La protecció de dades en la digitalització de fons fotogràfics. Una oportunitat per a la gestió documental.

Mercè Roselló
Documentalista i Pedagoga, amb Màster en Societat de la Informació i el Coneixement per la UOC, especialitat en *E-law* i *E-government*.
merce.rosello.c@gmail.com

Resum:
L'objectiu d'aquest article és doble: d'una banda, presentar els conceptes d'aplicació jurídica en protecció de dades i, concretament, de la Llei orgànica 15/1999 de protecció de dades de caràcter personal (LOPD), amb una casuística a tractar per als documentalistes; d'altra banda, indicar com el disseny del sistema de gestió documental ha de contemplar els requeriments de tota aquesta normativa d'obligat compliment, però a més aquells aspectes menys pautats per la regulació i que requereixen l'elaboració de nous instruments o recursos per fer-la efectiva. Al llarg de l'article es plantegen qüestions i supòsits a partir de l'exemple de la implementació de models de gestió de dades personals per a encàrrecs de digitalització de fons fotogràfics. Finalment, l'aproximació al tema convida a preveure mecanismes per a garantir drets relatius a les dades personals en l'entorn tecnològic, dins dels processos de gestió documental.

Paraules clau:
protecció de dades, dades personals, dret a la intimitat, drets a la pròpia imatge, gestió documental, normes ISO, digitalització

La protección de datos en la digitalización de fondos fotográficos. Una oportunidad para la gestión documental.

Resumen:
El objetivo de este artículo es doble: por una parte, presentar los conceptos de aplicación jurídica en protección de datos y, concretamente, de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), con una casuística a tratar por los documentalistas; por otro, indicar como el diseño del sistema de gestión documental debe contemplar los requerimientos de toda esta normativa de obligado cumplimiento, pero además aquellos aspectos menos pautados por la regulación y que requieren la elaboración de nuevos instrumentos o recursos para hacerla efectiva. A lo largo del artículo se plantean cuestiones y supuestos a partir del ejemplo de la implementación de modelos de gestión de datos personales para encargos de digitalización de fondos fotográficos. Finalmente, la aproximación al tema invita a prever mecanismos para garantizar derechos relativos a los datos personales en el entorno tecnológico, dentro de los procesos de gestión documental.

Palabras clave:
protección de datos, datos personales, derecho a la intimidad, derechos a la propia imágen, gestión documental, normas ISO, digitalización

Data protection on digitizing of photo collections. An opportunity for document management.

Abstract:
The aim of this paper is twofold: on the one hand, introducing concepts of legal application in data protection and, in particular, of the Organic Law 15/1999 on the Personal Data Protection (LOPD) to deal with a casuistry for Documents Specialists; on the other hand, showing how the design of document management system should meet the requirements of all these mandatory regulations, but also those aspects less ruled by law that require developing new tools or resources to make it effective. The article explains how apply personal data protection law taking as case study the digitization of photographic collections. Finally, the approach to this subject aims to become an opportunity inviting you foresee, within documentation processes, some assurance mechanisms for rights that involve personal data in the technological management.

Keywords:
data protection, personal data, privacy rights, own image rights, records management, ISO standards, digitization

1. Introducció

La protecció de les dades de caràcter personal en l'entorn de la Societat de la Informació i el Coneixement constitueix una àrea de compliment normatiu indispensable per a la seguretat de les organitzacions i, que és alhora, indissociable de la necessària gestió de la informació i dels documents, que no sempre ha estat prou coneguda o resolta.

A l'hora de dissenyar un sistema de gestió documental (SGD), es fa necessari conèixer la vigència dels aspectes d'aplicació de la normativa de protecció de dades, quins aspectes hi queden poc o gens regulats i com es poden integrar al sistema conjuntament amb els contemplats a la normativa.

Però a més, la digitalització i, les implicacions que comporta la difusió a Internet de documents que contenen dades personals, obliga a considerar una normativa en matèria de seguretat que es troba subjecte a canvis i a homologacions a escala europea per ajustar-se als nous contextos tecnològics.

Quan hem de dur a terme la digitalització d'un fons fotogràfic amb imatges de persones, ens hem de plantejar qüestions prèvies dels requeriments normatius com: Quina és la procedència del fons a tractar en l'encàrrec? S'aplica igual la Llei de protecció de dades si es tracta d'un fons procedent d'una persona física o d'un fons corporatiu? I en qualsevol cas, per part del propietari del fons, és suficient el consentiment dels afectats o titulars per a legitimar la captura i difusió de les imatges? Quins mitjans jurídics i tècnics disposem per aplicar els drets dels titulars?

El propòsit d'aquest article és revisar els aspectes bàsics del marc jurídic vigent en protecció de dades, així com les eines de gestió documental que ens poden permetre acomplir-los i complementar-los, qüestions que han de tenir en compte aquells professionals o organitzacions que es proposen la digitalització i gestió documental de fons culturals de fotografies que contenen dades personals.

Més enllà de perseguir una finalitat didàctica, amb aquest article es convida a preveure el desenvolupament d'uns sistemes de gestió documental, que complementin i millorin els mecanismes de garantia de drets relatius a les dades personals en l'entorn tecnològic, requerits pel marc jurídic.

2. Quin és el marc jurídic d'aplicació?

2.1. Els drets fonamentals en protecció de dades i el context jurídic de la LOPD

La protecció de dades, com a conjunt de tècniques normatives o jurídiques, té per objecte garantir el dret fonamental consistent a què "l'individu tingui la capacitat d'exercir un control real sobre la seva informació"[1].

