LA PRESERVACIÓN DIGITAL Y LA PROTECCIÓN DE DATOS PERSONALES. DEL MITO DE LA CONTRADICCIÓN A LA REALIDAD DE LA CONVERGENCIA

DIGITAL PRESERVATION AND DATA PROTECTION. FROM THE MYTH OF CONFLICT TO THE REALITY OF CONVERGENCE

Autores:

Carlota Bustelo. Gabinete UMBUS (Carlota Bustelo & Asociados) carlota@carlotabustelo.com ORCID 0000-0002-1859-7920

Miguel Umlauff. Gabinete UMBUS (Carlota Bustelo & Asociados) miguel@carlotabustelo.com ORCID 0000-0001-8434-6161

Resumen:

Los avances tecnológicos han cambiado el paradigma de como gestionamos la disponibilidad de la información. Mientras la información nacida digitalmente comienza a ser la norma, los riesgos para los derechos fundamentales que da el acceso ilimitado a los datos personales se ha incrementado. Tradicionalmente la preservación digital y la protección de datos personales han recorrido caminos separados. Dando lugar al mito de que la normativa de protección de datos impide el archivo de los datos personales. Los autores defendemos que pese a la existencia de posibles puntos de conflicto mediante el trabajo conjunto en materia de protección de datos y de preservación digital es posible un cumplimiento estricto de la legislación de protección de datos y la preservación digital a largo plazo de la información.

Abstract:

Technological advancement has changed the paradigm of how we manage the availability of information. As digital-born information becomes the norm, the risks to fundamental rights that unlimited access to personal data gives have increased. Traditionally, digital preservation and personal data protection have gone their separate ways. Giving rise to the myth that data protection legislation prevents the archiving of personal data. The

authors defend that despite the existence of possible points of conflict through joint work on data protection and digital preservation, strict compliance with data protection legislation and long-term digital preservation of information is possible.

Palabras clave:

Preservación digital; Archivo electrónico; Protección de datos personales

Keywords

Digital Preservation; Digital Archive; Data Protection

1. INTRODUCCIÓN

Los avances tecnológicos en el ámbito de las tecnologías de la información han cambiado el paradigma de como gestionamos la disponibilidad de la información. Hasta hace muy poco nadie dudaba que un Archivo era un edificio (o un conjunto o parte de ellos) donde se almacenaban los documentos en papel que una organización generaba a lo largo del tiempo preservando la memoria de la organización de cara a las generaciones futuras. Hoy, la prevalencia de la documentación nacida digitalmente ha cambiado completamente una técnica que había permanecido estable durante a lo largo del tiempo. Igualmente ha cambiado la importancia y disponibilidad de nuestros datos personales, poco se imaginaba el constituyente cuando formuló el Artículo 18.4 de la Constitución[1], recogiendo los pocos trabajos del Consejo de Europa al respeto, el volumen de información personal que circularía por redes interconectadas, ni el valor de mercado (legal o ilegal) generado por esta información cuatro décadas después.

La conversión de Internet en una realidad omnipresente en nuestra vida, donde sucede gran parte nuestra vida personal y profesional, y la mayor interconexión entre los repositorios de datos ha requerido desarrollar una legislación sobre la protección de datos personales cada vez más estricta. Desde la aprobación de la LORTAD en 1992, el tema ha ido a una velocidad mayor que otras legislaciones, para llegar a la ley actual

[1] Art. 18.4 CE: “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”.

(LOPGDD, 2018). Por otra parte, el incremento de los flujos transnacionales de datos ha llevado a una necesaria armonización de las legislaciones europeas y a la aprobación en 2018 del Reglamento General de Protección de Datos (RGPD), como una legislación directamente aplicable al conjunto del territorio de la Unión Europea.

Al amparo de este marco legal, la protección de datos personales ha recaído en el campo de la seguridad de la información, mientras que el desarrollo de archivos electrónicos y plataformas de preservación digital son las nuevas tareas de los archiveros digitales comprometidos con la idea de qué la información importante debe preservarse para el futuro, y no sólo por razones históricas, sino también cómo apoyo a la sostenibilidad de las organizaciones, la preservación del *know-how* y la defensa de los derechos de las personas.

