
Nocions bàsiques de protecció de les dades personals

PID_00227147

Enric Enrich Muls
Raquel Xalabarder Plantada

Temps mínim de dedicació recomanat: 2 hores



**Enric Enrich Muls**

Exerceix com a advocat a Barcelona des de 1980, especialitzat en dret internacional i dret de la propietat intel·lectual. És autor de diferents publicacions sobre dret mercantil, dret internacional i dret d'autor. Àrbitre de l'Organització Mundial de la Propietat Internacional (OMPI) i de l'American Film Market Association (AFMA). Membre de la International Association of Entertainment Lawyers (IAEL) i de la International Bar Association (ANAVA).

**Raquel Xalabarder Plantada**

Catedràtica de Propietat intel·lectual als Estudis de Dret i Ciència Política de la UOC. Master of Laws (1993) i Visiting Scholar a la Columbia University Law School de Nova York. Tutora de l'Acadèmia de l'Organització Mundial de la Propietat Intel·lectual (OMPI).

Índex

Introducció.....	5
1. La protecció de dades personals: marc jurídic i definicions...	7
2. Característiques principals de la protecció de dades.	
Dades protegides especialment.....	9
2.1. Principis	9
2.2. Inscripció dels fitxers en l'Agència Espanyola de Protecció de Dades	9
2.3. Dades sensibles o protegides especialment	10
2.4. Dret d'informació en la recollida de dades i consentiment de l'afectat	10
2.5. Seguretat	11
2.6. Drets dels interessats	12
3. Cessió de dades personals i transferència internacional.....	13
3.1. Cessió de dades	13
3.2. Transferència internacional de dades personals	15
4. Infraccions i sancions.....	17
5. L'anomenat "dret a l'oblit".....	18
Resum.....	21
Abreviatures.....	23
Bibliografia.....	24

Introducció

La normativa de protecció de dades personals deriva de les normes de tutela de drets fonamentals, a Espanya, de la Constitució (article 18). Com a dret fonamental, en aquesta norma, s'estableix el de la intimitat personal i familiar. Per a implementar aquest dret es va publicar l'any 1992 la Llei orgànica de regulació del tractament automatitzat de dades personals (LORTAD). Es va incloure en el títol els termes *tractament automatitzat* perquè en aquella època es considerava que la principal amenaça a la intimitat que es volia protegir venia de l'automatisme i de les possibilitats que generava la tecnologia informàtica. Posteriorment a aquesta norma es va publicar la Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, relativa a la protecció de les persones físiques pel que fa al tractament i a la lliure circulació de dades personals.

En aquesta matèria el legislador espanyol ha anat sempre per davant del comunitari, i ha donat compliment a les normes europees, ja que la LORTAD es va promulgar quan hi havia només un esborrany del que seria la Directiva 95/46/CE de Parlament Europeu o del Consell, de 24 d'octubre de 1995, relativa a la protecció de dades de les persones físiques pel que fa al tractament de dades personals i la seva lliure circulació. Per a implementar-la correctament, es va publicar la **Llei orgànica 15/1999, de 13 de desembre, de protecció de dades personals (LOPD)**, que va derogar la LORTAD.

La LOPD de 1999 ha estat modificada en diverses ocasions

La LOPD ha estat modificada per la Sentència 292/2000, de 30 de novembre, del Tribunal Constitucional (per la qual es declaren nuls determinats preceptes) i per la Llei 62/2003, de 30 de desembre, de mesures fiscals, administratives i d'ordre social (vegeu l'article 82 que modifica els articles 37 i 48 de la LOPD), i completada per la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic (LSSICE), i la Llei 32/2003, de 3 de novembre, general de telecomunicacions (LGT).

Aquesta normativa, que afecta qualsevol persona o entitat que recull, manté o tracta dades personals de tercers, és molt estricta i estableix sancions serioses en cas d'incompliment. Per això, n'és imprescindible el coneixement i el compliment correcte.

