de las bibliotecas en Internet. Para ello, hemos estudiado las sedes web de las bibliotecas de las Universidades públicas españolas, dado que las consideramos el conjunto de bibliotecas con un número mayor de prestaciones en la red y también las que poseen mayor capacidad y recursos para poner en marcha medidas de protección. El análisis se centra en algunos aspectos relacionados con la protección de los datos personales en el entorno digital, teniendo en cuenta el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD), que entró en vigor en mayo de 2018. Para el objetivo seleccionado hemos recopilado información de las sedes web de estas bibliotecas, partiendo de la relación de Universidades proporcionada por la CRUE en su sede web, un universo de cuarenta y nueve bibliotecas. La recogida de datos se ha realizado en los meses de febrero y marzo de 2018, consultando las sedes web con el navegador Firefox, que indica el nivel de seguridad de las páginas y la organización de certificación.

Dado el considerable número de prestaciones de las sedes web de las bibliotecas que pueden estar implicadas en la protección de datos privados, hemos centrado el análisis en la información proporcionada a sus usuarios en relación a la recopilación, tratamiento y seguridad de sus datos privados; en la seguridad de la conexión de las páginas de gestión de la identidad de los usuarios y en las consultas sobre sus catálogos o plataformas de descubrimiento; en el posible uso de datos privados en sus catálogos; y en la formación proporcionada a los usuarios por las bibliotecas a través de las actividades y recursos de formación. Por supuesto, no agotamos los temas que deberían ser analizados en una auditoría sobre la privacidad, tales como el uso de plataformas de libros y revistas electrónicos, conexiones wifi ofertadas a los usuarios, computación en la nube y un largo etcétera, más difíciles, sino imposibles, de analizar desde las sedes web.

2. De la privacidad a la protección de datos

El derecho a la protección de datos tiene su origen en el derecho a la privacidad, reconocido en el artículo 12 de la Declaración Universal de los Derechos Humanos (1948) y en el artículo 8 del Convenio Europeo de Derechos Humanos (1950) del Consejo de Europa, aunque existen hoy muchos autores que consideran privacidad y protección de datos como conceptos distintos (Grava, 2017).

De los documentos citados y otros posteriores se puede deducir un derecho clásico a la privacidad: "an individual has the right to respect for his or her privacy, family, home or correspondence, and shall not be subjected to arbitrary or unlawful interference with this right" (Vander Maelen, 2017: 7). Paralelamente a los desarrollos tecnológicos, se sintió la necesidad de diferenciar del derecho clásico a la privacidad una protección específica para los datos personales automatizados (Vander Maelen, 2017: 8), y se produjo un desarrollo de normas y directrices sobre los límites al tratamiento de datos personales, como las *Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales* de la OCDE y la *Convención para la protección de las personas en lo relativo al procesamiento automático del Consejo de Europa*, ambos documentos publicados en 1980, que en buena medida definieron los datos personales y establecieron principios para su tratamiento.

La legislación española sobre la protección de estos datos se fundamenta en el artículo 18 de la Constitución que reconoce el derecho a la intimidad. La Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) de 1992, define por primera vez en España los datos de carácter personal, siendo sustituida en 1999 por la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) y publicado posteriormente su Reglamento de desarrollo (R.D. 1720/2007), en cumplimiento de la Directiva sobre protección de datos 95/46/CE. La Directiva ha sido seguida por el RGPD, que entró en vigor el 25 de mayo de 2018, lo que ha llevado a la redacción de un nuevo Proyecto de Ley Orgánica en España, actualmente en trámite parlamentario.

El RGPD define los datos personales como "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" (Art. 4). La definición es similar a la incluida en la anterior Directiva y a la del Reglamento de desarrollo español de 2007, aunque añadiendo como datos personales los identificadores en línea.

La interpretación de estas definiciones y la complejidad del tratamiento de datos han dado lugar a distintos informes de expertos, así como a sentencias de los tribunales españoles y de la Unión Europea. En relación con el ámbito de los datos personales cabe citar el informe realizado por el Grupo de Trabajo del artículo 29, *Dictamen 4/2007 sobre el concepto de datos personales* (Unión Europea, 2007), que ha analizado detalladamente el sentido de "información sobre una persona física identificada o identificable", concluyendo:

- el ámbito de aplicación de las normas de protección de datos no debe llevarse a su extremo, pero también debe evitarse una limitación indebida del concepto de protección de datos;
- tanto la información objetiva como la subjetiva sobre una persona, cualquiera que sea su amplitud, y con independencia del soporte técnico que la contenga, puede considerarse como datos personales;
- para que pueda aplicarse la expresión "sobre" debe haber un elemento contenido, o un elemento finalidad, o un elemento resultado, que han de considerarse como condiciones alternativas y no acumulativas;
- el término "directamente identificada" se refiere comúnmente a la utilización de nombres y apellidos, que sirven para obtener otros datos que permiten asociar a la persona física de tal manera que puede ser distinguida de otras. "Indirectamente identificada o identificable" indica que la combinación de detalles pertenecientes a distintas categorías (edad, origen regional, etc.) también puede ser lo bastante concluyente en algunas circunstancias, en especial si se tiene acceso a información adicional de determinado tipo".

Los principios básicos de la protección de datos presentes hoy en la legislación de todos los países pueden sintetizarse en: finalidad legítima (especificación del propósito); proporcionalidad (limitación de recogida y uso); necesidad de consentimiento; transparencia (derecho al acceso y a la rectificación); responsabilidad (deber de custodia); y restricciones a la transmisión (Gómez Barroso, 2018).

A partir de estos principios se establecen los derechos fundamentales de los ciudadanos en relación a sus datos personales: derecho de información, derecho de acceso, derecho de rectificación, derecho de cancelación y derecho de oposición, a los que el nuevo Reglamento europeo añade el derecho de portabilidad.