En este articulo ponemos de relieve los puntos de conflicto y defendemos que aún en la estricta aplicación de la legislación, hay posibilidades y formas de aplicarla de tal forma que no se pierda información relevante de cara al futuro.

2. ARCHIVOS Y PROTECCIÓN DE DATOS PERSONALES

Tradicionalmente en los archivos en papel, se ha hecho la labor de protección de datos personales impidiendo el acceso del personal no autorizado a los expedientes o documentos que contenían información sensible sobre personas. Esto ha sido posible durante mucho tiempo y ha sido posible porque el acceso a la información en los archivos es más limitado (requiere desplazarse físicamente) y es controlado *in situ* por los archiveros. Cuando había que anonimizar un documento se hacía una copia anonimizada y a nadie se le ocurría anonimizar un original.

Sin embargo, con la última legislación se ha extendido el mito de que de que el RGPD y, por ende a protección de datos personales impide el archivado de datos personales en los países de la Unión Europea. (Debunking the Myths of GDPR for your Archives, 2019), y se ha llegado a plantear el anonimizado de documentos originales, ya sean en papel o electrónicos. En el contexto de las administraciones públicas esto puede comprometer

la función clave de los Archivos en el derecho a la información y la necesaria transparencia de los gobernantes.

Si nos creyésemos y aplicásemos este mito a la información de hoy en día, sería completamente posible tener acceso sin problemas a las transcripciones del juicio por indecencia pública de Oscar Wilde, pero que en el futuro seamos incapaces de acceder a las transcripciones del juicio del 11-M; que podamos saber de la prolija vida sentimental de Lope de Vega, pero que a duras penas en un futuro sepamos donde residió un autor actual.

El primer factor que se debe de tener en cuenta al afrontar la supuesta contradicción entre el archivo y la protección de datos personales es que tanto el RGPD en su artículo 5.1.b)[2] como la LOPDGDD en su artículo 26[3] recogen que el tratamiento de datos personales con fines de archivo de interés público es, en todo caso, un tipo de tratamiento lícito, incluyendo datos de características especiales. Igualmente debemos de tener en cuenta que ni el RGPD ni la LOPDGDD han derogado ninguna de las leyes vigentes en materia de archivo y transparencia pública. Si bien es cierto que el propio legislador nos deja una advertencia muy clara “En todo caso, el hecho de que el legislador se refiera a la licitud de los tratamientos no enerva la obligación de los responsables de adoptar todas las medidas de responsabilidad activa” (LOPGDD, 2018).

El segundo factor es que la protección de datos personales (al menos en el RGPD) sólo se refiere a las personas vivas, es decir, a un horizonte temporal muy diferente al que se

[2] Art 5.1. RGPD: “Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»)”

[3] Art 26 LOPDGDD: “Tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas. Será lícito el tratamiento por las Administraciones Públicas de datos con fines de archivo en interés público, que se someterá a lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica con las especialidades que se derivan de lo previsto en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, 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, así como la legislación autonómica que resulte de aplicación.”

maneja en los archivos. Por lo tanto, se podría defender que la protección de datos personales en los archivos debe tener una limitación temporal, en que datos inicialmente protegidos dejen de estarlo.

3. PRESERVACIÓN DIGITAL Y PROTECCIÓN DE DATOS PERSONALES

En un mundo encaminado a convertirse en completamente digital, las técnicas y actividades utilizadas tradicionalmente en los archivos tienen que reconvertirse y adaptarse para seguir cumpliendo con su función. Uno de los puntos clave del entorno digital es poder acometer la preservación digital cómo una de las funciones clave de los archivos digitales o electrónicos.

En este artículo, denominamos proyecto de preservación digital, a todas las actividades y decisiones que se han de tomar para crear un repositorio de información digital que pueda ser preservada a lo largo del tiempo.

En el estado del arte actual, cualquier proyecto de preservación digital se basa en el modelo OAIS (Open Archival Information System - ISO 14721:2012), el modelo de referencia internacionalmente aceptado cuando se acomete esta tarea. El modelo OAIS se resume en un esquema sobradamente conocido que se representa en la siguiente figura.