La convergència de les tecnologies de la informació i de les comunicacions ha multiplicat el potencial d'atemptats a la intimitat que poden patir els subjectes les dades personals dels quals han estat facilitades a un tercer, tant si és pel mateix subjecte, pel tercer a qui les va facilitar originàriament com per cessió a una altra persona. En la premsa han aparegut notícies de sancions importants a companyies de telecomunicacions (compiladors de dades en gran quantitat) per haver cedit dades a tercers sense el consentiment dels afectats. No fa falta, però, tenir dades, per exemple, de vint milions de subjectes per a estar en el

punt de mira de l'Administració. Qualsevol empresa que reculli dades personals de tercers (encara que sigui d'un, dos o tres subjectes, tant si són empleats, clients o proveïdors com si són mers contactes comercials) està afectada per aquesta normativa. Els mitjans de comunicació, certes productores i, sobretot, les agències de publicitat i relacions públiques també estan, per tant, subjectes a la normativa. I atès que complir-la no és complex, convé conèixer-la per evitar incórrer en responsabilitats.

1. La protecció de dades personals: marc jurídic i definicions

La LOPD és aplicable a les dades personals registrades en suport físic, sense distingir-ne la naturalesa analògica o digital, mentre siguin susceptibles de tractament, i a tota modalitat d'ús posterior d'aquestes dades, llevat que es dediquin a activitats personals o domèstiques.

Reglament LOPD

El Reial decret 1720/2007, de 21 de desembre, aprova el Reglament de desenvolupament de la LOPD.

Dades d'ús personal

En aquest sentit, per exemple, no està subjecta a la llei l'administració d'una agenda amb els noms i adreces d'amics, o dels restaurants favorits, però sí que ho està si aquests noms corresponen a persones que, a més de ser amigues, són clients, o si amb aquests restaurants mantenim una relació professional o empresarial.

En general hem de partir de la base que qualsevol empresari o professional de la comunicació, per petit que sigui, manté fitxers amb dades personals i, per tant, està obligat a complir la llei. La LOPD estableix al principi una sèrie de definicions, que és molt útil tenir presents:

Article 3

"1) **Datos de carácter personal:** cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

2) **Fichero:** todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

3) **Tratamiento de datos:** cualquier operación o procedimiento técnico, sea o no automatizado, que implique la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, bloqueo, modificación, o cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

4) **Responsable del fichero o del tratamiento:** persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

5) **Afectado o interesado:** persona física titular de los datos que sean objeto del tratamiento.

6) **Procedimiento de disociación:** todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

7) **Encargado del tratamiento:** la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la

existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

8) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

9) Cesión o comunicación de datos: tratamiento de datos que supone su revelación a una persona distinta del interesado.

10) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo.

Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación."

2. Característiques principals de la protecció de dades. Dades protegides especialment

La LOPD classifica les dades segons la transcendència que tenen per al subjecte afectat; a partir d'això, atorga diferents proteccions.

2.1. Principis

La llei estableix una sèrie de **principis** que sintetitzarem en tres:

- **Adequació i pertinència.** Les dades personals solament es poden recollir per a tractar-les, i també sotmetre-les a aquest tractament, quan són adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut. Són cancel·lades quan han deixat de ser necessàries o pertinents per a la finalitat per a la qual havien estat recollides o registrades. No són conservades en forma que permeti la identificació de l'interessat durant un període superior al necessari per als fins sobre la base dels quals havien estat recollides o registrades.
- **Ús de les dades per a la finalitat per a la qual s'han recollit.** Les dades personals objecte de tractament no es poden usar per a finalitats incompatibles amb aquelles per a les quals les dades havien estat recollides.
- **Exactitud i veracitat.** Les dades personals han de ser exactes i han de ser posades al dia de manera que responguin amb veracitat a la situació actual de l'afectat. Per això l'afectat, a qui es reconeix el dret d'accés, ha de poder notificar les rectificacions de les dades, que ha de mantenir un responsable de fitxer.

Només per la finalitat prevista

No podem utilitzar les dades de tota la relació de clients per a enviar-los una comunicació comercial d'una empresa, producte o servei que no tingui res a veure amb la que va recollir les dades.

2.2. Inscripció dels fitxers en l'Agència Espanyola de Protecció de Dades

Aquesta és la norma que ha de recordar tota persona que manté dades personals:

Cal **notificar** a l'Agència Espanyola de Protecció de Dades (AEPD), amb caràcter previ, la creació de fitxers de dades personals.