El RGPD establece la necesidad de protección de datos desde el diseño y por defecto. La privacidad desde el diseño fue promovida por Ann Cavoukian (2012), caracterizándose por su carácter proactivo en lugar de reactivo. Implica que la protección de datos personales ha de estar presente en los productos y servicios tecnológicos desde el momento de su concepción y que la máxima protección de los datos privados debe ser la opción por defecto de las prestaciones tecnológicas.

3. Políticas de privacidad

Los datos recogidos en 2015 por el Eurobarómetro 431 sobre protección de datos (European Commission, 2015) y el Barómetro del CIS de febrero de 2017 (Centro de Investigaciones Sociológicas, 2017) muestran la existencia de una conciencia de la ciudadanía europea sobre la recopilación de datos personales y un interés sobre el uso de los mismos. En el Eurobarómetro, a la pregunta sobre las consultas que realizan los ciudadanos a las políticas de privacidad, solo el 18% de los encuestados dicen leerlas completas, mientras el 49% afirman leerlas parcialmente, unas cifras algo inferiores en España. Pero cuando se pregunta por las razones de no leerlas, del 80% que las lee parcialmente o no las lee, el 67% aduce que son

demasiado largas y el 38% las encuentra poco claras o incomprensibles, cifra esta última que sube al 46% en España. En el Barómetro del CIS, un 70,7% de los encuestados está total o parcialmente en desacuerdo con que tales políticas sean claras o sencillas de entender.

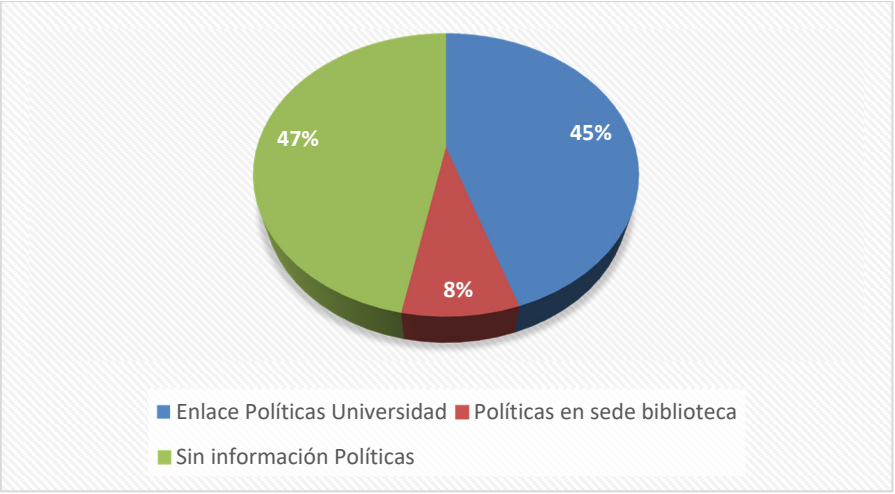
Por tanto, hacer disponibles las medidas sobre el tratamiento de datos privados en las bibliotecas posiblemente tiene efectos limitados sobre el conocimiento de los usuarios de las mismas; sin embargo, su publicación en la sede web de la biblioteca indica al menos la conciencia de estar tratando datos personales y de la obligación legal de informar a los usuarios del tratamiento de los mismos (LOPD, art. 5; RGPD, art. 1a). La Declaración de la IFLA (Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas, 2015) insiste en este aspecto: "Siempre que los servicios bibliotecarios y de información ofrezcan acceso a recursos, prestaciones o tecnología que pueda comprometer la privacidad de los usuarios, las bibliotecas deben favorecer que los usuarios sean plenamente conscientes de las implicaciones que esto conlleva y proporcionar una orientación sobre la protección de datos y de la privacidad".

Hay que señalar que en las bibliotecas analizadas la referencia a su política de privacidad, cuando existe, figura de dos formas distintas: como una página web de la biblioteca, opción claramente minoritaria, o como un enlace a la página de la Universidad correspondiente; y también bajo dos denominaciones distintas: como "Aviso legal", generalmente junto a otras cuestiones legales, o como "Política de privacidad". Es preciso indicar también que de las bibliotecas que poseen página específica sobre el tema en su sede web, solo una incorpora una redacción distinta a la página correspondiente de la Universidad, incluyendo una mayor información sobre la política de *cookies*.

Los datos del gráfico siguiente muestran que hay un amplísimo número de bibliotecas que no ofrecen en su sede web ninguna información respecto a las políticas de privacidad, aunque en algún caso aparece una declaración genérica al respecto en su carta de servicios, en las normas de acceso a la biblioteca digital o en el código ético de la biblioteca.

Por su parte, la información proporcionada por las Universidades sobre la protección de datos privados es muy variable, abarcando páginas que prácticamente se limitan a hacer una referencia a la legislación vigente o a las *cookies*, a otras más detalladas (**URL solicitadas por el IP**, tipos de *cookies*, analíticas web, etc.). En todo caso, una revisión de las mismas parece indicar una baja sensibilidad hacia la protección de datos en el medio universitario, como ya ha sido puesto de relieve en análisis sobre otros aspectos de protección de datos (Troncoso Reigada, 2006), o como parece indicar el hecho de que en la página web de Códigos Tipo de la AEPD (Agencia Española de Protección de Datos) solo figuren los de dos Universidades.

Gráfico 1. Políticas de protección de datos



En todo caso, las políticas de privacidad de las Universidades no comprenden el abanico de casos de tratamiento de datos personales que es factible encontrar en una biblioteca, y de los que es un buen ejemplo el documento de más de veinte páginas de la Biblioteca Pública de San Francisco (San Francisco Public Library, 2015), que señala para cada prestación los datos recopilados, su formato, dónde se localizan, quién tiene acceso y cuánto tiempo se guardan.