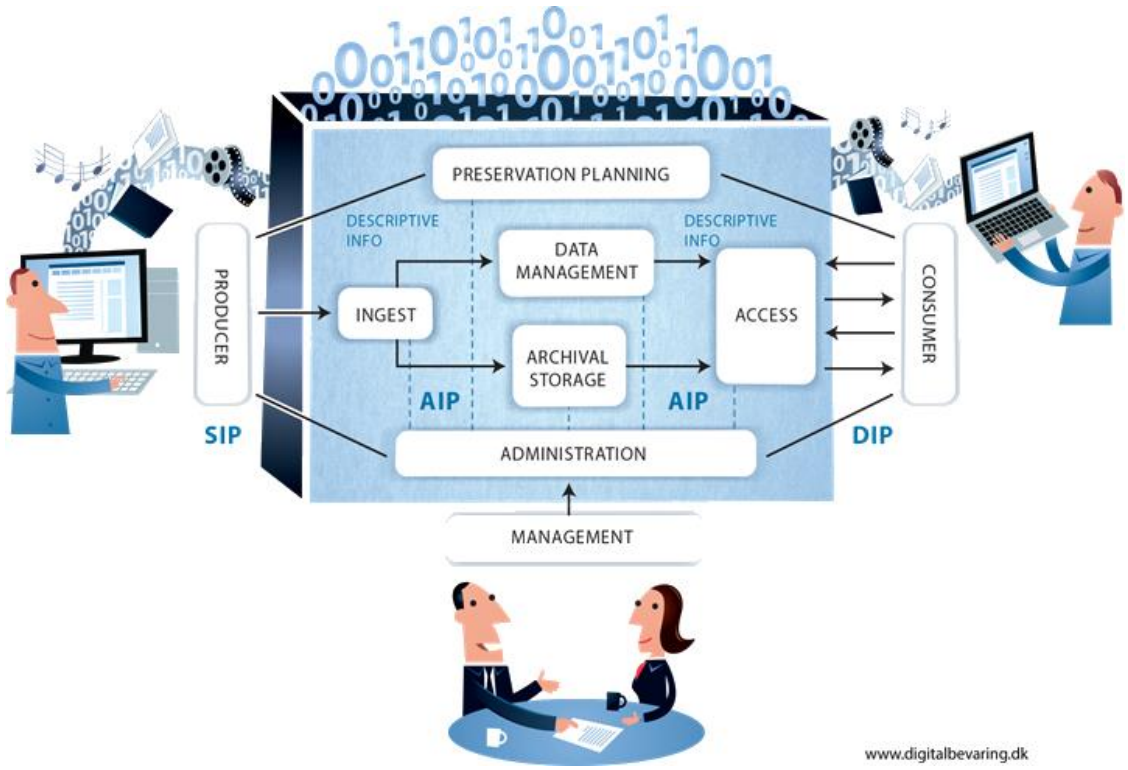

Figura 1
Modelo OAIS
Fuente: https://digitalbevaring.dk

El modelo OAIS está basado en los paquetes de información (de transferencia, de archivo y de difusión) que componen los objetos digitales, que son objetos de información, sobre los que se realiza la preservación. Estos objetos de información son objetos autocontenidos que contienen información suficiente para entender su formato y los metadatos que nos proporcionan la información que nos permite entender su contexto y sus condiciones de uso.

Cuando se acometen proyectos de preservación digital, el tema de la protección de datos personales suele ser también uno de los puntos en discusión. Desafortunadamente en algunos casos se plantea de la misma forma en que hemos expuesto en el capítulo anterior: si los datos personales no se pueden archivar, mucho menos se tendrán que preservar.

Sin embargo, los paquetes de información del modelo OAIS pueden ser tan complejos como sea necesario para poder archivar datos personales, pero asegurarse de que no se utilizan durante todo el periodo de tiempo que estén protegidos.

4. PUNTOS DE CONFLICTO

Pueden existir diferentes puntos de conflicto entre la protección de datos personales y la necesidad de preservarlos a largo plazo. En este capítulo tratamos de poner de relieve algunas de las circunstancias en las que esto sucede, que principalmente se deben a diferentes interpretaciones de los dos corpus legislativos.