Web recomanat

Els formularis de notificació es poden obtenir per Internet en el lloc web de l'AEPD. L'adreça és la següent: <http://www.agpd.es>

2.3. Dades sensibles o protegides especialment

La llei considera que les dades referents a la ideologia, origen racial, salut i vida sexual són especialment sensibles i mereixen un nivell especial de protecció. En l'article 7 LOPD hi ha una llista detallada dels requisits que ha de complir la recollida, emmagatzemament o tractament d'aquests tipus de dades.

Dades sobre ideologia

L'afiliació sindical o política i l'orientació religiosa són algunes dades sobre ideologia que han de ser protegides especialment.

2.4. Dret d'informació en la recollida de dades i consentiment de l'afectat

El nucli de la LOPD se centra en el fet que el subjecte les dades del qual es recullen i tracten ha de conèixer i consentir la recollida i finalitat que pretén el responsable del tractament.

1) Dret d'informació

En el moment que sol·licitem dades personals a una persona física, o si les dades no les rebem directament de l'interessat, hem d'informar clarament i expressament l'interessat sobre els aspectes següents:

- a) De l'existència d'un fitxer o tractament de dades personals, de la finalitat de recollir-les i dels destinataris de la informació.
- b) Del caràcter obligatori o facultatiu de la seva resposta a les preguntes que els plantegen.
- c) De les conseqüències de l'obtenció de les dades o de la negativa de subministrar-les.
- d) De la possibilitat d'exercitar els drets d'accés, rectificació, cancel·lació i oposició.
- e) De la identitat i adreça del responsable del tractament o, si escau, del seu representant.

Dades d'ús particular

Com s'ha indicat més amunt, quan la seva finalitat és particular no cal dur a terme aquest procés.

Tanmateix, les comunicacions comercials a interessats que constin en **fonts accessibles al públic** i es destinin a l'activitat de publicitat o prospecció comercial, no necessiten el compliment del que s'ha mencionat aquí damunt, però en cada comunicació que es dirigeix a l'interessat se l'ha d'informar de l'origen de les dades i de la identitat del responsable del tractament, i també dels drets que té.

2) Consentiment de l'afectat

La LOPD estableix el principi pel qual no hi ha infracció si hi ha el consentiment de l'afectat, que accepta una pràctica que, d'una altra manera (és a dir, sense consentiment), hauria comportat un atemptat contra els seus drets personals.

El principi del consentiment

Aquest principi de consentiment de l'afectat està reconegut en altres drets fonamentals, com per exemple el dret a la pròpia imatge.

La llei exigeix per al tractament de les dades personals el **consentiment** inequívoc de l'afectat, i la **interpretació** d'aquest terme s'ha d'efectuar de manera **estricta**. Per reforçar el dret dels afectats, estableix que aquest consentiment pot ser revocat quan hi ha causa justificada per a fer-ho, sense que aquesta revocació produeixi efectes retroactius.

2.5. Seguretat

El responsable del fitxer i, si escau, l'encarregat del tractament han d'adoptar les mesures tècniques i d'organització necessàries que garanteixin la seguretat de les dades personals i n'evitin l'alteració, pèrdua, tractament o accés no autoritzat. Igualment, la llei estableix l'obligació de guardar en secret aquestes dades.

El **document de seguretat** és un document intern de l'empresa o persona responsable del fitxer que conté les dades personals, en què es detallen les mesures de seguretat obligatòries legalment.

Mesures de seguretat

La concreció de les mesures de seguretat dels fitxers es recull en els articles del 79 al 114 del Reglament de la LOPD.

En el document de seguretat s'han de definir els procediments, funcions i obligacions del personal respecte a l'accés i tractament de les dades, i també el seu responsable.

Amb el document de seguretat es regula tota la política d'emmagatzemament i tractament de dades personals en l'empresa.