La Constitució espanyola de 1978 va ser-ne pionera en el reconeixement d'aquest dret fonamental, en preveure la **greu afectació en la intimitat de les persones que el tractament informàtic de dades pot comportar**, com recull en el seu article 18.4:

> *"4. La llei limitarà l'ús de la informàtica per tal de garantir l'honor i la intimitat personal i familiar dels ciutadans i el ple exercici dels seus drets."*

A Catalunya, l'Estatut d'Autonomia de Catalunya (2006), feia referència a l'accés, especialment el seu article 31, quant al dret de totes les persones a "la protecció de les dades de caràcter personal contingudes en els fitxers de la Generalitat, a accedir-hi, a examinar-les i a corregir-les". També s'hi contemplava l'accés i confidencialitat en matèria de salut en el seu article 23.3 i en matèria d'informació mediambiental en els art. 27.3 i 46.5.

1. Ricard Martínez, *Protección de datos de carácter personal en la Sociedad de la Información*. Barcelona: FUOC, 2005, Mòdul1, p.8.

I en línia amb el que recull la Constitució espanyola, trobem la Llei orgànica 1/1982, de 5 de maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge. Segons el seu art. 1.3 "El dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge és irrenunciable, inalienable i imprescriptible". Tanmateix com diu en el seu art. 8.1 "No es regularà com a intrusió al dret l'honor, a la intimitat i a la imatge quan predomini un interès històric, científic o cultural rellevant". D'altra banda, l'article 8.2, regula el dret a la pròpia imatge.

Pel que fa a la protecció de dades a l'Estat espanyol, queda regulada per:

– Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD), base de regulació modificada i desenvolupada posteriorment per altres reglamentacions, que defineixen les mesures a prendre:
– Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei orgànica 15/1999 , de 13 de desembre de protecció de dades de caràcter personal -d'ara endavant RDLOPD.

L'objecte de protecció de dades abasta qualsevol tipus d'informació personal, sigui o no íntima o relativa a la vida privada, el coneixement o ús del qual per tercers pugui afectar els seus drets.

Segons l'article 5 del RDLOPD, la **dada de caràcter personal** és: "qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus que concerneix persones físiques identificades o identificables". I amb relació a la persona identificable l'article diu "de la qual es pugui determinar, directament o indirectament, qualsevol informació referida a la identitat física, fisiològica, psíquica, econòmica, cultural o social". Però entenem que "una persona física no es considera identificable si la dita identificació requereix terminis o activitats desproporcionats".

En l'àmbit de la Unió Europea, el dret fonamental a la protecció de dades s'inclou en el Projecte de Tractat, –fracassat, per cert– pel qual s'institueix una Constitució per a Europa i prové de l'article 8 de la Carta de drets fonamentals de la Unió Europea (2000).

2.2. El marc jurídic de la digitalització a Espanya i a Europa

L'origen del dret a la protecció de dades resideix en l'evolució de les tecnologies de la informació i de la comunicació (TIC), i per tant, es tracta d'un dels anomenats drets de tercera generació. Aquest fet obliga a una comprensió de la realitat material sobre la qual s'aplica, així com un profund coneixement dels conceptes definits per la LOPD i pel RDLOPD i de tot el sector jurídic d'aplicació a causa del caràcter instrumental i/o transversal del dret fonamental a la protecció de dades[2].

En el marc espanyol, haurem de considerar la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic, que en el seu Annex, concep el "servei d'intermediació" com aquell servei pel qual es facilita la prestació o utilització d'altres serveis de societat de la informació.

A escala europea, la protecció de dades ha estat un dret desenvolupat originalment per la Directiva 95/46/CE del Parlament Europeu i del Consell de 24 de juliol de 1995, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades, i modificada posteriorment per la Directiva 97/66/CE, de 15 de desembre, amb mesures sobre l'àmbit de les comunicacions i la privacitat.

Més tard, la Directiva 2000/31/CE de 8 de juny de 2000, que fou objecte de transposició la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic, prenia com a base la definició de Serveis de

2. Ricard Martínez, "El dret fonamental a la protecció de dades". Agustí Cerrillo, *Les transformacions del dret a la societat de la informació*. Barcelona: FUOC, 2009, p.2.

©istockphoto/MikeLaptev

Societat de la Informació que en va fer la Directiva 98/34/CE del Parlament Europeu i del Consell, de 22 de juny de 1998. I cal contemplar també la Directiva 2009/136/CE del Parlament Europeu i del Consell, apareguda després, que modifica directives anteriors del sector de les comunicacions electròniques i protecció dels consumidors.

Actualment, com es va comentar en el número anterior d'aquesta revista[3] entorn de les dades que es troben al cloudcomputing, la dificultat per regular la complexitat de la diferent casuística de models de serveis cloud i clàusules de contractes amb proveïdors d'aquest àmbit, comporta la pèrdua de control de la informació i el seu impacte en el dret fonamental a la protecció de dades de caràcter personal. Tanmateix, per respondre a tots i cadascun dels supòsits de tractament de dades personals, mentre el Reglament Europeu resta pendent d'aprovació per al 2015, ens podem acollir a la regulació vigent feta per la Directiva Europea de Protecció de Dades[4], la prevista per la pròpia Proposta de Reglament Europeu[5], i el Dictamen del Grupo de Protección de Datos del Artículo 29[6] sobre la informàtica en núvol, de 1 de juliol de 2012, que ofereix una base per a la transició entre la Directiva i el Reglament.