— Existen situaciones donde puede prevalecer **el derecho a la transparencia** sobre el derecho a la protección de datos. Un ejemplo puede ser la actividad parlamentaria, donde se debe de entender que es fundamental preservar y dar acceso a datos personales incluso de carácter especial, como puede ser la adscripción ideológica (Actividad parlamentaria y protección de datos: el derecho al olvido en nuestro ámbito, 2019).

— Otra contradicción puede encontrase en las **firmas electrónicas** con certificado. A nadie le cabe duda de que los documentos firmados deben preservarse, pero las firmas pueden incluir datos considerados personales. Así por ejemplo la firma electrónica, está basada en un dato personal único como es el número de DNI, y que este debe ser visible, al menos en los metadatos, no existiendo forma de disociar esta información de un documento firmado que debamos de preservar. Esto incluye las firmas de los empleados públicos en el ejercicio de sus funciones. En el reciente Real Decreto 203/2021[4] se recoge la posibilidad de que ciertos

[4] RD 203/2021: “Artículo 23. Certificados electrónicos de empleado público con número de identificación profesional. 1. Sin perjuicio de lo previsto en el artículo 22.3 de este Reglamento, de acuerdo con lo previsto en el artículo 43.2 de la Ley 40/2015, de 1 de octubre, los prestadores cualificados de servicios de confianza podrán consignar un número de identificación profesional en el certificado electrónico de empleado público, a petición de la Administración en la que presta servicios el empleado o empleada de que se trate, si dicho certificado se va a utilizar en actuaciones que afecten a información clasificada, a la seguridad pública, a la defensa nacional o a otras actuaciones para cuya realización esté legalmente justificado el anonimato. Estos certificados se denominarán «certificados electrónicos de empleado público con número de identificación profesional».”

empleados públicos utilicen certificados electrónicos basados en el número de identificación profesional ocultando por lo tanto el nombre y el numero DNI, esto supone que la administración debe de guardar la relación entre el numero profesional y la identidad de la persona correspondiente que tendrá que ser revelada cuando se requiera por ejemplo por la administración de justicia. Desde el punto de vista de la preservación y la protección de datos esta medida elimina muchos problemas de cara al acceso a los documentos; pero abre otros nuevos como puede serla evaluación de la necesidad de preservar los registros de los números de identificación profesional.

— Uno de los grandes avances del RGPD es regular mejor los **derechos del interesado** para garantizar a las personas el control sobre sus datos personales. Esto puede parecer a veces contradictorio con la función de un archivo digital y la preservación a largo plazo. Aun así existen una serie de exenciones a estos derechos que están muy tasadas. El archivo por motivos de interés general es una de ellas. (European Archives Group, 2018). Debemos de entender que las exenciones no son absolutas y que todo proyecto de preservación digital debe de tener en cuenta algunas cuestiones clave de cara a ejecutarse. La “Guía para la protección de datos en los servicios de archivo” del Grupo Europeo de Archivos da muchas de las claves para compatibilizar los derechos del interesado con los Archivos. Resaltamos a continuación algunos de los elementos que se deben de tener en cuenta:

  - En relación con la **transparencia** se debe de mantener informados a los interesados sobre el procesamiento de sus datos, el objeto de este procesado, los plazos de conservación, el origen de sus datos si este no proviene de los mismos y a la forma de ejercer el acceso. Así, siempre que se recaben datos personales, en procedimientos que sean o puedan ser objeto de preservación permanente (o a muy largo plazo) es preciso

informar al interesado desde el inicio. En el caso de que las actividades de preservación digital recaigan o puedan recaer en una organización distinta a la que fue responsable inicial del tratamiento de datos esto debe indicarse desde el inicio. Igualmente es indispensable que los responsables del archivo digital lleven un control exhaustivo de los registros de tratamiento, tanto para su consulta pública como por parte de las autoridades de control.

- En un mundo más integrado e interoperable, el RGPD[5] garantiza a la ciudadanía el derecho a la **portabilidad** de sus datos entre distintos responsables de tratamiento. Aunque las transferencias entre archivos son poco comunes, ya se están realizando esfuerzos para poder garantizar estas en el futuro, un ejemplo de ellos ha sido el eArchiving Building Block de la Comisión Europea que plantea trabajar la necesaria interoperabilidad entre archivos electrónicos en un mercado único digital.