Estan obligats a elaborar el document de seguretat tota empresa o professional que tinguin dades personals en els sistemes d'ordinadors i altres equips tècnics. En general, per tant, qualsevol empresa que tingui dades personals sobre els clients, proveïdors, treballadors, etc. està obligada a elaborar, implementar i mantenir actualitzat un document de seguretat en què estableixi la seva política de seguretat respecte a les dades personals. El Reial decret 1720/2007 (article 80) estableix mesures de nivell bàsic, mitjà o alt, depenent del tipus de dades que s'emmagatzemen i es tracten en un fitxer en concret.

Sobre les dades

El contingut del document de seguretat varia depenent del tipus de dades que contingui el fitxer de l'empresa o professional en qüestió.

Tipus de dades

- **Dades de nivell alt.** Són, per exemple, les dades relatives a la ideologia, religió i salut de les persones o la seva afiliació sindical.

- **Dades de nivell mitjà.** Són, per exemple, les dades relatives a la solvència i al crèdit de les persones físiques.
- **Dades de nivell bàsic.** Són, per exemple, el nom, correu, correu electrònic i adreça.

2.6. Drets dels interessats

Els subjectes de qui es recullen dades, a part de poder consultar el Registre General de Protecció de Dades, que és públic i gratuït, tenen els drets següents:

1) **Dret d'accés.** L'interessat té dret de sol·licitar i obtenir gratuïtament informació de les dades personals sotmeses a tractament, l'origen, i també les comunicacions que se n'han fet o que se'n preveuen fer.

2) **Dret de rectificació i cancel·lació.** L'interessat pot sol·licitar la rectificació de les dades inexactes o incompletes i la cancel·lació de les que no s'ajusten a la llei. El responsable del tractament té l'obligació de fer efectiu el dret de rectificació o cancel·lació de l'interessat en el termini de deu dies.

Els interessats poden fer efectius els seus drets mitjançant reclamació a l'AEPD i, en cas de tenir danys, tenen dret de ser indemnitzats pels perjudicis que se'ls ha causat.

3. Cessió de dades personals i transferència internacional

El concepte i abast de la cessió de dades queda establert en la mateixa LOPD i en el seu Reglament (RD 1720/2007).

La **cessió o comunicació de dades** és tota revelació de dades feta a una persona diferent de l'interessat (article 3.i de la LOPD i article 5.1.c del Reglament de la LOPD, RD 1720/2007).

La **norma general**, llevat comptades excepcions, és que la cessió de dades personals requereix el consentiment del titular de les dades o interessat.

La majoria de moviments i comunicacions de dades es fan electrònicament. En el cas de moviments a tercers països, la transferència de dades passa a denominar-se **transferència internacional**, i requereix el compliment d'unes formalitats especials per a poder-se efectuar.

És necessari subratllar que la majoria de les cessions de dades es fan amb la finalitat que les empreses les utilitzin per a fins comercials, principalment per a enviar informació dels productes de les empreses a clients o a clients potencials. L'altre ús majoritari de la cessió de dades és utilitzar-les per a estudis de mercat i elaboració d'estadístiques. Així mateix, és necessari destacar la importància d'aquesta matèria i que els responsables de les àrees de màrqueting i comunicació de les empreses n'han de complir la legislació.

La llei espanyola és molt restrictiva i poc inclinada a cedir dades, particularment a la transferència internacional. No obstant això, l'adopció de les empreses d'una bona política de dades, correcta i garant dels drets reconeguts als ciutadans únicament requereix que es compleixin els requisits establerts per la LOPD i el Reial decret 1720/2007.

3.1. Cessió de dades

L'ús d'Internet pels ciutadans ha significat els dos grans canvis següents en matèria de dades personals:

1) Internet és un mitjà pel qual els usuaris cedeixen les dades personals a les empreses. Això ha comportat un augment de l'ús de fitxers personals que tinguin un alt valor econòmic per a les empreses.

2) A causa de l'estructura global d'Internet, cada vegada són més freqüents les transferències internacionals de dades entre multinacionals i entre empreses que operen a Internet, amb la dificultat afegida de les diferències que hi ha entre els nivells de protecció legal, que els Estats Units d'una banda, Europa de l'altra i altres països ofereixen als titulars de les dades personals.

Empreses a Internet

Quan comprem productes o serveis en la Xarxa o bé quan ens donem d'alta en serveis de notícies electròniques o *newsletters* cedim les dades personals a empreses vinculades a Internet.

En termes generals, la cessió de dades és un tractament definit en la LOPD de la manera següent:

Article 3.c

"[La cesión de datos es la] operación y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."

En la mesura que la cessió de dades n'és un tractament, de conformitat amb l'article 6 de la LOPD, requereix el consentiment de l'afectat:

Article 11

"1) Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado."

En l'apartat 2 s'estableix la **llista d'excepcions** al principi general de necessitat del consentiment (vegeu també l'article 10 del RD 1720/2007).

a) Accés de les dades per compte de tercers

Sovint les empreses responsables dels fitxers que contenen dades encarreguen a tercers fer el servei de tramesa de comunicacions als seus titulars o afectats. Per a aquests casos, la LOPD ha fet una excepció a les normes de cessió de dades, amb la qual cosa les empreses que fan la prestació de serveis de tractar dades de tercers, per compte i en interès dels responsables del fitxer, únicament estan obligades a complir el que estableix l'article 12 de la LOPD, que, sota el nom d'accés de les dades per compte de tercers, estableix el següent:

Article 12

"1) No se considera comunicación de datos el acceso a los datos, cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento."

2) La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipu-

larán, además, las medidas de seguridad a las que se refiere el artículo 9 de esta ley que el encargado del tratamiento está obligado a implementar.

3) Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento.

4) En caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente."

b) Fonts d'accés al públic

Hi ha dades que, malgrat que són personals, figuren en el cens promocional, en repertoris telefònics, o són relatives a les llistes de persones pertanyents a grups de professionals que consten en fonts d'accés al públic.

Segons l'article 3 de la LOPD, són **fonts accessibles al públic** els fitxers que poden ser consultats per qualsevol persona, cosa que no és impedita per una norma limitadora, o sense més exigència que, si escau, abonar una contraprestació. També tenen el caràcter de fonts d'accés públic els diaris i butlletins oficials i els **mitjans de comunicació**.

Aquestes dades s'han de limitar a les que són estrictament necessàries per a complir la finalitat a què es destina cada llista. La inclusió de dades addicionals per les entitats responsables de mantenir aquestes fonts, o la cessió a tercers per a qualsevol altra finalitat, requereix el consentiment de l'interessat, que pot ser revocat en qualsevol moment.

3.2. Transferència internacional de dades personals

Podem definir la **transferència internacional de dades** com el transport de dades entre sistemes informàtics per qualsevol mitjà de transmissió, i també el transport de suports de dades per correu o qualsevol altre mitjà convencional amb destinació a tercers països.

L'Agència Espanyola de Protecció de Dades ha regulat la transferència internacional de dades mitjançant la Instrucció 1/2000, d'1 de desembre, de l'APD, relativa a les normes per les quals es regeixen els moviments internacionals de dades.

No es poden fer transferències temporals ni definitives de dades personals amb destinació a països que no proporcionin el nivell de protecció que presta la LOPD. En aquest sentit, l'Ordre de 2 de febrer de 1995, del Ministeri de Justícia i Interior, estableix la relació de països amb protecció de dades personals equiparable a l'espanyola, que són els següents: Alemanya, Àustria, Bèlgica,

LOPD i Reglament

Vegeu els articles 33 i 34 de la LOPD i els articles del 65 al 70 del Reglament de la LOPD (RD 1720/2007).

Web recomanat

Aquesta instrucció està disponible en l'adreça següent: <http://www.agpd.es>

Dinamarca –amb l'excepció del territori de les illes Fèroe i de Groenlàndia–, Eslovènia, Finlàndia, França, Grècia, Irlanda, Islàndia, Itàlia, Luxemburg, Noruega –amb l'excepció del territori de Svalbard–, els Països Baixos, Portugal, el Regne Unit –inclusivament el territori de les illes de Man i Jersey– i Suècia.

Els acords de port segur

Els **Estats Units** mai no ha estat un país de referència en relació amb la protecció dels drets de les persones relatius al tractament i ús de les dades personals. Europa sempre ha atorgat més protecció que els Estats Units en aquesta matèria. Per aquest motiu, la Comissió de la Unió Europea, d'acord amb la Directiva 95/46/CE del Parlament Europeu i del Consell, ha formalitzat acords amb certes empreses dels Estats Units que es coneixen amb el nom d'*acords de port segur* o *safe harbour agreements*. Les empreses que hi estan adherides són responsables de portar a terme unes mesures de protecció i control de les dades personals equiparables a les requerides per la legislació comunitària.

Èxit dels acords

Cada vegada hi ha un nombre més gran d'empreses nord-americanes que s'adhereixen als *acords de port segur*.

La transferència internacional de dades requereix l'**autorització prèvia** de l'AEPD, excepte en uns casos concrets, com, per exemple, per motius de procediments judicials o administratius, quan l'afectat hagi donat el seu consentiment inequívoc, o quan es realitza entre els països que es consideren "equiparables" en la protecció de dades.

En qualsevol cas, de conformitat amb la norma tercera de la Instrucció 1/2000, qualsevol persona o entitat que pretén efectuar una transferència internacional de dades ho ha de fer **constar expressament** quan fa la notificació del fitxer al **Registre General de Protecció de Dades**.

La **notificació**, en tot cas, ha d'incloure el següent:

- 1) El país de destinació de la transferència.
- 2) Els motius que habiliten la persona o l'entitat per a no necessitar l'autorització expressa del director de l'Agència de Protecció de Dades.

4. Infraccions i sancions

La LOPD estableix en els articles 44 i 45 una relació d'infraccions (lleus, greus i molt greus) que poden ser sancionades amb multes de fins a 600.000 euros, per la qual cosa convé conèixer i complir degudament aquesta normativa.

A més a més de la responsabilitat i sancions administratives que són aplicables per infracció de la normativa de protecció de dades personals, el tractament de dades personals pot donar lloc a casos de responsabilitat civil pels danys i perjudicis causats a tercers pel responsable del fitxer (article 19.1 de la LOPD) i fins i tot casos de responsabilitat penal (article 197 del Codi penal) per delictes contra la intimitat.

El procés sancionador

És recollit en els articles del 120 al 129 del Reglament de la LOPD (RD-1720/2007).

5. L'anomenat "dret a l'oblit"

L'anomenat "dret a l'oblit" no és pròpiament un dret recollit a cap llei, ni Constitució, ni tractat internacional, sinó simplement una interpretació que ha fet el TJUE en la **sentència del 13 maig de 2014, *Google Spain v. AEPD y Costeja* (C 131/12)**, i que permet exercir els drets d'oposició i cancel·lació (recollits a la Directiva 95/46/CE, sobre protecció de dades personals) per obligar que els motors de cerca eliminin, de la llista de resultats que s'obté en fer una cerca a partir del nom d'una persona, els enllaços a pàgines web (de tercers) que continguin informació relativa a aquesta persona, que sigui "no acurada, no pertinent i excessiva o que no estigui actualitzada o es conservi per un període superior al necessari".

Per fer possible l'exercici d'aquests drets davant dels motors de cerca, el TJUE va haver de concloure que:

- Als efectes de la Directiva 95/46/CE, l'activitat d'un motor de cerca (trobar informació publicada a internet per tercers, indexar-la de manera automàtica, emmagatzemar-la temporalment i posar-la a disposició dels internautes segons un ordre de preferència determinat) s'ha de qualificar de "**tractament de dades personals**" quan aquesta informació conté dades personals, i que el gestor d'un motor de cerca ha de considerar-se "**responsable**" de l'esmentat tractament.
- Els drets de rectificació, supressió o bloqueig (art.12(b) Directiva 95/46/CE) que el titular pot exercir quan es tracti de dades "**incompletes o inexactes**," i el dret d'oposició al tractament de les dades (art.14(a) Directiva 95/46/CE) també són d'aplicació a aquelles dades que siguin "**no acurades, no pertinents i excessives o que no estiguin actualitzades o es conservin per un període superior al necessari**" / "Inadequats, no pertinents i excessius (en relació amb la finalitat del tractament) o que no estiguin actualitzats o es conservin durant un període superior al necessari".
- I tot això, encara que la publicació d'aquesta informació en la pàgina web d'origen sigui lícita (o fins i tot, vingui imposada normativament) i amb independència que la informació s'elimini (o no) en l'origen.