Pel que fa a l'ús de mitjans electrònics en el sector públic, cal preveure en cada cas també els requeriments en protecció de dades de la legislació estatal i autonòmica corresponent.

3. Ricard Miralles, "Europa cloudcomputing i protecció de dades de caràcter personal." *Item*. Núm. 57 (2013), p. 81- 96.
4. La pedra angular de la legislació vigent a la UE: Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 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, DO L 281 de 23.11.1995. [En línia]. [Data de consulta: 18.04.2014]. Disponible a: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.4-cp--Directiva-95-46-CE.pdf
5. Propuesta de Reglamento del Parlamento Europeo y del Consejo 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. [En línia]. Bruselas, 25.1.2012 [Data de consulta: 18.04.2014]. Disponible a: http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF
6. Grupo del Artículo 29 sobre la Protección de Datos. Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y encargado del tratamiento» [En línia]. [Data de consulta: 18.04.2014]. Disponible a: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf

2.3. Quina altra legislació hem de contemplar?

A més de la legislació que es refereix estrictament a la protecció de dades, en el disseny d'un servei de digitalització que tracti gestió de documents i fons documentals caldrà contemplar-ne el marc jurídic específic, com les esmentades lleis del patrimoni i les dels arxius, en els àmbits català i espanyol:

La Llei 16/1985 Llei del patrimoni històric espanyol (LPHE), especialment en el seu article 57, pel que fa a la consulta dels documents del Patrimoni Documental.

La Llei 9/1993 del patrimoni cultural català (LPCC), l'objectiu d'aquesta Llei és la protecció, la conservació, el creixement, la investigació, la difusió i el foment del patrimoni cultural català.

La Llei 10/2001 d'arxius i documents (LAD), que distingeix entre documents públics i privats, que defineix en els capítols 6 i 7 respectivament.

3. Raons per adoptar les normes ISO

El fet de seguir les normes ISO, aquests estàndards tècnics que no són d'obligat compliment tret que ho requereixin alguns procediments institucionals, ens permetrà adoptar unes pautes a l'hora de sistematitzar processos en el treball de millora contínua dels serveis, així com contribuir a facilitar l'acompliment de la regulació jurídica vigent.

L'Organització Internacional de Normalització (ISO) és una federació mundial d'organismes nacionals, que en són membres. Des d'una perspectiva multidisciplinària, són diversos els Comitès Tècnics d'ISO que han assumit el repte de normalitzar els processos i tècniques aplicables a la gestió de documents i evidències electròniques.

Entre la sèrie de textos normatius, traduïts per l'AEN/CTN 50 d'AENOR *Documentació* i adoptats com a Normes UNE, els principals que fan referència als processos de digitalització i gestió documental són els següents:

- UNE-ISO 30300:2011 "Información y documentación. Sistemas de gestión para los documentos. Fundamentos y vocabulario." Aquesta norma aglutina la terminologia i aspectes transversals en l'eix estratègic d'un sistema de gestió documental. D'aquesta forma, permet treballar de forma integrada àrees, com la seguretat de la informació i la gestió documental.
- UNE-ISO 30301:2011 "Información y documentación. Sistemas de gestión para los documentos. Requisitos." Part de la mateixa sèrie que la norma anterior "Informació i Documentació. Sistemes de Gestió de Documents". Especifica els requisits per implantar un sistema de gestió de documents (SGD).
- UNE-ISO 13028:2011 IN "Informació i documentació. Directrius per a la implementació de la digitalització de documents".

Segons el contingut d'aquesta darrera norma, en són indispensables:

- UNE-ISO 15489-1:2001 "Informació i Documentació: Gestió de documents. Part 1: Generalitats".
- UNE-ISO/TR 15801:2009 "Imagen electrónica. Información almacenada electrónicamente. Recomendaciones sobre veracidad y fiabilidad". Equivalències amb: ISO/TR 15801:2004 (IDT). Amb solucions per garantir la fiabilitat de les imatges escanejades.
- UNE-ISO 23081-1:2006 "Información y documentación: Procesos de gestión de documentos. Metadatos para la gestión de documentos". Amb referència, especialment, la part 1 de Principis.
- UNE-ISO 2308-2:2009 "Información y documentación. Gestión de metadatos para documentos". Part 2, "Elementos de gestión y conceptuales".
- I en matèria de seguretat, tot ampliant els requeriments de la LOPD disposem de:
- UNE-ISO 27001 "Sistemas de Gestión de Seguridad de la Información".

Cal considerar també que, quan les comandes en els serveis de digitalització impliquin una negociació a la carta de característiques tècniques i certa indefinició dels procediments, aquestes recomanacions dels estàndards de qualitat, ens seran especialment útils.

4. El tractament de les dades i els diferents supòsits segons la LOPD

4.1. Els conceptes de tractament de les dades i de fitxer

El **tractament de les dades** personals, es farà des del primer moment de recepció i preparació per a la digitalització de la documentació, que segons l'art. 5 t) de la RDLOPD consisteix en:

> *"qualsevol operació o procediment tècnic, ja sigui **automatitzat o no**, que permeti la recollida, gravació, conservació, elaboració, modificació, consulta, utilització, modificació, cancel·lació, bloqueig o supressió, així com les cessions de dades que resultin de comunicacions, consultes, interconnexions i transferències."*

I d'acord amb l'article 5 (n) del RDLOPD, el **sistema de tractament** és la "manera en què s'organitza o utilitza un sistema d'informació" i existeixen sistemes d'informació automatitzats, no automatitzats o parcialment automatitzats.