- El **derecho de supresión o derecho al olvido** es para los archivos el más complejo los derechos de los interesados, ya que comúnmente se puede entender como incompatible con la información designada como de preservación permanente. Es indudable que las exenciones del art. 17.3 del RGPD[6] a este derecho son de directa aplicación para los archivos. Aun así,

[5] Art 20 RGPD: "Derecho a la portabilidad de los datos 1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y b) el tratamiento se efectúe por medios automatizados. 2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible. 3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. 4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros"

[6] Art. 17.3 RGPD: "3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:
a) para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; c) por razones de interés público

es conveniente recordar que se deben de tomar medidas para evitar el acceso sin control a los datos personales contenidos en el archivo. La doctrina del Tribunal de Justicia de la Unión Europea ha entendido que algunas de las medidas que pueden dar cumplimiento al derecho al olvido sin poner en peligro la preservación permanente de un documento pueden ser acciones como el desindexado en buscadores, no permitir consultas automáticas de documentos con datos personales o no permitir las búsquedas que puedan menoscabar la dignidad de las personas.

5. POTENCIALES SOLUCIONES

5.1. Actuaciones en el origen de los datos

Por el contrario de lo que pudiera parecer, los proyectos de preservación digital no deberían entenderse cómo soluciones finalistas que recogen la información que ya ha sido creada bajo unas condiciones que le han sido ajenas.

Aunque el modelo OAIS, con su diferencia entre productores y archivo, pudiera indicar que el archivo no influye en la creación de la información, cada vez hay más voces autorizadas que concluyen que es fundamental la actuación desde la fase de diseño, es decir, antes incluso de la creación de la información.

En este sentido tanto la perspectiva a largo plazo cómo la protección de datos personales debería ser tenida en cuenta cuando se diseñan los sistemas que crean la información. Es curioso ver cómo se van llegando a las mismas conclusiones desde las distintas perspectivas, convergiendo en este caso en lo que se ha empezado a denominar *archiving by design* (Saaman, 2018) y *privacy by design* (Agencia Española de Protección de Datos, 2020) respectivamente.

en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3; d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o e) para la formulación, el ejercicio o la defensa de reclamaciones”

En estas actuaciones, en el origen de los datos podemos tener en cuenta los siguientes puntos:

- **Minimización de datos**

  Uno de los principios clave del RGDP y de la LOPGDD es el principio de minimización de datos. Si los datos no se necesitan realmente no se deben recoger, evitando tener que protegerlos posteriormente.

  Un ejemplo paradigmático de la necesidad de minimización de datos se encuentra en el procedimiento administrativo común que da lugar a la creación de expedientes electrónicos que posteriormente hay preservar. Existía una arraigada costumbre en papel de incluir una fotocopia del DNI y/o cualquier otra documentación de identificación del interesado en cualquier expediente, y esto se ha trasladado sin más al procedimiento electrónico, lo que convierte a veces a estas reproducciones en objetos de protección. Partiendo de la base de que es absolutamente innecesario con la legislación actual y con los servicios de interoperabilidad guardar estos documentos, si realmente se dejaran de pedir resolveríamos muchos de los problemas y tensiones entre archivo y protección de datos de expedientes electrónicos.

- **Armonización de cuadros de clasificación y registros de tratamientos**

  La metodología de elaboración de los cuadros de clasificación, misión tradicional del archivero o gestor documental, es similar o muy parecida a la forma en que se elabora del registro de tratamientos de datos personales por parte del delegado de protección de datos (El archivero/a como DPD, 2021). La convergencia de estos procesos es necesaria para garantizar el éxito del cumplimiento normativo en materia de protección de datos en los proyectos de preservación digital a largo plazo.

  En este sentido definiendo claramente al comienzo de cualquier proyecto de preservación digital el qué y para qué estamos preservando la información la organización nos ayudará las necesidades de protección de datos de nuestro archivo digital. Ya que no es lo mismo la preservación de datos estadísticos de la

organización, las actas de un pleno municipal o la correspondencia de un directivo de la organización. Igualmente debemos de definir quién es el usuario del archivo, ya que no requiere los mismos niveles de protección el usuario interno que el usuario externo. E incluso en caso del usuario externo, no es lo mismo el ciudadano que accede al archivo en ejercicio del derecho de transparencia que el envío de documentación a juzgados y tribunales. Nuestra experiencia profesional nos ha venido demostrando que conocer y definir estas cuestiones es fundamental al principio del proyecto.

— **Análisis de riesgos**

Una vez definidos los datos personales que se están preservando en un archivo electrónico se debe de tener en cuenta en cuenta los riesgos potenciales para las derechos y libertades[7] que estos puedan entrañar. En caso de que, tras una evaluación preliminar, se entienda que existe un riesgo alto, el RGPD en su art. 35.1 recoge la obligación de realizar un Evaluación de Impacto Relativa a la de Protección de Datos (EIPD). La EIPD es un proceso para identificar y evaluar el riesgo que puede suponer para un individuo el procesado de sus datos personales (European Archives Group, 2018). Este proceso debe de estar integrado en la gestión del riesgo e indica las acciones a tomar para mitigar los riesgos y demostrar el cumplimiento normativo (Agencia Española de Protección de Datos, 2021). Al afrontar la mitigación de riesgos puede darse la tentación por parte de algunos

[7] RGPD: “Considerando 75 Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la pseudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados”

responsables de protección de datos de proponer que determinados datos no se encuentren sujetos a preservación permanente, especialmente si estos carecen de la perspectiva de la profesión archivística. Por ello entendemos que la participación o al menos el acompañamiento por parte de los responsables de archivo es fundamental en este proceso para evitar la pérdida de información por exceso de celo.

5.2. Actuaciones en el archivo

La preservación digital da una importancia clave a las actuaciones a realizar durante el ciclo de vida de la información archivada. Tras siglos sabiendo y perfeccionando como preservamos y proteger la información en papel, nos enfrentamos a nuevas situaciones tales como la degradación de datos, la obsolescencia de formatos o los accesos remotos no autorizados entre otros.

El modelo OAIS integra estás acciones en las funciones de Almacenamiento de Archivo, Administración de los datos y Acceso cuando se refieren a la información preservada y las funciones de Planificación para la Preservación y Administración del archivo cuando se refieren al propio archivo.

Las medidas orientadas a la protección de los datos personales deben de entenderse como una parte integral las funciones de Planificación y Administración.

Por otro lado, los paquetes de información de archivo (PIA) van incorporando nuevos metadatos que responden a las distintas acciones que se realizan o los potenciales cambios de estado en las condiciones de protección y acceso.

Los aspectos claves a tener en cuenta son:

— **Seguridad**

Para garantizar la protección de datos personales en los proyectos de preservación digital es indispensable trabajar en la seguridad del propio archivo digital. Los archiveros son responsables de la seguridad de los datos personales

bajo su cuidado, y en conformidad con las prácticas profesionales existentes, salvaguardan su integridad y autenticidad y la protegen de accesos no autorizados, alteraciones, daños pérdidas y destrucciones. (European Archives Group, 2018). Para implementar las medidas de seguridad necesarias en los repositorios digitales, nuestra experiencia nos ha demostrado la importancia de integrar en los proyectos de preservación digital al Área de Seguridad de la Información, haciéndole parte del proceso de toma de decisiones en la implementación de cualquier tipo de proyecto de preservación digital, así como la importancia de estar al día de las innovaciones, amenazas en materia de seguridad.

— **Acceso**

Un aspecto fundamental para la protección de datos personales en los proyectos de preservación digital está en el control de acceso. El acceso de la información a largo plazo es una de las motivaciones de un archivo digital o un proyecto de preservación. Este acceso puede producirse internamente por la organización productora, para ser usados como elemento probatorio ante los tribunales de justicia o por la ciudadanía como forma de acceso a la memoria colectiva y al patrimonio documental. Así, siempre han existido salvaguardas legales para la protección de datos en los archivos, la Ley de Patrimonio Histórico ya recoge en su Art. 57 1.c) el plazo para la consulta de documentos que contengan datos personales (25 años después del fallecimiento o de 50 años en caso de que se desconozca la fecha de la muerte[8]). Aunque la legislación de 1985 más que previsiblemente no contemplase la idea de un archivo digital, nada nos debe de hacer dudar que este plazo se debe seguir aplicando a la hora de dar acceso público a los documentos de un repositorio digital, ya que el RGPD no ha alterado

[8] Ley de Patrimonio Histórico Español, artículo 57 1.c): “Los documentos que contengan datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida o, en otro caso, de cincuenta años, a partir de la fecha de los documentos.”

los periodos de conservación de la información y su acceso (European Archives Group, 2018).

Para hacerlo posible es necesario tener presentes los distintos perfiles de acceso que se pueden dar a la información que se está preservando. En terminología OAIS las comunidades designadas. Asociando estos niveles de acceso a los objetos digitales, e incluso a las distintas representaciones de un paquete de información, estaremos tomando las medidas necesarias para garantizar la protección de datos conforme al nivel de acceso. Así, por ejemplo, el acceso a documento electrónico archivado para su uso en un juicio no será igual que el de un investigador o el de un ciudadano.

— **Anonimización y pseudonimización**

En los proyectos de preservación digital, los procesos de despersonalización de la información tales como la anonimización y pseudonimización, orientados a impedir la identificación de las personas a lo largo del tiempo (Agencia Española de Protección de Datos, 2016) si bien pueden garantizar el acceso de una forma más generalizada, deben de ser contemplados con cautela, especialmente los procesos de anonimización ya que estos son de carácter permanente y pueden suponer una pérdida de información clave para las finalidades del archivo. Así, siempre que existan procesos de despersonalización debemos de entender que estos deben de realizarse siempre sobre una copia de consulta independiente.

6. CONCLUSIONES

Cuando se alían los proyectos de preservación digital y los proyectos de protección de datos personales pueden convertirse en un motor del cambio organizativo necesario en las organizaciones que transitan hacia un entorno completamente digital. Para ello es imprescindible el trabajo en grupos multidisciplinares que comprendan el punto de vista de los demás. A veces, en curso normal de las actividades es difícil de conjugar, porque cada grupo de personas tiene unas funciones encomendadas y unos objetivos de cumplir. Sin embargo, estamos seguros de que lo que en un inicio puede vislumbrarse como

potenciales retrasos en la implantación de un proyecto, acaba ofreciendo unos resultados que merecen la pena.

Cuando las circunstancias no se dan y las visiones no se comparten, las organizaciones corren riesgos importantes implantar proyectos que supongan pérdidas de información esencial o brechas de seguridad en la protección de datos personales; pero quizás el mayor riesgo que hemos observado es que los proyectos se queden en formulaciones teóricas cuya implantación práctica se retrase *sine die*.

La formulación de una metodología para trabajar con equipos multidisciplinares que incluyan la visión de la seguridad de la información, la protección de datos personales y la necesidad de conservación de la información comprensible a largo plazo, en el diseño de los sistemas de información es la gran esperanza de cara al futuro. De alguna manera hemos asumido que vamos a tener una laguna en el futuro sobre la información digital que ya se ha producido. Centrar los esfuerzos en que no vuelva a pasar es sin duda más eficiente y sostenible, que tratar arreglarlo a posteriori, por más técnicas que tengamos disponibles.

7. BIBLIOGRAFÍA

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2021). *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales.*
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2020). *Guía de Protección de Datos por Defecto.*
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2016). *Orientaciones y Garantías en los procesos de anonimización de Datos Personales.*
- AUZMENDI DEL SOLAR, Montserrat (2019) Actividad parlamentaria y protección de datos: el derecho al olvido en nuestro ámbito. En *Anuari del Dret Parlamentari*, p. 247-273.

- EUROPEAN ARCHIVES GROUP (2018). *Guidance on Data Protection for Archive Services.* Bruselas : Comisión Europea.

- GIMÉNEZ MARTÍN, Francesc. (2021). El archivero/a como DPD. En *Tabula,* p. 231-237.

- *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.* Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

- SAAMAN, Erik (2018). *Archiving by design. National Archives of the Netherlands.* [En línea] Disponible en https://www.nationaalarchief.nl/en/archive/knowledge-base/archiving-by-design

- SIMMONS, John. (2019). *Debunking the Myths of GDPR for your Archives.* Edinburgo: National Records of Scotland.