4. Datos privados en la gestión de identidades y búsquedas

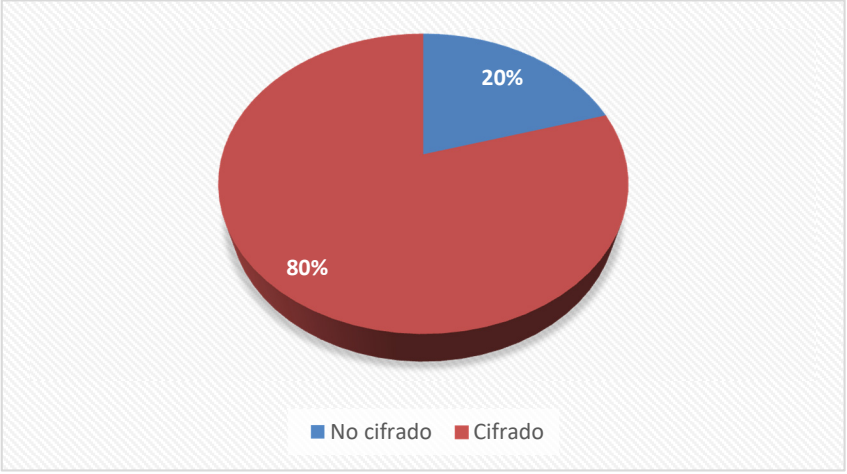
Tradicionalmente, anonimizar datos personales era un proceso sencillo, ya que resultaba suficiente eliminar los datos que permitían identificar a las personas (nombres, direcciones, etc.), lo que situaba a los datos restantes fuera de la protección de la legislación de datos, como indica el RGPD en su Considerando 26. Sin embargo, en plena fase de datos masivos (*Big Data*), la re-identificación de los individuos es un proceso sencillo (Gil González, 2016: 83), ya que el IP del usuario, almacenado por el proveedor de servicios de Internet, por el navegador y el buscador, por el alojamiento web del recurso consultado, y por los rastreadores de terceras partes embebidos en la página web, facilitan conocer datos personales. Las posibilidades de que esta información sea cruzada con otras que puedan identificar al usuario ha llevado a afirmar que los registros de uso de Internet en la biblioteca deben ser tratados con igual protección que los registros de préstamo de los usuarios (Chmara, 2009: 27). Todo ello ha planteado la redefinición del concepto de privacidad, cambiando el foco de la recopilación de datos al proceso y análisis de los datos (Mai, 2016: 198).

Dadas las facilidades de identificación proporcionadas por la tecnología, en el momento actual todas las búsquedas o accesos a través de Internet son susceptibles de ser interceptados y los usuarios que acceden a ellas pueden ser identificados, a

no ser que se cifren mediante algoritmos que transforman los datos haciéndolos en mayor medida indescifrables en el tráfico entre el buscador del usuario y el servidor al que se accede. La transmisión segura entre ambos es validada por una organización de certificación, identificándose por el protocolo https. Este protocolo es considerado la mejor forma de proteger a día de hoy la privacidad de los usuarios (Breeding, 2016).

Antes de comenzar este trabajo dábamos por supuesto que todas las páginas que demandan la autenticación de los usuarios (reservas, renovación de préstamos, acceso a recursos electrónicos, etc.) estaban cifradas en las bibliotecas. En muchos casos, especialmente en el acceso a bases de datos, revistas y libros electrónicos, la autenticación se realiza sobre servicios de identificación centralizados de las Universidades en páginas con el protocolo https. Sin embargo, para otras prestaciones, la identificación se realiza en la sede web de la biblioteca, habiendo un número significativo de bibliotecas en las que las páginas no están cifradas. En el gráfico siguiente se muestra el estado de las páginas donde el usuario hace reservas, renovaciones de préstamo, valoraciones o comentarios de libros:

Gráfico 2. Codificación de la identificación del usuario



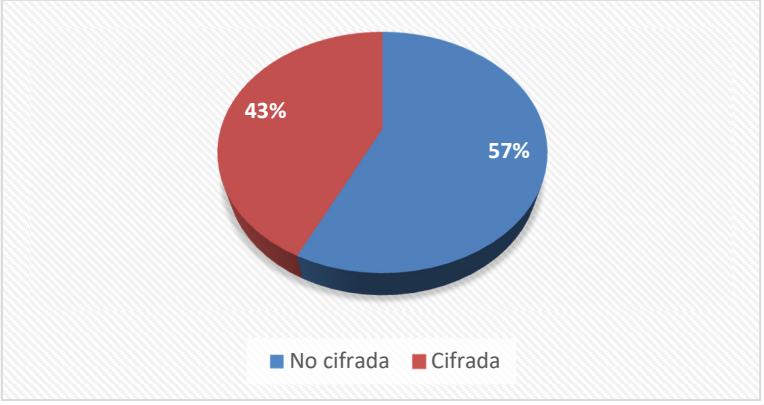
Por su parte, las páginas de búsqueda y resultados en los catálogos y de plataformas de descubrimiento carecen en mayor medida de codificación, pese a que hoy en día el coste de computación de cifrarlas es bajo. Si bien es cierto que tales búsquedas acostumbran a realizarse sin identificación previa del usuario, las capacidades tecnológicas de reidentificación han llevado a recomendar a las asociaciones profesionales (American Library Association, 2016) y a expertos en la materia (Breeding, 2015) que las páginas de búsqueda, lista de resultados y visualización de registros estén cifradas.

Hemos analizado el nivel de codificación de las páginas de búsqueda, generalmente la página principal, y las páginas con la lista de resultados en las bibliotecas analizadas. Los resultados pueden verse en los gráficos siguientes. El

primero de ellos analiza las páginas principales de las sedes web, que en la mayoría de los casos tienen la opción de realizar una búsqueda, aunque esta puede ser en la plataforma de descubrimiento, en el catálogo o en ambos. Cuando no existe la opción de búsqueda en la página principal hemos analizado la página que la permite.