Precisem alguns conceptes vinculats amb aquest procediment:

Sistema d'informació: "conjunt de fitxers, tractaments, programes, suports i, si s'escau, equips utilitzats per al tractament de dades de caràcter personal." (RDLOPD, art. 5)

I per **fitxer**, trobem una definició força genèrica: "qualsevol conjunt organitzat de dades de caràcter personal que permeti l'accés a les dades d'acord amb uns criteris determinats (...)". (RDLOPD, art. 5).

..., sempre que el fitxer jurídic s'utilitzi per a les finalitats d'un mateix àmbit de gestió, pot estar integrat per una diversitat de documents i suports que, poden incloure segons el tipus de tractament, fitxers automatitzats i/o fitxers manuals o no automatitzats.

Es fa necessari explicar el concepte de fitxer en aquestes definicions. Així, si bé el RDLOPD es refereix en aquestes definicions al fitxer lògic, que pot correspondre a documents de tipus i suports diversos, hem de distingir aquest concepte, del fitxer jurídic que hem d'inscriure al Registre de Protecció de Dades de Catalunya (RPDC).

Identifiquem com a fitxer jurídic aquell que el seu responsable utilitza i inscriu al RPDC per treballar un únic àmbit funcional de gestió amb unes finalitats determinades, i que està integrat per un conjunt de fitxers lògics, com poden ser el programari, els fulls de càlcul i els llistats d'una base de dades.

Per tant, sempre que el fitxer jurídic s'utilitzi per a les finalitats d'un mateix àmbit de gestió, pot estar integrat per una diversitat de documents i suports que, poden incloure segons el tipus de tractament, fitxers automatitzats i/o fitxers manuals o no automatitzats. I en cas que contingui fitxers d'ambdós tipus de tractament diferenciat, el procés d'inscripció del fitxer jurídic, preveu que fem constar que es tracta d'un fitxer mixt.

4.2. Casos d'aplicació i exclusió de la normativa

4.2.1. Fons culturals procedents d'una persona jurídica

Quant a les activitats professionals, l'article 2 del RDLOPD indica exclosos de l'àmbit d'aplicació de la normativa, les dades referides a: persones jurídiques; fitxers que es limitin a incorporar les dades de les persones físiques que hi prestin els seus serveis- i quan siguin consistents únicament en el nom i cognoms, les funcions o llocs exercits, l'adreça postal o electrònica, telèfon i fax professionals; dades relatives a empresaris individuals, quan hi facin referència en la seva qualitat de comerciants, industrials o naviliers; o persones mortes.

Per tant, els fons corporatius, en pertànyer a una persona jurídica, queden exclosos de la normativa.

4.2.2. Fons culturals procedents d'una persona física

Segons l'article 2 del RDLOPD esmentat, quan els fons pertanyen a un client final, és a dir, en qualitat de persona física, no queden exclosos de l'àmbit de protecció, i per tant, sí que haurem d'aplicar la normativa.

Recordem, però, que es tracta de fitxers que siguin usats per activitats professionals tant en els sectors públic com privat, i que no s'aplica a fitxers fets per a ús domèstic o personal, segons l'art. 4 del RDLOPD.

4.3. Àmbit subjectiu a aplicar per tipologia de fitxers:

Quant a l'àmbit subjectiu de competència de fitxers, hem de distingir tres figures: el titular de les dades; el responsable del fitxer o tractament, i l'encarregat de tractament.

©istockphoto/Andrew Rich

4.3.1. Titular de les dades

L'article 5è del RDLODP, defineix per afectat o interessat, com "la persona física titular de les dades que siguin objecte del tractament".

Cal tenir en compte que els titulars només podran ser persones físiques, en lògica coherència amb el que disposa l'art. 1 LOPD que remet el seu objecte de protecció als drets de les persones físiques[7]. Per tant, aquells fitxers o tractaments que continguin dades únicament procedents de persones jurídiques quedaran exclosos de l'aplicació de la norma. I pel que fa als empresaris individuals, tindrem en compte el que disposa l'article 2 del RDLODP, que n'exclou "quan hi facin referència en la seva qualitat de comerciants, industrials o naviliers".

7. Ricard Martínez, Protección de datos de carácter personal en la Sociedad de la Información. Barcelona: FUOC, 2005. Mòdul 1, p. 15.

4.3.2. Responsable del tractament o fitxer, habitualment dels propis

Quant a l'àmbit subjectiu de competència dels fitxers, sempre hi ha un responsable del fitxer o tractament, que segons la definició del RDLOPD és "la persona física o jurídica, de naturalesa pública o privada", qui decidirà, sola o juntament amb altres, "sobre la finalitat, contingut i ús del tractament, encara que no ho realitzi materialment"; i també, són responsables dels fitxers, "els ens sense personalitat jurídica que actuïn en el tràfic com a subjectes diferenciats".

Serà doncs, el responsable del fitxer o tractament, qui decideixi sobre l'ús de les dades personals i en l'àmbit privat, com a titular de l'activitat i dels seus propis fitxers. Tanmateix, hi ha empreses que realitzen el tractament d'aquestes dades a través d'un proveïdor extern, a qui fan un encàrrec de tractament.