El TJUE va establir també el **procediment per exercir aquests drets**: el responsable del tractament (i.e., el gestor del motor de cerca) haurà d'examinar el fonament de la petició que fa el titular de les dades i, si ho considera oportú –tenint en compte totes les circumstàncies de la situació concreta de l'interessat– posarà fi al tractament de les dades en qüestió (i.e., eliminar l'enllaç o bloquejar l'accés). Si aquest no accepta la petició feta, el titular pot adreçar-se a

l'agència de protecció de dades o a la jurisdicció ordinària per tal que aquests facin les comprovacions necessàries i ordenin al gestor del motor de cerca les mesures que calgui.

Curiosament, l'**advocat general** (2013) havia proposat justament el contrari, justificant que el dret a l'oblit no és un dret reconegut normativament, que Google no és "responsable" d'un tractament de dades personals (perquè no té el control sobre les dades que mostra a través del seu cercador), i que si la informació continguda en una pàgina web lesiona algun dret fonamental de l'individu (honor, reputació, imatge, nom...), aleshores la responsabilitat per aquesta infracció o delictes correspondria a qui l'hagi publicat (o la mantingui publicada) i no pas al cercador. En general, l'AG opinava que l'acceptació de la pretensió del senyor Costeja comportaria una "ingerència en la llibertat d'expressió de l'editor de la pàgina web" i equivaldria a permetre la "censura del contingut realitzada pel particular", en base a "una **preferència subjectiva**" que no equival a una "**raó legítima**".

La resolució que va fer el TJUE va ser sorprenent ja que, d'una banda, quan es va adoptar la Directiva 95/46/CE no es pensava pas en què els motors de cerca fossin responsables del tractament de dades personals i, de l'altra, perquè deixa en mans de cada individu i dels gestors dels motors de cerca (empreses privades, al cap i a la fi) la decisió de quin és el just equilibri entre l'exercici de diferents drets fonamentals: com ara el dret al nom, la imatge, la reputació o la intimitat de les persones (que exerceixen el "dret a l'oblit") i la llibertat d'expressió dels altres individus o el dret d'accés a la informació del públic, en general. Conscient del risc que l'exercici d'aquests drets individuals pugui conculcar la protecció de l'interès públic, el TJUE ja va excloure dos supòsits on no serà possible exercir aquest "dret a l'oblit": "llevat que s'imposi la seva conservació per a fins històrics, estadístics o científics" o que "l'interessat tingui un paper en la vida pública".

D'altra banda, en la mesura en què no es "resol" el problema "en origen" (el web que conté la informació que ha trobat el cercador no té cap obligació d'eliminar-la), aquest "dret a l'oblit" simplement farà més difícil trobar certa informació *online*. Cal tenir present que Google només elimina/bloqueja l'enllaç a través dels cercadors europeus –on és d'aplicació la Directiva 95/46/CE–, però la informació continuarà essent accessible des d'altres motors de cerca (per exemple, a www.google.com).

Queda per veure, doncs, quina és la praxis que es vagi acumulant en l'exercici d'aquest "dret a l'oblit" (entre motors de cerca i individus afectats) i si aquesta mateixa conclusió serà extensible a altres proveïdors de serveis *online* (més enllà dels cercadors) com ara els gestors de xarxes socials o de blogs, etc.

Nota

La UE està treballant en l'adopció d'un Reglament que actualitzi i substitueixi la D.95/46/CE.

Certament, la protecció dels drets fonamentals de la persona a internet és un tema molt sensible i difícil de resoldre de manera efectiva. Altra cosa és si realment la normativa sobre tractament de dades personals (i els drets de rectificació, supressió o bloqueig i d'oposició) són la millor eina per assegurar-ne la protecció.