Los dos siguientes gráficos analizan de forma separada las páginas de resultados en los catálogos y en las plataformas de descubrimiento. En las bibliotecas universitarias españolas encontramos tres sistemas disponibles en la actualidad para acceder a sus recursos: la interrogación directa al sistema de gestión de la biblioteca, la dirigida a una plataforma de descubrimiento separada del sistema de gestión de la biblioteca y la plataforma de descubrimiento, que se basa en un índice central dirigiendo la búsqueda al catálogo del sistema integrado, las bases de datos suscriptas y los repositorios digitales, generalmente fusionados con sistemas externos. A efectos de analizar la protección de datos en estos sistemas de recuperación, hemos tratado separadamente la búsqueda en los catálogos y la búsqueda en plataformas de descubrimiento, dado que los primeros podrían estar basados sobre programas que no permiten la codificación, en el caso de que se alojasen en sistemas de gestión antiguos, mientras que las plataformas, desarrolladas en los últimos años, deberían permitir la codificación.

Gráfico 3. Codificación en la página de búsqueda



El gráfico siguiente muestra los resultados de las bibliotecas que proporcionan la opción de consultar el catálogo separadamente de la plataforma de descubrimiento, en total cuarenta bibliotecas, mientras que el segundo presenta los resultados de las búsquedas en plataformas de descubrimiento instaladas en treinta y seis bibliotecas.

Gráfico 4. Codificación de la página de resultados en catálogos

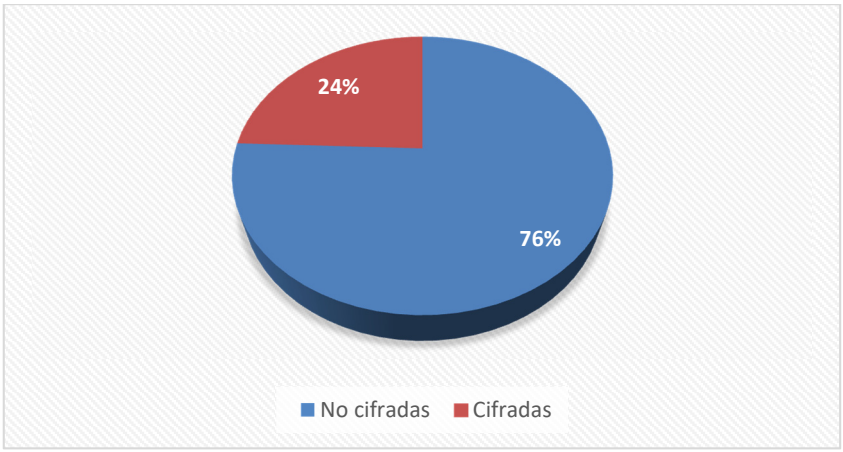
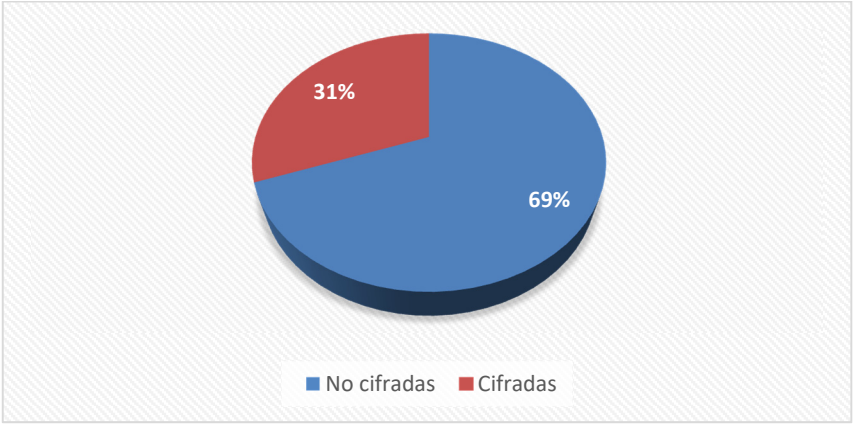


Gráfico 5. Codificación de la página de resultados en plataformas de descubrimiento



El análisis de los tres gráficos muestra que la codificación es baja cuando el usuario establece el término de búsqueda, pero todavía es menor cuando se le muestran los resultados en los catálogos. En las plataformas de descubrimiento, el porcentaje de páginas de resultados cifradas es ligeramente superior, pero muy bajo. Hay que señalar que todas las plataformas instaladas en las bibliotecas analizadas funcionan cifradas o dan la posibilidad de hacerlo (Breeding, 2016), como muestra el hecho de que en todas hay alguna biblioteca que muestra los resultados con una conexión cifrada, excepto la que tiene una sola instalación en bibliotecas universitarias, pero que, sin embargo, está cifrada en bibliotecas no incluidas en este análisis. El bajo nivel de codificación encontrado en los datos expuestos parece de nuevo indicar una limitada conciencia y/o formación en privacidad de los responsables de las bibliotecas que ponen en marcha estas plataformas, al tiempo que los aspectos referidos a la protección de datos privados