4.3.3. L'encàrrec de tractament: serveis prestats a d'altres organitzacions

L'encarregat del tractament, és la "persona física o jurídica, pública o privada, o òrgan administratiu que, sol o conjuntament amb altres, tracti dades personals per compte del responsable del tractament", i ho faci a través d'un contracte, tal com regula l'article 5, paràgraf i, del RDLOPD. Així per exemple, quan una empresa o institució contracta un proveïdor extern per tal que digitalitzi el seu fons, aquest proveïdor extern esdevé l'encarregat del tractament.

Aquest tipus de contracte de serveis ha de dur una clàusula que contempli els aspectes previstos a l'art. 12 de la LOPD, com el fet que l'encarregat del tractament només ha de tractar les dades d'acord amb les instruccions del responsable del tractament i que no les pot aplicar ni utilitzar amb una finalitat diferent de la que figuri en el contracte esmentat, ni comunicar-les a altres persones, ni tan sols per conservar-les.

Així mateix, el contracte ha d'estipular les mesures de seguretat a què es refereix l'article 9 d'aquesta Llei i que l'encarregat del tractament està obligat a implementar, i el reconeixement de les circumstàncies concretes en què es realitzi la prestació de l'encarregat es faci constar en el document de seguretat d'acord amb l'art. 88 del RDLOPD.

Independentment, haurem de tenir en compte que quan aquest encàrrec provingui d'una persona jurídica, com pot ser el cas de la digitalització d'un fons corporatiu, no és de l'àmbit d'aplicació del RDLOPD. En aquest cas, la tasca de l'encarregat es limitarà a contribuir a acomplir les mesures de seguretat acordades per a la prestació del servei.

4.3.4. Subcontracte de serveis a un tercer:

La possibilitat de subcontractació de serveis amb un tercer per part de l'encarregat de tractament –per ex. un servidor d'Internet-, es regirà per les condicions establertes a l'article 21 del Reial Decret 1720/2007. La primera d'elles és que el responsable del fitxer, li hagi encomanat o l'hagi autoritzat a fer-ho, sempre a nom i per compte del mateix responsable.

5. Elements per evidenciar la legitimació i els principis de qualitat

Un cop hàgim identificat els fitxers a tractar, procedirem a la fase de legitimació per al tractament de les dades personals, que segons la llei inclou les següents subfases:

1. El deure d'informació previ al tractament
2. Principis i requeriments de legitimitat per a la recollida de dades:
   a) Principis: Consentiment, qualitat i finalitat de les dades, previs al tractament (art. 8 del RDLOPD).
   b) Deure de guardar Secret, durant i després del tractament.

3. Drets d'accés, rectificació, cancel·lació i oposició (ARCO), d'autodeterminació informativa per part dels titulars de les dades, com a garanties a partir de la recollida i tractament, que anomenats també d'*Habeas Data*, són drets personalíssims, independents i gratuïts, recollits al Títol III del RDLOPD.

Pel que fa als principis de qualitat descrits al RDLOPD són els següents:
- Tractar les dades de **manera lleial i lícita**, garantint així els drets de les persones segons els quals aquestes han de ser protegides des de la seva obtenció i ús fins a la finalització del seu tractament.
- Recollir dades adequades, pertinents i no excessives en relació amb **finalitats determinades, explícites i legítimes**, cosa que comporta que les dades objecte de tractament no es poden utilitzar per a finalitats incompatibles amb aquelles per a les quals han estat recollides.
- Aconseguir dades **exactes i mantenir-les actualitzades**, de manera que responguin amb veracitat a la situació actual del seu titular. Es consideren exactes les dades que faciliti directament l'interessat.
- **Conservar les dades personals només durant el temps necessari** per a les finalitats del tractament per al qual han estat recollides, i cancel·lar-les quan hagin deixat de ser necessàries o pertinents per al fi amb què es van obtenir.

La mateixa Llei prescriu eines per evidenciar aquests principis de qualitat i acomplir els requeriments normatius, com el *document de seguretat*, que és un deure regulat pel Capítol II del RD 720/2007, per a tots els nivells de seguretat. El document de seguretat és un document intern, que esdevé una eina útil per treballar la política de seguretat de l'empresa, transmetre'n els seus continguts als usuaris involucrats en el seu sistema d'informació, i evidenciar-ne el grau d'adopció per part de l'organització.

Aquests principis i fases de legitimació els hauríem de recollir també al nostre sistema de gestió documental, i per tal de facilitar l'acompliment del darrer principi de conservació de les dades, des dels estàndards de qualitat és recomanable utilitzar un *calendari de conservació*.

Finalment, no oblidem que el responsable del fitxer té el deure de fer la Notificació al Registre de la Protecció de Dades de Catalunya en 30 dies, mitjançant formulari, registre que en dóna trasllat al Registro General de Protección de Datos Español de la Agencia Española de Protección de Datos.

6. Què es pot fotografiar i què és publicable?

A escala europea allò que es pot difondre a Internet, es troba contemplat a la Proposta de Reglament encara pendent d'aprovació al Parlament Europeu. Tanmateix, tindrem present el darrer Reglament publicat pel Parlament Europeu, que qualifica les imatges identificables com a "dades biomètriques" (art. 11) i determina que, en les situacions de risc per als drets i llibertats dels interessats, es procedirà a l'avaluació d'aquestes dades (art. 3).

A escala nacional, per respondre ambdues qüestions disposem, d'una banda de la LOPD pel que fa a la legitimitat en la recollida de dades i la finalitat de les mateixes, però de l'altra tenim una llei anterior.