Resum

Arran de la difusió de la tecnologia digital, les dades personals han adquirit una rellevància i han fet necessari establir lleis que protegeixin els interessos específics (intimitat, honor, reputació, etc.) que poden ser objecte d'atemptats mitjançant el tractament informatitzat de les dades personals. És essencial que qualsevol professional de la comunicació que mantingui o tracti dades personals de tercers conegui i compleixi les obligacions de protecció de dades, per evitar incórrer en sancions elevades. Aquestes obligacions són essencialment tres:

- Notificar els fitxers de dades personals a l'Agència Espanyola de Protecció de Dades.
- Adoptar les mesures de seguretat que estableix la normativa (LOPD i el seu Reglament).
- Complir les obligacions cap als subjectes dels quals es recullen dades inclosos els drets d'accés de rectificació i cancelació.

Abreviatures

AEPD *f* Agència Espanyola de Protecció de Dades

CE *f* Constitució espanyola

LGT *f* Llei general de telecomunicacions

LOPD *f* Llei orgànica de protecció de dades personals

LORTAD *f* Llei orgànica de regulació del tractament automatitzat de dades personals

LSSICE *f* Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç-electrònic

TJCE *f* Tribunal de Justícia de les Comunitats Europees

WIPO *f* World Intellectual Property Organization. Vegeu *OMPI*

Bibliografia

Álvarez-Cienfuegos Suárez, J. M. (2000). "Notas a la nueva regulación de la protección de datos de carácter personal". *La Ley* (núm. 5036, 17 d'abril).

Aparicio Salom, J. (2002). *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal* (2a. ed.). Cizur Menor: Aranzadi.

Aparicio Salom, J. (2009). *Estudio sobre la Ley Orgánica de protección de datos de carácter personal* (3a. ed.). Elcano (Navarra): Aranzadi.

Asís Roig, A. de (2002). "Protección de datos y derecho de las telecomunicaciones". A: J. Cremades; M. A. Fernández-Ordóñez; R. Illescas (coord.). *Régimen jurídico de Internet* (pàg. 201-228). Madrid: La Ley.

Díez-Picazo Giménez, L. M. (2005). *Sistema de derechos fundamentales*. Madrid: Civitas.

Freixas Gutiérrez, G. (2001). *La protección de los datos de carácter personal en el derecho español: aspectos teóricos y prácticos*. Barcelona: Bosch.

Miralles Miravet, S.; Baches Opi, S. (2001). "La cesión de datos de carácter personal: análisis de la legislación vigente y su aplicación a algunos supuestos prácticos". *La Ley* (vol. XXII, núm. 5306, 11 de maig).

Peso Navarro, E. (2000). *Ley de Protección de Datos: la nueva LORTAD*. Madrid: Díaz de Santos.

Ribas Alejandro, J. (2000). "Riesgos legales en Internet. Especial referencia a la protección de datos personales". A: R. Mateu de Ros; J. M. Cendoya Méndez de Vigo (coord.). *Derecho de Internet. Contratación electrónica y firma digital* (pàg. 143-161). Navarra: Aranzadi.

Rodríguez Casal, C.; Loza Corera, M. (2002). "Protección de la privacidad. Aproximación al opt-in/opt-out". *Revista de la Contratación Electrónica* (núm. 23, pàg. 3-18, gener). Cadis.

Simón Castellano, P. (2015). *El reconocimiento del derecho al olvido digital en España y en la UE: efectos tras la sentencia del TJUE de mayor de 2014*. Barcelona: Bosch.

Suñé Llinás, E. (2002). "Introducción y protección de datos personales". *Tratado de Derecho informático* (2a. ed., vol. I). Madrid: Universidad Complutense, Facultad de Derecho, Servicio de Publicaciones.

Téllez Aguilera, A. (2001). *Nuevas tecnologías y protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*. Madrid: Edisofer.

Ull Pont, E. (2003). *Derecho público de la informática (Protección de datos de carácter personal)* (2a. ed.). Madrid: UNED.

Veleiro, B. (2008). *Protección de datos de carácter personal y sociedad de la información*. Madrid: Boletín Oficial del Estado.

Vizcaíno Calderón, M. (2001). *Comentarios a la Ley Orgánica de protección de datos de carácter personal* (1a. ed.). Madrid: Civitas.