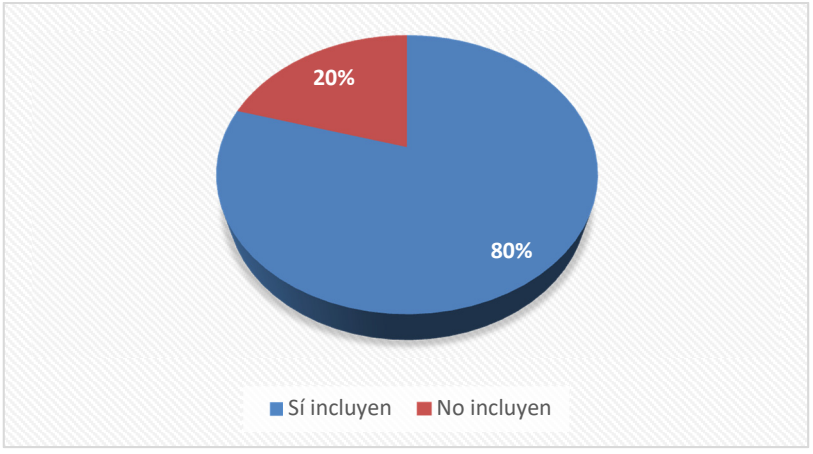
no son citados en la bibliografía española que analiza las funcionalidades de las mismas (Ávila-García; Ortiz-Repiso; Rodríguez-Mateos, 2015 y Rodríguez Yunta, 2015, entre otros).

5. Del control de autoridades a la gestión de identidades

Uno de los problemas presentes en el control de autoridades es la coincidencia de apellidos y nombres de dos o más autores distintos. Ya en 1961, la Declaración de Principios de Catalogación de la IFLA señalaba la necesidad de desambiguación en los casos de puntos de acceso de autores con nombres idénticos, pero sin indicar cómo debía de hacerse (Sandberg, 2016: 2). Las Reglas de Catalogación españolas (1999: 448) optaron por deshacer la ambigüedad añadiendo especificaciones que "pueden ser nombres de profesión, títulos, orden o congregación religiosa, «padre», «hijo», «jr.», «sénior», etc. Cuando se conozca, es suficiente con indicar el año de nacimiento o, en su caso, de nacimiento y de muerte". Además, las Reglas ofrecen también la opción de añadir a cualquier nombre de personas las fechas de nacimiento y muerte, sin especificar si deben ser ambas o podría utilizarse solamente la primera. Este aspecto no resulta baladí, teniendo en cuenta que el RGPD solo protege a las personas vivas.

La práctica de comunicar las fechas de nacimiento de los autores en el catálogo está ampliamente representada en las bibliotecas analizadas, como puede verse en el gráfico siguiente, en el que se analiza la aparición de fechas de nacimiento de autores vivos presentes en los catálogos en los casos en que no existe ningún otro autor o autora en el catálogo con iguales apellidos y nombre, lo que no es compatible con la minimización de datos (LOPD, art. 4.1, RGPD, art. 5, 1c).

Gráfico 6. Fechas de nacimiento presentes en los catálogos



Un caso semejante es la divulgación de nombres de autores que firman con pseudónimos, práctica también frecuente en los catálogos analizados. En este caso el Texto Refundido de la Ley de Propiedad Intelectual (Art. 14.2) indica que es un derecho moral de un autor "Determinar si tal divulgación ha de hacerse con su nombre, bajo seudónimo o signo, o anónimamente".

Pero en el panorama internacional no parecen desparecer estos problemas, sino más bien multiplicarse. La IFLA, en *Functional Requirements for Authority Data* (Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas, 2009), introduce, en el marco de los desarrollos tecnológicos y la web semántica, los atributos aplicados a entidades, que en el caso de las personas amplían considerablemente los incluidos en *Requisitos Funcionales de los Registros Bibliográficos* (FRBR), entre otros lugar y fecha de nacimiento, género, lugar de residencia y dirección. Paralelamente se han desarrollado campos MARC adicionales para almacenar estos nuevos datos.

El nuevo estándar de catalogación, *Recursos, Descripción y Acceso* (RDA), basado en FRBR y FRAD, comenzó a aplicarse en los países anglosajones en 2013 y también ha sido adoptado por algunas bibliotecas europeas. Nos fijamos aquí en las pautas generales sobre la identificación de personas de RDA, ya que abarcan un gran número de datos personales. Hay que señalar, en primer lugar, que algunos de los datos desde la perspectiva europea de protección de datos son especialmente delicados (género, dirección), y que las fuentes permitidas para la obtención de estos datos son ilimitadas en RDA. En cuanto a la fecha de nacimiento, se indica como obligatoria si es necesaria para distinguir una autoridad de otra y, opcionalmente, aunque no lo fuese. En ambos casos forma parte del punto de acceso. Otros datos, como género, lugar de nacimiento, dirección, etc. no se registran como puntos de acceso, es decir, formarán parte de la base de datos pero no tendrán un despliegue público. Esta identificación de las personas mediante atributos ha sido objeto de distintas críticas de profesionales y académicos del área, muy especialmente los referidos al género (Billey; Drabinski; Roberto, 2014 y Thompson, 2016), sin que falten alertas sobre otros atributos relacionados con la privacidad.

Todo ello, desde nuestro punto de vista, plantea problemas en relación a la protección de datos, teniendo en cuenta que tales datos entran en conflicto con lo señalado en el RGPD sobre el tratamiento de datos, que requeriría, en nuestro caso, consentimiento del interesado o cumplimiento de una misión de interés público (Art. 6.1), pero para esta última se exige que la base del tratamiento esté establecida sobre el Derecho de la Unión o el Derecho de los Estados miembros (Art. 6.3). Es posible, aunque para nosotros dudoso, que tales datos pudieran justificarse en función de la finalidad de archivo de interés público (Art. 89), un concepto que el RGDP no aclara, pero que en todo caso requiere minimización de los datos. Entendemos, por tanto, que el tratamiento de datos personales que carece de finalidad de desambiguación no podría ser nunca utilizado y el que es válido para este fin no podría ser aplicado, al menos de momento, mientras no exista la base jurídica. Los actuales trabajos sobre el uso de identificadores de autores en el control de autoridades y técnicas automáticas de desambiguación no basadas en datos personales (Zhang, 2017) podrían llevar a solucionar este problema en el futuro.