Es tracta de la *Llei orgànica 1/1982 de 5 de maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge*, que en el seu article 8, indica que no es consideren intromissions il·legítimes, i per tant, són permeses actuacions com:
- les autoritzades o acordades per la Llei, o quan predomini un interès històric, científic o cultural rellevant.

I la captació, reproducció o publicació de les imatges en referència a:
- persones que tinguin un càrrec públic o una professió de notorietat o projecció pública i la imatge es capti durant un acte públic o en llocs oberts al públic;

... el termini de protecció del dret a la pròpia imatge i a la intimitat, així com el període en què els hereus podran exercir el dret, és de vuitanta anys des de la mort de la persona.

©istockphoto/Rasmus Rasmussen

– un succés o esdeveniment públic, quan una persona determinada apareix de manera accessòria.

Tanmateix es requereix la protecció de l'anonimat en els casos de persones que executen una professió de risc –com les forces o cossos de seguretat de l'Estat–, o d'edificis judicials i sales de vista, entre altres.

En canvi, l'article 7.5, recull com a intromissions il·legítimes: "quan la captació, reproducció o publicació per fotografia de la imatge d'una persona sigui en llocs o moments de la seva vida privada o fora d'aquests, llevat dels esmentats de l'article 8".

Amb tot, no es considerarà intromissió si la persona fotografiada dóna el seu consentiment per accedir a l'àmbit que determini (art.2). I caldrà disposar d'un consentiment de l'interessat per a cadascun tres actes: la captació, reproducció o publicació.

Així, sempre que hi hagi habilitació legal, per exemple, mitjançant un consentiment, previ lliure, específic i informat com el que preveu la LODP, serà possible fotografiar al carrer o en espais oberts al públic, o quan es tracta de contextos de rellevància informativa pública. I no oblidarem tampoc els altres requeriments de la LOPD, com el fet que la captació sigui legítima i adequada a la finalitat del tractament o del fitxer.

D'altra banda, caldrà respectar els drets les imatges dels menors que queden més especificats en la *Llei Orgànica 1 / 1996, de 15 de gener, de protecció jurídica del menor*.

Finalment, segons l'article 4t de la *Llei orgànica 1/1982*, hem de recordar que el termini de protecció del dret a la pròpia imatge i a la intimitat, així com el període en què els hereus podran exercir el dret, és de vuitanta anys des de la mort de la persona.

6.1. Què hem de preveure quant a la difusió d'imatges per Internet?

Com dèiem, la difusió per Internet d'aquelles imatges que facin identificables persones, igual com la captació, ha de comptar a més amb el consentiment de la persona afec-

tada, llevat que tingui cobertura en el que estableix la *Llei orgànica 1/1982, de 5 de maig, de protecció del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge*, o en una altra norma amb rang de llei. Però a més, d'acord amb la *Recomanació 1/2008* de l'Autoritat Catalana de Protecció de Dades (APDCAT), fora d'aquests supòsits, la difusió es farà quan resulti legítima i proporcionada, i de manera que no es facin identificables persones concretes.

La solució de fer que les imatges siguin no identificables i que, d'aquesta manera, no siguin dades de caràcter personal acollides per la LOPD, exigeix pixel·lar-les i fer anònimes les persones que hi apareixen. Es procedirà al **pixellat** en els següents casos:

- Quan es tracti de fitxers en format digital on de forma incidental o accessòria s'incloguin les dades sense tenir relació amb la seva finalitat.
- Sempre que no es considerin intromissions il·legítimes, a la vida privada o fora d'aquesta, d'acord amb l'art. 7.5 de la *Llei orgànica 1/1982*. Per exemple, en alguna entrega de pis, al seu inquilí o propietari, amb el seu consentiment.
- En tots aquells altres casos, on les persones no s'hi han prestat voluntàriament i/o requereixin aplicar nivells de seguretat de mitjà o alt per tal de fer-les no identificables.

A més de tot això, en el cas no previst que un document formés part del patrimoni documental, caldria tenir en compte, el que diu de l'accés i consulta l'art. 57 de la LPHE i de la Llei 10/2001, de 13 de juliol, d'arxius i documents.

7. Nivells i mesures de seguretat a adoptar pel sistema de gestió documental

Un sistema de protecció de les dades s'ha d'aplicar a tot el cicle vital del document: organització, accés i emmagatzematge. D'acord amb els nivells de seguretat adoptats, per a les qüestions d'arxiu, accés i comunicació de dades, així com el control d'incidències i la revisió periòdica del sistema d'informació, caldrà seguir també l'establert per la LOPD i, complementar-ho, quan manqui, amb altres criteris que haurem de preveure per al sistema de gestió documental. Quant al control d'incidències i les auditories del sistema, se seguirà tot el que estableix el RDLOPD.

7.1. Breu apunt sobre els nivells de seguretat a adoptar

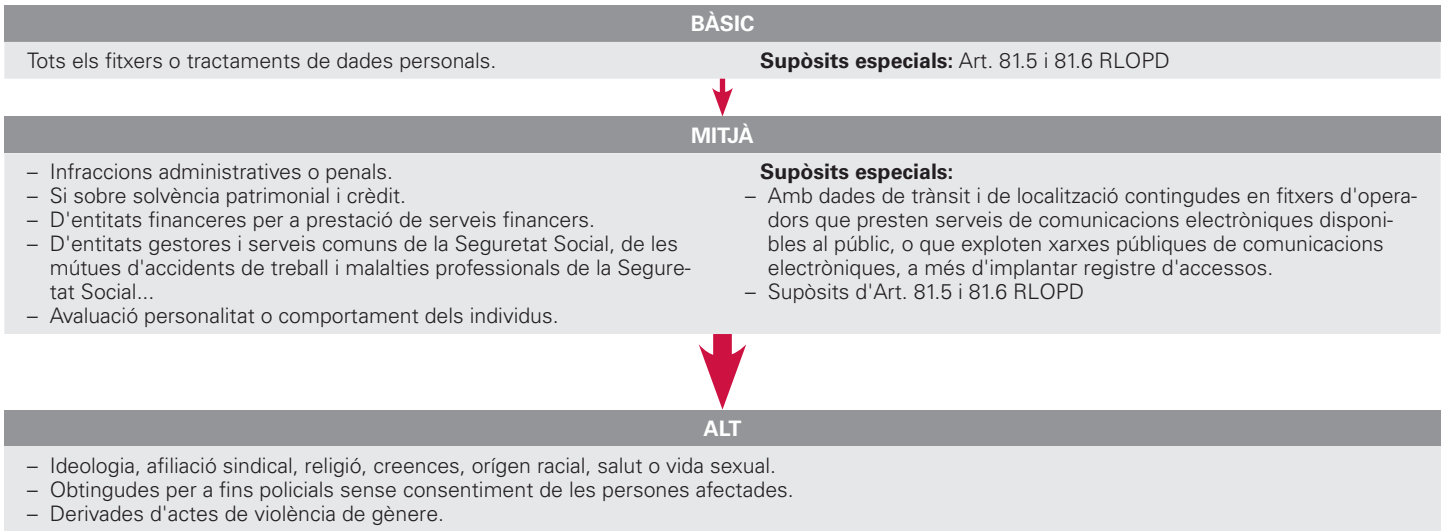
El RDLOPD en el seu article 80 identifica tres nivells de mesures de seguretat aplicables als fitxers que continguin dades de caràcter personal: bàsic, mitjà i alt. L'establiment d'un o altre nivell de seguretat s'adopta en funció de la diferent sensibilitat de les dades personals incloses en els arxius. I aquests nivells són acumulatius, de forma que per exemple, els fitxers de nivell alt han de complir les mesures previstes per als fitxers de nivell alt, mitjà i bàsic (figura 1).

Així, per exemple, el reportatge fotogràfic d'una manifestació sindical, requerirà mesures de nivell alt, a menys que es doni algun dels supòsits de l'art. 81.5 del RDLOPD, segons el qual seran només de nivell bàsic, quan:

> "a) Les dades s'utilitzin amb l'única finalitat de realitzar una transferència dinerària a les entitats de què els afectats siguin associats o membres.
>
> b) Es tracti de fitxers o tractaments no automatitzats on de forma incidental o accessòria s'incloguin les dades sense tenir relació amb la seva finalitat."

Les mesures que ha d'adoptar l'empresa per tal de garantir la seguretat de les dades personals, d'acord amb el Títol VIII del RDLOPD, es fixen en funció del nivell de seguretat corresponent al fitxer, i en funció del suport del mateix (automatitzat o no automatitzat).

FIGURA 1



Font: Elaboració pròpia a partir de la bibliografia de l'APDCAT.

Per tal d'analitzar els recursos que disposa l'organització en matèria de seguretat i dotar dels elements i mesures necessàries que requereixi el disseny de la seva política de seguretat, es recomana una anàlisi DAFO (Debilitats, Amenaces, Fortaleses i Oportunitats) que ajudi a determinar els riscos externs i interns, juntament amb l'observació de punts forts interns i oportunitats externes amb què poder-los fer front.

Aquesta anàlisi pot distingir també la tipologia de riscos: de tipus físic, informàtic, documental i de personal. I tot allò que afecti la integritat i la identitat de les imatges, caldrà contemplar-ho, atès que tindrà conseqüències en el tractament de les dades personals que contenen.

7.2. Criteris d'arxiu, gestió de suports i preservació de dades

Tot i que el RDLOPD només contempla l'obligació d'aplicar criteris d'arxivament per als fitxers no automatitzats, com a mesura de nivell bàsic en el seu article 106, hem de preveure també aplicar-ne per als fitxers automatitzats, siguin digitals o digitalitzats, i atesa la necessitat d'establir criteris homogenis i comprensibles, per tal de garantir-ne la seva localització i consulta, així com una correcta preservació de les dades que contenen.

El disseny del sistema de gestió documental, juntament amb les recomanacions de la normativa ISO 30300 i d'altres ISO, haurà de preveure aquests aspectes poc o gens regulats per la Llei, així com assegurar que s'adeqüi al compliment de la política de seguretat.

El document de seguretat que es requereix a la normativa per a tots els nivells de seguretat (Cap. III del RDLOPD), tindrà annexats tots els models de registres que permetin la gestió de suports i arxius, com: l'inventari de suports amb opcions de reutilització i destrucció, el registre d'entrades i sortides de suports, i les autoritzacions corresponents.

I aquestes plantilles annexes aniran d'acord també amb els criteris d'arxiu i gestió de suports contemplats en els ins-

truments propis del sistema de gestió documental, com són el calendari de conservació aplicat a les classes del quadre de classificació, la política de digitalització i les estratègies per a la preservació dels documents electrònics.