6. Desarrollo de la competencia digital

Los términos que se utilizan para denominar los procesos formativos en competencias relacionadas con el acceso, uso y creación de información en el contexto tecnológico actual son variados (alfabetización informacional, alfabetización digital) y también las competencias desarrolladas en esta formación han recibido diversos nombres (competencias informacionales, competencias informáticas e informacionales). También se ha propuesto una nueva área, la alfabetización en privacidad, como un campo independiente de instrucción para las bibliotecas (Wissinger, 2017). Aquí utilizaremos el concepto de alfabetización digital de la IFLA (Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas, 2017), y el de competencia digital, tal y como ha sido denominado por el proyecto DIGCOMP del Joint Research Centre de la Comisión Europea (Ferrari, 2013). De las áreas establecidas en este último informe, Información, Comunicación, Creación de contenido, Seguridad y Resolución de problemas, las dos últimas son transversales. La seguridad se refiere a protección personal, protección de datos, protección de la identidad digital, medidas de seguridad y uso seguro y sostenible.

Rebiun publicó una adaptación del texto del proyecto DIGCOMP (Red de Bibliotecas Universitarias, 2016) y estableció las equivalencias con el modelo CI2 (Red de Bibliotecas Universitarias, 2016). En el último documento se muestra la cobertura de CI2 en relación a muchos aspectos de protección de datos del modelo de competencia digital, sin embargo, existe escasa presencia de su desarrollo en las bibliotecas que estudiamos. Hemos revisado en los cursos de formación (presenciales o virtuales e integrados o no en la formación reglada) y en los tutoriales en línea, la presencia de contenidos referidos al área de Seguridad. En los cursos de formación hemos analizado los contenidos en las páginas web y guías docentes, cuando están disponibles, y, a falta de ambas, en los objetivos de los cursos. En muy pocos casos hemos encontrado objetivos o contenidos que correspondan al área de Seguridad, y en menos a la protección de datos personales, aunque algunos aspectos podrían figurar bajo denominaciones genéricas como “aspectos legales” que, cuando se explicitan, generalmente guardan relación con la propiedad intelectual y el plagio. Por tanto, no creemos que los resultados estén muy alejados de los que se muestran en el gráfico siguiente. En él no distinguimos la información correspondiente a cursos y tutoriales, dado que la protección de datos solo aparece en los últimos y en páginas web, en ambos casos de forma exigua.

Gráfico 7. Presencia de formación sobre protección de datos personales en las sedes web

7. Conclusiones y recomendaciones

La protección, exigida por la legislación que intenta regular el considerable tráfico de datos privados, responde al fortísimo impacto de la tecnología sobre multitud de aspectos de la vida de los ciudadanos. Estos son conscientes de la desprotección de sus datos en el entorno digital, como muestran los barómetros a los que hemos hecho referencia. Las bibliotecas no son ajenas a estas implicaciones, ya que son cada vez más dependientes de la tecnología. Los resultados encontrados en este trabajo indican carencias de protección en las bibliotecas que deberían subsanarse. Es preciso advertir que estudios realizados sobre bibliotecas de otros países no han producido resultados mucho más satisfactorios (Bailey, 2018, Dixon, 2008 y Magi, 2008).

El hecho de que en estas bibliotecas todavía exista un porcentaje significativo de páginas en las que se establecen las búsquedas en el catálogo que no están encriptadas, y que este porcentaje sea próximo o superior al 70% en las páginas de resultados de las plataformas de descubrimiento y catálogos, es altamente indicativo de la escasa conciencia o formación de los responsables de la seguridad de las bibliotecas en relación con la protección de datos personales en el entorno digital. La existencia de un 20% de bibliotecas que no cifran las páginas en las que los usuarios introducen su identificación para las prestaciones que se permiten realizar a través del catálogo es altamente preocupante. Esta situación puede disuadir a usuarios y a determinados colectivos a plantear búsquedas sobre ideas controvertidas, ya que pueden ser monitorizados, con las consiguientes implicaciones en la libertad de pensamiento y expresión (Ard, 2014: 6). La situación será todavía más grave si las bibliotecas no analizan y negocian con detenimiento el tratamiento de datos hechos por terceras partes que dan acceso a contenidos, especialmente cuando su identificación no está cifrada, y más aún si no conocen si los datos serán transferidos a otras empresas u otros países fuera de la Unión Europea.

El uso y divulgación de datos personales de autores vivos en los catálogos de las bibliotecas es altamente mayoritario y parece imposible que se cuente con su

autorización explícita para incluirlos, una condición que el 69% de los encuestados en el Eurobarómetro citado considera ineludible en todos los casos, cifra que se eleva al 80% en España (European Commission, 2015: 58-60). En cumplimiento del principio de minimización de datos de RGPD, estos no deberían ser usados cuando no existe homonimia en los nombres de los autores. La comunidad bibliotecaria internacional debería buscar nuevos sistemas que permitan la desambiguación de la autoría sin comprometer datos personales.

Por todo esto, consideramos necesario que las bibliotecas universitarias realicen una auditoria sobre la gestión de los datos personales que tratan, incluyendo las políticas de sus proveedores al respecto, con especial atención a las transferencias de datos a países fuera de la Unión Europea, ampliamente reguladas por el RGPD. Registrados los lugares en que tales datos están implicados, deberían de analizar las debilidades de seguridad a los que pueden ser sometidos los datos personales y poner en marcha las medidas necesarias para el cumplimiento del RGPD, así como de la Ley española resultante de su aplicación. En relación a los nuevos desarrollos de productos tecnológicos, las bibliotecas deberían analizar cuidadosamente la protección por diseño y por defecto, también presentes en estos textos legales.

Hasta el momento, las bibliotecas analizadas no han desarrollado políticas transparentes sobre el tratamiento de los datos personales que utilizan, para qué los utilizan, si son o no transferidos a terceros, cuándo se destruyen, etc. Los datos encontrados en nuestro análisis sobre la presencia de políticas de privacidad en las bibliotecas de Universidades públicas españolas requieren una actuación urgente en este aspecto, que permita conocer dónde y qué datos personales se recopilan de cada sede web. Teniendo en cuenta la diversidad de prestaciones implicadas, encontraríamos adecuado que, más allá de los enlaces a las políticas de las propias Universidades, las bibliotecas elaborasen una política propia, que debería ser redactada a partir del análisis de la gestión de datos personales que realizan y no una mera transposición de la política de la institución a la que pertenecen.

Vistos los resultados del Eurobarómetro 431 y del Barómetro del CIS 2017 en relación a las dificultades que muestran los ciudadanos en la lectura de estas políticas, sería conveniente que las bibliotecas, en aquellas páginas en las que los datos personales podrían estar más comprometidos, incluyesen información específica sobre el uso de datos en el servicio concreto, o un enlace al lugar de la política general donde se especificase el tratamiento realizado. Cuando los servicios son contratados con terceras partes, incluyendo los servicios de métricas web, debería también ofrecerse en las políticas de privacidad de las bibliotecas un enlace a las políticas de esos proveedores.

Teniendo en cuenta la situación encontrada, otras dos acciones parecen ineludibles para los responsables de las bibliotecas universitarias aquí analizadas: formar a su propio personal en protección de datos y formar ciudadanos más competentes en los temas de seguridad de sus datos. En este último aspecto, los resultados incluidos en nuestro análisis no son tampoco optimistas, aunque esperamos que las acciones futuras para la implantación de los programas de competencia digital puedan subsanar este problema y, a la vez, servir para que el

personal de las bibliotecas tome conciencia de la necesidad de proteger los datos personales implicados en sus sistemas de gestión.

8. Refrencias bibliográficas

American Library Association (1939). *Code of Ethics for Librarians*. <www.ala.org/Template.cfm?Section=History1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=8875>. [Consulta: 17/02/2018]

American Library Association (2015). *Library Privacy Guidelines for E-book Lending and Digital Content Vendors*. <www.ala.org/advocacy/privacy/guidelines/ebook-digital-content>. [Consulta: 15/04/2018]

American Library Association (2016). *Library Privacy Guidelines for Data Exchange Between Networked Devices and Services*.
<http://www.ala.org/advocacy/privacy/guidelines/dataexchange>. [Consulta: 15/04/2018]

American Library Association (2016). *Library Privacy Guidelines for Library Management Systems*. < www.ala.org/advocacy/privacy/guidelines/library-management-systems>. [Consulta: 26/02/2018]

American Library Association (2016). *Library Privacy Guidelines for Library Websites, OPACs, and Discovery Services*. < www.ala.org/advocacy/privacy/guidelines/OPAC>. [Consulta: 15/04/2018]

American Library Association (2016). *Library Privacy Guidelines for Public Access Computers and Networks*. < www.ala.org/advocacy/privacy/guidelines/public-access-computer>. [Consulta: 15/04/2018]

American Library Association; Canadian Library Association; CILIP (2017). *RDA Toolkit.* <https://access.rdatoolkit.org>. [Consulta: 18/03/2018]

Ard, B.J. (2014). Confidentiality and The Problem of Third Parties: Protecting Reader Privacy in the Age of Intermediaries. *Yale Journal of Law and Technology*, 16 (1), Article 1. <http://digitalcommons.law.yale.edu/yjolt/vol16/iss1/1>. [Consulta: 29/03/2018]

Ávila-García, L.; Ortiz-Repiso, V.; Rodríguez-Mateos, D. (2015). "Herramientas de descubrimiento: ¿una ventanilla única?". *Revista Española de Documentación Científica*, 38, 1, 1-17. <http://dx.doi.org/10.3989/redc.2015.1.1178>. [Consulta: 27/02/2018]

Bayle, J. (2018). Data Protection in UK Library and Information Services: Are We Ready for GDPR?. *Legal Information Management*, (18), 28–34.

Biblioteca Pública de San Francisco. *Library Patron Privacy Inventory*. <https://sfpl.org/index.php?pg=2000001301>. [Consulta: 26/02/2018]

Billey, A.; Drabinski, E.; Roberto, K.R. (2014). What's Gender Got to Do With It? A Critique of RDA Rule 9.7. *Cataloging & Classification Quarterly*, 52, (4), 412-421.

Breeding, M. (2016). The Current State of Privacy and Security of Automation and Discovery Products. *Library Technology Reports*, may/june, 13-28. <https://journals.ala.org/index.php/ltr/article/view/5974>. [Consulta: 27/02/2018]

Breeding, M. (2015). Perspectives on Patron Privacy and Security. *Computers in Libraries*, 35, 5, 12-14.

Centro de Investigaciones Sociológicas (2017). *Barómetro de febrero 2017*. <http://www.cis.es/cis/opencm/ES/1_encuestas/estudios/ver.jsp?estudio=14329>. [Consulta: 10/03/2018]

Cavoukian, A. (2012). *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*. <www.ontla.on.ca/library/repository/mon/26012/320221.pdf>. [Consulta: 07/02/2018]

Chmara, T. (2009). *Privacy and confidentiality issues: a guide for libraries and their lawyers*. Chicago: ALA Editions.

Dixon, P. (2008). Ethical Issues Implicit in Library Authentication and Access Management: Risks and Best Practices. *Journal of Library Administration*, 47:3-4, 141-162. <https://doi.org/10.1080/01930820802186480>. [Consulta: 07/02/2018]

European Commission (2015): *Special Eurobarometer 431. Data protection. Report*. <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/yearFrom/1974/yearTo/2015/surveyKy/2075>. [Consulta: 06/03/2018]

Ferrari, A. (2013). *DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe*. <http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=6359>. [Consulta: 15/03/2018]

Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas (2014). *Manifiesto de la IFLA sobre Internet*. <https://blogs.ifla.org/lac/2014/11/manifiesto-de-internet-de-la-ifla-2014>. [Consulta: 05/02/2018]

Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas (2015). *Declaración de la IFLA sobre la privacidad en el Entorno bibliotecario*. < www.ifla.org/node/9811>. [Consulta: 05/02/2018]

Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas (2017). *IFLA Statement on Digital Literacy*. <www.ifla.org/publications/node/11586>. [Consulta: 20/03/2018]

Federación Internacional de Asociaciones de Bibliotecarios y Bibliotecas. Working Group on Functional Requirements and Numbering of Authority Records (2009). *Functional Requirements for Authority Data: A Conceptual Model*. <www.ifla.org/publications/functional-requirements-for-authority-data>. [Consulta: 25/03/2018]

Gil González, E. (2016). *Big Data, privacidad y protección de datos*. Madrid: Agencia Española de Protección de Datos.

Gómez-Barroso, J.-L. (2018). Uso y valor de la información personal: un escenario en evolución. *El profesional de la información*, 27 (1), 5-18.

Grava, L. (2017). *Personal Data Protection in the Eu –Cooperation and Competences of Eu and National Data Protection Institutions and Bodies. RGSL Research 18*. <hwww.rgsl.edu.lv/wp-content/uploads/2017/04/05_Grava_final.pdf>. [Consulta: 10/02/2018]

Magi, T. (2008). A study of US library directors' confidence and practice regarding patron confidentiality. *Library Management*, 29, 8/9, 746-756. <https://doi.org/10.1108/01435120810917341> . [Consulta: 05/03/2018].

Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society*, 32 (3), 192-199. https://doi.org/10.1080/01972243.2016.1153010 . [Consulta: 25/01/2018]

Pekala, S. (2017). Privacy and User Experience in 21st Century Library Discovery. *Information Technology and Libraries*, june, pp. 48-58. <https://doi.org/10.6017/ital.v36i2.9817>. [Consulta: 25/01/2018]

Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. *Boletín Oficial de las Cortes Generales*, 24 de noviembre de 2017. <www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF>. [Consulta: 25/01/2018]

Red de Bibliotecas Universitarias (2016). *Marco de Competencia Digital para estudiantes de Grado: Adaptación de DIGCOMP*. CRUE, 2016.

<http://rebiun.xercode.es/xmlui/handle/20.500.11967/65>. [Consulta: 14/04/2018]

Red de Bibliotecas Universitarias (2016). *Equivalencia de descriptores de la Competencia Digital (DIGCOMP) con el Decálogo CI2*. <www.rebiun.org/lineas-estrategicas/aprendizaje-investigacion/competencia-digital>. [Consulta: 14/04/2018]

"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…". *Diario Oficial de la Unión Europea*, 4 de mayo de 2016, pp. 1-88. <www.boe.es/diario_boe/txt.php?id=DOUE-L-2016-80807>. [Consulta: 10/02/2018]

Rodríguez-Yunta, Luis (2015). Servicios de descubrimiento basados en un índice centralizado: su expansión en las bibliotecas académicas españolas y futuras líneas de investigación. *Anuario ThinkEPI*, 9, 49-55.

San Francisco Public Library (2015). *Library Patron Privacy Inventory*. <https://sfpl.org/?pg=2000001301>. [Consulta: 28/02/2018]

Sandberg, J.; Jin, Q. (2016). How Should Catalogers Provide Authority Control for Journal Article Authors? Name Identifiers in the Linked Data World. *Cataloging & Classification Quarterly*, 54 (8), 537-552. <https://doi.org/10.1080/01639374.2016.1238429>. [Consulta: 28/02/2018]

Starr, J. (2004). "Libraries and National Security: An Historical Review". *First Monday*, vol. 9, nº 12. <http://firstmonday.org/article/view/1198/1118>. [Consulta: 08/03/2018]

Thompson, K. J. (2016). More Than a Name. A Content Analysis of Name Authority Records for Authors Who Self-Identify as Trans. *Library Resources & Technical Services*, 60, 3 (2016), pp. 140-155.

<https://journals.ala.org/index.php/lrts/article/view/6036>. [Consulta: 20/03/2018]

Troncoso Reigada, A. (2006). La publicación de datos de profesores y alumnos y la privacidad personal. Acerca de la protección de datos personales en las Universidades. *Revista de Derecho Político*, 67, 79-163.

Unión Europea. Grupo de Trabajo del Artículo 29 (2007). *Dictamen 4/2007 sobre el concepto de datos personales (WP 136)*. <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm>. [Consulta: 28/02/2018]

Vander Maelen, K. (2017). *Digital Privacy Protection Against Corporate Actors in the European Union: Benefits, Flaws and Repercussions*. Thesis submitted in partial fulfillment of the requirements for the degree of Master of Laws. Universiteit Gent. <https://lib.ugent.be/nl/catalog/rug01:002349516>. [Consulta: 17/02/2018]

Wissinger, C.L. (2017). Privacy Literacy: From Theory to Practice. *Communications in Information Literacy*, 11 (2), pp. 378-389. <https://doi.org/10.15760/comminfolit.2017.11.2.9>. [Consulta 14/04/2018]

Zhang, B.; AlHasan, M. (2017). *Name Disambiguation in Anonymized Graphs using Network Embedding*. In Proceedings of CIKM'17, Singapore, november 6–10. <https://arxiv.org/abs/1702.02287v4>. [Consulta: 20/03/2018].