En matèria de seguretat, quant al dret de portabilitat de les imatges i dades recollida en l'article 18 de la proposta del Reglament Europeu, mentre aquesta proposta continuï pendent d'aprovar-se, cal seguir el més semblant que disposa el RDLOPD, pel que fa a les mesures per als dispositius portàtils i les xarxes de comunicacions (art. 85, 86 i 101 RDLOPD). La política de seguretat i la política de digitalització, haurà de pautar registres també en aquests aspectes, a banda de les mesures de seguretat de nivell més alt, com l'encriptació d'imatges, quan s'escaigui.

7.3. Criteris d'accés i comunicació de dades

Pel que fa als criteris d'accés, per a les mesures per a fitxers de tractament automatitzat, es contempla un procediment d'assignació, distribució i emmagatzematge de contrasenyes que en garanteixi la confidencialitat i al qual es limitarà la possibilitat d'intentar reiteradament l'accés no autoritzat al sistema d'informació, segons l'article 98 RDLOPD.

L'evidència d'aquest procediment amb les mesures del control d'accés, constarà al document de seguretat, però els criteris han de ser compartits amb el quadre d'accés i seguretat del propi del sistema de gestió documental. Així mateix, caldrà recollir qüestions com els nivells d'accés assignats a les classes del quadre de classificació i l'esquema temporal de les restriccions d'accés basades en la LOPD.

8. Reflexió final

Com observem, la implementació d'una política de seguretat que compleixi els requeriments en protecció de dades, ha d'anar forçosament vinculada amb el disseny del sistema de gestió documental de l'organització, i la seva implementació posterior. Per tant, hem de tenir en compte que l'eficàcia de la implantació de la política de seguretat, no dependrà només del seu disseny inicial, sinó de la cultura organitzativa que s'hagi establert per tal d'implementar-la i per integrar-la en el sistema de gestió de documents propi de l'organització.

En l'adopció de les mesures de seguretat, hem vist que hi ha aspectes tècnics i organitzatius de la gestió dels documents digitals, que deixant de banda els avenços de la tecnologia més recent, no queden regulats per la legislació vigent.

Per tal de complementar tots aquests requeriments normatius i en els supòsits en què siguin més restrictius al mínim normatiu exigible, hem d'incorporar i adoptar també aquests requeriments i d'altres de més exigents en el disseny del sistema de gestió documental i podem ajudar-nos de les eines recomanades pels principals estàndards de qualitat actuals promoguts per les normes ISO en gestió de documents.

L'exposició dels requeriments normatius bàsics en protecció de dades és prou extensa, i la longitud d'aquest article només permet suggerir alguns dels aspectes i instruments que haurà d'incloure el sistema de gestió del fons fotogràfic per tal d'assegurar l'acompliment i complementació dels mecanismes en la garantia dels drets.

No obstant, creiem que la revisió del tema constitueix una oportunitat per a la gestió documental, pel seu paper a l'hora de detectar mancances i sobretot de reduir riscos en matèria de seguretat de les dades. L'adopció de criteris i recomanacions de les normatives ISO multidisciplinàries i transversals més recents, suposen una contribució recomanable en el disseny dels sistemes de gestió documental, que no ha de desestimar la reflexió constant per a l'adaptació en els nous contextos tecnològics i als conseqüents canvis de la normativa d'obligat compliment.

9. Bibliografia

Guies, recomanacions i articles

Agència Catalana de Protecció de Dades. *Recomanació 1/2008 sobre la difusió d'informació que contingui dades de caràcter personal a través d'Internet* [en línia]. 2008. [Data de consulta: 21/03/2011]. Disponible a: http://www.apd.cat/ca/articlesPage.php?cat_id=28&art_id=49

Agència Catalana de Protecció de Dades. *Recomanació 1/2010 de l'Agència Catalana de Protecció de Dades, sobre l'encarregat del tractament en la prestació de serveis per compte d'entitats del sector públic de Catalunya.* [en línia]. 2010. [Data de consulta: 21/03/2011]. Disponible a: http://www.apd.cat/media/2184.pdf

Agencia Española de Protección de Datos. *Guía modelo del Documento de Seguridad* [en línia]. 2010. [Data de consulta: 20/05/2011]. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/modelo_doc_seguridad.doc

Inteco. *Guía para empresas: cómo adaptarse a la normativa sobre protección de datos* [en línia]. 2009. [Data de consulta: 22/03/2011]. Disponible a: http://www.inteco.es/Seguridad/Observatorio/manuales_es/GuiaManual_LOPD_pymes

MARTÍNEZ, R. "El dret fonamental a la protecció de dades". Agustí Cerrillo, *Les transformacions del dret a la societat de la informació*. Barcelona: FUOC, 2009.

MARTÍNEZ, R. *Protección de datos de carácter personal en la Sociedad de la Información*. Barcelona: FUOC, 2005.

MIRALLES, R. "Europa cloudcomputing i protecció de dades de caràcter personal." *Item*. Núm. 57 (2013), p. 81- 96.

Normativa citada a peu de pàgina

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 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, DO L 281 de 23.11.1995. [En línia]. [Data de consulta: 18.04.2014]. Disponible a: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.4-cp–Directiva-95-46-CE.pdf

Grupo del Artículo 29 sobre la Protección de Datos. Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y encargado del tratamiento» [En línia]. [Data de consulta: 18.04.2014]. Disponible a: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf

Propuesta de Reglamento del Parlamento Europeo y del Consejo 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. [En línia]. Bruselas, 25.1.2012 [Data de consulta: 18.04.2014]. Disponible a: http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF