# PROTECCIÓN DE DATOS
## *en la* ***práctica diaria*** *del* ***profesorado***

Colegio Concertado
*Ruta de la Plata*
*Almendralejo.*


Colegio Concertado

*Ruta de la Plata*

*Almendralejo.*

***Finis origine pendet***.
*El final depende del principio.*

Marcus Manilus.
*«Astronomía.»*

"***Un buen profesor***
***tiene poca historia propia que contar,***
***su vida pasa a otra vidas,***
***los profesores son los pilares***
***de la estructura más íntima***
***de nuestros colegios,***
***son más fundamentales***
***que las piedras o que las vigas,***
***y siguen siendo una fuerza impulsora***
***y una energía reveladora***
***que nos guiará,***
***día a día,***
***en nuestras vidas***."

De Deepak Mehta al Sr. William Hundert.
De alumno a profesor.
The Emperor´s Club.

***El buen maestro***
***seduce al alumno***
***para que quiera***
***volver a ir a clase***.

Jaime Funes.

## Nota legal:

Almendralejo, 7 de octubre de 2019.

El **Colegio Concertado "Ruta de la Plata" de Almendralejo NO se hace responsable de las opiniones recogidas, comentarios y manifestaciones vertidas por los autores**. La presente guía recoge exclusivamente la opinión de su autor como manifestación de su derecho de libertad de expresión y en ejercicio del mismo los autores han expresado su opinión sobre diversas cuestiones legales que en la actualidad son objeto de controversia, polémica o admiten varias soluciones jurídicas. Por tanto, las opiniones vertidas en la presente Guía representan exclusivamente las de los autores, sin que en absoluto se niegue la validez a otras que puedan diferir de las mismas.

Se ha realizado un importante esfuerzo para verificar el rigor, la corrección, la exactitud y la actualidad de los artículos, referencias legales y jurisprudencia que se contienen en la presente Guía. La obra refleja las pautas y recomendaciones legales vigentes y **adaptadas a la Comunidad Autónoma de Extremadura** en el momento de su publicación, pero al ser el Derecho una ciencia en constante evolución, puede variar su contenido según se aprueben nuevas normas y también debido al avance de la jurisprudencia dictada por Jueces y Tribunales.

Además, el alumno debe tener presente que es posible que existan erratas no detectadas en la transcripción de todo el volumen legislativo que la presente obra contempla. Por ello, advertimos expresamente a los lectores de la presente Guía que no podemos hacernos responsables de las consecuencias que puedan derivarse de errores inadvertidos en el texto de la Guía.

Por último, advertimos expresamente que no podemos hacernos responsables de las consecuencias de las decisiones tomadas en base a las opiniones contenidas en la presente Guía, aconsejando en todo momento, tanto la consulta de textos especializados, publicaciones de la Agencia Española de Protección de Datos AEPD, publicaciones jurídicas periódicas y obras más extensas y detalladas, como el asesoramiento jurídico por profesionales cualificados y preceptiva intervención del Delegado de Protección de Datos que todo centro educativo debe poseer. Es igualmente necesario seguir las recomendaciones y actualizaciones legales que regularmente proporcionan tanto las Autoridades como los departamentos legales de los Centros e Instituciones educativas a los que se encuentre adscrito el personal docente.

De conformidad con el Real Decreto Legislativo 1/1996, de 12 de abril, *por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia*; en su artículo 32 «*Es lícita la inclusión en una obra propia de fragmentos de otras ajenas de naturaleza escrita, sonora o audiovisual, así como la de obras aisladas de carácter plástico o fotográfico figurativo, siempre que se trate de obras ya divulgadas y su inclusión se realice a título de cita o para su análisis, comentario o juicio crítico. Tal utilización solo podrá realizarse con fines docentes o de investigación, en la medida justificada por el fin de esa incorporación e indicando la fuente y el nombre del autor de la obra utilizada.*»

La presente guía **carece** de todo **fin comercial** y su **uso está destinado de forma exclusiva con un fin docente** del Curso de "*Protección de datos en la práctica diaria del profesorado*", impartido en el Colegio Concertado "Ruta de la Plata" de Almendralejo.

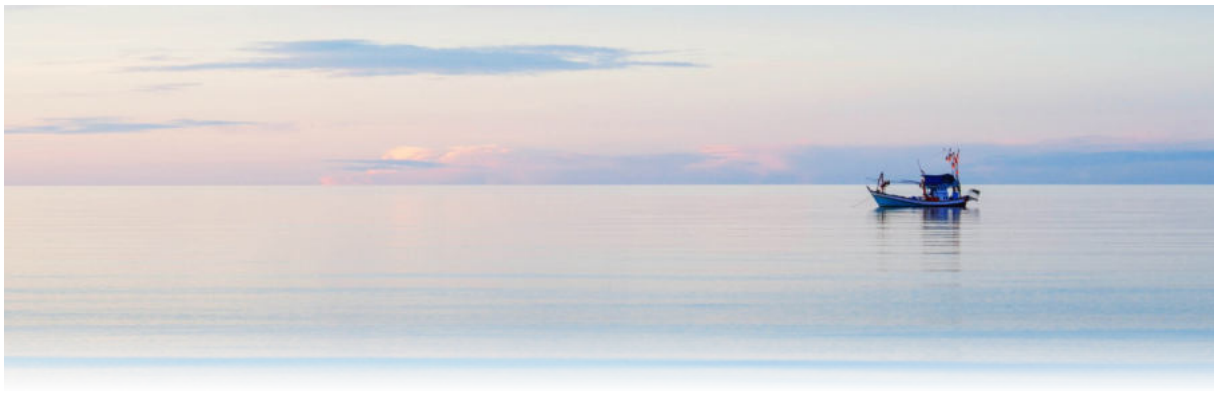
La presente guía está adaptada al contenido de las publicaciones de la Agencia Española de Protección de Datos y de la Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa.

Se ha puesto especial cuidado en el cumplimiento del deber de cita, con indicación de la fuente y nombre del autor de las obras utilizadas, no obstante, si por error involuntario el titular comprobare que su obra y nombre no ha sido incluida en el apartado de Bibliografía, rogamos nos lo indique a la mayor brevedad con la finalidad de incluirse su cita a esta guía, podrá realizar la comunicación en el correo electrónico: **hello@datadata.es**

# ÍNDICE


**Colegio Concertado**
***Ruta de la Plata***
***Almendralejo.***

# Nuestro DELEGADO DE PROTECCIÓN DE DATOS Y AUTOR



## EL EQUIPO

data data®

Derecho Administrativo
Derecho Digital
Protección de Datos
Compliance

Alonso Ramón
Abogado

Ricardo Barrasa
Ingeniero Informático.

Eduardo Sanz
Abogado

José Antonio López
Abogado

Diana Bernabé
Abogada

Monika Golinska
Abogada

## NUESTRO DPD

Alonso Ramón-Díaz.
aramon@icam.es
Tlf. 681.18.87.56

Funcionario de Carrera desde 1997 (actualmente e.v.) que ingresó por oposición como nº 1 de su promoción. Letrado.

Abogado del Ilustre Colegio de Abogados de Madrid -ICAM- nº 92090.

Doctorando en Ciencias Jurídicas en la Universidad Pablo de Olavide de Sevilla. Ámbito investigación: Derecho de las nuevas tecnologías y Protección de Datos.

Máster OFICIAL en Protección de Datos por la Universidad Internacional de la Rioja - UNIR.

Delegado de Protección de Datos (DPD) de la AFA y del Colegio RUTA DE LA PLATA de Almendralejo (Badajoz). También has sido Delegado de Protección de Datos del Ayuntamiento de Montijo y, actualmente, es el DPD de diversas empresas y profesionales.

Máster en Mediación, Negociación y Resolución de Conflictos en la Universidad Carlos III de Madrid.

Es asociado de la Asociación Profesional Española de Privacidad -APEP-.

Es asociado a la International Association of Privacy Professionals -IAPP-.

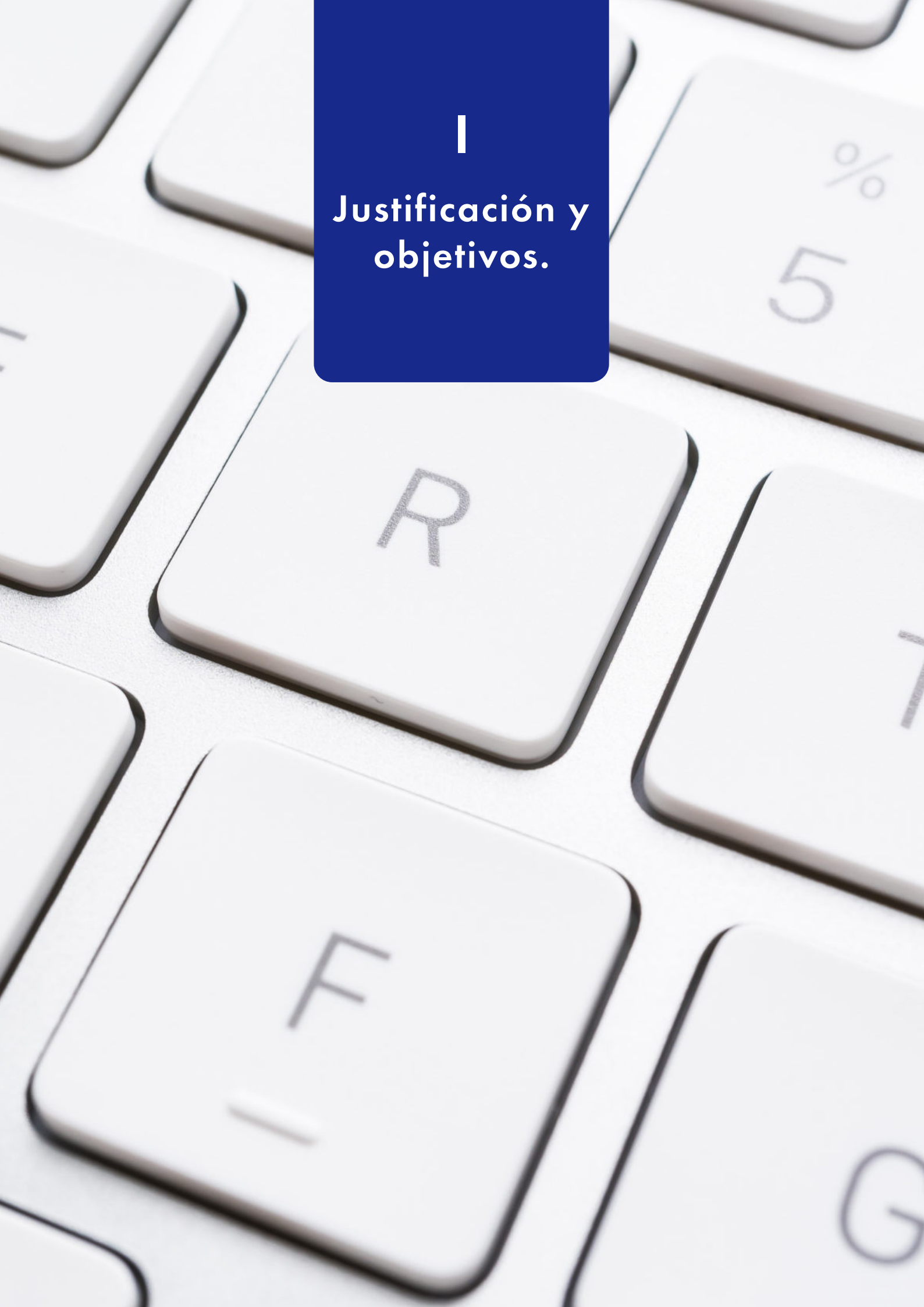
Es asociado a la European Association of Data Protection Professionals -EADPP-

Es asociado de la Asociación Nacional expertos Abogacía TIC -ENATIC-.


**Colegio Concertado**
***Ruta de la Plata***
***Almendralejo.***

# I

# Justificación y objetivos.




**Colegio Concertado**
***Ruta de la Plata***
***Almendralejo.***

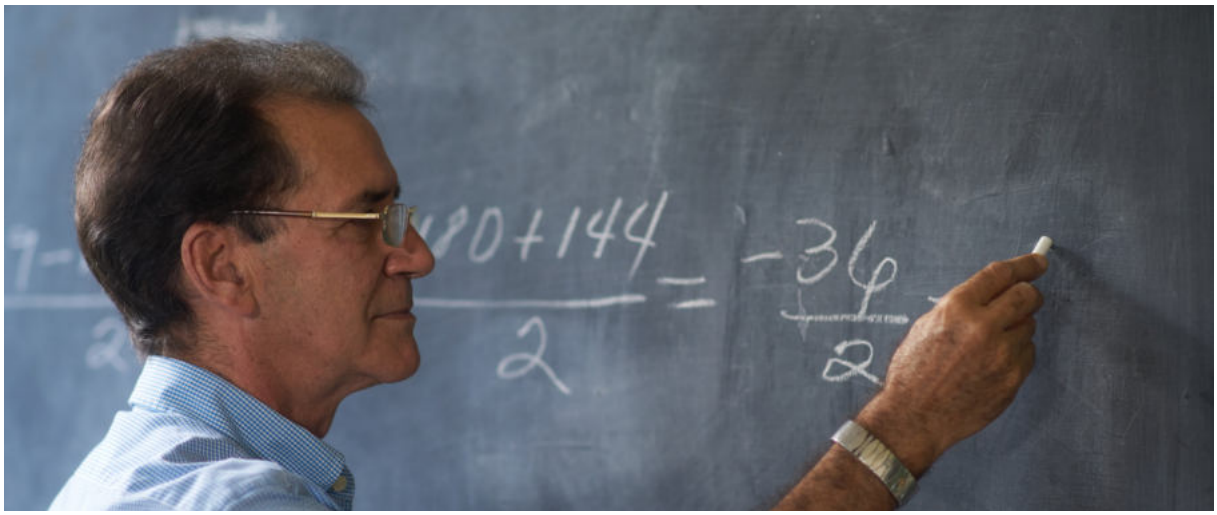
# I. Justificación y objetivos.

La presente actividad formativa se **justifica** por encontrarnos ante una sociedad hiperconectada y donde los denominados "nativos digitales" conviven y respiran tecnología desde su ingreso en los centros educativos hasta la finalización de su periodo educativo, dicha tecnología se alimenta principalmente de datos de carácter personal: redes sociales, reconocimiento facial, videovigilancia, etc.; y, además, del propio examen de los objetivos propuestos y de los contenidos que se pretenden abordar puede colegirse la necesidad de adquirir unos conocimientos básicos en materia de datos de carácter personal por parte del profesorado, máxime cuando nuestra Constitución reconoce como fundamental el derecho a la Protección de Datos de Carácter Personal.

El profesorado debe enfrentarse diariamente al tratamiento de datos personales, el presente curso se justifica en dotarles de una formación teórica en la materia, que les permita afrontar con éxito las situaciones cotidianas que en materia de Protección de Datos de Carácter Personal se producen en nuestros Centros Escolares, también, su enfoque práctico para que el docente se familiarice con la terminología, procedimientos, derechos y actuación en la materia.

El **objetivo** marcado para el presente curso de formación es dotar al docente del **Colegio Concertado** "***Ruta de la Plata***" de los conocimientos básicos en materia de Protección de Datos de Carácter Personal (PDCP), para que este pueda desempeñar su práctica profesional diaria de forma respetuosa con la normativa vigente, esto es, el Reglamento Europeo de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos (LOPDGDD).

Así mismo, se abordará la actividad formativa desde una necesaria perspectiva teórica pero sin olvidar la necesaria realidad diaria del profesorado en el aula y enfocada a los alumnos y alumnas, por ello, se adaptará el curso en la medida de lo posible a un enfoque totalmente práctico de la normativa de Protección de Datos a las distintas situaciones más habituales que puedan presentarse a nuestros docentes.




**Colegio Concertado**
***Ruta de la Plata***
***Almendralejo.***

# II

# El origen de la Protección de datos: EE.UU.

# II. Origen del derecho a la Protección de Datos: EE.UU

El origen del **derecho a la intimidad** puede establecerse en los Estados Unidos de América, en el año 1890, al sentar sus bases jurídicas los abogados **Samuel Dennis Warren** y a **Louis Dembitz Brandeis** quienes el 15 de diciembre de 1890 publicaron el artículo "*Right to Privacy*" (El derecho a la privacidad) en la prestigiosa revista jurídica The Harvard Law Review.

Samuel D. Warren

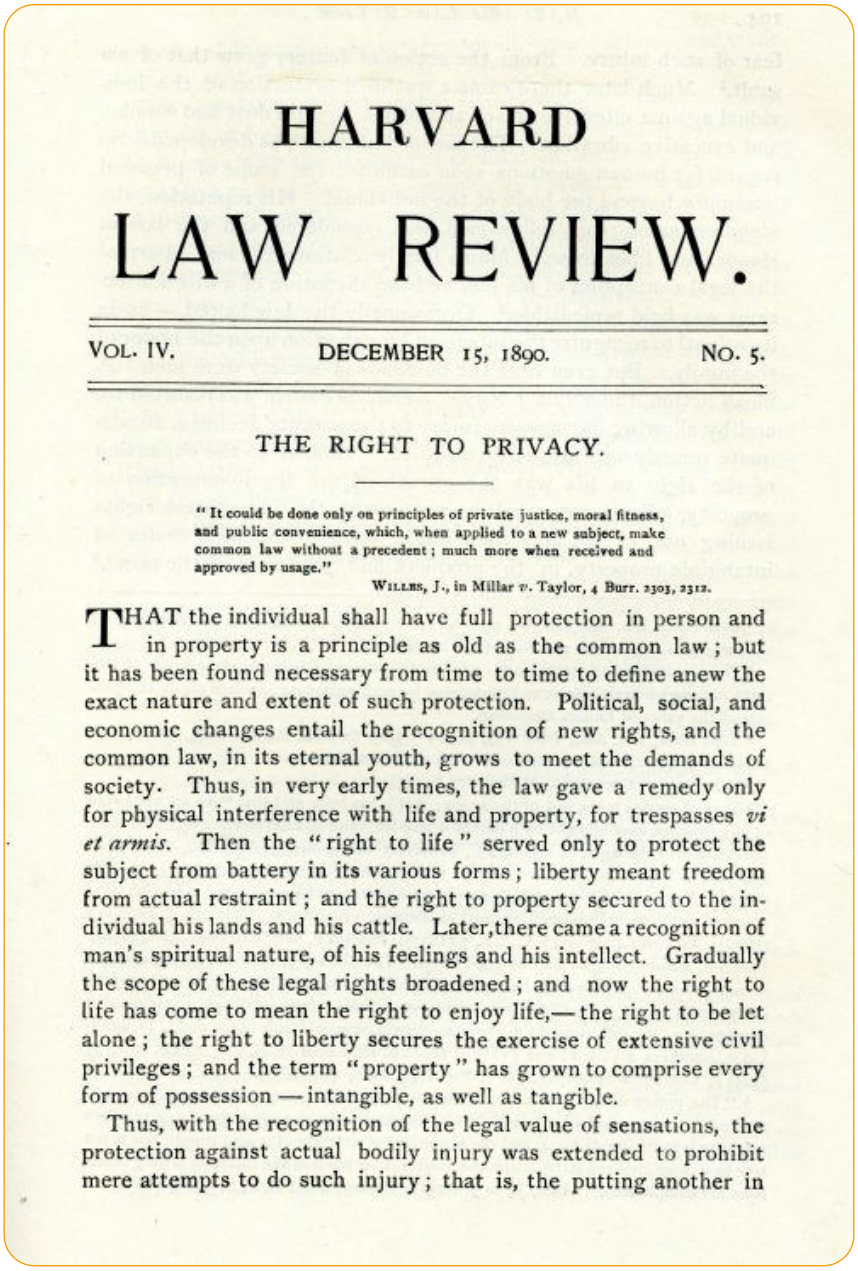
Louis D. Brandeis

¿Qué ocurrió? En el año **1854** fue Antonio Meuci quien inventó el "teletrófono", posteriormente llamado teléfono; en el año **1877** John Thompson fue uno de los máximos exponentes de la fotografía social, publicando el álbum titulado "La vida de las calles de Londres"; esto es, **a finales del S. XIX emerge una sociedad tecnológica** que en opinión de Warren y Brandeis amenazaban con lograr una masiva e indiscriminada difusión de información privada de los ciudadanos, llegando a alcanzar la misma hasta la publicación en los periódicos de información íntima con la finalidad de colmar la curiosidad lasciva de los lectores mediante la intromisión en el ámbito privado. Así, Warren y Brandeis manifiestan su preocupación en su artículo *Right to Privacy*, siendo uno de los fragmentos más citados el que sigue:

*La vida de las calles de Londres.*
J. Thompson.

> *"Los recientes inventos y los nuevos métodos de hacer negocios fueron los focos de atención en el siguiente paso que hubo de darse para amparar a la persona, y para garantizar al individuo lo que el juez Cooley denomina el derecho 'a no ser molestado'. Las instantáneas fotográficas y las empresas periodísticas han invadido los sagrados recintos de la vida privada y hogareña; y los numerosos ingenios mecánicos amenazan con hacer realidad la profecía que reza: 'lo que se susurre en la intimidad, será proclamado a los cuatro vientos' [ ... ] La intensidad y complejidad de la vida, que acompañan a los avances de la civilización, han hecho necesario un cierto distanciamiento del mundo, y el hombre, bajo la refinada influencia de la cultura, se ha hecho más vulnerable a la publicidad, de modo que la soledad y la intimidad se ha convertido en algo esencial para la persona; por ello, los nuevos modos e inventos, al invadir su intimidad, le producen un sufrimiento espiritual y una angustia mucho mayor que la que le pueden causar los meros daños personales"* - *The Right to Privacy, Harvard Law Review. Vol IV. Dec 15, 1890. Pags 195-196.*

Warren y Brandeis reivindican en su artículo la necesidad de definir un **principio que pueda ser invocado para proteger la vida privada del individuo** frente a la invasión de una prensa demasiado pujante, del fotógrafo, o del poseedor de cualquier aparato de reproducción o grabación de imágenes y sonidos[1]. De esta forma, el principio invocado se materializó en el **derecho a la privacidad** (right to privacy), que otorgaba a toda persona una plena disponibilidad para decidir en qué medida *"pueden ser comunicados a otros sus pensamientos, sentimientos y emociones"*[2], esto es, un derecho amplio consistente en poder disfrutar de la propia vida (*the right to enjoy life*) ligado al *right to be let alone* (derecho a ser dejado en paz), concepto este último acuñado por el juez Cooley en 1888 en referencia al derecho a no ser víctima de ataques o agresiones físicas.



HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar v. Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession—intangible, as well as tangible.

Thus, with the recognition of the legal value of sensations, the protection against actual bodily injury was extended to prohibit mere attempts to do such injury; that is, the putting another in

**1** The Right to Privacy, Harvard Law Review. Vol IV. Dec 15, 1890. Pag. 206.

**2** The Right to Privacy, Harvard Law Review. Vol IV. Dec 15, 1890. Pag. 198.

No obstante, debemos subrayar que Warren y Brandeis destacaron que el derecho a la privacy o intimidad no es un derecho absoluto y, por tanto, estaba sujeto a límites que han llegado intactos a nuestro tiempo presente, así los **límites** del *right to privacy* serían[3]:

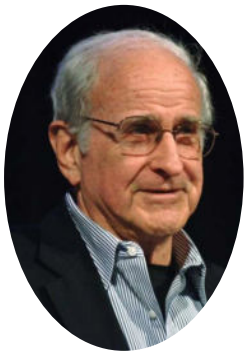
- No impide la publicación hechos o noticias que posean un **interés público o general**, considerando la condición pública o privada de la persona sobre la que verse la noticia. Reconocen también el derecho de las personas públicas a ver protegida una parte de su vida privada.
- No excluye la publicación de determinados asuntos sobre hechos o manifestaciones relativos a **instituciones o corporaciones públicas**.
- Debe entenderse afectada de manera distinta según el medio y el grado de publicidad de su vulneración; así, el derecho no otorga, en principio, **ninguna reparación por violación de la intimidad cuando la publicación de hechos se haga en forma oral y sin causar daños especiales**.
- Obliga a prestar atención a la conducta del propio interesado o afectado, considerando los autores que **el derecho a la *privacy* decae con la publicación de los hechos por él mismo o con su consentimiento**.
- No permite alegar la ausencia de malicia ni la *exceptio veritatis* [Excepción material que puede oponerse frente a una pretensión indemnizatoria por difamación si el demandado demuestra que son ciertos los hechos del relato presuntamente difamatorio.]

Seguidamente, en el **año 1903**, el derecho a la intimidad fue incluido en la Ley de Derechos Civiles de Nueva York en los siguientes términos: "*Una persona, firma o corporación que usa con fines de propaganda o de comercio el nombre, retrato o imagen de una persona viviente, sin haber obtenido su previo consentimiento escrito, o el de sus padres o tutores si es menor, comete infracción.*"

En la **década de los 60** del pasado Siglo XX se produce la mejora significativa de las cámaras fotográficas con la aparición del teleobjetivo, también los micrófonos inalámbricos o se inicia la utilización de grabadoras portátiles; lo cual generó un nuevo debate sobre la protección de los ciudadanos frente a las «*nuevas tecnologías*» de aquélla época, en general, y del impacto negativo en la **aparición de grandes almacenes de datos electrónicos** (bancos de datos o silos de información) y los posibles **riesgos en la utilización de la informática**.

Así, el uso de **la informática** comenzó a permitir una **recogida** de datos para su inclusión en **grandes bases de datos** lo que permitía a las Autoridades un mayor conocimiento general sobre la población, y, potencial sobre cualquier ciudadano en particular. La cuestión que se plantea es la garantía del respeto de los derechos de las personas ante el nuevo panorama social y tecnológico de los años 60.

**3** Origen y evolución del derecho fundamental a la protección de datos. UNiR. Pág. 6.


Alan F. Westin

En las anteriores circunstancias, el abogado americano **Alan Furman Westin** propuso un nuevo concepto para el término "*privacy*" que, partiendo de la propuesta de Warren y Brandeis, tenía en consideración como en los años 60 las "nuevas tecnologías" lograban recopilar un número importante de huellas documentales sobre los ciudadanos, y, utilizando dichas huellas mediante el uso de la informática, las Autoridades y/o el Estado lograban obtener un gran poder.

Westin propuso definir el *right to privacy* como el **derecho de los individuos a controlar la información sobre ellos y a decidir cómo, cuándo y de qué manera se transmite esa información a terceros**. Planteó así un enfoque claramente informacional de la vida privada, cuya protección alcanza incluso a ciertos comportamientos en lugares públicos. El derecho así delimitado y conceptualizado por Westin se puede denominar ***informational privacy*** o *privacidad informativa*, pero se dio a conocer más simplemente como *privacy*, o privacidad[4].

Brandeis llegó a la Corte Suprema de Estados Unidos en el año 1928 pero sus tesis sobre el *right to privacy* no fueron asumidas por aquélla hasta el año 1967 mediante la trascendental sentencia del *caso Berger y Katz vs. The United States* y donde la Corte, al resolver un caso de espionaje electrónico, declaró que la Cuarta Enmienda de la Constitución de EE.UU[5] tiene el propósito de proteger personas y no únicamente lugares, declarando que: "*El derecho a ser dejados solos, el más amplio de los derechos y el más valioso del hombre civilizado, debe ser protegido de toda intromisión injustificable del gobierno en la intimidad del individuo, cualesquiera sean los medios utilizados, debiendo considerarse una violación de la Cuarta Enmienda. Y el uso como prueba, en un procedimiento criminal, de hechos revelados por esa intromisión, debe considerarse una violación de la Quinta Enmienda*[6"7].

Siguiendo a Westin y su visión de la privacidad como el derecho del individuo a controlar la información de carácter personal, en el año 1973, por parte del comité consultivo *Secretary's Advisory Committee on Automated Personal Data Systems*, se publicó el informe Registros, Informática y los Derechos de los Ciudadanos -***Records, Computers and the Rights of Citizens***- o también conocido como el "informe Ware" en relación al Presidente del Comité Willis Howard Ware. Una de las grandes aportaciones del citado informe fue su definición de los **principios de tratamiento justo de datos personales** o *Fair Information Practice Principles (FIPPs)*.

---

**4** Origen y evolución del derecho fundamental a la protección de datos. UNiR. Pág. 7.

**5** Enmienda IV a la Constitución EE.UU: El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas.

**6** Enmienda V a la Constitución EE.UU: Nadie estará obligado a responder de un delito castigado con la pena capital o con otra infamante si un gran jurado no lo denuncia o acusa, a excepción de los casos que se presenten en las fuerzas de mar o tierra o en la milicia nacional cuando se encuentre en servicio efectivo en tiempo de guerra o peligro público; tampoco se pondrá a persona alguna dos veces en peligro de perder la vida o algún miembro con motivo del mismo delito; ni se le compelera a declarar contra sí misma en ningún juicio criminal; ni se le privará de la vida, la libertad o la propiedad sin el debido proceso legal; ni se ocupará la propiedad privada para uso público sin una justa indemnización.

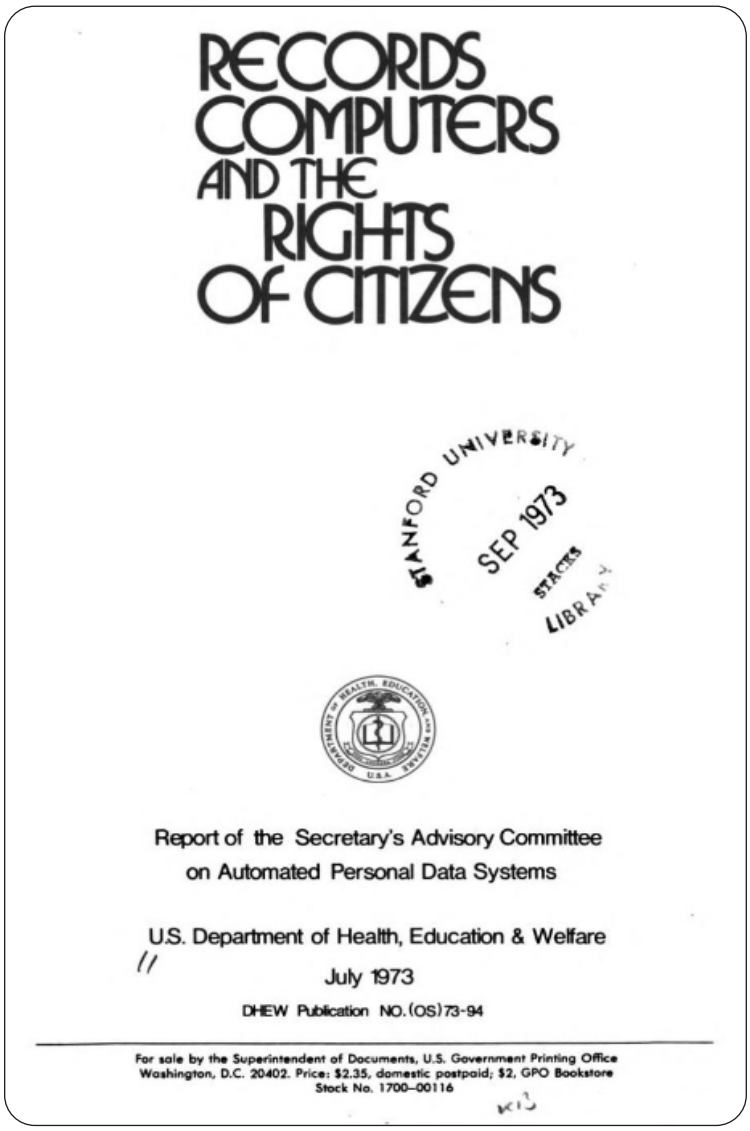
**7** Alan Barth; Alfred A. Knopf , Prophets With Honor, N. York, 1974.

**Principios del Tratamiento Justo de Datos Personales en el Informe Ware:**

- Los ciudadanos deben tener **información y/o conocimiento** del tratamiento de sus datos personales, no pudiendo existir sistemas de información secretos que recopilen datos personales.
- Los ciudadanos deben que **poder impedir que la información que fue recabada con un propósito concreto se utilice o comunique a terceros con otros fines**, para realizar tales acciones es necesario su consentimiento.
- Toda persona debe tener a su disposición el poder de **saber qué información sobre ellos se ha recopilado por un tercero y para qué la utiliza**.
- Cualquier persona debe tener el poder de **rectificar las informaciones** que sobre él tengan terceros cuando aquéllas sean incorrectas.
- Quien realice un tratamiento de datos de carácter personal debe **garantizar la calidad y seguridad de los mismos**, garantizando su fiabilidad y adoptando las medidas necesarias para prevenir un uso indebido de los mismos.

Willis Howard Ware

Por último, destacar que en el año 1974 se produjo la dimisión del Presidente de EE.UU Richard Nixon por el escándalo *Watergate* relativo al sistema de grabación y espionaje de conversaciones. Por tal motivo, el legislador estadounidense adoptó el *Privacy Act* de 1974, que fue una ley destinada a evitar el uso indebido de información sobre las personas por parte de las autoridades gubernamentales.



RECORDS COMPUTERS AND THE RIGHTS OF CITIZENS

STANFORD UNIVERSITY SEP 1973 STACKS LIBRARY

Report of the Secretary's Advisory Committee on Automated Personal Data Systems

U.S. Department of Health, Education & Welfare

July 1973

DHEW Publication NO.(OS)73-94

For sale by the Superintendent of Documents, U.S. Government Printing Office Washington, D.C. 20402. Price: $2.35, domestic postpaid; $2, GPO Bookstore Stock No. 1700-00116

# III

# Marco Normativo.

# III. Marco normativo.

Actualmente el marco normativo principal en materia de Protección de Datos de Carácter Personal estaría conformado por:

- **Consejo de Europa**[8]:

.- **Convenio Europeo de Derechos Humanos** (CEDH) de 1950[9].

Artículo 8.- *Derecho al respeto a la vida privada y familiar.*

1. *Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*
2. *No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.*

.- **Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal** (Convenio 108) de 1981[10].

A comienzos de los años 70 del Siglo XIX el Consejo de Europa comenzó a plantearse los riesgos de la informática sobre los derechos de las personas y si la protección otorgada por el artículo 8 CEDH sobre la vida privada y familiar resultaba suficiente para los retos que la irrupción de la informática planteaba, se llegó a la conclusión que no y por tal motivo se desarrolló un instrumento específico: el Convenio 108. Así, el **Convenio 108 fue el primer instrumento de carácter internacional y legalmente vinculante para los Estados pertenecientes al Consejo de Europa cuyo objetivo era la garantía de la protección de los datos de carácter personal realizada mediante tratamientos automatizados** (se excluyen los ficheros manuales), habiendo sido actualmente ratificado por 47 países.

Aunque el Convenio 108 es legalmente vinculante para los Estados no resulta directamente ejecutable y requiere que los países que lo ratifiquen adopten en su ordenamiento jurídico los mecanismos necesarios para la garantía de la protección de los datos de carácter personal cuyo tratamiento se realice mediante medios automatizados.

---

**8** El Consejo de Europa es una organización internacional que tiene como objetivo principal la defensa, protección y promoción de los derechos humanos (en particular los civiles y políticos), la democracia y el Estado de Derecho. Creado el 5 de mayo de 1949, se trata de la institución de este tipo más antigua de nuestro continente y engloba las 47 naciones europeas con la sola excepción de Bielorrusia. En 1950, se redactó el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH) donde se garantiza la protección de los derechos humanos y que creó el Tribunal Europeo de Derechos Humanos (TEDH). El Consejo de Europa tiene su sede en la ciudad francesa de Estrasburgo, que hace visible su relación con la reconciliación europea tras una historia jalonada por enfrentamientos. España se convirtió en miembro de la Organización el 24 de noviembre de 1977.

**9** https://www.echr.coe.int/Documents/Convention_SPA.pdf

**10** https://rm.coe.int/16806c1abd

.- **Convenio 108+** de 2018[11].

Como hemos dicho, el Consejo de Europa elaboró hace casi cuarenta años el Convenio 108 con la finalidad de proteger a las personas físicas respecto del tratamiento automatizado de sus datos personales.

El transcurso de los años y la aparición de nuevas tecnologías e Internet provocó que la regulación que establecía para 1981 necesitase de una urgente adaptación a los tiempos actuales, modernizándose a las nuevas realidades de la era digital.

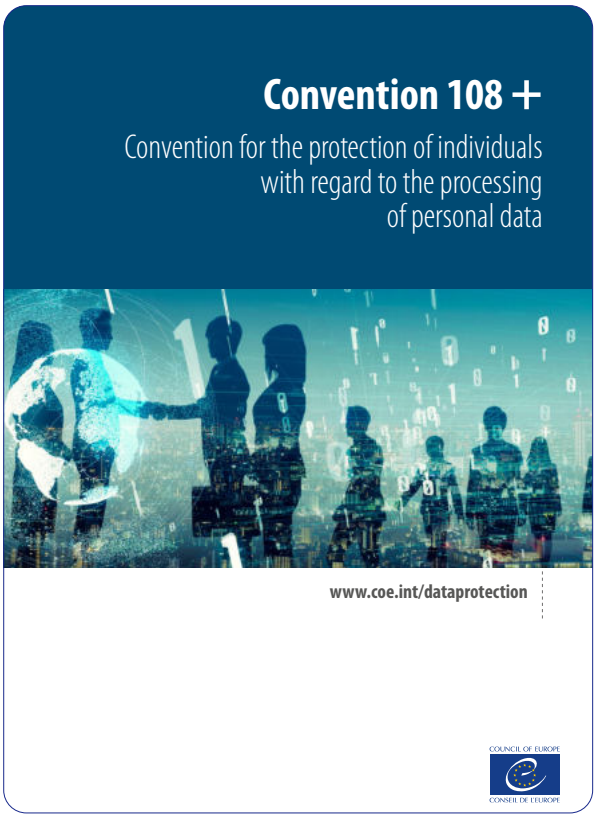
El Convenio 108+ es la versión adaptada a la actualidad y el Consejo de Europa lo abrió a la firma de los países el día 10 de octubre de 2018 en Estrasburgo.

El Reino de España ha sido uno de los firmantes del Convenio 108+ y teniendo una excelente acogida por el resto de países.

El derecho al respeto a la vida privada y familiar es objeto del artículo 1 del Convenio:

Artículo 1.- *Derecho al respeto a la vida privada y familiar.*

*El fin del presente Convenio es proteger a cada persona física, sean cuales fueren su nacionalidad o su residencia, con respecto al tratamiento automatizado de los datos de carácter personal, contribuyendo así al respeto de sus derechos y libertades fundamentales y, en particular, el derecho a la privacidad.*




**Chapter I – General provisions**

**Article 1 – Object and purpose**

The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy.

**Article 2 – Definitions**

For the purposes of this Convention:

*a.* "personal data" means any information relating to an identified or identifiable individual ("data subject");

*b.* "data processing" means any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data;

11 https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

.- **Carta de los Derechos Fundamentales de la Unión Europea** (CDFUE) de 2000[12].

Artículo 7.- *Derecho de la vida privada y familiar.*

*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.*

Artículo 8.- *Protección de datos de carácter personal.*

1. *Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*
2. *Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*
3. *El respeto de estas normas quedará sujeto al control de una autoridad independiente.*

Para que se pueda establecer una limitación de los derechos que reconocen los artículos 7 y 8 de la Carta se deberán cumplir los requisitos que establece su artículo 52.1, a saber:

Artículo 52.- *Alcance de los derechos garantizados.*

1. *Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.*


**12** https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Aunque la Carta fue proclamada en el año 2000 **careció de fuerza vinculante hasta el año 2009** porque su destino estuvo ligado al proyecto constitucional de la Unión Europea y, aunque el Tratado de Lisboa fue rubricado en diciembre de 2007, éste no entró en vigor hasta diciembre de 2009 y en dicho momento la Carta adquirió su fuerza vinculante, gozando en la actualidad el mismo valor jurídico que los Tratados constitutivos de la Unión Europea por mandato del art. 6.1 del Tratado UE.

.- **Tratado de Funcionamiento de la Unión Europea de 2010 (TFUE)**[13].

Artículo 16.

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

.- **Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (Reglamento general de protección de datos -RGPD)**[14].

Artículo 1.- *Objeto.*

1. *El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.*
2. *El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.*
3. *La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.*

.- **Constitución Española de 1978 (CE)**[15].

Artículo 18.

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. (...)
4. 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.

**13** https://www.boe.es/doue/2010/083/Z00047-00199.pdf
**14** https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807
**15** https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

.- **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (LOPDGDD)**[16].

Artículo 1.- *Objeto de la ley.*

*La presente ley orgánica tiene por objeto:*

a) ***Adaptar** el ordenamiento jurídico español al Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y **completar** sus disposiciones.*

*El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.*

b) ***Garantizar** los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.*


**16** https://boe.es/buscar/act.php?id=BOE-A-2018-16673

**PUNTOS CLAVE**

## ¿Qué es el Derecho Fundamental a la Protección de Datos?

Para establecer una definición del derecho fundamental a la Protección de Datos de carácter personal acudimos a la interpretación realizada por nuestro Tribunal Constitucional:

Sentencia 94/1998, de 4 de mayo:

> Nos encontramos ante un derecho fundamental a la protección de datos por el que se **garantiza a la persona el control sobre sus datos**, cualesquiera datos personales, y sobre su uso y destino, para **evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados**; de esta forma, el derecho a la protección de datos se configura como una **facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención**.

Sentencia 292/2000, de 30 de noviembre, FJ 7º:

> ... el contenido del derecho fundamental a la protección de datos consiste en un **poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero**, sea el Estado o un particular, **o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso**. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos **se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero**, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la **facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos**.
>
> En fin, son **elementos característicos** de la definición constitucional del derecho fundamental a la protección de datos personales **los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos**. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del **derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos**. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele.

PUNTOS CLAVE

## ¿Limitaciones al derecho a la Protección de Datos Personales?

- El derecho a la protección de los datos de carácter personal **no** es un derecho absoluto; por tanto, puede limitarse si es necesario para alcanzar un objetivo de interés general o para proteger los derechos y libertades de los demás.

- Las condiciones para limitar los derechos al respeto de la vida privada y a la protección de los datos personales están recogidas en el artículo 8 del Convenio Europedo de Derechos Humanos y en el artículo 52, apartado 1, de la Carta. Se han desarrollado e interpretado en la jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea.

- En la legislación sobre protección de datos del Consejo de Europa, el tratamiento de datos personales constituye una injerencia lícita en el derecho del respeto de la vida privada y sólo puede llevarse a cabo si:
  - » se realiza de conformidad con la ley;
  - » sirve a un fin legítimo;
  - » respeta la esencia de los derechos y libertades fundamentales;
  - » es necesario y proporcionado en una sociedad democrática para alcanzar un fin legítimo.

- El ordenamiento jurídico de la Unión Europea impone condiciones similares a las limitaciones del ejercicio de los derechos fundamentales protegidos por la Carta. La limitación de un derecho fundamental, incluido el derecho a la protección de los datos personales, solo puede ser lícita si:
  - » se realiza de conformidad con la ley;
  - » respeta la esencia del derecho;
  - » es necesaria en virtud del principio de proporcionalidad; y
  - » sirve a un objetivo de interés general reconocido por la Unión o a la necesidad de proteger los derechos de los demás.

Cuadro obtenido del Manual de legislación europea de protección de datos. Ed 2018. Pag 41.

**Sentencia Ejemplo**

Asunto: ***Khelili contra Suiza***.

Tribunal Europeo de Derechos Humanos - **TEDH**.

Sentencia nº 16188/07, 18 de octubre de 2011.

Durante un control policial, la policía descubrió que la demandante llevaba tarjetas de visita en las que podía leerse:

> «Mujer bonita y agradable, bien entrada en la treintena, desearía encontrar a un hombre para tomar una copa o salir de vez en cuando. Número de teléfono [...]»

La demandante alegó que, a raíz de ese descubrimiento, la policía le abrió un expediente como prostituta, una profesión a la que ella había negado dedicarse de forma reiterada. La demandante pidió que se eliminase la palabra «prostituta» de los registros informáticos de la policía.

El TEDH reconoció en principio que la conservación de los datos personales de un particular sobre la base de que dicha persona podría cometer otro delito podría ser proporcionada en determinadas circunstancias. Sin embargo, en el caso de la demandante, la alegación de prostitución ilícita parecía demasiado vaga y general, no se apoyaba en hechos concretos ya que aquella jamás había sido condenada por prostitución ilícita y, por lo tanto, no podía considerarse que existiera una «necesidad social imperiosa», en el sentido del artículo 8 del CEDH.

En vista de que correspondía a las autoridades demostrar la exactitud de los datos conservados sobre la demandante, así como de la gravedad de la injerencia en los derechos de esta persona, el Tribunal dictaminó que la conservación de la palabra «prostituta» en el expediente policial no había sido necesaria en una sociedad democrática. El Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

**Sentencia Ejemplo**

Asunto: ***Leander contra Suecia***.

Tribunal Europeo de Derechos Humanos - **TEDH**.

Sentencia nº 92481/81, 26 de marzo de 1987, apdos. 59 y 67.

En el asunto Leander contra Suecia el TEDH resolvió que el control secreto de personas que se postulan a puestos de importancia de la seguridad nacional no es contrario, en sí mismo, al requisito de ser necesario en una sociedad democrática.

Las garantías específicas establecidas en la legislación nacional para proteger los intereses del titular de los datos —por ejemplo, los controles ejercidos por el Parlamento y el Ministro de Justicia— llevaron al TEDH a concluir que el sistema de control de personal de Suecia cumplía los requisitos del artículo 8, apartado 2, del CEDH. Visto el amplio margen de apreciación de que disponía, el Estado demandado estaba autorizado a considerar que, en el caso del demandante, los intereses de la seguridad nacional prevalecían sobre los intereses individuales.

El Tribunal concluyó que no había existido una violación del artículo 8 del CEDH.

Es habitual **CONFUNDIR** los siguientes derechos fundamentales consagrados por el **artículo 18** de la Constitución:

- al **HONOR**,
- a la **INTIMIDAD**,
- a la **PROPIA IMAGEN**,
- a la **PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**.

### .- Derecho al honor y la reputación personal[17].

El derecho al honor y la reputación personal son bienes que se refieren a la estimación de la persona en y por la sociedad y contribuyen a configurar el estado social de la misma. Se distinguen **dos aspectos** del honor: inmanente y trascendente. El primero consiste en la estima que cada persona tiene de sí misma; el segundo, por su parte, radica en el reconocimiento de los demás de nuestra dignidad (STS 23/03/87), se vincula así, pues, con la fama, con la opinión social.

No obstante, nuestro Tribunal Constitucional ha declarado que no puede ofrecerse una definición concreta y unívoca del "honor", toda vez que su adecuada protección dependerá de la interpretación realizada conforme a las "*normas, valores e ideas sociales vigentes en cada momento*".

La **afectación al honor** se valora en atención a la relevancia pública de la persona, su afectación a la vida profesional o a la privada, y las circunstancias concretas en la que se produce así como su repercusión exterior.

Se considerará un **atentado al honor** de la persona toda aquella manifestación que persiga el descrédito, el desmerecimiento e incluso la humillación.

### .- Derecho a la intimidad[18].

El derecho a la intimidad **se vincula a la esfera más reservada de las personas**, al ámbito que éstas siempre preservan de las miradas ajenas, aquél que **desea mantenerse oculto a los demás por pertenecer a su esfera más privada** (STCo 151/97, de 29 sep.), vinculada con la dignidad y el libre desarrollo de la personalidad (art. 10.1 CE).

Las personas más expuestas al público también tienen reconocido el derecho a un núcleo inaccesible de intimidad (STCo 134/99, de 15 jul.).

La intimidad se reconoce no sólo al individuo aisladamente considerado, sino también al núcleo familiar (SSTCo 197/91, de 17 oct. ó 231/88, de 2 dic).

**17** Díez-Picazo, L.; Gullón, A. *Instituciones de derecho civil.* 2ª ed. Tecnos. 1995. Pág. 223.
**18** https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2.

.- **Derecho a la propia imagen**.

El derecho a la propia imagen consiste, en última esencia, en el **poder de decidir** -consentir o impedir- **la reproducción de la imagen física de nuestra persona por cualquier medio** (fotografía, grabado, dibujo, etc.), **así como su exposición o divulgación sin nuestro consentimiento**.

Por tanto, el derecho a la propia imagen **salvaguarda la proyección exterior de dicha imagen** como medio de evitar injerencias no deseadas (STCo 139/01, de 18 jun.), de velar por una determinada imagen externa (STCo 156/01, de 2 jul.) o de preservar nuestra imagen pública (STCo 81/01, de 26 mar).

Este derecho está íntimamente condicionado por la actividad del sujeto, por ejemplo, las personas con una actividad pública verán más expuesta su imagen.

.- **Derecho a la protección de datos (o a la autodeterminación informativa)**.

La STCo 94/1988 señaló del derecho a la protección de datos de carácter personal que nos encontramos ante un **derecho fundamental por el que se garantiza a la persona el control sobre sus datos**, cualesquiera datos personales, y **sobre su uso y destino**, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una **facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención**.

Según la STCo 292/2000 consiste en un **poder de disposición y de control sobre los datos personales** que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Sus **elementos característicos** son el derecho del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Resultando indispensable para su efectividad el derecho a ser informado de quién posee sus datos personales y con qué fin, y, también el poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Otorga el poder de exigir al titular del fichero que contenga los datos a que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele.

Estos cuatro derechos fundamentales al honor, intimidad, propia imagen y protección de datos podrán verse afectados, por tanto de manera independiente, pero también, con frecuencia, de forma conjunta, dada su evidente proximidad.

Por último, destacar que estos derechos tienen su más inmediato riesgo en el ejercicio de las libertades de expresión e información, lo que llevará al ejercicio de la ponderación de bienes jurídicos entre los derechos del artículo 18 [honor, intimidad, propia imagen y protección de datos] y del artículo 20 [libertad de expresión e información] de la Constitución constituyan un ejercicio habitual por parte de los operadores del derecho.


**Colegio Concertado**
***Ruta de la Plata***
***Almendralejo.***


# IV

# Terminología y Conceptos Básicos.

# IV. Terminología y conceptos básicos.

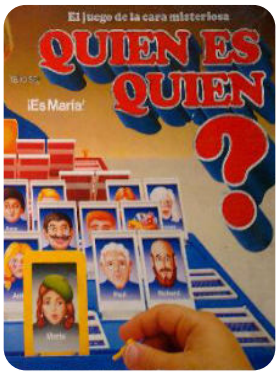
## ¿Qué es un dato de carácter personal?

**Toda información sobre una persona identificada o identificable** («el interesado»).

Persona identificada:

Foto: François GOGLINS

Persona identificable:




Toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

El dato personal **REQUIERE** que concurran, por un lado, la **existencia de una información** y, por otro, que ésta pueda **vincularse a una persona física** identificada o identificable.

**EJEMPLOS:** el nombre y apellidos de un alumno, de sus padres, su dirección, su número de teléfono o su correo electrónico son datos de carácter personal. También lo son las imágenes de los alumnos o, por ejemplo, la profesión, los estudios o el lugar donde trabajan los padres, o su número de cuenta bancaria.

El Derecho de la Unión Europea UE y el Derecho del Consejo de Europa consideran que una información contiene datos sobre una persona si:

- la persona es identificada o identificable con dicha información; o
- en la información se singulariza a la persona, aunque no se identifique, de manera que fuera posible averiguar quién es el interesado si se llevara a cabo una mayor investigación.

Ambos tipos de información están protegidos del mismo modo por la legislación europea en materia de protección de datos. La identificabilidad directa o indirecta de las personas físicas requiere una apreciación continua, "*teniendo en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos*"[19].

**19** Reglamento General de Protección de Datos UE 2016/679. Considerando 26.

Los **principios de protección de datos no deben aplicarse a la información anónima** (inclusive con fines estadísticos o investigación), es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo.

En el Derecho de la Unión Europea **únicamente se protege** por la normativa de protección de datos a la **persona física viva**, a quien se conoce como «**el interesado**». Sin embargo, en el ámbito del Consejo de Europa la protección también se extiende a las personas jurídicas (empresas) y el Tribunal Europeo de Derechos Humanos TEDH se ha pronunciado[20] en supuestos donde se alegó la violación del derecho de una empresa a la protección contra el uso de sus datos de conformidad con el art. 8 CEDH.

**Sentencia Ejemplo**

Asunto: ***Patrick Breyer contra Bundesrepublik Deutschland***.

Tribunal de Justicia de la Unión Europea - **TJUE**.

Sentencia nº C-582/14, 19 de octubre de 2016, apartado 43.

El TJUE examinó el concepto de la identificabilidad indirecta de los interesados.

El asunto trataba de las direcciones IP dinámicas, que cambian cada vez que se establece una nueva conexión a internet. Los sitios web gestionados por las instituciones federales alemanas registraban y almacenaban las direcciones IP dinámicas para evitar ataques cibernéticos y para ejercitar acciones penales en caso necesario. Solo el proveedor de servicios de internet que utilizaba Mr. Breyer disponía de la información adicional necesaria para identificarle.

El TJUE consideró que una dirección IP dinámica, que un proveedor de servicios de medios en línea registra cuando una persona accede a un sitio web que dicho proveedor hace accesible al público, constituye datos personales cuando solo un tercero —el proveedor de servicios de internet en este caso— tiene los datos adicionales necesarios para identificar a esa persona.

Sostuvo que «*no es necesario que toda la información que permita identificar al interesado deba encontrarse en poder de una sola persona*» para que la información sea constitutiva de datos personales. Los usuarios de una dirección IP dinámica registrada por un proveedor de servicios de internet pueden ser identificados en determinadas situaciones, por ejemplo en el marco de un proceso penal en caso de ataques cibernéticos, con la ayuda de otras personas.

Según el TJUE, cuando el proveedor «*disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional de que dispone el proveedor de acceso a internet de dicha persona*», esto constituiría «un medio que pueda ser razonablemente utilizado para identificar al interesado». Por tanto, estos datos se consideran datos de carácter personal.

**20** TEDH, *Bernh Larsen Holding AS y otros contra Noruega*, nº 24117/08, 14 de marzo de 2013. Véase asimismo, en cambio, TEDH, *Liberty y otros contra Reino Unido*, nº 58243/00, 1 de julio de 2008.

## ¿Qué son **categorías especiales** de datos de carácter personal?

Los datos personales **más delicados para la esfera personal e íntima** se engloban dentro de la categoría especial. Esta tipología de datos son especialmente protegidos y el ordenamiento jurídico les presta una especial atención, exigiendo de las personas que los traten una especial diligencia y la adopción de medidas de carácter técnico y organizativo para evitar que dicho tratamiento pueda lesionar los derechos y libertades de los interesados.

**PUNTOS CLAVE**

Tanto el Convenio 108 modernizado (artículo nº 6) como el RGPD (artículo nº 9) consideran los siguientes datos de carácter personal como de **CATEGORÍA ESPECIAL**:

- Los que revelan el origen racial o étnico;
- Los que revelan opiniones políticas, creencias religiosas y otras creencias, incluidas las filosóficas;
- Los que revelan la pertenencia a un sindicato;
- Los relativos a los datos genéticos y datos biométricos cuando son tratados con el fin de identificar a una persona;
- Los relativos a la salud, la vida sexual o la orientación sexual.

**Sentencia Ejemplo**

Asunto: ***Procedimiento penal entablado contra Bodil Lindqvist***.

Tribunal de Justicia de la Unión Europea - **TJUE**.

Sentencia nº C-101/01, 6 de noviembre de 2003, apartado 51.

La señora Lindqvist era empleada de mantenimiento y desempeñaba funciones de catequista en la parroquia de Alseda (Suecia). Hizo un curso de informática en el que, entre otras cosas, tenía que crear una página web en Internet. A finales de 1998, la Sra. Lindqvist creó, en su domicilio y con su ordenador personal, varias páginas web con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieran obtener fácilmente la información que necesitaran.

Las páginas web de que se trata contenían información sobre la Sra. Lindqvist y 18 de sus compañeros de la parroquia, incluido su nombre completo o, en ocasiones, sólo su nombre de pila. Además, la Sra. Lindqvist describía en un tono ligeramente humorístico las funciones que desempeñaban sus compañeros, así como sus aficiones. En varios casos se mencionaba la situación familiar, el número de teléfono e información adicional. Asimismo, señaló que una de sus compañeras se había lesionado un pie y se encontraba en situación de baja parcial por enfermedad.

La Sra. Lindqvist no había informado a sus compañeros de la existencia de estas páginas web, no había solicitado su consentimiento, ni tampoco había comunicado su iniciativa a la Datainspektion (organismo público para la protección de los datos transmitidos por vía informática). En cuanto supo que algunos de sus compañeros no apreciaban las páginas web controvertidas, las suprimió.

A la Sra. Lindqvist se le impuso una pena de multa y se elevó consulta al TJUE quien declaró que:

1) La conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales».
2) Un tratamiento de datos personales de esta naturaleza no está comprendido en la excepción de tratamiento de carácter doméstico o privado.
3) La indicación de que una persona se ha lesionado un pie y está en situación de baja parcial constituye un dato personal relativo a la salud.

PUNTOS CLAVE

**Código Civil.**

**Artículo 6.1** *"La ignorancia de las leyes no excusa de su cumplimiento."*

**EJEMPLOS de categorías especiales datos en centros escolares:**

- Los centros educativos recaban en muchos casos, a través de sus **servicios médicos o botiquines**, datos de salud relacionados con las lesiones o enfermedades que pudieran sufrir los alumnos durante su estancia en el centro.
- También recogen datos de salud de los alumnos para el ejercicio de la **función educativa**, discapacidades físicas o psíquicas, por ejemplo del síndrome TDAH.
- Para prestar el **servicio de comedor** también es necesario recabar datos de salud que permitan conocer los alumnos que son celiacos, diabéticos o que padecen alergias alimentarias.
- También son datos de salud los contenidos en los informes psicopedagógicos de los alumnos.
- **OJO** -> No tiene la consideración de categoría especial de datos o datos sensibles el que un alumno curse la asignatura de religión, ya que el mero hecho de cursar la misma no implica revelación de su confesión religiosa.

## ¿De **QUIÉN** son los datos de carácter personal?

De la persona física titular de los datos, por ejemplo, de los alumnos, padres, tutores, profesores o personal de administración y servicios. Son los afectados o interesados.

PUNTOS CLAVE

**Cada PERSONA FÍSICA es la TITULAR de sus respectivos DATOS de carácter personal.**

## ¿Qué es un **TRATAMIENTO** de datos de carácter personal?

Según el artículo 4 RGPD un tratamiento es cualquier **operación** o conjunto de operaciones realizadas **sobre datos personales** o conjuntos de datos personales, ya sea por **procedimientos automatizados o no**, como los siguientes:

| | | | |
|---|---|---|---|
| **Recogida.** | **Registro.** | **Organización.** | **Estructuración.** |
| **Conservación.** | **Adaptación.** | **Modificación.** | **Extracción.** |
| **Consulta.** | **Utilización.** | **Cotejo.** | **Interconexión.** |
| **Limitación.** | **Supresión.** | **Destrucción.** | **Preservación.**[21] |

**Comunicación** por:

- Transmisión.
- Difusión.
- Cualquier otra forma de habilitación de acceso.

PUNTOS CLAVE

- Por **«tratamiento de datos»** se entiende cualquier operación realizada con datos personales.
- El término **«tratamiento»** comprende el tratamiento automatizado y no automatizado.
- En el Derecho de la UE, el **«tratamiento»** se refiere, además, al tratamiento manual en ficheros estructurados.

Sentencia Ejemplo

Asunto: ***František Ryneš contra Úřad pro ochranu osobních údajů***.

Tribunal Justicia de la Unión Europea - **TJUE**.

Asunto nº C-212/13, 11 de diciembre de 2014, apdo. 25.

El Sr. Ryneš captó la imagen de dos personas que rompieron ventanas de su vivienda por medio del sistema doméstico de vigilancia por CCTV que había instalado para proteger su propiedad.

El TJUE determinó que la grabación y conservación de datos personales por medio del sistema de videovigilancia constituye un tratamiento de datos automatizado que está comprendido en el ámbito de aplicación de la legislación de la UE en materia de protección de datos.

**21** El Convenio 108 modernizado añade la preservación de los datos a la definición en su artículo 2, letra b). El verbo preservar es definido por DRAE como "*proteger, resguardar anticipadamente a alguien o algo, de algún daño o peligro*".

Sentencia Ejemplo

Asunto: ***Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni***.

Tribunal Justicia de la Unión Europea - **TJUE**.

Asunto nº C-398/15, 9 de marzo de 2017, apdo. 35.

El Sr. Manni solicitó que se eliminasen sus datos personales del registro de una empresa de calificación crediticia que le vinculaba a la liquidación de una empresa inmobiliaria, con menoscabo de su reputación.

El TJUE resolvió que «*al transcribir y conservar esta información en el registro y al comunicarla, en su caso, a terceros previa petición, la autoridad encargada de éste lleva a cabo un "tratamiento de datos personales" del que es "responsable"*».

.- **TRATAMIENTO DE DATOS AUTOMATIZADO**.

Hemos visto que la normativa de protección de datos se aplica a un "*tratamiento total o parcialmente automatizado de datos personales*" lo que, en la práctica, viene a significar que cualquier tratamiento de datos personales realizado por medios automatizados con ayuda, por ejemplo, de un **ordenador personal**, un **dispositivo móvil** o un **enrutador**[22], está sujeto a las normas de protección de datos de la Unión Europea y del Consejo de Europa.

.- **TRATAMIENTO DE DATOS NO AUTOMATIZADO**.

El tratamiento de datos manual también requiere de protección y respeto a la normativa de protección de datos de carácter personal de la Unión Europea que no se limita, en modo alguno, al tratamiento de datos automatizado.

Un fichero manual es un fichero en papel especialmente estructurado.

Un fichero estructurado es aquel que clasifica un conjunto de datos personales, de modo que sean accesibles en virtud de determinados criterios. Por ejemplo, el Director de un Colegio mantiene un expediente denominado «bajas de empleados», que contiene todos los datos de las bajas que han tenido los docentes durante el último año y que está clasificado por orden alfabético, este expediente constituirá un fichero manual sujeto a las normas de protección de datos de la UE porque:

- los ficheros en papel pueden estructurarse de modo que faciliten y agilicen la búsqueda de información;
- el almacenamiento de datos personales en ficheros en papel estructurados hace que sea más sencillo eludir las limitaciones establecidas legalmente para el tratamiento de datos automatizado.

**22** Un enrutador, del inglés router, es un dispositivo que permite conectar distintos ordenadores que funcionan en el marco de una red. Función: establecer la ruta que destinará a cada paquete de datos dentro de una red informática. En su interior contiene las instrucciones y protocolos adecuados como para permitir el envío y la recepción de los paquetes de información entre ambos, de modo que esta llegue a su destino y no se pierda, usando siempre la ruta más adecuada en cada momento.

**EJEMPLOS de tratamientos en centros escolares:**

- La recogida de los datos de los alumnos y de sus padres al inicio del curso escolar es un ejemplo claro de tratamiento de datos de carácter personal.
- Igualmente lo es el mantenimiento y la actualización del expediente del alumno y su transmisión a un nuevo centro en caso de traslado, así como la captación y grabación de imágenes a través de sistemas de videovigilancia.

## ¿Quién es el **RESPONSABLE** del tratamiento de datos personales?

El responsable del tratamiento es la persona física o jurídica, pública o privada, que **decide sobre la finalidad, contenido y uso** del mismo, bien por decisión directa o porque así le viene impuesto por una norma legal.

En los **centros educativos públicos** el responsable del tratamiento será, normalmente, la Administración pública correspondiente, es decir la Consejería de Educación de la Junta de Extremadura.

En los **centros concertados y privados** los responsables del tratamiento de los datos serán los propios centros.

## ¿Quién es el **ENCARGADO** del tratamiento de datos personales?

El encargado del tratamiento es la persona física o jurídica, la autoridad pública, servicio u otro organismo que **trate datos personales por cuenta del responsable del tratamiento**.

En determinados casos, los centros educativos para cumplir sus funciones necesitan contar con la colaboración de otras personas o entidades que no forman parte de su organización, por ejemplo, para el servicio de comedor, servicio médico, transporte o para la realización de actividades extraescolares.

Estas personas y entidades para prestar sus servicios también tratan los datos de carácter personal de los alumnos y de sus padres o tutores, pero **lo hacen por encargo del responsable** del tratamiento, es decir del centro o de la Administración educativa; teniendo la consideración de encargados del tratamiento respecto al tratamiento de datos personales que realizan.

El Reglamento General de Protección de Datos establece un **deber de diligencia en la elección del encargado** del tratamiento y la suscripción de contrato con un contenido detallado. La Agencia Española de Protección de Datos publicó las Directrices para la elaboración de estos contratos entre responsable y encargado del tratamiento.

Como decimos, resulta **necesario que el tratamiento** de datos que implica la prestación del servicio **se rija por un contrato** que deberá incluir las garantías adecuadas y que detallamos:

- La **obligación del encargado** del tratamiento de tratar los datos únicamente conforme a las instrucciones del centro o Administración educativa que ostente en cada caso la condición de responsable del tratamiento.
- Que **los datos no se utilizarán** para finalidades distintas de las previstas en el contrato, ni se comunicarán a otras personas, ni siquiera para su conservación.
- Las **medidas de seguridad a implantar** por el encargado del tratamiento.
- La **devolución de los datos** al centro o a la Administración educativa que sea responsable o al encargado del tratamiento que ésta designe o, en su defecto, su destrucción una vez finalizado el contrato.

**NUNCA se considera encargado del tratamiento a las personas físicas que tengan acceso a los datos personales en su condición de empleados(*) del centro o de la Administración que son los responsables del tratamiento [(*)Destinatarios]. TAMPOCO son encargados del tratamiento el equipo directivo del centro, los profesores o el personal de administración y servicios del centro educativo.**

IMPORTANTE

PUNTOS CLAVE

- La persona a quien corresponde determinar los medios y fines del tratamiento de los datos personales de otras personas es el «**responsable del tratamiento**» conforme a la legislación en materia de protección de datos; si varias personas toman esta decisión conjuntamente, podrán ser «corresponsables del tratamiento».
- Un «**encargado del tratamiento**» es una persona física o jurídica que trata datos personales por cuenta del responsable del tratamiento.
- El **encargado del tratamiento pasa a ser el responsable** del tratamiento si es él mismo quien determina los medios y fines del tratamiento de los datos o no respeta las condiciones de tratamiento establecidas por el responsable.
- Cualquier persona a quien se comunican datos personales es un «**destinatario**».
- Un «**tercero**» es una persona física o jurídica distinta del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

**EJEMPLOS de encargados de tratamiento de datos:**

- Las empresas que sean contratadas por el centro o la Administración educativa para prestar los servicios de comedor, servicio médico, transporte escolar o el de seguridad del centro educativo.
- Servicio de asesoría laboral para la elaboración de las nóminas de los trabajadores del responsable del tratamiento.
- La gestión de una Comunidad de propietarios por el administrador de fincas.
- El alojamiento de un sitio web por un prestador de servicios de la sociedad de la información.

La consecuencia más importante de ser un responsable del tratamiento o un encargado del tratamiento es la **responsabilidad jurídica** de cumplir con las obligaciones respectivas, de conformidad con la legislación en materia de protección de datos.

## Tratamientos de datos personales por **PARTICULARES.**

PUNTOS CLAVE

**Reglamento General de Protección de Datos -RGPD-.**

**Artículo 2.2** *"El presente Reglamento* ***NO*** *se aplica al tratamiento de datos personales: (...) c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas."*

Las **personas físicas pueden ser responsables del tratamiento** con arreglo al Derecho de la Unión Europea y al Derecho del Consejo de Europa. Sin embargo, cuando tratan datos acerca de otras personas en relación con una actividad puramente personal o doméstica, los particulares no están sujetos a las normas del RGPD y del Convenio 108 modernizado y no tienen la consideración de responsables del tratamiento.

Así una persona que conserva su correspondencia, un diario personal en el que describe incidentes con amigos y compañeros y el historial médico de miembros de su familia, puede estar exento de las normas de protección de datos, ya que estas actividades podrían ser puramente personales o meramente domésticas y, por tanto, sin conexión alguna con una actividad profesional o comercial.

El RGPD especifica además que las actividades personales o domésticas también podrían incluir la actividad en redes sociales y la actividad en línea realizada en el contexto de las citadas actividades[23].

**23** RGPD - Considerando 18. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. **No obstante**, el RGPD se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

El acceso de los ciudadanos a internet y la posibilidad de utilizar plataformas de comercio electrónico, redes sociales y blogs para compartir información personal acerca de sí mismos y de otras personas hace que sea cada vez más difícil distinguir el tratamiento de datos para actividades personales del tratamiento de datos para actividades no personales[24].


- La consideración de las actividades como puramente personales o domésticas **depende de las circunstancias**.
- Una actividad personal o doméstica que **tenga aspectos profesionales o comerciales** constituye un tratamiento que está **sometido a la normativa de protección de datos**.

Cuando la **magnitud y la frecuencia** del tratamiento de los datos de carácter personal revele que nos encontramos ante una **actividad profesional o a tiempo completo**, un particular puede tener la consideración de **responsable del tratamiento**.

También hay otro factor a tener en cuenta al respecto y consiste en saber si el **particular expone datos personales accesibles a un elevado número de personas ajenas al ámbito privado de la persona**. Así, los pronunciamientos del Tribunal de Justicia de la Unión Europea TJUE ha interpretado la normativa en el sentido de establecer que **la legislación de Protección de Datos resulta de aplicación** al ciudadano particular que, mediante la utilización Internet, realice una publicación de datos de carácter personal sobre otras personas en un sitio web de acceso público.


Asunto: ***Procedimiento penal entablado contra Bodil Lindqvist***.

Tribunal de Justicia de la Unión Europea - **TJUE**.

Sentencia nº C-101/01, 6 de noviembre de 2003, apartado 51.

La señora Lindqvist trataba de la mención de diferentes personas por su nombre o por otros medios, como su número de teléfono o información sobre sus aficiones, en una página de internet. El TJUE mantuvo que «*la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios [...] constituye un "tratamiento total o parcialmente automatizado de datos personales"*».

Dicho tratamiento de datos personales no está comprendido en el ámbito de aplicación de las actividades exclusivamente personales o domésticas, que quedan fuera del ámbito de aplicación de las normas de protección de datos de la UE, ya que esta excepción «*debe [...] interpretarse en el sentido de que contempla únicamente las actividades que se inscriben en el marco de la vida privada o familiar de los particulares; evidentemente, no es este el caso de un tratamiento de datos personales consistente en la difusión de dichos datos por Internet de modo que resulten accesibles a un grupo indeterminado de personas*».

**24** Véase la declaración del Grupo de Trabajo del Artículo 29 sobre las negociaciones relativas al paquete de reforma de la protección de datos (2013), Anexo 2: Propuestas y modificaciones relativas a la exención para actividades personales o domésticas, 27 de febrero de 2013.

También el Tribunal de Justicia de la Unión Europea TJUE ha declarado que la normativa de Protección de Datos de la Unión Europea, en determinadas circunstancias, también es aplicable a las **grabaciones visuales** que hayan sido realizadas por una **videocámara de seguridad instalada de forma privada**.

Sentencia Ejemplo

Asunto: ***František Ryneš contra Úřad pro ochranu osobních údajů***.

Tribunal Justicia de la Unión Europea - **TJUE**.

Asunto nº C-212/13, 11 de diciembre de 2014, apdo. 25.

El Sr. Ryneš captó la imagen de dos personas que rompieron ventanas de su vivienda por medio del sistema doméstico de vigilancia por Circuito Cerrado de Televisión -CCTV- que había instalado para proteger su propiedad. La grabación se entregó posteriormente a la policía y se utilizó en el proceso penal.

El TJUE declaró que «*[e]n la medida en que una vigilancia por videocámara [...] se extiende, aunque sea en parte, al espacio público, abarcando por ello una zona ajena a la esfera privada de la persona que procede al tratamiento de datos valiéndose de ese medio, tal vigilancia por videocámara no puede considerarse una actividad exclusivamente "personal o doméstica" [...]*».

## ¿Qué es una **COMUNICACIÓN DE DATOS?**

Se realiza una comunicación de datos de carácter personal **cuando se revelan a una persona distinta de su titular**.

Los **interesados** (personas físicas titulares de los datos) **no realizan NUNCA una "comunicación" de datos de carácter personal**, aunque los datos se obtengan de ellos mismos.

Los destinatarios de la comunicación de los datos serán las personas físicas o jurídicas, autoridades públicas, servicios u otros organismos a los que se les revelen los datos.

**NO** se considera comunicación de datos su transmisión a empresas[25] que tengan la condición de encargados de tratamiento.

IMPORTANTE

| | |
|---|---|
| **SÍ** es una comunicación de datos. | Cuando se transfieren los datos de los alumnos de un centro a otro con motivo de un cambio de matrícula o se comunican a las asociaciones de madres y padres (AMPA) o a los Servicios Sociales o Sanitarios, Jueces, Tribunales, Cuerpos y Fuerzas de Seguridad. |
| es una comunicación de datos. | Cuando se revelan o transmiten los datos a las empresas para que, en nombre y previo contrato con el centro o la Administración educativa, presten servicios, por ejemplo, de comedor, médico o transporte. |

**25** RGPD Art. 4.18 «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica.

## ¿Qué son **TRANSFERENCIAS O FLUJOS INTERNACIONALES** de datos?

**Dentro de la Unión Europea** el Reglamento general de protección de datos -RGPD- viene a consagrar la **libre circulación de los datos** de carácter personal.

Una transferencia internacional de datos de carácter personal se produce cada vez que los **datos personales sean enviados fuera del ámbito del Espacio Económico Europeo** [espacio comprendido por la Unión Europea más Noruega, Islandia y Liechtenstein]. Por ejemplo, en el ámbito educativo puede realizarse para que el destinatario[26] de los datos preste un servicio al centro educativo o para que los trate para una finalidad propia.

Sin embargo, contiene **requisitos específicos para las transferencias** de datos personales a **terceros países externos a la Unión Europea y a organizaciones internacionales**.

Aunque el Reglamento destaca su importancia, especialmente en relación al comercio y la cooperación internacionales, también reconoce el incremento del riesgo para los datos personales en dichas transferencias internacionales a terceros países tratando de ofrecer el Reglamento el mismo nivel de protección a los datos personales transferidos a terceros países ajenos al EEE.

**IMPORTANTE**

| | |
|---|---|
| **SÍ** es una transferencia internacional de datos. | Cuando se contratan servicios de cloud computing en los que, por ejemplo, el alojamiento de datos se realiza en servidores fuera del EEE, o cuando se comunican a centros educativos establecidos en países fuera de este ámbito para realizar intercambios de alumnos o periodos de formación. |
| es una transferencia internacional de datos. | Aquellas que se realicen con destino a Estados de la Unión Europea o del EEE, aunque dichas transmisiones deberán cumplir los requisitos establecidos por la Ley para la validez de las comunicaciones de datos o la contratación de un encargado del tratamiento. |

## ¿Qué es un **DELEGADO DE PROTECCIÓN DE DATOS** -DPD-?

La entrada en vigor el 25 de mayo de 2018 del Reglamento -RGPD- supuso una revolución en cuanto al modo de cumplimiento y garantía del derecho fundamental a la Protección de Datos.

**26** RGPD Art. 4.9 «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

Se olvida un modelo "*reactivo*" y se **instaura una verdadera cultura de cumplimiento normativo (Compliance) en materia de Protección de Datos**, ya no es suficiente cumplir el RGPD sino que debe poder demostrarse que se cumple y para ello se instila a las organizaciones y empresarios el principio de "*accountability*" o de **actitud consciente, diligente y proactiva** frente al tratamiento de datos.

Dentro del elenco de medidas se prevé como obligación del centro educativo que ofrezca enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación[27] la siguiente: nombrar un **Delegado de Protección de Datos -DPD-** (Data Protection Officer -DPO-).

Básicamente el DPD tiene la función de **supervisar, asesorar e informar** con absoluta independencia al responsable y encargado del tratamiento en el cumplimiento de la normativa de protección de datos. Es una nueva figura y, como tal, se está construyendo ahora con un desafío importante: **dar a conocer la importancia de la protección de datos** en la institución para la que se trabaja fomentando las actividades de formación, difusión y concienciación.

El DPD participa en la **resolución de las reclamaciones** que en materia de protección de datos se puedan plantear y es el **interlocutor** con la Agencia Española de Protección de Datos y con los interesados.

**RECUERDA:**

- Para el **cumplimiento de sus funciones** y poder **armonizar los tratamientos** de datos personales en los centros educativos, las **dudas que puedan surgir** han de trasladarse al **delegado de protección de datos**.

**PUNTOS CLAVE**

- La responsabilidad proactiva obliga a los responsables y encargados del tratamiento a aplicar medidas de manera activa y continuada para promover y garantizar la protección de los datos en sus actividades de tratamiento.
- Los responsables y encargados del tratamiento tienen la responsabilidad de que sus operaciones de tratamiento de datos cumplan con la legislación en materia de protección de datos y sus obligaciones respectivas.
- Los responsables del tratamiento deben ser capaces de demostrar el cumplimiento de las disposiciones sobre protección de datos ante los interesados, el público en general y las autoridades de control en cualquier momento.

**27** L.O 3/2018 LOPDGDD, Art. 34: Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades: b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

# V

# El Reglamento Europeo de Protección de Datos -RGPD-.

# V. El Reglamento Europeo de Protección de Datos -RGPD-.

Un "reglamento" es una norma o acto legislativo vinculante que debe aplicarse en su integridad en toda la Unión Europea[28], convive junto al resto de actos como son las Directivas y a la decisiones.

El Reglamento General de Datos UE 2016/679 es una norma directamente aplicable desde el 25 de mayo de 2018, que no requiere de normas internas de transposición ni tampoco, en la mayoría de los casos, de normas de desarrollo o aplicación. Por ello, constituye la norma de referencia en materia de Protección de Datos y a la que se acompaña, desde el 5 de diciembre de 2018, la Ley Orgánica de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales LOPDGDD.

## La **LEGITIMACIÓN** para tratar datos de carácter personal.

PUNTOS CLAVE

### ¿Qué es un **TRATAMIENTO** de datos de carácter personal?

Según el artículo 4 RGPD un tratamiento es cualquier **operación** o conjunto de operaciones realizadas **sobre datos personales** o conjuntos de datos personales, ya sea por **procedimientos automatizados o no**, como los siguientes:

| | | | |
|---|---|---|---|
| **Recogida.** | **Registro.** | **Organización.** | **Estructuración.** |
| **Conservación.** | **Adaptación.** | **Modificación.** | **Extracción.** |
| **Consulta.** | **Utilización.** | **Cotejo.** | **Interconexión.** |
| **Limitación.** | **Supresión.** | **Destrucción.** | **Preservación.**[21] |

**Comunicación** por:

- Transmisión.
- Difusión.
- Cualquier otra forma de habilitación de acceso.

En primer lugar y centrados en el ámbito educativo debemos tener en cuenta que la normativa de protección de datos de carácter personal **NO** resulta de aplicación cuando el tratamiento de los datos es efectuado por una persona física en el ejercicio de **actividades exclusivamente personales o domésticas**[29]; tampoco se aplica a los tratamientos de **datos de personas fallecidas**[30].

**28** https://europa.eu/european-union/eu-law/legal-acts_es

**29** Art. 2.2.c) RGPD.

**30** Art. 2.2.b) LOPDGDD. Tener en cuenta también el art. 3: 1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión. Como excepción (...) no podrán acceder a los datos cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante. (...) 3. En caso de **fallecimiento de menores** ... también sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada. (...)

PUNTOS CLAVE

Los datos personales pueden ser objeto de tratamiento de forma lícita[1] si se cumple, al menos, uno de los siguientes criterios porque cada uno de los supuestos tiene su propia autonomía:

a. El tratamiento se basa en el **consentimiento expreso del interesado**;

b. Una **relación contractual** requiere del tratamiento de datos personales para su ejecución;

c. El tratamiento es necesario para el **cumplimiento de una obligación legal** aplicable al responsable del tratamiento (P.ej. mantenimiento actualizado de los datos del Padrón municipal de habitantes);

d. Los **intereses vitales**[2] de los interesados o de otra persona requieren el tratamiento de sus datos;

e. El tratamiento es necesario para cumplir una **misión de interés público**[3] **o** en el **ejercicio de poderes públicos**[4] conferidos al responsable del tratamiento;

f. El motivo del tratamiento son los **intereses legítimos** de los responsables del tratamiento o de terceros, aunque solo mientras no prevalezcan los intereses o los derechos fundamentales de los interesados que requieran la protección de datos personales, **en particular** cuando el interesado sea un **niño**. **OJO ->** Este motivo **NO** será de aplicación al tratamiento realizado por las **autoridades públicas en el ejercicio de sus funciones**.

El tratamiento lícito de datos personales **sensibles** está sometido a un régimen especial más estricto.

---

**1** RGPD Artículo 6.

**2** RGPD Considerando 46: los datos personales únicamente deben tratarse sobre la base del **interés vital** de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

**3** Según Dictamen 06/2014 G29. **Cumplimiento de una misión realizada en interés público**: comprende situaciones en las que el mismo responsable del tratamiento tiene una potestad pública o una misión de interés público (pero no necesariamente una obligación jurídica de tratar los datos) y el tratamiento es necesario para el ejercicio de dicha potestad o para la ejecución de dicha misión. P.ej: una autoridad fiscal puede recopilar y tratar la declaración de la renta de una persona física con el fin de establecer y verificar el importe del impuesto pagadero. Otro ejemplo podría ser un organismo gubernamental a la que se encarga la tarea de gestionar un servicio de biblioteca, un colegio o una piscina local.

**4** Según Dictamen 06/2014 G29. **Ejercicio de poderes públicos conferidos al responsable del tratamiento**: comprende situaciones en las que el responsable del tratamiento no tiene una potestad oficial, pero una tercera parte con dicha potestad le solicita que revele los datos. P.ej, un funcionario de un organismo público competente para investigar delitos puede pedir al responsable del tratamiento que coopere en una investigación en curso, en vez de ordenar al responsable del tratamiento que cumpla una solicitud específica de cooperación.

| | | | |
|---|---|---|---|
| **Recogida.** | **Registro.** | **Organización.** | **Estructuración.** |
| **Conservación.** | **Adaptación.** | **Modificación.** | **Extracción.** |
| **Consulta.** | **Utilización.** | **Cotejo.** | **Interconexión.** |
| **Limitación.** | **Supresión.** | **Destrucción.** | **Preservación.**[21] |

**Comunicación** por:

- Transmisión.
- Difusión.
- Cualquier otra forma de habilitación de acceso.

## ¿Es lícito nuestro tratamiento?

**IMPORTANTE**

| | Sí | No |
|---|---|---|
| ¿Actividad personal o doméstica? | ☐ | ☐ |
| ¿Datos de un fallecido? | ☐ | ☐ |
| ¿Tengo consentimiento expreso? | ☐ | ☐ |
| ¿Existe relación contractual? | ☐ | ☐ |
| ¿Actúo en cumplimiento de una obligación legal? | ☐ | ☐ |
| ¿El tratamiento responde a intereses vitales? | ☐ | ☐ |
| ¿Cumplo una misión de interés público? | ☐ | ☐ |
| ¿Actúo en ejercicio de poderes públicos? | ☐ | ☐ |
| Si no actúo en funciones públicas: ¿Existe un interés legítimo del Responsable o terceros? | ☐ | ☐ |

La **Ley Orgánica de Educación** (LOE)[31] legitima a los centros docentes para que puedan recabar y realizar el tratamiento de los datos de carácter personal de los alumnos, también de sus padres o tutores, vamos a ver el contenido de la **Disposición Adicional 23ª**:

1. *Los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia:*
   - *al origen y ambiente familiar y social,*
   - *a características o condiciones personales,*
   - *al desarrollo y resultados de su escolarización,*
   - *a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos.*

**31** Ley Orgánica 2/2006, 3 may. *de Educación* -LOE-. https://boe.es/buscar/pdf/2006/BOE-A-2006-7899-consolidado.pdf

2. *Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo.*

   *La incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos.*

   *En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.*

3. *En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad.*

   ***El profesorado y el resto del personal** que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias **quedará sujeto al deber de sigilo**[32].*

4. *La cesión de los datos, incluidos los de carácter reservado, necesarios para el sistema educativo, se realizará preferentemente por vía telemática y estará sujeta a la legislación en materia de protección de datos de carácter personal.*

Sentencia Ejemplo

Revelación de secretos.

Audiencia Provincial de Málaga, Sección 7ª.

Sentencia nº 14/2018 de 19 febrero, recurso nº 4/2018.

**Hechos probados:** El administrador del gimnasio X, en fecha próxima al día 13 de noviembre de 2013, colocó en la puerta del local dos partes médicos de baja de incapacidad temporal por contingencias comunes de dos empleadas, en donde obraban, entre otros extremos, sus nombres, dirección completa, número de teléfono particular, número de afiliación a la Seguridad Social, número de DNI, y la fecha de baja, debajo de un cartel en el que se decía "*debido a la baja por enfermedad de las dos monitoras, el gimnasio permanecerá cerrado hasta el lunes, las usuarias podrán recuperar los días perdidos sin costes alguno perdonen las molestias*".

Dichos partes de baja por incapacidad le habían sido aportados por las perjudicadas para tramitar la correspondiente baja sin que el acusado dispusiera de autorización para poder exhibirlos al público.

**Condena**: Al administrador como autor de dos delitos de revelación de secretos (previsto y penado en el artículo 199.1 Código Penal), a la pena de dos años de prisión, y 12 meses de multa; y al pago de las costas procesales, incluyendo las de la acusación particular.

**32** Código Penal, artículo 199: *1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.*
*2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.*

## Principios de **LICITUD, LEALTAD Y TRANSPARENCIA.**

En este apartado vamos a continuar estudiando **qué datos de carácter personal se pueden tratar y cómo**. Así, los datos han de ser tratados de manera **lícita, leal y transparente**[33] en relación al interesado. En el apartado anterior hemos estudiado la licitud (legitimación) del tratamiento, veamos ahora los principios de lealtad y transparencia.

### 1.- EL PRINCIPIO DE LEALTAD.

La normativa de protección de datos establece de forma clara que, además de ser lícito, el tratamiento de los datos de carácter personal deberá realizarse de manera leal[34]. El principio de lealtad.

Son los Responsables del Tratamiento quienes deben poner en conocimiento de los interesados que el tratamiento de los datos se realizará de forma lícita y transparente y, además, deberán poder demostrar que dichas operaciones de tratamiento de datos personales cumplen el RGPD.

El principio de tratamiento leal exige que la información sea fácil de comprender para los interesados. Debe utilizarse lenguaje adecuado para los destinatarios. El nivel y el tipo de lenguaje que se utilicen tendrán que ser distintos en función de si el público destinatario es, por ejemplo, adulto o infantil, el público en general o expertos académicos.

**EJEMPLO:**

El departamento de investigación de una universidad realiza un experimento para analizar los cambios de estado de ánimo de 50 sujetos, que deben registrar sus pensamientos en un fichero electrónico cada hora, en un momento concreto.

Las 50 personas dieron su consentimiento para este proyecto concreto y para este uso concreto de los datos por la universidad.

El departamento de investigación pronto descubrió que el registro electrónico de pensamientos sería muy útil en otro proyecto orientado a la salud mental, coordinado por otro equipo. Aunque la universidad, como responsable del tratamiento, podría haber utilizado los mismos datos en el trabajo de otro equipo sin hacer nada más para garantizar la licitud del tratamiento de esos datos, puesto que las finalidades son compatibles, la universidad informó a los sujetos y les pidió un nuevo consentimiento, en aplicación de su código ético de investigación y del principio de lealtad del tratamiento.

**33** RGPD. Principios relativos al tratamiento. Artículo 5.1 *Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»).*
**34** Reglamento general de protección de datos, artículo 5, apartado 1, letra a); Convenio 108 modernizado, artículo 5, apartado 4, letra a).

Ninguna operación de tratamiento puede ser llevada a cabo de modo oscuro o secreto, debiendo conocer los interesados cualquier riesgo potencial que pueda existir en relación al mismo y es ahí donde entra en juego el principio de transparencia.

## 2.- EL PRINCIPIO DE TRANSPARENCIA.

Tanto las normativa de la Unión Europea[35] como la del Consejo de Europa[36] vienen a establecer de forma taxativa que todo tratamiento de datos de carácter personal deba realizarse «*de manera transparente en relación con el interesado*».

Gracias al Principio de Transparencia se establece la obligación del Responsable del tratamiento para que adopte las medidas oportunas para mantener informado al interesado sobre cómo van a ser utilizados sus datos.

La información deberá facilitarse de forma **concisa, transparente, inteligible y de fácil acceso**, con un **lenguaje claro y sencillo**, en particular cualquier información dirigida específicamente a un niño[37]. Cuando facilite información, el responsable puede utilizar iconos normalizados[38] para facilitar la información de manera fácilmente visible e inteligible, por ejemplo, se puede utilizar un icono que represente un candado para indicar que los datos se han obtenido de manera segura o que están cifrados. También destacar que los interesados deben tener claro cuáles son los riesgos, las normas, las salvaguardas y los derechos que conciernen al tratamiento de sus datos personales[39].

La transparencia puede referirse a la información proporcionada a la persona antes de comenzar el tratamiento de los datos[40], a la información que debe estar a disposición de los interesados durante el tratamiento[41], o a la información proporcionada a los interesados cuando estos hayan solicitado acceso a sus propios datos[42].

**Excepciones a la obligación de informar**. La obligación de informar a los interesados no es de aplicación si el interesado ya dispone de toda la información pertinente[43]. Además, cuando los datos personales no se hayan obtenido del interesado, la obligación de informar no será de aplicación cuando la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos[44].

**35** RGPD. Reglamento general de protección de datos, artículo 5, apartado 1, letra a).
**36** Convenio 108 modernizado, artículo 5, apartado 4, letra a) y artículo 8.
**37** RGPD. Reglamento general de protección de datos, artículo 12, apartado 1.
**38** La Comisión Europea desarrollará posteriormente la información que se ha de presentar por medio de iconos y los procedimientos para proporcionar iconos normalizados por medio de actos delegados; véase el Reglamento general de protección de datos, artículo 12, apartado 8.
**39** RGPD. Reglamento general de protección de datos, considerando 39.
**40** RGPD. Reglamento general de protección de datos, artículos 13 y 14.
**41** Grupo de Trabajo del Artículo 29, Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, p. 23..
**42** RGPD. Reglamento general de protección de datos, artículo 15.
**43** RGPD. Reglamento general de protección de datos, artículo 13, apartado 4 y artículo 14, apartado 5, letra a).
**44** RGPD. Reglamento general de protección de datos, artículo 14, apartado 5, letras b) hasta e); Convenio 108 modernizado, artículo 11.

Vamos a poner un **ejemplo** de cumplimiento del principio de lealtad y transparencia en la **información que ofrece una página web** de una Academia en el que se trataran datos de carácter personal:

**¿Quiénes somos?**

El «responsable» del tratamiento de los datos es la Academia DATA, con domicilio social en [dirección: xxx], Tel.: xxx; Fax: xxx; Correo electrónico: yy@academiadata.com; los datos de contacto con el delegado de protección de datos: [xxx].

El aviso de información de datos personales forma parte de los términos y condiciones por los que se rigen nuestros servicios formativos.

**¿Qué datos recogemos de usted?**

Recogemos de usted los siguientes datos personales: nombre, dirección postal, número de teléfono, dirección de correo electrónico, información académica, número de tarjeta de crédito y débito y direcciones IP o nombres de dominio de los ordenadores que utiliza para conectarse a nuestra web.

**¿Por qué recogemos sus datos?**

Tratamos sus datos con su consentimiento y con objeto de realizar la reserva de plazas, formalizar y cumplir los contratos relativos a los servicios de formación que le ofrecemos y cumplir los requisitos que impone la ley, como por ejemplo la Ley del Impuesto sobre el Valor Añadido, que nos obliga a recoger datos personales con el fin de confeccionar facturas y poder realizar el pago del impuesto a la Hacienda pública.

**¿Cómo tratamos sus datos?**

Sus datos personales se conservarán durante el tiempo de formación en nuestra academia y, posteriormente, el plazo legal para atender los requerimientos de abono de impuestos. Sus datos no están sujetos a procedimientos de decisión automatizados.

Nuestra Academia sigue estrictos procedimientos de seguridad para cuidar de que sus datos personales no sean dañados, destruidos o revelados a terceros sin su permiso, así como para evitar accesos no autorizados. Los ordenadores que conservan la información se mantienen en un entorno seguro con acceso físico restringido. Utilizamos cortafuegos y otras medidas para limitar el acceso electrónico. Si debemos transferir los datos a un tercero, exigimos que apliquen medidas similares para proteger sus datos personales.

El acceso a toda la información que recogemos o registramos está restringido a nuestras oficinas. Solo las personas que necesitan dicha información para cumplir con sus obligaciones en virtud del presente contrato reciben acceso a los datos personales. Cuando necesitemos información que le identifique, se la solicitaremos expresamente. Es posible que les pidamos que colaboren con nuestros controles de seguridad antes de poner información a su disposición. Podrán actualizar los datos personales que nos faciliten en cualquier momento poniéndose en contacto con nosotros directamente.

### ¿Cuáles son sus derechos?

Tiene derecho de acceso a sus datos, a obtener una copia de sus datos, a solicitar su supresión o rectificación o a solicitar la portabilidad de sus datos a otro responsable.

Puede enviarnos sus peticiones a la dirección de contacto: X. Academia DATA tiene la obligación de contestar a su petición en el plazo de un mes, pero si dicha petición es excesivamente compleja o recibimos un número demasiado elevado de peticiones, le comunicaremos que este periodo puede prorrogarse otros dos meses. También puede ponerse en contacto con nuestro Delegado de Protección de Datos en la dirección X.

### Acceso a sus datos personales

Tiene usted derecho de acceso a sus datos, a ser informado —cuando lo solicite— de las razones que motivan el tratamiento de los datos, a solicitar su supresión o rectificación y a no ser objeto de una decisión puramente automatizada sin que se tengan en cuenta sus puntos de vista. Puede enviarnos sus peticiones a la dirección de contacto X. También tiene derecho de oposición al tratamiento, a retirar su consentimiento y a presentar una reclamación ante la autoridad de control nacional (Agencia Española de Protección de Datos) si considera que este tratamiento de los datos vulnera la ley y a reclamar que se le indemnice por los daños y perjuicios ocasionados a consecuencia del tratamiento ilícito.

**IMPORTANTE**

Aunque los Centros Educativos hemos visto que no necesitan el consentimiento para recabar u obtener algunos datos de carácter personal de los interesados, **SÍ** han de facilitarles la siguiente información:

- de la existencia de un tratamiento de datos personales,
- de la finalidad para la que se recaban los datos y su licitud, por ejemplo, para el ejercicio de la función educativa, o para difundir y dar a conocer las actividades del centro,
- de la obligatoriedad o no de facilitar los datos y de las consecuencias de negarse,
- de los destinatarios de los datos,
- de los derechos de los interesados y dónde ejercitarlos,
- de la identidad del responsable del tratamiento: el centro o la Administración educativa.

## ¿Cuándo debo facilitar la anterior información?

La información se puede facilitar, por ejemplo, al cumplimentar los formularios de admisión de los alumnos en los centros o al matricularse o a través de su propia web.

## La **CONFIDENCIALIDAD** y el deber de secreto (artículo 5 LOPDGDD).

Los responsables y encargados, así como todas las personas que intervengan en cualquier fase del tratamiento de datos personales están sujetas al **deber de confidencialidad**[45].

Esta obligación general de confidencialidad será **complementaria** de los deberes de **secreto profesional** de conformidad con su normativa aplicable.

Las anteriores obligaciones **se mantendrán** aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

**EJEMPLO:**

Un administrativo de un centro educativo recibe una llamada de teléfono en su lugar de trabajo de alguien que dice ser un familiar de un alumno y le solicita información sobre su expediente escolar y posibles faltas de asistencia a clase.

El deber de mantener la confidencialidad de los datos de los alumnos exige que el empleado público aplique unas medidas de seguridad mínimas antes de revelar los datos personales. Por ejemplo, puede ofrecer a su interlocutor comparecer personalmente en el centro y acreditar su identidad, o, formular escrito de solicitud siguiendo el conducto establecido al efecto.

## El principio de **MINIMIZACIÓN** de datos.

El tratamiento de datos debe **limitarse a lo necesario** para cumplir un fin legítimo, en este sentido únicamente deberán tratarse los datos de carácter personal que resulten «*adecuados, pertinentes y no excesivos en relación con el fin para el que se obtienen o tratan*»[46].

Las categorías de datos seleccionados para su tratamiento deben ser **necesarias para lograr el objetivo declarado** de las operaciones tratamiento, y el responsable del tratamiento deberá proceder a la **recogida de los datos mínimos** o estrictamente necesarios que estén directamente **relacionados con el fin específico** que persiga el tratamiento.

## El principio de **EXACTITUD** de los datos.

Los datos personales serán **exactos** y, si fuera necesario, **actualizados**; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan[47].

**45** LOPDGDD. Ley Orgánica 3/2018 de protección de datos, artículo 5, apartado 1.
**46** Reglamento general de protección de datos, artículo 5, apartado 1, letra c); Convenio 108 modernizado, artículo 5, apartado 4, letra c).
**47** Reglamento general de protección de datos, artículo 5, apartado 1, letra d); Convenio 108 modernizado, artículo 5, apartado 4, letra d).

## El principio de **SEGURIDAD** de los datos.

Este principio requiere la aplicación de **medidas técnicas u organizativas** apropiadas en el tratamiento de los datos personales para **proteger** dichos datos contra el acceso, uso, modificación, difusión, pérdida, destrucción o daño accidental, no autorizado o ilícito[48].

Para la aplicación de las medidas técnicas y organizativas de seguridad el propio Reglamento establece que el responsable y el encargado del tratamiento deben tener en cuenta «*el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como fines riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas*»[49].

Las Administraciones educativas deberán cumplir, en su caso, con los principios básicos y requisitos mínimos que permitan una protección adecuada de la información de conformidad con lo establecido en la Disposición adicional 1ª de la Ley como base en el Esquema Nacional de Seguridad[50].

**IMPORTANTE**

El RGPD, **no** establece un catálogo de medidas de seguridad a aplicar, sino que parte de las siguientes premisas:

- En primer lugar, relacionado con el principio de **responsabilidad activa**, los responsables deben realizar una valoración del riesgo de los tratamientos que realicen, a fin de establecer qué medidas se deben aplicar y cómo hacerlo.
- En segundo lugar, y en función de los riesgos detectados en el análisis realizado anteriormente citado, los responsables y encargados deben adoptar las medidas de seguridad, teniendo en cuenta:
  - el coste de la técnica.
  - los costes de aplicación.
  - la naturaleza, alcance, contexto y fines del tratamiento.
  - los riesgos para los derechos y libertades.

Asimismo, el RGPD prevé que **cada responsable, centro o Administración educativa** deberá mantener **documentación** relativa a las **actividades de tratamiento** efectuadas bajo su responsabilidad que incluya, cuando sea posible, una descripción general de las medidas de seguridad adoptadas teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

**48** Reglamento general de protección de datos, artículo 5, apartado 1, letra f) y considerando 39; Convenio 108 modernizado, artículo 7.
**49** Reglamento general de protección de datos, artículo 32, apartado 1.
**50** Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Por su parte, los centros y las Administraciones educativas, como responsables del tratamiento, tomarán medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales solo pueda tratar dichos datos en el ejercicio de las funciones que tenga asignadas.

La **seguridad de los datos NO se logra únicamente con el equipo adecuado** (hardware y programas informáticos), sino que también **exige la existencia de normas internas de organización adecuadas**. Lo ideal sería que dichas normas internas comprendieran las siguientes cuestiones:

- el **suministro regular de información** a todos los miembros de la organización sobre normas de seguridad de los datos y sus obligaciones con arreglo a la legislación en materia de protección de datos, en especial en lo referente a sus obligaciones de confidencialidad;
- la **distribución clara de las responsabilidades y** un esquema claro de las **competencias** en materia de tratamiento de datos, en especial en lo que respecta a las decisiones de tratar datos personales y transmitir datos a terceros o a interesados;
- el **uso de los datos** personales únicamente **con arreglo a las instrucciones** de la persona competente o de conformidad con las normas generales establecidas;
- la **protección del acceso** a las ubicaciones y al hardware y programas informáticos del responsable del tratamiento o del encargado del tratamiento, incluidos los controles de las autorizaciones de acceso;
- **garantizar** que las autorizaciones para acceder a los datos personales han sido atribuidas por la persona competente y exigen la documentación adecuada;
- **protocolos** automatizados sobre el acceso electrónico a los datos personales y verificaciones periódicas de tales protocolos por el departamento de control interno (con la consiguiente obligación de registrar todas las actividades de tratamiento de datos);
- la **documentación** cuidadosa de otras formas de difusión distintas al acceso automatizado de los datos para poder demostrar que no se han producido transmisiones de datos ilegales.

Ofrecer a los miembros del personal **formación y educación** adecuadas **sobre la seguridad** de los datos es también un elemento importante de las precauciones de seguridad efectivas que deben adoptarse.

Entre las **medidas para mejorar el nivel de seguridad** del responsable del tratamiento o del encargado del tratamiento se incluyen instrumentos como los delegados de protección de datos personales, la educación sobre seguridad para los empleados, las auditorías periódicas, los ensayos de penetración y los sellos de calidad.

Sentencia Ejemplo

Asunto: ***I. contra Finlandia***.

Tribunal Europeo de Derechos Humanos - **TEDH**.

Sentencia nº 20511/03, 17 de julio de 2008.

La demandante (Sra. I.) no pudo demostrar que otros empleados del hospital donde trabajaba habían accedido a su historial médico de forma ilegítima y su reclamación de que se había violado su derecho a la protección de datos fue, por tanto, desestimada por los órganos jurisdiccionales nacionales.

El TEDH concluyó que había existido una violación del artículo 8 del CEDH, ya que el sistema de registro de las historias clínicas del hospital «*era tal que no era posible aclarar de forma retroactiva el uso de las historias de los pacientes tal como habían revelado las cinco últimas consultas y que dichos datos fueron suprimidos una vez que el expediente fue devuelto a los archivos*».

En opinión del Tribunal, resultó decisivo que el sistema de archivo existente en el hospital incumplía claramente los requisitos legales establecidos en la legislación nacional, un hecho que no fue valorado debidamente por los órganos jurisdiccionales nacionales.

## 1.- LA NOTIFICACIÓN EN SUPUESTOS DE BRECHAS DE SEGURIDAD.

Se entiende por "violación de datos personales" o "brecha de seguridad" a toda **violación de la seguridad que ocasione** la destrucción, pérdida o alteración accidental o ilícita de datos personales tratados o la comunicación o acceso no autorizados a dichos datos.

Aunque las nuevas tecnologías nos ofrecen más posibilidad de garantía de la seguridad y potentes herramientas como el cifrado de datos, lo cierto y verdad es que las violaciones de los datos siguen siendo un problema de actualidad, siendo sus **causas** variadas que abarcan desde errores accidentales de los empleados hasta amenazas externas, como la ciberdelincuencia o la piratería informática.

Las violaciones de datos pueden ser **muy perjudiciales para la privacidad y los derechos de protección de datos de las personas físicas** que, a causa de la violación, pierden el control de sus datos personales.

Las violaciones **pueden dar lugar a** robos de identidad o fraudes, pérdidas financieras o daños materiales, pérdida de confidencialidad de datos personales protegidos por el secreto profesional y daños para la reputación del interesado.

Si no se notifican las violaciones de seguridad, ni las autoridades de control (Agencia Española de Protección de Datos) ni las personas físicas serán conocedoras de que se ha producido una violación de datos y esto impedirá que las personas físicas actúen para protegerse de sus consecuencias negativas. Así, para **reforzar los derechos** de las personas físicas y limitar el impacto de las violaciones de datos, la normativa de protección de datos **impone a los responsables del tratamiento un requisito de notificación** en determinadas circunstancias.

El RGPD establece en sus artículos 33 y 34 un régimen detallado que regula el momento y el contenido de las notificaciones. En consecuencia, los **responsables del tratamiento deben notificar determinadas violaciones de datos a la Agencia Española de Protección de Datos sin dilaciones indebidas y, cuando sea viable, en un plazo de 72 horas desde el momento en que sean conocedores de la violación**. En los supuestos en que se sobrepase el plazo de 72 horas, el responsable del tratamiento deberá acompañar a la notificación de una explicación razonada de los motivos de la dilación en el plazo de notificación.

La notificación de una brecha de seguridad a la Agencia Española de Protección de Datos debe incluir, como mínimo, una descripción de:

- La naturaleza de la violación de los datos,
- las categorías y el número aproximado de interesados afectados,
- las posibles consecuencias de dicha violación, y
- las medidas adoptadas por el responsable del tratamiento para abordar y mitigar las citadas consecuencias.
- También el nombre y los datos de contacto del delegado de protección de datos u otro punto de contacto, para que la Agencia Española de Protección de Datos pueda obtener más información si es preciso.

En el supuesto de que una brecha de seguridad conlleve un **alto riesgo** para los derechos y libertades de las personas físicas, los responsables del tratamiento deberán **comunicar**, sin dilaciones indebidas, la violación **a los interesados**.

La única **causa de exención** de la obligación de **notificación** de una brecha de seguridad es que el responsable del tratamiento pueda demostrar que no es probable que la violación de la seguridad de los datos ocasione un riesgo para los derechos y libertades de las personas afectadas.

# VI

# Recogida de datos en los Centros Educativos.

# VI. Recogida de datos en los Centros Educativos.

Para desarrollar con normalidad el trabajo de los centros docentes resulta necesario recabar datos de carácter personal toda vez que su **finalidad** es la de educar y orientar a los alumnos, misión para la que han de tratar sus datos de carácter personal, así como los de sus padres y tutores.

Este tratamiento se **inicia** desde el mismo momento en el que se solicita plaza en un centro, continúa con la matriculación del alumno y se mantiene durante toda su estancia académica, e incluso una vez que haya finalizado sus estudios mediante la conservación del expediente académico.

## ¿Qué **TIPOS DE DATOS** puede **RECABAR** un centro educativo?

La LOE[51] resuelve la cuestión en su disposición adicional 23ª al **legitimar** a los centros a recabar distintos datos de carácter personal que resultan necesarios para el correcto desempeño de la función docente y orientadora de los alumnos, en concreto:

- Datos relativos al origen y ambiente familiar y social.
- Las características o condiciones personales.
- El desarrollo y resultados de su escolarización.
- Las circunstancias cuyo conocimiento sea necesario para educar y orientar a los alumnos.

Es la Ley Orgánica de Educación la que expresamente legitima a los centros educativos para que puedan realizar operaciones de tratamiento de los datos de alumnos y, también, de sus padres o tutores, incluyendo también las categorías especiales de datos, como pueden ser los de salud o los de religión, cuando fuesen necesarios para el desempeño de la función docente u orientadora.

**IMPORTANTE**

Los centros educativos deberán tener ciertas **CAUTELAS**:

- Los datos personales no podrán usarse para fines diferentes al educativo (función docente y orientadora).
- El profesorado y resto del personal que acceda a los datos personales de los alumnos o sus familias está sometido al deber de guardar secreto.
- no podrán recabarse datos que sean excesivos para dicha finalidad.
- Por ejemplo, en el caso de las solicitudes de plaza en un centro no es necesario recabar los datos bancarios para el pago de actividades extraescolares hasta que no se hubiera resuelto el proceso y fuese admitido el alumno.

**51** Ley Orgánica 2/2006, 3 may. *de Educación* -LOE-. https://boe.es/buscar/pdf/2006/BOE-A-2006-7899-consolidado.pdf

### 1.- ¿Es posible recabar por el centro educativo datos sobre la situación familiar relativa a los padres de los alumnos?

**SÍ**, los centros educativos pueden recabar la información sobre la situación familiar de los alumnos. Esta información debe estar actualizada y los progenitores han de informar a los centros sobre cualquier modificación.

Si los padres del alumno están **separados o divorciados**, debe recabarse información sobre quién ostenta la **patria potestad**, si ambos o uno sólo, y quién ostenta la **guarda y custodia**.

También de quiénes son las **personas autorizadas** a recoger al alumno.

### 2.- ¿Es posible recabar datos de SALUD?

**SÍ** cuando resultan necesarios para el normal ejercicio de la función educativa o sean necesarios para la función docente u orientadora que desarrollan los centros escolares.

### 3.- ¿Cuándo se pueden recabar datos de SALUD?

Es posible distinguir dos momentos:

- **En el acto de matriculación del alumno**: donde se puede recabar información sobre discapacidad, enfermedad crónica, TDAH, intolerancias alimentarias, alergias u otros que resulten necesarios para el correcto ejercicio de la función educativa.
- **Durante el curso escolar**: relativo a tratamientos médicos que reciba un alumno a través del servicio médico o de enfermería del centro o los informes de centros sanitarios a los que se le haya trasladado como consecuencia de accidentes o indisposiciones sufridas en el centro o los informes de los equipos de orientación psicopedagógica.

PUNTOS CLAVE

- Los **datos médicos o de salud son datos sensibles** y, por tanto, gozan de una **protección específica**.
- El Reglamento general de protección de datos, entre otros, incluye en la categoría especial de datos a los «**datos personales relativos a la salud**» entendidos como «*todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro*».
- Se incluye como "*dato de salud*" la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del

interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

- Es preciso dar una **interpretación amplia de la expresión datos de salud**, de modo que comprende la información relativa a todos los aspectos tanto físicos como psíquicos de la salud de una persona, por lo que se considera que la indicación de que una persona se ha lesionado un pie y está en situación de baja parcial constituye un dato personal relativo a la salud (TJUE 6-11-03 asunto C-101/2001 *Lindqvist*).
- Son **categorías especiales** de datos personales los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

## 4.- ¿Se pueden recabar datos BIOMÉTRICOS?

Tienen la consideración de **datos biométricos** aquéllos datos que reúnen determinadas propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad[52]. Son ejemplos típicos de datos biométricos los que proporcionan:

- las huellas dactilares,
- los modelos retinales,
- la estructura facial,
- la voz,
- la geometría de la mano,
- las estructuras venosas,
- determinada habilidad profundamente arraigada u otra característica del comportamiento (como la caligrafía, las pulsaciones, una manera particular de caminar o de hablar, etc.).

No obstante, el **RGPD** considera **categoría especial únicamente** a los **datos biométricos** dirigidos a **identificar de manera unívoca a una persona física** y que define como aquéllos «*datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*»[53].

**52** Grupo de Trabajo del Artículo 29 -GT29- Dictamen 4/2007, sobre el concepto de datos de carácter personal.
**53** Reglamento general de protección de datos, artículo 4, apartado 14.

El GT29 indicó que los datos biométricos pueden ser considerados como:

- **Contenido de la información** sobre una determinada persona (María tiene estas huellas dactilares),
- Elemento para **vincular una información** a una determinada persona (este objeto lo ha tocado alguien que tiene estas huellas dactilares y estas huellas dactilares corresponden a María; por lo tanto María ha tocado este objeto).

Las muestras de tejido humano (al igual que las muestras de sangre) son fuentes a partir de las cuales se extraen datos biométricos, pero no son en sí mismas datos biométricos (como, por ejemplo, un modelo de huellas dactilares es un dato biométrico, pero no así un dedo). Por lo tanto, la extracción de información de las muestras supone la obtención de datos personales, a los que se aplican las normas de protección de datos.

Los **datos biométricos** cambian irrevocablemente la relación entre el cuerpo y la identidad, ya que **hacen** que las **características del cuerpo** humano sean **legibles** mediante máquinas y estén sujetas a un uso posterior.

La normativa de protección de datos exige que los datos que se recaben respondan al **principio de proporcionalidad** y sean adecuados, pertinentes y no excesivos. Se persigue que los datos recabados sean idóneos para la finalidad que se pretende conseguir con su recogida, que no haya otros medios menos intrusivos para ello y que de su tratamiento se deriven más beneficios para el interés general que perjuicios sobre otros bienes y valores.

Teniendo en cuenta la intromisión en la intimidad de las personas que el tratamiento de este tipo de datos puede ocasionar, la Agencia Española de Protección de Datos ha **admitido la utilización de la huella dactilar** para finalidades como el control de acceso al servicio de comedor en centros escolares con un gran número de alumnos, siempre que se adopten medidas que refuercen la confidencialidad de los datos como:

- la conversión de la huella a un algoritmo,
- el cifrado de la información,
- la vinculación a un dato distinto de la identificación directa del alumno (seudonimización), o
- la limitación de los protocolos de acceso a los datos.

## 5.- ¿Se pueden recabar imágenes (fotografías) de los alumnos para el expediente académico?

Sí, la fotografía o imagen es un dato personal que puede recabarse por los centros educativos para el ejercicio de la función docente y orientadora sin consentimiento de los alumnos, pudiendo la misma incluirse en el expediente para su identificación.

### 6.- ¿Se pueden recabar datos para finalidades distintas a la propiamente educativa?

Al margen de la función educativa, los centros pueden recabar datos para **otras finalidades legítimas**, por ejemplo:

- la gestión de la relación jurídica derivada de la matriculación de los alumnos,
- dar a conocer la oferta académica,
- participar con los alumnos en concursos educativos,
- ofrecer servicios deportivos, de ocio o culturales.

En estos casos, se podrán recabar bien como consecuencia de la relación jurídica establecida con la **matrícula** o también si media el **consentimiento previo y expreso** de los alumnos o de sus padres o tutores.

**NO** olvidar nunca que, con carácter previo a la obtención del consentimiento, se debe cumplir con el derecho de información de los titulares de los datos o a sus padres o tutores si son menores de 14 años.

## PROCEDIMIENTO de recogida de los datos por los centros educativos.

### 1.- ¿Es necesario informar cuando se recaban datos personales?

**SÍ.** Siempre debe informarse al interesado cuando se recaban datos de carácter personal, incluso si no resulta necesario obtener su consentimiento.

La información deberá facilitarse de forma **concisa, transparente, inteligible y de fácil acceso**, con un **lenguaje claro y sencillo**, en particular cualquier información dirigida específicamente a un niño[54].

**IMPORTANTE**

Aunque los Centros Educativos hemos visto que no necesitan el consentimiento para recabar u obtener algunos datos de carácter personal de los interesados, **SÍ** han de facilitarles la siguiente información:

- de la existencia de un tratamiento de datos personales,
- de la finalidad para la que se recaban los datos y su licitud, por ejemplo, para el ejercicio de la función educativa, o para difundir y dar a conocer las actividades del centro,
- de la obligatoriedad o no de facilitar los datos y de las consecuencias de negarse,
- de los destinatarios de los datos,
- de los derechos de los interesados y dónde ejercitarlos,
- de la identidad del responsable del tratamiento: el centro o la Administración educativa.

**54** RGPD. Reglamento general de protección de datos, artículo 12, apartado 1.

## 2.- ¿Deben los padres o tutores facilitar los datos al centro educativo?

La LOE[55] establece que los padres o tutores y los propios alumnos **deberán colaborar** en la obtención de la **información necesaria** sin la que no sería posible el **desarrollo de la función educativa**, estando los centros exceptuados de solicitar el consentimiento previo en relación a aquellos datos de carácter personal que sean necesarios para el buen fin de dicha finalidad (función educativa).

También deben facilitar los datos necesarios para el cumplimiento de la relación jurídica que se establece con la matrícula.

## 3.- ¿Cuándo y cómo recabar el CONSENTIMIENTO de alumnos y/o padres o tutores?

PUNTOS CLAVE

- El **consentimiento**, como base jurídica para **legitimar el tratamiento** de datos, se ha de **obtener** con carácter previo a la recogida de los datos y debe ser **otorgado** de manera libre, específica, informada e inequívoca por medio de una clara acción afirmativa que signifique aceptación del tratamiento, sin que pueda entenderse prestado de manera tácita.
- Para los **datos especialmente protegidos** que hagan referencia al origen racial, a la salud y a la vida sexual el consentimiento ha de ser expreso, y si los datos revelan ideología, afiliación sindical, religión o creencias se exige un consentimiento explícito, esto es, el consentimiento ha de prestarse por escrito.

**TRES** son los **elementos** para que el **consentimiento** sea **válido**, teniendo por objeto el garantizar que los interesados realmente accedieron a que sus datos fueran utilizados[56]:

- El consentimiento debe otorgarse por medio de un claro acto afirmativo con que el interesado efectúe una manifestación de voluntad libre, específica, informada e inequívoca de aceptación del tratamiento de sus datos personales. Este acto puede ser una acción o una declaración.
- El interesado debe tener derecho a retirar su consentimiento en cualquier momento.
- En el contexto de una declaración escrita que también comprenda otros conceptos, como «*condiciones de servicio*», las solicitudes de consentimiento deben realizarse en lenguaje claro y sencillo y con una formulación inteligible y de fácil acceso, que distinga claramente el consentimiento de otras cuestiones; si parte de esta declaración viola el RGPD no será vinculante.

El consentimiento solo será válido en el contexto de la legislación sobre protección de datos si se cumplen todos estos requisitos. **Corresponde al responsable** del tratamiento **demostrar que el interesado ha consentido** el tratamiento de sus datos[57].

**55** Ley Orgánica 2/2006, 3 may. *de Educación* -LOE-. https://boe.es/buscar/pdf/2006/BOE-A-2006-7899-consolidado.pdf
**56** RGPD. Reglamento general de protección de datos, artículo 7.
**57** RGPD. Reglamento general de protección de datos, artículo 7, apartado 1º.

Resulta suficiente con que el consentimiento se obtenga una sola vez, siempre que el tratamiento de los datos responda a la información que al respecto se haya facilitado.

La edad mínima para que un **menor pueda consentir** por sí solo sin necesidad de que conste el consentimiento del titular de la patria potestad o tutela son los **14 años** (LOPD art.7).

El consentimiento se puede recabar en el mismo impreso de recogida de los datos.

Bastaría con que el consentimiento se preste al comienzo de cada curso, sin que sea necesario recabarlo nuevamente en cada actividad de tratamiento siempre que responda a la misma finalidad, por ejemplo, para los eventos que organice el centro.

### 4.- ¿Qué datos se consideran EXCESIVOS y el centro educativo NO DEBERÁ solicitarlos de los padres para tramitar la matriculación de los futuros alumnos?

La Agencia Española de Protección de Datos en su *Plan Sectorial de Oficio a la Enseñanza Reglada no universitaria*[58] destacó como **"excesivos"** el hecho de recabar los siguientes datos sobre los padres o tutores:


- Confesión religiosa.
- Estudios.
- Profesión.
- Empresa donde trabajan.
- Fecha de nacimiento.
- Y, en relación a los hermanos, se consideró también excesivo el recabar los datos personales de los hermanos que no estudian en el mismo centro.

### 5.- ¿Qué datos se consideran adecuados y el centro educativo podrá solicitarlos de los padres para tramitar la matriculación de los futuros alumnos?

Se han considerado **adecuados**, entre otros, los siguientes:

- Identificativos básicos del alumno y de los padres o tutores,
- el domicilio familiar,
- la existencia de hermanos en el mismo centro,
- el título de familia numerosa,
- el importe de la renta de la unidad familiar - para centros públicos o concertados en relación a la matriculación en cursos sujetos al concierto-,
- situaciones de discapacidad física, psíquica o sensorial de alguno de los miembros de la unidad familiar,
- enfermedad crónica del alumno, o
- información relativa a necesidades educativas especiales que este pueda tener.

**58** Agencia Española de Protección de Datos -AEPD-, Plan Sectorial de Oficio a la Enseñanza Reglada no universitaria. Madrid, 2006, página 54.

### 6.- ¿Pueden los profesores recoger datos personales directamente de los alumnos?

Hemos visto como los centros o las Administraciones educativas recaban datos personales al matricularse los alumnos, y que éstos serán facilitados a los profesores para el ejercicio de la función docente.

Ahora bien, cuando los profesores recaben otros datos de carácter personal, como grabaciones de imágenes o sonido con la **finalidad** de evaluar sus conocimientos u otros datos relacionados con la realización de dichos ejercicios, o los resultados de su evaluación, estarían **legitimados** para hacerlo, en el marco de las instrucciones, protocolos o régimen interno que el centro o la Administración educativa haya adoptado.

### 7.- ¿Pueden los profesores solicitar datos de los padres o tutores de los alumnos?

Los datos de los padres de los alumnos se recaban por los centros al estar legitimados para ello por la LOE[59], a cuya información podrán tener acceso los profesores si la necesitasen para el ejercicio de la docencia.

No obstante, si se diera alguna **circunstancia** en la que los profesores necesitaran conocer los datos de los padres de los alumnos, como podría ser ante situaciones de riesgo, y no dispusieran de ellos, estarían igualmente habilitados para recabarlos de los alumnos.

### 8.- ¿Puede un profesor acceder a los expedientes de los alumnos?

Un profesor tendrá legitimidad para acceder a los expedientes educativos de **SUS propios alumnos**, siempre que dicho acceso tenga una **finalidad académica** y, por tanto, compatible con las finalidades para las que se recabaron los datos.

No obstante, debe destacarse que el acceso de los profesores al expediente de los alumnos no puede ser indiscriminado, sino que cada profesor debe tener acceso solamente a los datos de sus propios alumnos, pues **NO estaría justificada la finalidad del acceso a los datos del resto de los alumnos**.

Por último, y en atención al **principio de minimización**, un profesor sólo debería tener acceso a aquellos datos que resulten necesarios para poder desarrollar correctamente su función docente.

### 9.- ¿Puede un centro educativo acceder al contenido de dispositivos electrónicos de los alumnos, como los sistemas de mensajería instantánea (WhatsApp) o redes sociales?

Dada la información que se contiene en los dispositivos con acceso a internet, así como la trazabilidad que se puede realizar de la navegación efectuada por los usuarios, el acceso al contenido de estos dispositivos de los alumnos, incluyendo su clave, supone un acceso a datos de carácter personal que requiere el consentimiento de los interesados o de sus padres o tutores si se trata de menores de 14 años.

**59** Ley Orgánica 2/2006, 3 may. *de Educación* -LOE-. https://boe.es/buscar/pdf/2006/BOE-A-2006-7899-consolidado.pdf

No obstante, la Guía de la AEPD[60] resalta que en situaciones en las que pudiera estar presente el **interés público**, como cuando se ponga en **riesgo la integridad de algún alumno** (situaciones de ciberacoso, sexting, grooming o de violencia de género) el centro educativo podría, previa ponderación del caso y conforme al protocolo que tenga establecido, acceder a dichos contenidos sin el consentimiento de los interesados. En caso de duda, aconsejamos evacuar consulta urgente al Delegado de Protección de Datos.

## 10.- ¿Pueden los profesores crear grupos con aplicaciones de mensajería instantánea con los alumnos?

Con **carácter general**, las comunicaciones entre los profesores y los alumnos deben tener lugar dentro del ámbito de la función educativa y NO llevarse a cabo a través de aplicaciones de mensajería instantánea.

Si fuera preciso establecer canales específicos de comunicación, deberían emplearse los medios y herramientas establecidas por el centro educativo y puestas a disposición de alumnos y profesores (por ejemplo, áreas específicas en la intranet del centro o uso de plataformas que cumplan los requisitos que se verán más adelante) o por medio del correo electrónico.

En situaciones concretas, como la realización de una tarea o trabajo específico, por ejemplo con motivo de la participación en un concurso escolar, o de refuerzo que fueran necesarias, se podrían crear con **carácter excepcional**, siendo aconsejable la participación en el grupo de un tercero, padre o madre de los alumnos.

## 11.- ¿Pueden los profesores crear grupos con aplicaciones de mensajería instantánea para que sean miembros los padres de los alumnos de su clase?

Al igual que en supuesto anterior, debe destacarse que las comunicaciones entre los profesores y los padres de los alumnos **deben llevarse a cabo** a través de los medios puestos a disposición de ambos por el centro educativo.

**Excepcionalmente**, y siempre que se contase con el **consentimiento** de los padres, sería posible la creación de estos grupos, de los que sólo formarían parte los padres que hubieran consentido a ello. No obstante, la Agencia Española de Protección de Datos destaca que **sería preferible** que los grupos fueran gestionados por los propios padres (por ejemplo, a través de un delegado) y la incorporación al grupo no dependiera directamente de los profesores[61].

Para el **excepcional caso** de que sean los propios padres quienes soliciten la creación de un grupo con los profesores dadas las especiales circunstancias del alumno (por ejemplo, requerir necesidades especiales o como consecuencia de su estado de salud), sería posible la creación del grupo, si bien sería igualmente aconsejable que su administración corriera a cargo de los propios padres y no de los profesores.

**60** Agencia Española de Protección de Datos -AEPD-, Guía Sectorial para centros educativos. Página 25.
**61** Agencia Española de Protección de Datos -AEPD-, Guía Sectorial para centros educativos. Página 25.

## 12.- ¿Pueden los profesores grabar imágenes de los alumnos y difundirlas a través de aplicaciones de mensajería instantánea a los padres?

En el supuesto del ejercicio de la función educativa de la que es responsable el centro docente **NO** sería posible.

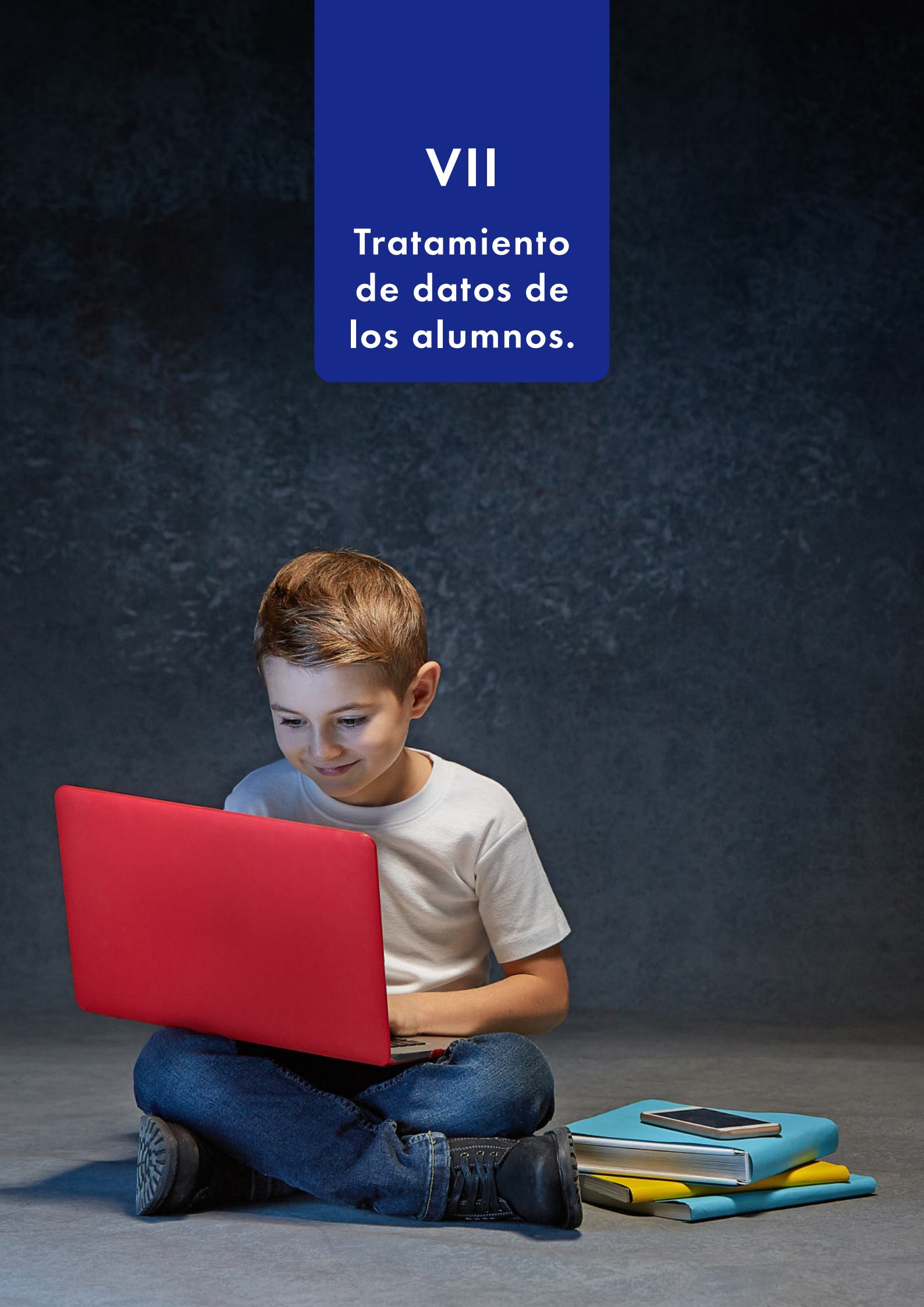
**Excepcionalmente**, con la debida ponderación y en aquellos casos en los que el interés superior del menor estuviera comprometido, como en caso de accidentes o indisposiciones en una excursión escolar, y con la finalidad de informar y tranquilizar a los padres, titulares de la patria potestad, se podrían captar las imágenes y enviárselas.

También podría ser posible en los grupos generados a través de aplicaciones de mensajería instantánea relacionados con la específica situación del alumno, a los que se ha hecho referencia en la pregunta anterior.


**Colegio Concertado**
***Ruta de la Plata***
***Almendralejo.***

# VII

# Tratamiento de datos de los alumnos.



# VII. Tratamiento de datos de los alumnos.

## **PUBLICACIÓN** de datos por centros educativos.

En el ejercicio de la función docente y orientadora que tienen asignados los centros educativos resulta necesario dar publicidad a diversa información personal derivada de diversas acciones o actividades para las que les legitima la Ley, vamos a desarrollar distintas cuestiones que resultan trascendentes al respecto.

### 1.- ¿Puede un centro dar PUBLICIDAD a las listas de alumnos admitidos?

**SÍ**. El proceso de admisión a los centros educativos se realiza mediante un procedimiento público de concurrencia competitiva lográndose la plaza mediante la baremación de distintas circunstancias que son valorados y puntuadas conforme a la normativa de la convocatoria, por tal motivo, los centros educativos resultan **obligados a informar** sobre los alumnos que han resultado admitidos.

Pero el hecho de que se deba dar publicidad a la lista de los alumnos admitidos no significa que ésta deba ser de acceso universal e indiscriminado, así, la Agencia Española de Protección de Datos **recomienda** que la publicación de las listas se realice únicamente en los tablones de anuncios existentes en el interior del centro y/o en una página web de acceso restringido a las personas interesadas que hayan solicitado la admisión[62].

La publicación de la lista de alumnos será respetuosa con la normativa de protección de datos si únicamente recoge el **resultado final del baremo**, debe **evitarse ofrecer resultados parciales** que puedan responder a datos o información sensible o poner de manifiesto la capacidad económica de la familia, información ésta última que únicamente debe estar disponible para los interesados que ejerciten su derecho a reclamar.

Transcurrido un plazo prudencial o cuando ya no sean necesarios estos listados, hay que retirarlos de los tablones o dejar sin efecto al website de acceso restringido, lo anterior sin perjuicio de su conservación por el centro a fin de atender las reclamaciones que pudieran plantearse.

### 2.- En caso de situaciones de VIOLENCIA DE GÉNERO, ¿se puede oponer una madre, tutor o alumno a la publicación de su admisión en los listados de un centro educativo?

**SÍ**. La Ley Orgánica 1/2004, de 28 de diciembre, *de Medidas de Protección Integral contra la Violencia de Género*; regula las **limitaciones a la publicidad** en su art. 63.1 al disponer que «*[e]n las actuaciones y procedimientos relacionados con la violencia de género se protegerá la intimidad de las víctimas; en especial, sus datos personales, los de sus descendientes y los de cualquier otra persona que esté bajo su guarda o custodia*.»

**62** Agencia Española de Protección de Datos -AEPD-, Guía Sectorial para centros educativos. Página 27.

Por tanto, los centros educativos deberán proceder con **especial cautela** a tratar los datos de los menores que se vean afectados por estas situaciones.

Resulta de interés como el RGPD[63] ampara a que un **alumno se pueda oponer** a la publicación de su admisión en un centro educativo si se alegan motivos fundamentados y legítimos relativos a su concreta situación personal, como, por ejemplo, así lo son las razones de seguridad que le amparan por ser víctima de violencia de género o sufrir algún tipo de amenaza, etc. Si el alumno es un menor de 14 años, el derecho lo tiene que ejercer su madre o tutor legal. **El centro educativo lo tiene que excluir del listado de admitidos que se publique**.

### 3.- ¿Pueden los centros hacer públicas las relaciones de los BENEFICIARIOS de becas, subvenciones y otras ayudas públicas?

**SÍ**. La Ley 19/2013, de 9 de diciembre, *de transparencia, acceso a la información pública y buen gobierno*; dentro de la publicidad activa, destaca en su artículo 8.1.c) que «... *[d]eberán hacer pública, como mínimo, la información relativa a los actos de gestión administrativa con repercusión económica o presupuestaria que se indican a continuación: c) Las subvenciones y ayudas públicas concedidas con indicación de su importe, objetivo o finalidad y beneficiarios*».

Sin perjuicio de la publicación por parte de la Administración convocante de la beca, subvención y otras ayudas públicas; los **centros escolares** también **podrán publicar esta información** a efectos informativos de los afectados.

Si para la concesión de la beca, subvención o ayuda pública fueran varios los requisitos a valorar, se podría dar el resultado total y no parcial de cada uno de los requisitos.

En los supuestos donde los criterios de las ayudas no se basen en circunstancias que impliquen el conocimiento de categorías especiales de datos debe valorarse por el centro si dicha publicación pudiere afectar a la esfera íntima de la persona, por ejemplo, al ponerse de manifiesto su capacidad económica o su situación de riesgo de exclusión social. Ante esta situación debería analizarse caso por caso si resulta necesario hacer pública dicha información para garantizar la transparencia de la actividad relacionada con el funcionamiento y control de la actuación pública.

### 4.- ¿Cuál es la FORMA CORRECTA de PUBLICAR las RELACIONES de los BENEFICIARIOS de becas, subvenciones y otras ayudas públicas?

Cuando sea necesaria la **publicación de un acto administrativo** que contuviese **datos personales del afectado**, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

**63** RGPD. Reglamento general de protección de datos, artículo 18, apartado 1º, letra d); en relación al artículo 21, apartado 1º de la misma norma.

i) Así, dado un **DNI** con formato 12345678X, se publicarán los dígitos que en el formato que ocupen las posiciones cuarta, quinta, sexta y séptima. En el ejemplo: ***4567**.

**Rosa Gil Rodríguez; DNI ***4567** | Expediente Nº XXX/2020 | Importe xxx €**

ii) Dado un **NIE** con formato L1234567X, se publicarán los dígitos que en el formato ocupen las posiciones, evitando el primer carácter alfabético, cuarta, quinta, sexta y séptima. En el ejemplo: ****4567*.

**Jon Yiba Gitg; NIE ***4567* | Expediente Nº XXX/2020 | Importe xxx €**

iii) Dado un **Pasaporte** con formato ABC123456, al tener sólo seis cifras, se publicarán los dígitos que en el formato ocupen las posiciones, evitando los tres caracteres alfabéticos, tercera, cuarta, quinta y sexta. En el ejemplo: ***3456.

**Grace Katie Brown; Pasaporte ***3456 | Expediente Nº XXX/2020 | Importe xxx €**

iv) Dado **otro tipo de identificación**, siempre que esa identificación contenga al menos 5 dígitos numéricos, se numerarán dichos dígitos de izquierda a derecha, evitando todos los caracteres alfabéticos, y se seguirá el procedimiento de publicar aquellos caracteres numéricos que ocupen las posiciones cuarta, quinta, sexta y séptima.

Si ese tipo de identificación es distinto de un pasaporte y tiene menos de 7 dígitos numéricos, se numerarán todos los caracteres, alfabéticos incluidos, con el mismo procedimiento anterior y se seleccionarán aquellos que ocupen las posiciones cuarta, quinta, sexta y séptima.

## 5.- ¿Cuál es la FORMA CORRECTA de PUBLICAR las RELACIONES de los BENEFICIARIOS de becas, subvenciones y otras ayudas públicas si debe realizarse en la forma prevista en el artículo 44 LPACAP?

Cuando se trate de la **notificación por medio de anuncios**, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

i) Si el alumno tiene DNI, se publica así:

**DNI nº 12345678X | Expediente Nº XXX/2020 | Importe xxx €**

ii) Si el alumno tiene NIE, se publica así:

**NIE nº L1234567X | Expediente Nº XXX/2020 | Importe xxx €**

iii) Si el alumno tiene PASAPORTE, se publica así:

**Pasaporte nº ABC123456 | Expediente Nº XXX/2020 | Importe xxx €**

### 6.- ¿Pueden los centros colocar en los tablones de anuncios o a las puertas de las aulas la RELACIÓN DE ALUMNOS por clases y/o actividades?

Para la organización de la actividad docente los centros distribuyen al inicio de cada curso a los alumnos por clases, materias, actividades y servicios.

Para dar a conocer a los alumnos y a sus padres o tutores esta distribución, **se pueden colocar** dichas relaciones en los tablones de anuncios o en las entradas de las aulas, durante **un tiempo razonable** para permitir el conocimiento por todos los interesados.

Si el centro educativo utiliza una **plataforma para la gestión educativa**, se recomienda que cada alumno, sus padres o tutores **accedan** a dicha información mediante el uso de una identificación de **usuario y contraseña**.

### 7.- ¿Se puede PUBLICAR en el comedor del centro el MENÚ DE LOS ALUMNOS?

En el comedor de los centros educativos se pueden publicar los diferentes menús, ya que pueden existir alumnos con necesidades alimentarias especiales, ya sea por razones de salud o religión, pero **NO** se **considera proporcionado ni necesario** que exista un **listado con nombre y apellidos de los alumnos asociándolo al menú** que le corresponde a cada uno de ellos.

Cuestión distinta es que el centro sí disponga de estos listados destinados de forma exclusiva para su uso por el personal del servicio de comedor, pero dichos trabajadores no podrán darles publicidad.

### 8.- ¿Pueden los PROFESORES EN PRÁCTICAS utilizar datos personales de los alumnos para trabajos propios universitarios?

En la medida que no se estarían tratando los datos para la educación de los alumnos, sino para otra finalidad como la formación de los profesores, resulta aconsejable que procedan a anonimizar (disociar) los datos de manera que no se puedan identificar a los alumnos. Si no, tendrán que contar con el consentimiento de los alumnos que sean mayores de 14 años, o, para el supuesto de alumnos menores de 14 años deberán contar con el consentimiento de sus padres o tutores.

## **CALIFICACIONES** de los alumnos.

La función educativa implica la evaluación continuada de los alumnos, calificarlos y comunicarles las notas obtenidas. La publicidad de esta comunicación, a diferencia de la educación universitaria, no está regulada, por lo que se suelen albergar dudas sobre cómo proceder.

### 1.- ¿Se pueden hacer PÚBLICAS las calificaciones escolares?

Lo **recomendable** es que las calificaciones de los alumnos sean facilitadas a los propios alumnos y/o a sus padres o tutores.

En el caso de comunicar las calificaciones a través de **plataformas educativas**, éstas sólo deberán estar accesibles para los propios alumnos, sus padres o tutores, sin que puedan tener acceso a las mismas personas distintas.

No obstante, **SÍ** sería posible comunicar la situación del alumno en el entorno de su clase, por ejemplo, mostrando su calificación frente a la media de sus compañeros.

### 2.- ¿Pueden los profesores facilitar las calificaciones ORALMENTE en clase?

Tal y como hemos explicado anteriormente, no existe una regulación respecto de la forma de comunicar las calificaciones. Aunque sería preferible que las calificaciones se notificasen a los propios alumnos y/o a sus padres o mediante plataforma educativa, no existiría inconveniente en enunciar las calificaciones oralmente, evitando comentarios adicionales que pudieran afectar personalmente al alumno.

### 3.- ¿Pueden los PADRES solicitar las calificaciones de sus hijos mayores de edad?

Si los alumnos fueran mayores de edad (18 años) sus padres podrán solicitar el acceso a las calificaciones cuando éstos fueran los que **corrieran con los gastos educativos o de alimentos**, pues en ese caso existiría un interés legítimo de los padres, derivado del mantenimiento de sus hijos mayores de edad, en conocer su evolución académica sobre el que no prevalecerían los derechos y libertades de éstos.

## **ACCESO** a la información de los alumnos.

Los centros educativos disponen de datos de los alumnos de muy diversa naturaleza: identificativos, académicos, familiares, económicos, sociales, de salud, a los que han de acceder sólo las personas que lo necesiten para ejercer la función que tengan encomendada, ya sean del equipo directivo, del claustro de profesores o tutores, profesores, personal de administración o de servicios.

### 1.- ¿Pueden los profesores acceder a los expedientes académicos de los alumnos matriculados en el centro?

Con carácter general y salvo que existiese alguna causa debidamente justificada, el profesor ha de tener acceso al expediente académico de los alumnos a los que imparte la docencia, sin que esté justificado acceder a los expedientes de los demás alumnos del centro.

### 2.- ¿Y acceder también a la información de salud de los alumnos?

Los profesores han de conocer y, por tanto, acceder a la información de salud de sus alumnos que sea necesaria para la impartición de la docencia, o para garantizar el adecuado cuidado del alumno, por ejemplo, respecto a discapacidades auditivas, físicas o psíquicas, trastornos de atención, TDAH o enfermedades crónicas.

Igualmente, han de conocer la información relativa a las alergias, intolerancias alimentarias o la medicación que pudieran requerir para poder prestar el adecuado cuidado al alumno tanto en el propio centro como con ocasión de actividades fuera del centro, como visitas, excursiones o convivencias guiadas por profesores.

## 3.- ¿Pueden los padres solicitar los exámenes de sus hijos para llevárselos a casa y repasarlos?

La normativa de protección de datos no regula esta cuestión toda vez que no se trata de un derecho de acceso a los datos de carácter personal, sino de acceso a una documentación (examen) que, en su caso, deberá ser resuelta por el centro o la Administración educativa correspondiente con arreglo a su normativa interna y demás legislación sectorial que sea de aplicación.

**Educación Primaria:**

Orden de la Consejería de Educación y Cultura de la Junta de Extremadura, de 6 de agosto de 2014, *por la que se regula la evaluación del alumnado en la Educación Primaria* [DOE nº 156, 13 agosto 2014].

Artículo 17. Información y participación de las familias.

"3. (...) ... *[P]adres, madres y tutores legales tendrán acceso a los documentos oficiales de evaluación y a los exámenes y documentos de las evaluaciones que se realicen a sus hijos o tutelados, que deberán consultar necesariamente en el interior del centro educativo*."

**Educación Secundaria:**

Orden de la Consejería de Educación y Cultura de la Junta de Extremadura, de 26 de noviembre de 2017, *por la que se regula la evaluación del alumnado en la Educación Secundaria Obligatoria* [DOE nº 139, 1 diciembre 2007].

Artículo 17. Información al alumnado y a las familias.

"4. *[L]os tutores y los profesores de las distintas materias mantendrán una comunicación fluida con los alumnos y sus tutores legales en lo relativo a la valoración del proceso de aprendizaje de los alumnos con el fin de favorecerlo.*

*Por su parte, el alumnado podrá solicitar información al profesorado de las distintas materias acerca de la evaluación de su proceso de aprendizaje. Los padres o tutores legales podrán solicitar, asimismo, información sobre el citado proceso a través del tutor.*

5. *Los alumnos, o sus representantes legales, podrán formular reclamaciones sobre las calificaciones obtenidas de acuerdo con lo que establece la normativa vigente al respecto.*"

**Bachillerato:**

Orden de la Consejería de Educación de la Junta de Extremadura, de 15 de abril de 2009 *por la que se regula la evaluación del alumnado en el Bachillerato* [DOE nº 79, 27 de abril de 2009].

Artículo 17. Información al alumnado y a las familias.

"5. *Los tutores y los profesores de las distintas materias mantendrán una comunicación fluida con el alumnado y sus familias en lo relativo a la valoración del proceso de aprendizaje de los alumnos con el fin de favorecerlo.*

6. *El alumnado o sus representantes legales podrán solicitar información al profesorado de las distintas materias acerca de la evaluación de su proceso de aprendizaje. Los centros establecerán procedimientos que faciliten la comunicación directa entre los profesores y los padres o representantes legales de los alumnos.*

7. *Los alumnos, o sus representantes legales, podrán formular reclamaciones sobre las calificaciones obtenidas de acuerdo con lo que establece la normativa vigente al respecto.*"

## 4.- ¿Pueden los padres o tutores acceder a la información sobre las AUSENCIAS ESCOLARES de sus hijos?

**SÍ**, dado que ostentan la patria potestad y ésta les impone la obligación de educarlos y procurarles una formación integral, los padres tienen acceso a la información sobre el absentismo escolar de sus hijos.

Los centros educativos pueden facilitar la información de ausencias escolares a través de un mensaje enviado al número de móvil que los padres o tutores hayan facilitado.

## 5.- ¿Y qué ocurre en el supuesto de que los hijos sean MAYORES DE EDAD?

Al igual que ocurre con las calificaciones escolares, los padres podrán ser informados del absentismo escolar de sus hijos mayores de edad cuando corrieran con sus gastos educativos o de alimentación, al existir un interés legítimo derivado de su mantenimiento y manutención.

## 6.- ¿Pueden los padres solicitar a los EQUIPOS DE ORIENTACIÓN ESCOLAR información sobre la salud de sus hijos?

**SÍ**, cuando son los hijos son menores de edad (18 años) y se formula la solicitud en ejercicio de la patria potestad que se realiza siempre en su beneficio y les impone el deber de educarlos y procurarles una formación integral.

El acceso a dicha información se rige por la legislación sectorial sanitaria, en concreto por la Ley 41/2002, de 14 de noviembre, *básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica*; o para el caso de la Comunidad Autónoma de Extremadura por la Ley 3/2005, de 8 de julio, *de información sanitaria y autonomía del paciente*.

## 7.- ¿Se puede facilitar la información escolar de los alumnos a sus FAMILIARES?

La información escolar de los alumnos únicamente puede facilitarse a los padres que ostente la patria potestad o a los tutores, **nunca se facilitará a otros familiares**, salvo que estuvieren expresamente autorizados por ellos y constase de forma clara dicha autorización.

## 8.- Acceso a la información académica en supuestos de separación o divorcio.

Debemos distinguir entre patria potestad y guarda y custodia, así, aunque se produzca una separación o divorcio lo normal es que la patria potestad sea compartida, con independencia de a quién se asigne la custodia.

Por tanto, en condiciones de normalidad, **el padre y la madre tienen derecho a recibir la misma información** sobre las circunstancias que concurran en el proceso educativo del menor, lo que obliga a los centros a garantizar la duplicidad de la información relativa al proceso educativo de sus hijos, salvo que se aporte una certificación de resolución judicial que establezca la privación de la patria potestad a alguno de los progenitores o algún tipo de medida penal de prohibición de comunicación con el menor o su familia.

En caso de **conflicto entre los progenitores** sobre el acceso a la información académica de sus hijos, **deberán plantearlo ante el juez** competente en materia de familia.

Sentencia Ejemplo

Asunto: ***Civil: familia y relaciones familiares***.

Audiencia Provincial de Guipuzcoa, Sección 3ª - **APGui**.

Sentencia de 24 de junio de 2010. Fuente Memento Familia EFL - nº 4267

En cuanto al **requerimiento al centro escolar**, a fin de tener acceso a la documentación y evolución de los menores, se realiza de conformidad con la propia naturaleza de la patria potestad como derecho-deber configurado para el desarrollo integral de los menores, entre el que la educación supone uno de los elementos primordiales. En consecuencia, **se reconoce** la **posibilidad de los progenitores** de intervenir en ese ámbito esencial de la formación de los menores.

## **COMUNICACIONES** de los datos de los alumnos.

La **comunicación** de los datos personales de los alumnos a **personas distintas de los interesados** constituye una situación que no es inusual en la práctica de los centros docentes. Por tanto, siempre hay que ver **a quién** y **con qué legitimación** se pueden comunicar los datos de carácter personal de cuyo tratamiento es responsable el centro docente o la Administración educativa.

Los centros educativos reciben peticiones de otros centros, instituciones y organismos de otras administraciones e incluso de entidades privadas para que se les facilite información personal de los alumnos, a título ejemplificativo de los Servicios Sociales de Atención Social Básica (SSASB)[64], de las Fuerzas y Cuerpos de Seguridad[65] o de la Administración sanitaria, quienes serían destinatarios[66] de los datos.

**IMPORTANTE**

El RGPD define «**destinatario**» como *la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante,* ***no*** *se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.*

La comunicación de datos **requiere**, con carácter general, el **consentimiento** de los interesados, de los alumnos o de sus padres o tutores si son menores de 14 años, salvo que la **comunicación esté legitimada por otras circunstancias**, como que permita u obligue a ella una Ley (p.ej, solucionar una urgencia médica), o se produzca en el marco de una relación jurídica aceptada libremente por ambas partes (p.ej, la establecida entre los padres y el centro al matricular a sus hijos). En estos supuestos se pueden comunicar los datos sin necesidad de obtener el consentimiento de los afectados.

En la fase de admisión de alumnos, la LOE[67] permite a las Administraciones educativas solicitar la **colaboración** de otras instancias administrativas para garantizar la autenticidad de los datos que los interesados y los centros aporten en el proceso de admisión del alumnado.

### 1.- ¿ Se pueden facilitar los datos de los alumnos a OTROS CENTROS educativos?

En caso de traslado, la LOE ampara la comunicación de datos al nuevo centro educativo en el que se matricule el alumno sin necesidad de recabar su consentimiento o el de sus padres o tutores.

**64** Ley 14/2015, de 9 de abril, de Servicios Sociales de Extremadura, artículo 16.
**65** Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, artículos 2, 11 y 53.
**66** RGPD - Reglamento General de Protección de Datos, artículo 4, apartado 9º.
**67** LOE- Ley Orgánica de Educación, artículo 84, apartado 4º.

## 2.- ¿Y a CENTROS EDUCATIVOS SITUADOS EN OTROS PAÍSES para intercambios de alumnos o estancias temporales?

**SÍ**, dado que el acceso a los datos del alumno sería necesario para que el centro en el que se vaya a desarrollar el intercambio pueda realizar adecuadamente su función educativa, teniendo en cuenta que la participación del alumno en el programa deberá haber contado con la solicitud o autorización de los titulares de la patria potestad. En este concreto caso la comunicación de los datos responderá al adecuado desarrollo de la relación jurídica solicitada por los propios representantes legales del alumno.

La transmisión deberá **limitarse** a los datos que resulten necesarios para el adecuado desarrollo de esa acción educativa y para el cuidado del menor que el centro de destino pudiera requerir.

Cuando el centro destinatario de los datos se encuentre en un país fuera del Espacio Económico Europeo, la comunicación constituye una transferencia internacional de datos.

## 3.- ¿Y a la ADMINISTRACIÓN EDUCATIVA?

**SÍ**, los centros educativos, públicos, concertados y privados, comunicarán los datos personales de los alumnos necesarios para el ejercicio de las competencias que tienen atribuidas las Administraciones educativas como, por ejemplo, la expedición de títulos.

Debemos destacar la reciente modificación del artículo 155 de la Ley 40/2015, 1 oct., *del Régimen Jurídico del Sector Público*; operada por el Real Decreto-ley 14/2019, de 31 de oct., quedando el mismo del siguiente tenor:

Artículo 155. Transmisiones de datos entre Administraciones Públicas.

*"1. De conformidad con lo dispuesto en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo,* ***cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder****, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad.*

*2.* ***En ningún caso podrá procederse a un tratamiento ulterior de los datos para fines incompatibles con el fin para el cual se recogieron inicialmente los datos personales****. De acuerdo con lo previsto en el artículo 5.1.b) del RGPD*[68]*, no se considerará incompatible con los fines iniciales el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos."*

**68** RGPD - Reglamento General de Protección de Datos, artículo 5, apartado 1º, letra d): Los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»).

### 4.- ¿Se pueden comunicar los datos a las FUERZAS Y CUERPOS de Seguridad?

Las comunicaciones de datos a las Fuerzas y Cuerpos de Seguridad son obligatorias siempre que sean necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

En todo caso, la petición que realicen las Fuerzas y Cuerpos de Seguridad, en el ejercicio de sus competencias, debe ser concreta, específica y motivada, de manera que no haya una comunicación de datos indiscriminada.

Aunque se cumplan los requisitos para la comunicación de datos a las Fuerzas y Cuerpos de Seguridad, es aconsejable que el centro documente la comunicación de los datos.

### 5.- ¿Se pueden comunicar a los SERVICIOS SOCIALES de Atención Social Básica?

**SÍ**, siempre que se justifique para la determinación o tratamiento de situaciones de riesgo o desamparo competencia de los Servicios Sociales de Atención Social Básica. La comunicación estaría amparada en el interés superior del menor, recogido en la Ley Orgánica de Protección Jurídica del Menor. En estos supuestos no se necesita el consentimiento de los interesados.

### 6.- ¿En qué supuestos están los centros educativos obligados a comunicar datos de sus alumnos a las AUTORIDADES O SUS AGENTES?

Se debe comunicar a la Autoridad o a sus agentes ante situaciones en las que se tenga conocimiento de una posible situación de desprotección de un menor:

- de maltrato,
- de riesgo, o
- de posible desamparo.

También cuando se tenga conocimiento de la falta de asistencia de un menor al centro de forma habitual y sin justificación, durante el periodo lectivo, deberá trasladarse a la autoridad competente.

En estos casos no ha de mediar solicitud de ninguna autoridad o institución, *debe aquí tenerse presente que en el ámbito del Derecho de Menores existe implícita una* ***obligación de colaboración interinstitucional*** *que se impone a los entes, órganos e instituciones públicas y privadas, a fin de* ***proporcionar a los menores en riesgo, desamparo o conflicto social una atención coherente y organizada*** *que, además de facilitar la detección de situaciones de desprotección, permita intervenciones eficaces*[69].

**69** Fiscalía General del Estado. Instrucción 3/2008, de 30 de julio, sobre el Fiscal de Sala Coordinador de Menores y las Secciones de Menores de las Fiscalías. Apartado III, subapartado III.1.

### 7.- ¿Se pueden comunicar los datos a los CENTROS SANITARIOS?

**SÍ**, se pueden facilitar los datos sin consentimiento de los interesados a los centros sanitarios cuando el **motivo** sea la prevención o el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que se realicen por **profesionales sanitarios** sujetos al secreto profesional o por otras personas sujetas a la misma obligación.

Por ejemplo, cuando sea precisa la asistencia sanitaria a un alumno que se haya accidentado, indispuesto o intoxicado con la alimentación.

### 8.- ¿Y el CENTRO EDUCATIVO PODRÁ SOLICITAR INFORMACIÓN sobre la asistencia sanitaria prestada?

**SÍ**, en caso de que fuera necesaria para abonar al centro educativo la asistencia sanitaria en los supuestos en los que la misma se encontrase cubierta por el seguro de responsabilidad civil que hubiera suscrito el centro para responder de las lesiones causadas como consecuencia del normal desarrollo de la actividad escolar.

### 9.- ¿Se pueden COMUNICAR los datos a los SERVICIOS SANITARIOS autonómicos, o a un AYUNTAMIENTO para campañas de vacunación o programas de salud escolar (bucodental, alimentaria, etc.)?

En los casos planteados en la pregunta los centros suelen actuar como **intermediarios** entre los servicios de salud y las familias, por lo que habrán de trasladar a las familias la información de la cual dispongan para que sean ellas las que presten el consentimiento o faciliten los datos a dichos servicios.

No obstante, se pueden facilitar los datos de los alumnos a los servicios de salud que los requieran sin necesidad de disponer del consentimiento de los interesados en respuesta a una petición de las autoridades sanitarias cuando sean estrictamente necesarios para garantizar la salud pública o si tiene por finalidad la realización de actuaciones de salud pública que tengan encomendadas.

**Ejemplo**:

Procedería la **comunicación** de los datos ante un caso de infección en un centro educativo, para la realización de estudios sanitarios que permitan descartar la presencia de la enfermedad en el entorno del centro educativo.

### 10.- ¿Se pueden COMUNICAR los datos a instituciones, entidades o empresas que van a ser visitadas por los alumnos en una actividad extraescolar, por ejemplo, una exposición, un museo, una fábrica o un club deportivo?

Es posible siempre que se cuente con el **consentimiento previo e inequívoco** de los interesados o de sus padres o tutores, cuando los datos sean comunicados para las finalidades propias del teatro, museo, exposición o de la fábrica, por ejemplo, el control de entrada, de aforos o para sus programaciones futuras.

La información que sobre estos eventos se facilita a los padres para su autorización debe incluir la relativa a la comunicación de datos a estas entidades, así como la propia autorización. La comunicación, en caso de ser autorizada, implicaría la posibilidad del tratamiento de los datos exclusivamente para los fines que se han indicado, al ser ésta necesaria para que el alumno pueda participar en esa actividad.

### 11.- ¿Se pueden COMUNICAR los datos de los alumnos y de sus padres y madres a las Asociaciones de Madres y Padres -AMPA- o a las Asociaciones de Familias -AFA-?

No sin el **previo consentimiento** de los interesados.

Las **AMPA son responsables del tratamiento** de los datos de carácter personal que hayan recabado, debiendo cumplir con la normativa de protección de datos en su tratamiento.

No obstante, en el caso de que las AMPA fueran contratadas para prestar un servicio al centro educativo para el que tuvieran que tratar los datos de los alumnos y de sus padres sí tendrían acceso a los datos pero en condición de encargadas del tratamiento.

# VIII

## Tratamiento de imágenes de los alumnos.

# VIII. Tratamiento de imágenes de los alumnos.

El **desarrollo de las tecnologías** de la información y de la comunicación ha **facilitado** enormemente la posibilidad de captación, grabación y reproducción de imágenes, proporcionando medios técnicos que prácticamente han convertido en un fotógrafo o realizador de vídeos a cualquier persona que disponga de un teléfono móvil o tablet.

Los centros educativos organizan numerosos **actos escolares y eventos** en los que los alumnos y los profesores son los protagonistas, en los mismos es habitual observar como los **familiares** asistentes **y** el propio **centro toman fotografías y graban vídeos** en los que se recogen diversas imágenes. Estos hechos, comunes en los eventos escolares, dan lugar a que se planteen muchas cuestiones sobre **quién y cómo** se pueden captar las imágenes, qué **requisitos** se han de cumplir, con qué **finalidad** y a quién se pueden **comunicar**.

**IMPORTANTE**

Según quién vaya a grabar las imágenes y la finalidad para la que se graben será necesario observar unos determinados **requisitos**:

- **Si la grabación de las imágenes se produjera por el centro escolar con fines educativos** (como trabajos escolares o evaluaciones): el centro o la Administración educativa estarían **legitimados** para dicho tratamiento sin necesidad del consentimiento de los alumnos o de sus padres o tutores.
- **Si la grabación de las imágenes NO se corresponde con una función educativa** (como imágenes de acontecimientos o eventos que se graban habitualmente con fines de difusión en la revista escolar o en la web del centro): se necesitará contar con el **consentimiento de los interesados**, a quienes se habrá tenido que informar con anterioridad de la finalidad de la grabación, en especial de si las imágenes van a estar accesibles de manera indiscriminada o limitada a la comunidad escolar.
- En caso de **conflicto entre los progenitores** sobre la **grabación** de las **imágenes de sus hijos** por parte del centro, deberán plantearlo aquéllos ante el juez competente en materia de familia para su resolución.

Se **recomienda** que la publicación de las imágenes (fotografías y vídeos) en la web de los centros tenga lugar en un **espacio privado**, al que se acceda mediante identificación y contraseña.

**IMPORTANTE**

Toma de **imágenes** (fotos y vídeos) en **actos escolares** o **eventos educativos**:

1. **Toma de fotografías o grabación de vídeo se produjera por los PADRES Y FAMILIARES de alumnos en eventos festivos, conmemorativos, deportivos o de otra índole, en los que participan los alumnos**: en estos casos la grabación de las imágenes suele corresponder a una actividad **exclusivamente personal y doméstica**, es decir, aquellas que se inscriben en el marco de la vida privada, familiar y de amistad, que están excluidas de la aplicación de la normativa de protección de datos.

2. **Toma de fotografías o grabación de vídeo se produjera por TERCEROS:**

   a. **Grabación por encargo del centro educativo**: se deberá obtener el consentimiento de los alumnos o de sus padres o tutores.

   b. **El tercero lo realiza para sus propias finalidades**: tendrá que contar con el previo consentimiento de los interesados, ya lo recabe él mismo o a través del centro, en cuyo caso se deberá especificar que el tercero es el responsable del tratamiento. Ejemplo:

La Ventana de las Vegas Bajas
VentanaDigital.com

PORTADA SECCIONES PUEBLOS VÍDEOS FOTOS REVISTA LIBROS DE LA VENTANA ESTUDIO DE DISEÑO

Educación Montijo

**FOTOS: Fiesta fin de curso en la Escuela Infantil Alborada de Montijo**

22 julio, 2019

Compartir en Facebook Compartir en Twitter

El viernes 12 de julio,se celebró como cada año la tradicional fiesta fin de curso en la Escuela Infantil **Alborada** de **Montijo**. La temática de la fiesta estaba basada en el proyecto educativo que se ha llevado a cabo durante el curso, **"La Granja de Mati"**, donde los auténticos protagonistas fueron los niños, que cantaron y bailaron bajo la expectante mirada de familiares.

URL: https://ventanadigital.com/fotos-fiesta-fin-curso-la-escuela-infantil-alborada-montijo/

*(Galería de fotos al final del texto)*

Síguenos:

4,388 Fans ME GUSTA
0 Seguidores SEGUIR
0 Seguidores SEGUIR
359 suscriptores SUSCRIBIRTE

Noticias de empresa

COMERCIO LOCAL
Sábado 21: Taller infantil gratuito de decoración de delantales para los pinches de nochebuena

## **GRABACIÓN** de imágenes de actividades docentes.

### 1.- ¿Pueden los centros educativos captar IMÁGENES DE LOS ALUMNOS durante las ACTIVIDADES ESCOLARES?

Para dar respuesta a la cuestión planteada debemos **distinguir dos supuestos** según la **finalidad** de la toma de imágenes como parte de la función educativa o no, así:

- **CON finalidad educativa**: los centros estarían **legitimados** para ello.
- **SIN finalidad educativa** (p.ej, difusión del centro y de sus actividades): se deberá disponer del **consentimiento** de los interesados o de sus padres o de los tutores.

En ocasiones los centros educativos **desarrollan en el entorno escolar** una serie de actos o celebran eventos en los que se realiza una **toma de imágenes** de los alumnos con la única **finalidad** de que los padres pudieran tener acceso a ellas.

En estos supuestos el centro debe habiliar el **acceso** a las imágenes en un **entorno seguro** que exija la previa identificación y autenticación de los alumnos, padres o tutores (por ejemplo, en un área restringida de la intranet del centro), limitándose a las imágenes correspondientes a eventos en los que el alumno concreto hubiera participado.

El centro debe **recordar** a quienes accedan a las imágenes que **NO** pueden, a su vez, proceder a su divulgación de forma abierta.

### 2.- ¿Puede un PROFESOR grabar imágenes de los alumnos para una actividad escolar?

Los profesores, en el desarrollo de la programación y enseñanza de las áreas, materias y módulos que tengan encomendados, pueden disponer la realización de ejercicios que impliquen la grabación de imágenes, normalmente de los propios alumnos, que sólo deberán estar accesibles para los alumnos involucrados en dicha actividad, sus padres o tutores y el profesor correspondiente.

IMPORTANTE

**EN NINGÚN CASO** el mero hecho de realizar la grabación supone que la misma se pueda difundir de forma abierta en internet y que se pueda acceder de manera indiscriminada. En estos casos el responsable del tratamiento es el propio centro o la Administración educativa.

## GRABACIÓN Y DIFUSIÓN de imágenes en eventos organizados y celebrados en los centros educativos.

### 1.- ¿Pueden los FAMILIARES de los alumnos que participan en un evento abierto a las familias GRABAR IMÁGENES del evento?

Sí, siempre y cuando se trate de imágenes captadas exclusivamente para su **uso personal y doméstico**, pues en ese caso esta actividad está excluida de la aplicación de la normativa de protección de datos.

IMPORTANTE

**ATENCIÓN:** Si las imágenes captadas por los familiares se difundieran fuera del ámbito privado, familiar y de amistad, por ejemplo mediante su publicación en internet accesible en abierto, los familiares asumirían la responsabilidad por la comunicación de las imágenes a terceros que **no podrían realizar salvo que hubieran obtenido el consentimiento** previo de los interesados.

**RECOMENDACIÓN:** Sería conveniente que el centro informase a los familiares de su responsabilidad en caso de que las imágenes fueran divulgadas en los entornos abiertos que acaban de señalarse.

### 2.- Si unos padres se NIEGAN a que se tomen IMÁGENES DE SU HIJO en un evento en el centro educativo ¿se ha de cancelar dicho evento?

El evento **NO** se debe cancelar, pero el centro educativo ha de informar a los padres o tutores que la toma de fotografías y vídeos es posible como actividad familiar, exclusivamente para la finalidad de **uso personal y doméstico**, que está excluida de la aplicación de la normativa de protección de datos.

### 3.- ¿Pueden los centros escolares PROHIBIR la TOMA DE IMÁGENES en sus INSTALACIONES?

Para resolver la cuestión debemos acudir al principio de autonomía de los centros educativos que consagra la vigente la Ley Orgánica de Educación en su artículo 120, en sus apartados 4º y 5º, a saber:

Artículo 120. Autonomía de los centros. *Disposiciones generales*.

"4. *Los centros, en el ejercicio de su autonomía, pueden adoptar experimentaciones, planes de trabajo, formas de organización, normas de convivencia y ampliación del calendario escolar o del horario lectivo de áreas o materias, en los términos que establezcan las Administraciones educativas y dentro de las posibilidades que permita la normativa aplicable, incluida la laboral, sin que, en ningún caso, se impongan aportaciones a las familias ni exigencias para las Administraciones educativas.*

5. *Cuando estas experimentaciones, planes de trabajo o formas de organización puedan afectar a la obtención de títulos académicos o profesionales, deberán ser autorizados expresamente por el Gobierno.*"

Por tanto, dado que la LOE dispone que los centros docentes gozan de **autonomía** para elaborar, aprobar y ejecutar normas de organización y funcionamiento del centro, con **fundamento** en dicha **organización** interna que les otorga la ley, el Centro escolar **puede establecer el criterio de NO permitir que las familias graben los eventos escolares**.

Es **RECOMENDABLE** que el **centro advierta a los asistentes** a los eventos de que se pueden grabar imágenes de los alumnos para su **utilización exclusivamente personal, familiar y de amistad**.

**No se deben publicar este tipo de grabaciones en internet en abierto**, a no ser que se cuente con el **consentimiento** de todos aquellos que aparecen en las imágenes, de sus padres o tutores si son menores de 14 años.

### GRABACIÓN de imágenes de actividades que sean desarrolladas fuera del centro escolar.

Se permite la grabación de imágenes fuera del recinto escolar por los centros cuando la misma se realice en **ejercicio de la función educativa**, fuera de esta finalidad se requiere el consentimiento de los interesados, o de sus padres o tutores.

Si la grabación **se realiza por terceros**, por ejemplo, por los responsables de la empresa, museo, exposición o club deportivo que se esté visitando, o en el que se desarrolle una actividad deportiva, será **obligación** de estos terceros disponer del **consentimiento** de los interesados que habrán podido recabar a través del centro.

# IX

# Tratamiento de datos en internet.

# IX. Tratamiento de datos en internet.

Cada vez son más los **centros educativos** que recurren a las soluciones que facilitan las **tecnologías de la información y comunicación**, en particular al uso de los servicios de *cloud computing*[70] o de computación en la nube, tanto para la gestión de recursos en los procesos educativos como para el propio aprendizaje de los alumnos.

**Definición**: puede entenderse como *cloud computing* al almacenamiento, tratamiento y uso de datos ubicados remotamente, accesibles a través de internet[71].

Las **ventajas** de contratar servicios *cloud* pueden resumirse, *grosso modo*, en:

1. **Flexibilidad**. Al permitir una gran agilidad en la escalabilidad de la contratación, permitiendo al cliente escoger entre un mayor o menor número de servicios de conformidad a sus necesidades, pudiendo modificarlos sin necesidad de tener que adquirir y almacenar infraestructuras y/o soportes.
2. **Abstracción**. Los servicios virtuales ofrecidos en la nube son totalmente independientes de los soportes físicos que pueda tener el usuario y permitiendo un rápido dimensionamiento según evolucionen las necesidades del cliente.
3. **Portabilidad.** Gracias a la automatización de los sistemas informáticos que dan soporte al cloud es posible su portabilidad entre distintos prestadores del servicio en la nube.
4. **Accesibilidad**. Se puede acceder a los mismos cuando y donde los necesites con la única condición de disponer de una conexión a internet.
5. **Ahorro de costes**. Resulta más eficiente el alojamiento en la nube que la adquisición, configuración, instalación y mantenimiento del software y hardware físicos en las instalaciones o domicilio del usuario.

**70** El concepto de "Cloud Computing" fue acuñado en el año 2006 por George Gilder en el artículo de opinión "Information Factories" publicado en la revista Wired.

**71** Comisión Europea: *Liberar el potencial de la computación en la nube en Europa*, comunicación 2012, 529 final.

## Utilización de **plataformas educativas.**

Las implicaciones que en materia de protección de datos plantea el uso de plataformas educativas, tanto de gestión como de aprendizaje o entornos virtuales de aprendizaje, son objeto de diversos informes de la Inspección sectorial de la AEPD sobre el uso de servicios de cloud computing en el sector educativo.

### 1.- ¿Quién es el RESPONSABLE del tratamiento de los datos personales de los alumnos en las plataformas educativas?

Los centros o las Administraciones educativas son los responsables del tratamiento porque son los que suscriben el contrato de prestación de servicios con las empresas titulares de las plataformas educativas, actuando éstas últimas como encargadas del tratamiento.

### 2.- ¿Qué LEGITIMACIÓN ampara a los centros o las Administraciones educativas para el tratamiento de datos en las plataformas educativas?

Como regla general, el tratamiento de los datos por parte de los centros educativos para el desarrollo de su actividad se encuentra **amparado** por las previsiones de la **legislación estatal y autonómica** y las consiguientes relaciones jurídicas que se derivan de ella.

No obstante, **algunos supuestos** (como la difusión pública en internet de imágenes de los alumnos) **exigirían el consentimiento** de los afectados o sus representantes legales.

IMPORTANTE

**ATENCIÓN:** Las empresas encargadas del tratamiento sólo podrán remitir comunicaciones comerciales dirigidas a los usuarios de los centros educativos cuando hayan obtenido su consentimiento que deberá prestarse de manera expresa si se realiza a través de medios de comunicación electrónica, sin que esta autorización pueda ser otorgada por el centro.

### 3.- ¿Qué deben hacer los centros educativos si PRESTAN EL SERVICIO de adquisición de libros digitales de forma centralizada?

Cuando la adquisición implique la remisión de la relación de los alumnos con datos personales a las editoriales, se deberá **informar** de dicha comunicación de datos y de las finalidades de la comunicación a los **alumnos y/o a los padres o tutores**.

### 4.- ¿Pueden las editoriales realizar el tratamiento de los datos personales?

Las editoriales carecen de legitimación para el tratamiento de los datos personales para **fines distintos** de los previstos en la licencia del servicio (resultado de pruebas, perfiles, publicidad, etc.), por lo que tendrán que **recabar el consentimiento** específico.

### 5.- ¿Pueden los centros permitir la utilización de herramientas de almacenamiento en nube DISTINTAS de las plataformas educativas?

Sólo si reúnen las garantías previstas en la normativa de protección de datos. En tal caso deberán establecer unas normas que garanticen el adecuado tratamiento de los datos personales.

La utilización de aplicaciones por los profesores en dispositivos personales (tableta, móvil, etc.) debe garantizar la política de privacidad definida por el centro o la Administración educativa con las garantías establecidas en la normativa de protección de datos.

Es de **especial importancia** que el uso de esas aplicaciones no implique una transmisión de los datos de los alumnos al prestador del servicio contratado para que los utilice para sus propios fines o los almacene de forma permanente, incluso con posterioridad a la terminación del contrato o cuando el alumno ya no curse estudios en el centro educativo.

**Tampoco** debería implicar la renuncia del centro educativo al acceso a los datos o a su supresión.

### 6.- ¿Deben los centros o las Administraciones educativas interesarse por la UBICACIÓN DE LOS DATOS de los alumnos en estos recursos?

Se pueden plantear dos situaciones:

A. Que datos se ubiquen en terceros estados fuera del Espacio Económico Europeo y sobre los que la Comisión Europea haya decidido que **SÍ** garantizan un nivel de protección adecuado, existe una transferencia internacional que, sin embargo no requerirá ninguna autorización específica por parte de la Autoridad de control.

A. Que los datos se ubiquen en terceros estados fuera del Espacio Económico Europeo que **NO** garantizan un nivel adecuado de protección, existe una **transferencia internacional que exige** que el responsable aporte garantías suficientes. Estas garantías podrán derivarse, en particular, de cláusulas contractuales tipo adoptadas por la Comisión Europea o por la Agencia Española de Protección de Datos. Esta transferencia tampoco requerirá ninguna autorización específica.

### 7.- ¿Qué MEDIDAS deberán adoptar los centros o las Administraciones educativas en relación con la SEGURIDAD DE LOS DATOS?

Las medidas que deben adoptar los centros o las Administraciones educativas, como **responsables del tratamiento**, en relación con la seguridad de los datos serían:

- Desplegar la **diligencia debida** para que el encargado del tratamiento y, en su caso, los subencargados garanticen el cumplimiento de las medidas de seguridad exigibles.

- Especificar por **contrato** la naturaleza de los datos para poder definir e implementar las medidas de seguridad adecuadas que deben transmitirse a lo largo de todos los contratos establecidos con los subencargados.

- Los contratos suscritos deben **especificar** claramente las **responsabilidades** de todos los intervinientes en la prestación de los servicios de nube, tanto de los centros o Administraciones educativas como de las entidades que actúan como encargadas y subencargadas del tratamiento.

  Por ejemplo, se deben determinar las responsabilidades sobre las medidas de seguridad que deben implementarse.

- Establecer **procedimientos** de colaboración entre el responsable y los encargados y subencargados de tratamiento para la implantación y mantenimiento de las medidas de seguridad, ya que la **responsabilidad** puede ser, en muchos casos, **compartida**, por lo que deben delimitarse contractualmente las responsabilidades de cada uno de ellos.

- Los centros educativos deben poder conocer el **procedimiento** establecido para la **recuperación de los datos** en caso de posibles contingencias que puedan producirse tanto en las entidades encargadas del tratamiento como en las subencargadas.

- El centro educativo debe adoptar las medidas necesarias para que todos los usuarios del sistema sean **conocedores de las políticas** del centro en materia de seguridad.

## 8.- A la FINALIZACIÓN del contrato de prestación de servicios ¿cómo deben proceder los centros educativos?

Los centros educativos deben tener la **opción** de exigir al encargado del tratamiento la **portabilidad de la información** a sus propios sistemas, o a otro nuevo encargado de tratamiento, con garantías de la integridad de la información.

A tal efecto el responsable debe obtener información respecto a la manera de recuperar los datos, de forma que quede **garantizada contractualmente** la portabilidad.

Al finalizar la contratación, el encargado del tratamiento tiene que garantizar al responsable del tratamiento el **borrado seguro** de los datos personales donde se encuentren alojados, de tal forma que se **impida su reutilización**. Además, deberá asegurar el **bloqueo o borrado** de todos los **usuarios** para imposibilitar el acceso a la plataforma educativa.

Se considera una **buena práctica** que a la finalización del contrato se asegure la destrucción o devolución de los datos con un certificado de destrucción o con un acuse de recibo.

## Publicación de datos en la **WEB** de lo centros educativos.

Habitualmente las webs de los centros educativos contienen información referida a sus características, su organización, las materias que imparte, las actividades que desarrolla, los servicios que ofrece, las relaciones con otros centros, para lo que en ocasiones incluyen información de carácter personal sobre la dirección, el profesorado y los alumnos.

### 1.- ¿Se pueden PUBLICAR en la WEB del centro los DATOS de los profesores, tutores y otros responsables del centro?

Hay que distinguir dos supuestos:

- **Web en abierto**: sería necesario contar con su **consentimiento previo** dado que se trata de una comunicación de datos a los que puede acceder cualquier persona de manera indiscriminada y no resulta necesaria para el ejercicio de la función educativa encomendada a los centros.
- **Información restringida**: a los alumnos del centro y a sus padres o tutores **se puede publicar**, si bien se debería informar a los docentes y, en caso de incluir la dirección de correo electrónico para contacto, que sea la del centro y no las personales que tengan los profesores en el ámbito educativo.

### 2.- ¿Puede PUBLICARSE en la WEB del centro INFORMACIÓN relativa a los alumnos, como fotografías o vídeos?

Sí cuando se disponga del **consentimiento** de los alumnos o de sus padres o tutores. También podría llevarse a cabo de manera que no se pudiera identificar a los alumnos, por ejemplo, **pixelando** las imágenes.

También sería posible su publicación cuando responda a determinados eventos desarrollados en el entorno escolar con la única finalidad de que los padres pudieran tener acceso a ella. Este acceso debería llevarse a cabo siempre en un **entorno seguro** que exigiera la previa identificación y autenticación de los alumnos, padres o tutores (por ejemplo, en un área restringida de la intranet del centro), limitándose a la información correspondiente a eventos en los que el alumno concreto hubiera participado. En todo caso, sería preciso **recordar a quienes acceden a la información que no pueden, a su vez, proceder a su divulgación de forma abierta**.

### 3.- ¿Pueden publicarse DATOS PERSONALES de los alumnos en el BLOG del centro educativo?

Como en el supuesto de la web, si el contenido del blog en abierto del centro educativo incluyera datos que permitieran la identificación de los alumnos, se requeriría su **consentimiento** o el de sus padres o tutores.

En estos casos se aconseja disociar o anonimizar[72] los datos de los alumnos, de manera que no se les pueda identificar.

### 4.- ¿Y un PROFESOR puede publicar en SU BLOG las actas del departamento o los exámenes de los alumnos o sus fotografías?

El blog de un profesor es un medio de información y comunicación **al margen de la función docente** que desarrolla en los centros educativos. De su contenido será **responsable el profesor** que deberá observar la normativa de protección de datos en cuanto que incluya información de carácter personal.

Por tanto, salvo que se contase con el **consentimiento** de los afectados, o de sus padres o tutores, **NO** se podrían publicar en el blog de un profesor datos de carácter personal que permitan identificar a los alumnos.

Al igual que con los blogs de los centros educativos, se podría publicar la información previa disociación o anonimización[72] de los datos de los alumnos de manera que no se les pudiese llegar a identificar.


**72** RGPD. Considerando 26. *"... [P]or lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación."*


**Colegio Concertado**
***Ruta de la Plata***
***Almendralejo.***

# X

## Certificados del Registro Central de delincuentes sexuales.

# X. Certificados del Registro Central de delincuentes sexuales.

Para el acceso y ejercicio a las profesiones, oficios y actividades que impliquen contacto habitual con menores es **requisito** no haber sido condenado por sentencia firme por algún delito contra la libertad e indemnidad sexual, que incluye la agresión y abuso sexual, acoso sexual, exhibicionismo y provocación sexual, prostitución y explotación sexual y corrupción de menores, así como por trata de seres humanos. A tal efecto, quien pretenda el acceso a tales profesiones, oficios o actividades deberá acreditar esta circunstancia mediante la **aportación de una certificación negativa** del Registro Central de delincuentes sexuales.

Una vez iniciada la relación o aportado el certificado negativo no sería precisa una nueva aportación o renovación periódica del mismo, a pesar de que dicho certificado pueda datar de fecha muy anterior.

En ese caso, dada la existencia y permanencia de la relación, podrá considerarse que los datos objeto de conservación y tratamiento **mantienen su certeza** a menos que se tenga conocimiento de la concurrencia de nuevas circunstancias que exijan su actualización, lo que podrá implicar la exigencia al empleado de un nuevo certificado del Registro Central de delincuentes sexuales para comprobar la exactitud de los datos.

# XI

# Videovigilancia.

# XI. Videovigilancia.

La instalación de sistemas de videovigilancia con la finalidad de garantizar la **seguridad** de personas e instalaciones en los centros educativos es una realidad en un importante número de centros y cuya tendencia va en aumento.

La implantación de cámaras de videovigilancia, que responda al **interés legítimo** de los centros y de las Administraciones educativas en mantener la seguridad e integridad de personas y las instalaciones, ha de observar la normativa de protección de datos personales, en la medida que implica el tratamiento de los datos de alumnos, profesores, familiares, etc.

Dado el carácter **intrusivo** de estos sistemas en la intimidad de las personas, su instalación debe responder a los **criterios de necesidad, idoneidad** para los fines pretendidos, que no se puedan conseguir con una medida menos invasiva de la intimidad, **y proporcionalidad**, que ofrezca más beneficios que perjuicios.

**EJEMPLO:**

Un centro educativo está valorando la instalación de un sistema de videovigilancia por motivos de seguridad (**necesidad**), entre los distintos medios disponibles el que mejor se adapta al centro es el de videovigilancia (**idoneidad**) toda vez que la instalación de este sistema persigue el de evitar los daños materiales, robos y hurtos que se pueden llegar a producir en el interior del centro por lo que se ha decidido limitar su funcionamiento a las horas no lectivas (**proporcionalidad**), de forma que se minimizará el impacto en la privacidad del personal del centro, alumnos, padres y resto de personas interesadas.

## La **IMAGEN** como dato de carácter personal.

Hemos visto en el Capítulo III como nuestra Constitución Española de 1978 reconoce el derecho a la imagen en su artículo 18.1 (junto al honor y a la intimidad personal y familiar), integrándose en los denominados "*derechos de la personalidad*"[73]. Nuestro Tribunal Constitucional ha declarado en la sentencia 127/2003, 30 jun., FJ 6º:

> "... [e]n su dimensión constitucional, (la imagen) se configura como un derecho de la personalidad, que atribuye a su titular la facultad de disponer de la representación de su aspecto físico que permita su identificación, lo que conlleva tanto el derecho a determinar la información gráfica generada por los rasgos físicos que le hagan reconocible que puede ser captada o tener difusión pública, como el derecho a impedir la obtención, reproducción o publicación de su propia imagen por un tercero no autorizado" (STC 156/2001, FJ 6; en parecidos términos, STC 83/2002, de 22 de abril, FJ 4).

**73** ENCABO, M.A. *Derechos de la personalidad*. Marcial Pons, 1ª ed., 2012. Pag. 15. *Con la expresión «derechos de la personalidad» se suele hacer referencia a un conjunto de derechos de la propia persona, que constituyen, en definitiva, manifestaciones, tanto exteriores como interiores, diversas de la cada persona singular, su dignidad y su propio ámbito individual. También podemos decir que los derechos de la personalidad son aquellos que el ordenamiento jurídico concede para la protección de los intereses más personales de un individuo.*

Como nos dice nuestro Tribunal Constitucional, el derecho a la propia imagen incluye los rasgos físicos más característicos de la persona, así la sentencia 12/2012, de 30 ene., FJ 5º:

> "... [e]l derecho a la propia imagen, reconocido por el art. 18.1 de la Constitución al par de los de honor y la intimidad personal, forma parte de los derechos de la personalidad y como tal garantiza el ámbito de libertad de una persona respecto de sus atributos más característicos, propios e inmediatos como son la imagen física, la voz o el nombre, cualidades definitorias del ser propio y atribuidas como posesión inherente e irreductible a toda persona. En la medida en que la libertad de ésta se manifiesta en el mundo físico por medio de la actuación de su cuerpo y las cualidades del mismo, es evidente que con la protección de la imagen se salvaguarda el ámbito de la intimidad y, al tiempo, el poder de decisión sobre los fines a los que hayan de aplicarse las manifestaciones de la persona a través de su imagen, su identidad o su voz.". En el caso de una grabación oculta como la que aquí nos ocupa, la captación no sólo de la imagen sino también de la voz intensifica la vulneración del derecho a la propia imagen mediante la captación no consentida de específicos rasgos distintivos de la persona que hacen más fácil su identificación."

Aunque mediante la difusión de la imagen es posible vulnerar otros derechos relacionados como los del honor y la intimidad, lo verdaderamente relevante del derecho fundamental a la propia imagen es la **protección frente a su reproducción** y así el Tribunal Constitucional ha declarado mediante sentencia 18/2018, de 16 feb., FJ 4º:

> "... [e]l derecho a la propia imagen pretende salvaguardar un ámbito propio y reservado, aunque no íntimo, frente a la acción y conocimiento de los demás; un ámbito necesario para poder decidir libremente el desarrollo de la propia personalidad y, en definitiva, un ámbito necesario según las pautas de nuestra cultura para mantener una calidad mínima de vida humana. Ese bien jurídico se salvaguarda reconociendo la facultad de evitar la difusión incondicionada de su aspecto físico, ya que constituye el primer elemento configurador de la esfera personal de todo individuo, en cuanto instrumento básico de identificación y proyección exterior y factor imprescindible para su reconocimiento como sujeto individual. En definitiva, lo que se pretende, en su dimensión constitucional, es que los individuos puedan decidir qué aspectos de su persona desean preservar de la difusión pública a fin de garantizar un ámbito privativo para el desarrollo de la propia personalidad ajeno a las injerencias externas (ATC 28/2004, FJ 3)" (STC 176/2013, de 21 de octubre, FJ 6).

La captación de imágenes a través de sistemas de videovigilancia puede constituir un tratamiento de datos de carácter personal y, por tanto, sometido a la normativa de protección de datos y que también fue objeto de la Instrucción 1/2006, de 8 nov., de la Agencia Española de Protección de Datos[74], y que establece lo siguiente:

> Artículo 1. *Ámbito objetivo*.
>
> "1. *La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.*
>
> *El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.*
>
> *(...)*

**74** Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, *sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.* Accesible en https://www.boe.es/buscar/act.php?id=BOE-A-2006-21648

*Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma."*

## **VIDEOVIGILANCIA** en centros educativos.

### 1.- ¿Se pueden INSTALAR CÁMARAS de videovigilancia en TODAS las instalaciones del colegio?

No en todas las instalaciones. Dada la **intromisión** que supone en la **intimidad de las personas**, tanto de los alumnos como de profesores y demás personas cuya imagen puede ser captada por las cámaras, los sistemas de videovigilancia **no podrán instalarse** en aseos, vestuarios o zonas de descanso de personal docente o de otros trabajadores.

### 2.- ¿Se pueden instalar cámaras de videovigilancia en las AULAS alegando motivos de CONFLICTIVIDAD?

Resultaría **desproporcionado**, pues durante las clases ya está presente un profesor. Además de una intromisión en la privacidad de los alumnos, podría suponer un control laboral desproporcionado de los profesores.

Cabría la posibilidad de que, **fuera del horario lectivo** y en los supuestos de desocupación de las aulas, se pudieran activar mecanismos de videovigilancia con la **finalidad** de evitar daños en las instalaciones y materiales.

### 3.- ¿Se pueden instalar cámaras de videovigilancia en los PATIOS de recreo y COMEDORES?

**SÍ**, cuando la instalación responda a la protección del **interés superior del menor**, toda vez que, sin perjuicio de otras actuaciones como el control presencial por adultos, se trata de espacios en los que se pueden producir acciones que pongan en riesgo su integridad física, psicológica y emocional.

### 4.- ¿Se debe INFORMAR de la existencia de un sistema de videovigilancia?

Sí, para ello se deberá colocar un **distintivo específico** en lugar suficientemente visible en aquellos espacios donde se hayan instalado las cámaras, el modelo de cartel o distintivo es el incluido en la Instrucción 1/2006, de 8 nov., de la Agencia Española de Protección de Datos[75].

También se deberá disponer de una **cláusula informativa** que incluya los extremos exigidos por la normativa.

**75** Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, *sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.* Accesible en https://www.boe.es/buscar/act.php?id=BOE-A-2006-21648

**CARTEL DE VIDEOVIGILANCIA + CLÁUSULA INFORMATIVA:**

# ZONA VIDEOVIGILADA

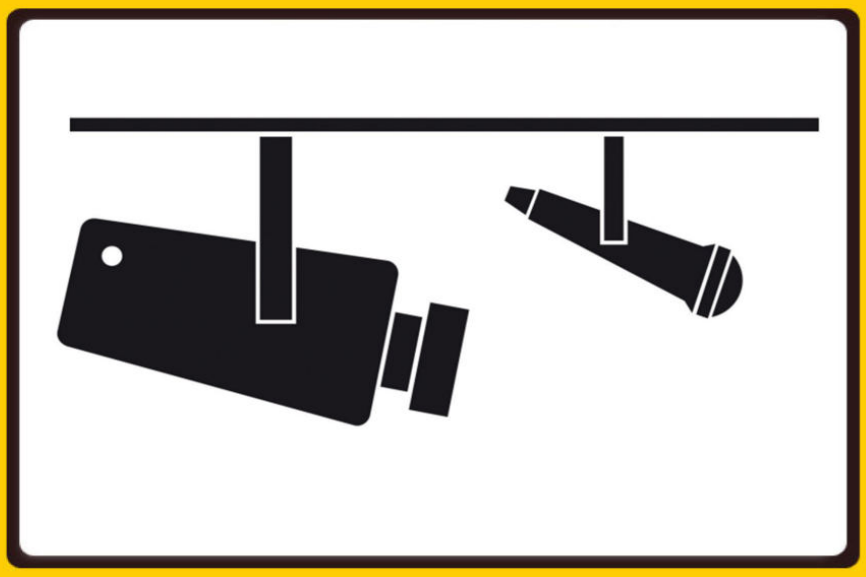
## Protección de datos

Reglamento (UE) 2016/679, de 27 de abril (GDPR), y Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD)

| | |
|---|---|
| **Responsable** | DATADATA PRIVACY & COMPLIANCE S.L |
| **Finalidad** | Control de acceso, seguridad de las instalaciones y control laboral |
| **Legitimación** | Interés público e interés legítimo del responsable |
| **Conservación** | Un máximo de 30 días |
| **Destinatarios** | Fuerzas y cuerpos de seguridad |
| **Derechos** | Acceso, rectificación, portabilidad y supresión de datos<br>Limitación y oposición al tratamiento |
| **Ejercicio derechos** | Calle León, 4 - 06800 Mérida (Badajoz). Email: dpd@datadata.es<br>Datos de contacto del DPO: Datadata Privacy & Compliance - dpd@datadata.es |
| **Reclamación** | Ante la autoridad de control en www.aepd.es |
| **Más información** | Diríjase al responsable de seguridad |

## CARTEL DE VIDEOVIGILANCIA + VOZ + CLÁUSULA INFORMATIVA:

# ZONA VIDEOVIGILADA



## Protección de datos

Reglamento (UE) 2016/679, de 27 de abril (GDPR), y Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD)

| | |
|---|---|
| **Responsable** | DATADATA PRIVACY & COMPLIANCE S.L |
| **Finalidad** | Control de acceso, seguridad de las instalaciones y control laboral |
| **Legitimación** | Interés público e interés legítimo del responsable |
| **Conservación** | Un máximo de 30 días |
| **Destinatarios** | Fuerzas y cuerpos de seguridad |
| **Derechos** | Acceso, rectificación, portabilidad y supresión de datos<br>Limitación y oposición al tratamiento |
| **Ejercicio derechos** | Calle León, 4 - 06800 Mérida (Badajoz). Email: dpd@datadata.es<br>Datos de contacto del DPO: Datadata Privacy & Compliance - dpd@datadata.es |
| **Reclamación** | Ante la autoridad de control en www.aepd.es |
| **Más información** | Diríjase al responsable de seguridad |

# XII

# Redes Sociales.

# XII. Redes Sociales.

## PUBLICACIÓN de datos en redes sociales por centros educativos.

La publicación de datos personales en redes sociales por parte de los centros educativos requiere contar con el **consentimiento de los interesados**, a los que habrá que informar previamente de manera clara de los datos que se van a publicar, en qué redes sociales, con qué finalidad, quién puede acceder a los datos, así como de la posibilidad de ejercitar sus derechos de acceso, rectificación, oposición y supresión. La normativa incluye la obligación de informar sobre el plazo durante el que se conservarán las imágenes o, si no fuera posible, de los criterios para determinarlo.

## REDES SOCIALES on line.

### 1.- ¿Qué son Redes Sociales?

Podemos definir de manera amplia las redes sociales online como aquellos **servicios de la sociedad de la información** que ofrecen a los usuarios una plataforma de comunicación a través de Internet para que éstos **generen un perfil con sus datos personales**, facilitando la creación de redes en base a criterios comunes y permitiendo la **conexión e interacción con otros usuarios**[76].

Otros autores han definido "Redes Sociales" como *aquella plataforma tecnológica que permite a sus usuarios, a través de sus correspondientes perfiles, vincularse entre sí, creando sistemas cruzados e interactivos de generación y difusión de información*[77].

IMPORTANTE

**CARACTERÍSTICAS que definen el funcionamiento de una Red Social:**

1. **Principio general de libertad bilateral de los usuarios.** Permite el compartir información como el acceder a la que deseen, a través de cualquier medio o formato, así como conectarse entre sí.
2. **Principio de control de la información ofrecida.** La información es compartida con quien el usuario decida, estableciéndose también unos controles por el operador de la red.
3. **Principio general de transparencia.** Se pretende así establecer un sistema general de ausencia de barreras técnicas o de cualquier otro tipo respecto al acceso a la información compartida.

**76** Rallo, A. Martínez, R. *Derecho y redes sociales*. 2012. Ed. Civitas, 2ª. Pág 22.
**77** Agustinoy, A; Monclús, J. *Aspectos legales de las redes sociales*. 2019. Ed. Bosch, 2ª. Págs 22-23.

En las redes sociales se produce el **fenómeno viral** cuya clave es la **vinculación entre usuarios**. Las vinculaciones se miden en grados, donde el primer grado estaría conformado por los contactos directos, el segundo grado por los contactos de los contactos y así sucesivamente de forma que, a mayor número de usuarios, mayor número de vinculaciones y mayor es la red.

## 2.- ¿Qué es la teoría de los seis grados de separación?

La **teoría de los seis grados de separación** es una hipótesis que intenta probar que cualquier persona en la Tierra puede estar conectado a cualquier otra del planeta a través de una cadena de conocidos que no tiene más de cinco intermediarios (conectando a ambas personas con sólo seis enlaces), algo que se ve representado en la popular frase «*el mundo es un pañuelo*»[78]. La teoría fue inicialmente propuesta en 1929 por el escritor húngaro Frigyes Karinthy en un cuento llamado Chains[79].

De acuerdo a la teoría, **una persona** llega a conocer a unas 100 personas de media, entre amigos, familiares y compañeros de trabajo o escuela. Si relacionamos a cada uno de ellos con otras 100 personas, si pedimos a esos amigos que pasen un mensaje a sus amigos sería posible llevarlo a 10.000 personas.

Las anteriores 10.000 personas son consideradas **contactos de segundo nivel**, que el emisor original no conoce pero que podría hacerlo fácilmente si pide a sus amigos y familiares que se los presenten.

Podríamos ampliar la red en el **tercer nivel** a 1.000.000 de personas toda vez que de las 10.000 personas de nuestro segundo nivel, éstas conocerán, de media, a otras 100 personas. En el **cuarto nivel** llegaríamos a 100.000.000, en el **quinto nivel** a 10.000.000.000 y, por último, en el sexto nivel a 1.000.000.000.000 de personas. Por tanto, en **seis pasos**, y con las tecnologías disponibles, se podría enviar un mensaje a cualquier individuo del planeta.

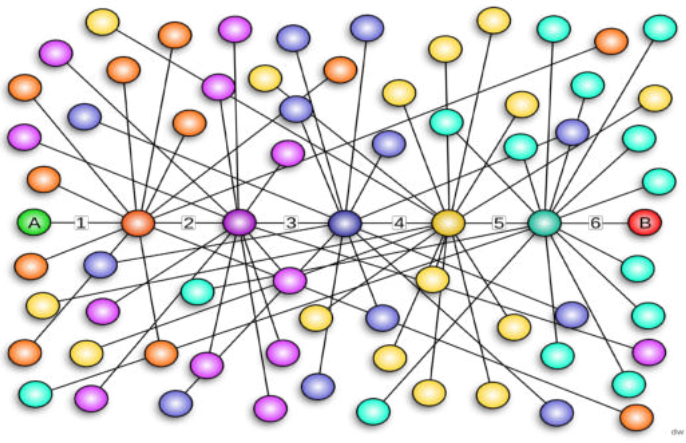



**Ilustración:**
De Daniel' (User:Dannie-walker) - Trabajo propio, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=8977072

**78** Wikipedia. https://es.wikipedia.org/wiki/Seis_grados_de_separación
**79** Karinthy, Frigyes "chains", 1929, accesible en https://djjr-courses.wdfiles.com/local--files/soc180%3Akarinthy-chain-links/Karinthy-Chain-Links_1929.pdf

Por ejemplo, imaginemos un repartidor de paquetería, quien conoce al portero de un hotel de dos estrellas; dicho portero conoce al dueño del hotel y éste al dueño de una cadena de hoteles prestigiosa; el dueño de esta prestigiosa cadena conoce a una persona que trabaja en el Palacio de la Moncloa y esta persona conoce al Presidente del Gobierno. En unos pocos enlaces se ha conseguido unir a un repartidor de paquetería con el Presidente del Gobierno.

Si la anterior teoría fue enunciada en el año 1930, debe ponerse en situación el lector de lo que sucede en 2020 donde Internet y las aplicaciones de mensajería instantánea se han democratizado creando verdaderas redes sociales de carácter mundial como, por ejemplo, Whatsapp®, Skype®, Instagram®, Facebook messenger®, etc.

## PRIVACIDAD DESDE EL DISEÑO *«Privacy by design».*

El concepto de "***privacy by design***" se atribuye a la canadiense **Ann Cavoukian** quien, a mediados de los años noventa del pasado siglo, propuso una modificación de los sistemas de protección de datos de carácter personal que trataban datos en los entornos tecnológicos.

Ann Cavoukian
foto: thestar.com

Ann propuso **abandonar** un punto de partida basado en un **enfoque relativo** (*donde las sanciones e infracciones eran parte inherente a los sistemas de protección de datos*) y, por tanto, **reactivo** (*que genera acciones correctoras de forma paralela a las incidencias que se producen*), de forma que **se estableciera** un **sistema de cumplimiento de carácter global y predeterminado** en cada organización, basado en unos estándares de protección que deben ser implementados desde el mismo momento en que se diera inicio al diseño de los sistemas técnicos y las redes de información.

**La idea de "privacy by design" cristalizó en el artículo 25 RGPD:**

Protección de datos desde el diseño y por defecto.

1. *Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas,* ***el responsable del tratamiento aplicará****, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.*
2. *El* ***responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas*** *con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas* ***garantizarán*** *en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.*
3. *Podrá utilizarse un* ***mecanismo de certificación*** *aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.*

Veamos ahora los **SIETE PRINCIPIOS** que sirven de **base** al "***Privacy by Design***"[80]:

1

## **Proactividad** (no reactividad) **y prevención** (y no corrección).

El enfoque a aplicar está exclusivamente basado en un sistema de medidas proactivas, anticipándose y previendo incidencias y problemas que puedan poner en riesgo los datos personales a ser recabados y tratados a través de la correspondiente red. En palabras de la autoridad de protección de datos de Ontario (Canada) un sistema basado en este enfoque «*no espera a que los riesgos se materialicen, ni ofrece remedios para resolver infracciones de privacidad una vez que ya ocurrieron, su finalidad es prevenir que ocurran. En resumen,* ***Privacy by Design llega antes del suceso no después***.»

2

## **Privacidad como configuración determinada**.

Los datos personales se protegerán de forma automática en el sistema técnico o en los procesos asociados al mismo. De este modo, si una persona implicada en tales procesos no adopta una determinada acción, la privacidad de los datos se mantendrá intacta. De modo que no se requerirá de las personas implicadas acción alguna para proteger la privacidad de los datos. Por el contrario, la propia configuración predeterminada del sistema técnico asegurará dicha privacidad.

3

## **Privacidad incrustada en el diseño**.

El diseño y la arquitectura de los sistemas informáticos así como de sus correspondientes procedimientos tendrán como pilar básico la garantía de una plena protección de los datos personales. En otras palabras, la privacidad no será un elemento complementario del proceso de diseño y construcción de los sistemas informáticos, sino la raíz y esencia de los mismos, constituyendo su parte integral sin reducir su funcionalidad.

4

## **Funcionalidad total**.

Se pretenden evitar dicotomías innecesarias como, por ejemplo, la búsqueda de un equilibrio entre privacidad y seguridad, de modo que la primera pueda llegar a sacrificarse en aras a garantizar la segunda. En términos técnicos, en los sistemas basados en Privacy by Design rige el principio general de «todos ganan» y se huye de la máxima «si alguien gana otro pierde», dado que su aceptación supondría dar por válida la posibilidad de una reducción en el grado de protección de datos a favor de otros elementos sustanciales del sistema como su estabilidad o seguridad.

**80** Agustinoy, A; Monclús, J. *Aspectos legales de las redes sociales.* 2019. Ed. Bosch, 2ª. Págs 63-64.

### Seguridad extremo a extremo.

Los sistemas de recogida y tratamiento de datos asegurarán unos niveles máximos de protección de la información tanto en su recogida como en las posteriores fases de las que se componga el ciclo de vida de tales datos en los citados sistemas. De este modo, los datos se recogerán, tratarán y finalmente se destruirán asegurando plena seguridad y sin demoras, estableciéndose una administración segura del ciclo de vida de la información (desde un extremo al otro de su existencia).

### Visibilidad y transparencia.

La explotación de los sistemas técnicos que vayan a utilizarse para el tratamiento de datos personales deberán estar estructurados y funcionar conforme a su diseño original, garante de unos niveles óptimos de protección de tales datos. Así, sus componentes y operaciones deberán ser transparentes para los usuarios, de modo que éstos tengan una imagen fiel en todo momento del status de cumplimiento de los niveles de protección de datos de carácter personal.

### Enfoque centrado en el usuario.

Los sistemas basados en los parámetros Privacy by Design deberán tener al usuario como elemento prioritario o principal. De este modo, los intereses de tales usuarios deberán configurar los sistemas, implicando el desarrollo de elementos en los mismos como, por ejemplo, configuraciones predefinidas de privacidad alta, sistemas adecuados de notificaciones así como establecer medios de opciones para los perfiles de usuario de fácil gestión.

## **REDES SOCIALES** y protección de datos.

Toda red social se alimenta de los contenidos que a su disposición ponen los participantes a través de sus perfiles personales y que, en la mayoría de casos, tienen una connotación personal. Así, no resulta nada extraño encontrar la narración de las vivencias del usuario o sus fotos o, incluso, vídeos de amigos o de carácter familiar; de forma que es posible la identificación de la persona que los comparte e, incluso, trazar un perfilado de su personalidad que incluya sus gustos, formación académica, aficiones en el tiempo libre, lugar de residencia o vacaciones, etc.

La información de carácter personal que se contiene en una red social es su *leitmotiv* para un adecuado funcionamiento y que implica el pleno sometimiento de la misma al cumplimiento de los principios y dictados de la normativa de protección de datos.

IMPORTANTE

La Universidad de Harvard publicó el informe "***Teens, social media and Privacy***" el 21 de mayo de 2013[1], en el mismo se estudió durante el año 2012 el comportamiento en redes sociales de teenagers de los Estados Unidos de América, arrojando los siguientes resultados:

- **92%** utilizaba su **nombre real** para identificarse en su perfil de la Red Social.
- **91%** había publicado **fotos con su imagen** en perfiles de redes sociales.
- **84%** había incluido una detallada **descripción de sus aficiones** en su perfil.
- **82%** indicaba en el perfil creado la **fecha de nacimiento real**.
- **71%** identificaba la **ciudad en la que residía**.
- **53%** hacía pública su dirección de **email** en el perfil publicado en la red social.

1 Accesible en URL: https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/

## ¿Son datos personales los contenidos de una red Social?

Como hemos visto anteriormente, debemos partir de la definición de «**datos personales**» que nos ofrece el RGPD del siguiente tenor: *toda información sobre una persona física identificada o identificable («el interesado»)*[81].

Sentencia Ejemplo

Asunto: ***Contencioso-administrativo. Protección de datos***.

Audiencia Nacional, Sala C-A, Sección 1ª - **AN**.

Sentencia nº 215/2013 de 2 de enero de 2013 -Recurso 577/2011-.

... [l]a grabación del citado **video** tuvo lugar en el curso de una **excursión realizada por el colegio** Safa de Urgel al Zoo de la Casa de Campo en Madrid, durante la mañana del día 26 de mayo de 2009, con **menores de entre 7 y 8 años**, a cuyo **cargo iban profesoras** del citado colegio. Según se relata en la denuncia, las **profesoras manifestaron** al hoy recurrente que **no podía grabar a los menores que se encontraban bajo su custodia y que borrara la grabación**, video que posteriormente fue colgado en el perfil del **facebook** del Sr. Armando, lo que motivó la denuncia de los hechos a la AEPD por el director del citado colegio.

El Sr. Armando recurre manifestando que el hecho no incumple la Ley al haber sido captadas las imágenes de los menores en un lugar abierto al público, sin finalidad comercial, por cuanto la Ley Orgánica 1/1982 que regula el uso de la imagen, no prohíbe el uso de imágenes ajenas en dichas circunstancias.

Respecto a dicho alegato cabe reseñar que **nos encontramos en el ámbito de la protección de datos de carácter personal** y que la imagen personal de los menores que aparecían en el video en cuestión, que miran a la cámara y permite su identificación, tiene la consideración de dato de carácter personal.

No ofrece dudas a la Sala la existencia del tratamiento de datos de carácter personal de los menores por el Sr. Armando que para el presente caso **la divulgación por medio de video** de la imagen de los menores, **constituye un tratamiento de sus datos** de carácter personal, que al ser menores de 14 años

81 RGPD. Artículo 4.1.

de edad, pues contaban entre 7 y 8 años de edad, requiere para poder efectuarlo el consentimiento de sus padres o tutores como exige la normativa de Protección de Datos. Por tanto, las alegaciones referentes a si los **menores no se encontraban acompañados por sus profesoras** en el concreto momento en que se grababa el video, **resultan irrelevantes** a los efectos del presente procedimiento, pues **los menores por su edad no podían consentir** ni la grabación ni la difusión de su imagen.

Cabe resaltar que **la imagen del menor tiene una consideración legal especialmente protectora**, como ha señalado el Tribunal Supremo (S 13/07/06 rec. 2947/2000 ) tras referirse a su jurisprudencia y a lo dispuesto en los arts. 18.1 y 20.1 CE, a la L.O 1/82 de protección del derecho al honor, intimidad y propia imagen, y la L.O 1/96, de protección jurídica del menor.

En cuanto a la apelación del Sr. Armando a su derecho a la libertad de expresión e información para divulgar dicho video, la Sala destaca que el presente caso se trata de la **difusión de imágenes de menores** que están mirando a la cámara, es decir captadas directamente, grabadas en el Zoo de la Casa de Campo de Madrid, y conversando con el recurrente, sin que **ningún interés informativo se aprecie en la difusión de las imágenes de dichos niños** de 8 y 9 años de edad, que son accesibles a un gran número de personas, como lo son los usuarios de la red social Faceebok, a los que es accesible en abierto.

La Sentencia del Tribunal Constitucional 158/09, de 29 jun., señala que cuando se trata "*de la captacióny difusión de fotografías de niños en medios de comunicación social,es preciso tener en cuenta ... que el ordenamiento jurídico establece en estos supuestos una protección especial, en aras a proteger el interés superior del menor .... cabe recordar que, de conformidad con el art. 20.4 CE, las libertades de expresión e información tienen su límite ..., especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia. Asimismo, deben ser tenidas en cuenta las normas internacionales de protección de la infancia, y, entre ellas, muy en particular, la Convención de la Naciones Unidas sobre los derechos del niño (ratificada por España por Instrumento de 30 de noviembre de 1990), que garantiza el derecho de los niños a la protección de la ley contra las injerencias arbitrarias o ilegales en su vida privada (art.16) (...) En suma,* ***para que la captación, reproducción o publicación por fotografía de la imagen de un menor de edad en un medio de comunicación no tenga la consideración de intromisión ilegítima en su derecho a la propia imagen*** *(art. 7.5 L.O 1/82),* ***será necesario el consentimiento previo y expreso del menor*** *(si tuviere 14 años),* ***o de sus padres o representantes legales*** *(art. 3 L.O 1/82), si bien incluso ese consentimiento será ineficaz para excluir la lesión del derecho a la propia imagen del menor si la utilización de su imagen en los medios de comunicación puede implicar menoscabo de su honra o reputación, o ser contraria a sus intereses (art. 4.3 L.O 1/96 )*".

Por tanto, **no apreciándose ni habiéndose tampoco alegado por el recurrente circunstancias de entidad que justifiquen la supremacía de un interés público en la difusión de las imágenes de los menores, debe darse prevalencia a la protección de la propia imagen de los menores entendida aquí como dato personal** ...

La Sala destaca que el hecho de que la grabación de las imágenes de los menores se hayan efectuado en un lugar público y pueda no existir un interés comercial directo en su difusión, **no exime** de tener que contar con el consentimiento de sus padres o representantes legales para su difusión.

Por último, respecto al hecho de que el **video no fuera grabado por el Sr. Armando** que estaba delante de la cámara, sino por una tercera persona con la que dicho Sr. se encontraba, **resulta irrelevante** a los efectos de atribuirle la responsabilidad de la infracción a la normativa de Protección de Datos, por cuanto **fue dicho Sr. Armando el que decidió subir o "colgar"** con terminología coloquial, dicho **video** del muro de **su perfil en Facebook**, desde el que era accesible a cualquier usuario de la citada red social, convirtiéndose de esta forma en **responsable del tratamiento**.

PUNTOS CLAVE

**Ley Orgánica Protección Datos y Garantía Derechos Digitales -LOPDGDD-.**

**Artículo 84. *Protección de los menores en Internet.***

1. *Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.*
2. *La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.*

En relación a **direcciones electrónicas de los usuarios** de las redes sociales, como pueden ser las de correo electrónico o e-mail, nuestra Audiencia Nacional también las ha considerado **datos personales**[82] en su sentencia de 30 de noviembre de 2018 dado que "... *[c]on independencia de que la denominación de la dirección corresponda o no con el nombre y apellido de su titular, país o empresa en la que trabaja, lo cierto es que se puede mediante una operación nada difícil, identificar perfectamente a una persona física, ya que esa dirección de correo electrónico aparecerá vinculada a un dominio concreto, por lo que sólo será necesario consultar al servidor en que se gestione dicho servicio*".

También los **nick-name o nombre de usuario** utilizados en redes sociales pueden ser considerados datos de carácter personal toda vez que el examen del perfil es muy probable que muestre indicios suficientes (fotografías, mensajes, vídeos, biografía, direcciones, etc.) para lograr la identificación sin necesidad de desarrollar un gran esfuerzo. Así lo declaró la Audiencia Nacional en la citada sentencia de 30 de noviembre de 2018[82] al destacar en su FD 2º que " "... *[l]a dirección de correo electrónico de una persona física, en la medida que permite identificar a su titular sin plazos ni actividades desproporcionadas, constituye un dato personal y su tratamiento en casos como el presente, y sin perjuicio de las previsiones específicas establecidas por la Ley de Servicios de Sociedad de la Información para otros supuestos, está sometido a las previsiones de la LOPD*".

Una de las características de las redes sociales es la **facilidad** de encontrar información y su **disponibilidad** para ser reutilizada por terceros que acceden a la misma, circunstancias las anteriores que **no eximen** del cumplimiento de la normativa de protección de datos.

**82** Audiencia Nacional, Sala Contencioso-administrativo, Secc 1ª, sentencia 30 noviembre 2018, rec. 302/2017. FD 2º.


**Colegio Concertado**
***Ruta de la Plata***
***Almendralejo.***

# XIII

## Tratamiento de datos por las AMPAS.

# XIII. Tratamiento de datos por las Asociaciones de Madres y Padres de Alumnos, AMPA.

Las asociaciones de madres y padres de alumnos (AMPA) son entidades con personalidad jurídica propia que forman parte de la comunidad educativa y desempeñan un papel significativo en la vida educativa al participar en el Consejo Escolar de los centros públicos.

Para el **ejercicio de sus funciones**, las AMPA suelen **tratar datos de carácter personal** como son los identificativos de los padres o tutores, de los alumnos, así como otros tipos de datos como pueden ser los económicos, profesionales, sociales, etc.

Al constituir las AMPAs entidades con personalidad jurídica propia tienen la capacidad de decidir sobre la finalidad, uso y contenido de los datos personales a recabar de los asociados y de sus hijos, por tanto, las **AMPA son responsables de su tratamiento**, por lo que deben cumplir con las obligaciones de la normativa de protección de datos.

## MARCO JURÍDICO de las AMPAs en la C.A de Extremadura.

### 1.- ¿Qué es una asociación de madres y padres de alumnos?

Se consideran asociaciones de madres y padres del alumnado aquellas que se constituyan en los centros docentes de titularidad pública o privada que impartan las enseñanzas reguladas en la Ley Orgánica 2/2006, de 3 de mayo, de Educación, en la Comunidad Autónoma de Extremadura[83].

### 2.- ¿Quiénes pueden ser miembros de las AMPA?

Pueden ser miembros de las asociaciones de madres y padres del alumnado, las madres y padres o, en su caso, tutores legales del alumnado que esté cursando estudios en los centros educativos que impartan las enseñanzas reguladas en la Ley Orgánica 2/2006, de 3 de mayo, de Educación, a que se refiere el artículo anterior[84].

**83** Decreto 111/2010, de 7 mayo, por el que se regulan las asociaciones de madres y padres de alumnos; **artículo 2**. (DOE nº 90 de 13 de mayo de 2010).
**84** Decreto 111/2010, de 7 mayo, por el que se regulan las asociaciones de madres y padres de alumnos; **artículo 3**. (DOE nº 90 de 13 de mayo de 2010).

IMPORTANTE

## FINES de las AMPAs:

a) Informar a las madres y padres de las actividades propias de la asociación y potenciar su participación activa en la vida de la misma.

b) Asistir a las familias en todo aquello que concierne a la educación de sus hijos.

c) Promover acciones formativas dirigidas a las familias con el fin de dar a conocer los derechos y deberes que como madres y padres asumen en el desarrollo de la educación de sus hijos.

d) Colaborar en las actividades educativas de los centros en el marco del proyecto educativo.

e) Promover la participación de las madres y padres en la gestión del centro, facilitar su representación y participación en los Consejos Escolares.

f) Promover la igualdad de derechos de todo el alumnado sin discriminación por razones socioeconómicas, confesionales, de raza o género o cualesquiera otras.

g) Defender los intereses de los padres, madres y tutores legales del alumnado.

h) Asesorar, orientar y ayudar a los padres, madres y tutores legales del alumnado en orden a la defensa y ejercicio de los derechos de sus hijos e hijas, y el mejor cumplimiento de sus deberes.

i) Promover todos aquellos aspectos que contribuyan al desarrollo de la educación integral del alumnado, los valores democráticos y la convivencia ciudadana.

j) Fomentar la participación de los padres, madres y tutores en la gestión democrática de la enseñanza.

k) Representar a los padres, madres y tutores, establecer relaciones y coordinar actuaciones con la propia Administración educativa, las Administraciones locales, los centros docentes y cualquier otra organización que promueva actividades educativas.

l) Cualesquiera otras que en el marco de la normativa vigente les asignen sus propios estatutos.

IMPORTANTE

## DERECHOS de las AMPAs:

**1.** Para el cumplimiento de sus fines las asociaciones de madres y padres del alumnado tendrán los siguientes **derechos**:

a) Presentar candidaturas diferenciadas para las elecciones de representantes de madres y padres al Consejo Escolar, en los términos que se establezcan.

b) Participar en cuantas acciones estén dirigidas a la elaboración y revisión del Proyecto Educativo del Centro.

c) Participar, a través de sus representantes, en cuantas actuaciones se desarrollen en el Consejo Escolar del centro y las comisiones que se constituyan.

d) Ser informados de todos los programas y actuaciones que se llevan a cabo en el centro y elaborar informes con la finalidad de mejorar aspectos concretos de la vida del centro.

e) Utilizar las instalaciones del centro para los fines propios de la asociación, siempre que no interfieran en el desarrollo de las actividades docentes y de las actividades y servicios complementarios, teniendo en cualquier caso un espacio claramente diferenciado para sus reuniones, en los términos que establezca el Consejo Escolar del centro.

f) Presentar y desarrollar proyectos de actividades extraescolares que se incorporen a la programación general anual, así como, en su caso, colaborar en el desarrollo de actividades y servicios complementarios.

g) Integrarse y/o constituir federaciones y confederaciones de asociaciones de madres y padres del alumnado con el fin de mejorar los cauces de comunicación con la Administración educativa y otros agentes de la comunidad escolar.

**2.** Asimismo, las asociaciones de madres y padres **podrán**:

a) Recibir información del Consejo Escolar sobre los temas tratados en el mismo, así como recibir el orden del día de dicho consejo antes de su realización, con el objeto de poder elaborar propuestas.

b) Conocer los resultados académicos y la valoración que de los mismos realice el Consejo Escolar.

c) Elevar al Consejo Escolar propuestas para la elaboración del Proyecto Educativo del Centro y de la Programación General Anual.

d) Recibir un ejemplar del Proyecto Educativo, de los Proyectos Curriculares de Etapa y de sus modificaciones.

e) Recibir información sobre los libros de texto y los materiales didácticos adoptados por el centro.

IMPORTANTE

## Cómo es el PLAN ANUAL de actividades del AMPA:

1. Las asociaciones de madres y padres del alumnado planificarán anualmente su actividad de acuerdo con los fines que tienen encomendados, a cuyos efectos elaborarán un plan de actividades.
2. El plan anual de actividades será presentado a la Dirección del centro y al Consejo Escolar.
3. Las actividades dirigidas a informar, asesorar y formar a madres y padres podrán ir destinadas a todos ellos, indistintamente de que pertenezcan, o no, a la asociación.
4. De las actividades organizadas por la asociación de madres y padres podrá participar todo el alumnado, cuando vaya dirigido a éstos.
5. El desarrollo de las actividades en ningún caso estará dirigido a la obtención de lucro por la realización o prestación de las mismas.

## Cuestiones de las AMPAs en materia de protección de datos.

### 1.- ¿Necesitan las AMPA obtener el consentimiento para recabar y tratar los datos de sus asociados y de sus hijos alumnos?

Depende de que los padres sean o no asociados al AMPA:

- Padres **asociados** al AMPA: el tratamiento estará amparado por la relación que vincula al AMPA con sus asociados, por lo que no será necesario el consentimiento de los progenitores pero sí que será obligatorio informarles acerca del tratamiento de sus datos personales.
- Padres **NO asociados** al AMPA: debe obtenerse el consentimiento.

### 2.- ¿Pueden los centros educativos facilitar a las AMPA la información personal de los alumnos y de sus familias para poder dirigirse a ellos?

Pueden facilitarla si son asociados al AMPA.

En el supuesto de que **NO** sean asociados al AMPA únicamente podrá el centro facilitar la información si dispone del **consentimiento previo** de los alumnos mayores de catorce años o, si son alumnos menores de 14 años, el de sus padres o tutores. En este supuesto los centros podrán recabar el consentimiento de los interesados a estos efectos, a los que habrá también que informar de la finalidad de la comunicación de datos y de sus derechos en materia de protección de datos.

### 3.- ¿Pueden las AMPA tratar los datos de los alumnos por cuenta del centro educativo?

Las AMPA únicamente pueden tratar los datos de los alumnos por cuenta del centro educativo (responsable del tratamiento) en aquellos casos en los que las propias AMPA le presten al centro un servicio que requiera el tratamiento de dichos datos, por ejemplo, que la AMPA se haga cargo de la prestación del servicio de comedor o del transporte escolar, actuando en estos supuestos la AMPA como un encargado del tratamiento y, por tanto, requiere la existencia de un contrato[85] que incluya las garantías adecuadas.

### 4.- ¿Pueden las AMPA publicar en su web los datos de los alumnos apuntados a un viaje fin de curso?

Podrán si cuentan con su consentimiento, o el de sus padres si son menores de 14 años.

### 5.- ¿Y las imágenes de los alumnos o de sus familiares en su web o en las redes sociales?

Igualmente, sólo en el caso de que dispongan del consentimiento de los interesados: alumnos y/o familiares, previa información sobre la finalidad de la publicación.

**85** RGPD. Artículo 28.3.


**Colegio Concertado**
***Ruta de la Plata***
***Almendralejo.***

# XIV

## Derechos en Protección de Datos.

# XIV. Los derechos en materia de Protección de Datos.

Hemos visto en las lecciones anteriores como la normativa de Protección de Datos establecía toda una serie de obligaciones en relación al tratamiento de los datos, ahora vamos a **estudiar los derechos** que esta normativa reconoce a los interesados y los mecanismos adecuados para hacerlos efectivos y se cumplan.

Vivimos en una era digitalizada que se alimenta de datos y donde las actividades de tratamiento son omnipresentes, lo anterior tiene consecuencias directas sobre las personas físicas por lo que la normativa de Protección de Datos les confiere diversos **derechos** para garantía de un mayor control sobre el tratamiento de sus datos, derechos éstos cuyo respeto y observancia se convierten en **obligaciones** para el responsable del tratamiento. Además de otorgarles derechos, la normativa también establece los **mecanismos** de protección que permiten a los interesados denunciar las violaciones de sus derechos, exigir responsabilidades a los responsables del tratamiento y reclamar indemnizaciones que resulten pertinentes.


Todos los interesados tienen derecho a ser **informados** acerca de cualquier tratamiento de sus datos personales que pueda estar efectuando un responsable, sujeto a exenciones limitadas.

Los interesados tendrán **derecho** a:

- obtener **acceso** a sus propios datos y cierta información sobre el tratamiento;
- que sus datos sean **rectificados** por el responsable del tratamiento en el caso de que sean inexactos;
- que el responsable del tratamiento **suprima** sus datos, si procede, en el caso de que esté efectuando el tratamiento de manera ilegal;
- **limitar** el tratamiento temporalmente;
- la **portabilidad** de sus datos a otro responsable en determinadas condiciones.

Además, los interesados tendrán derecho a **oponerse** al tratamiento:

- por razones relacionadas con su situación particular;
- cuando sus datos se utilicen con fines de mercadotecnia directa.

Los interesados tienen derecho a **no ser objeto de decisiones** basadas exclusivamente en un tratamiento **automatizado**, incluida la elaboración de perfiles, que tengan efectos jurídicos o que les afecten de manera significativa. Los interesados también tienen derecho a:

- obtener intervención humana por parte del responsable del tratamiento;
- expresar su punto de vista e impugnar las decisiones basadas en el tratamiento automatizado.

## El **DERECHO** a ser **INFORMADO.**

El responsable del tratamiento tiene el **deber** de informar al interesado sobre el tratamiento previsto sobre sus datos personales, y, el interesado tiene el **derecho** a ser informado de acerca de la existencia de tal tratamiento en el momento en que se recojan (o recaben) sus datos personales.

El derecho-deber de informar al interesado no se supedita a la previa petición de éste al responsable del tratamiento, sino que **debe ser cumplido** por éste de forma **proactiva**, lo anterior con absoluta independencia de si el titular de los datos de carácter personal muestra interés en la información o no.

El derecho a ser informado entronca de forma directa con el principio de transparencia en el tratamiento de los datos personales. Para las personas físicas debe quedar **totalmente claro** que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, de esta forma el principio de transparencia **exige** que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. También exige el principio de transparencia que **se informe** a los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben **tener conocimiento** de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento[86].

El RGPD distingue entre dos escenarios y dos momentos en los que el responsable del tratamiento debe facilitar información a los interesados:

- Cuando los datos personales se obtengan directamente del interesado[87], el responsable deberá comunicar al interesado toda su información y los derechos que le asisten en virtud del RGPD en el **momento de obtener los datos**.

  **OJO->** Si el responsable tiene intención de realizar un tratamiento ulterior de los datos personales con un **fin distinto**, deberá facilitar toda la información pertinente antes de llevar a cabo el tratamiento.

- Cuando los datos personales **NO** se hayan obtenido del interesado[88], el responsable está obligado a facilitar la información sobre el tratamiento al interesado «*dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes*», o antes de comunicar los datos a un tercero.

**86** RGPD. Considerando 39 y artículo 12. Convenio 108 modernizado, artículo 9.1.b).
**87** RGPD. Artículo 13.
**88** RGPD. Artículo 14.

IMPORTANTE

**EXCEPCIONES al deber de informar.**

La normativa de protección de datos contempla ciertas excepciones a la obligación de informar que no será de aplicación:

- Cuando el interesado ya dispone de toda la información pertinente.
- Si los datos no se han obtenido del interesado, decae la obligación de informar cuando la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.
- Cuando los Estados miembros de la UE los consideren una medida necesaria y proporcionada en una sociedad democrática, por ejemplo, para salvaguardar la seguridad nacional y pública, la defensa, la protección de las investigaciones y los procedimientos judiciales o la protección de intereses económicos y financieros, así como intereses privados que sean más imperiosos que los intereses de protección de los datos.

## El DERECHO de ACCESO a los propios datos.

El derecho de acceso **permite** a los titulares de los datos personales conocer y obtener gratuitamente información sobre si sus datos de carácter personal están siendo objeto de tratamiento, con qué finalidad, qué tipo de datos tiene el responsable del tratamiento, su origen, si no proceden de los interesados, y los destinatarios de los datos.

Es un derecho expresamente reconocido por el RGPD[89] y establece que toda persona física tiene derecho a obtener, cuando lo solicite, información acerca del tratamiento de datos personales relacionados con ella, y que le sea comunicada de manera inteligible.

PUNTOS CLAVE

**Carta de los Derechos Fundamentales de la Unión Europea -CDFUE-.**

**Artículo 8.** *Protección de datos de carácter personal.*

1. *Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*
2. *Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona* ***tiene derecho a acceder a los datos recogidos que la conciernan*** *y a su rectificación.*
3. *El respeto de estas normas quedará sujeto al control de una autoridad independiente.*

**89** RGPD. Artículo 15.

IMPORTANTE

## Derecho de ACCESO, el artículo 15 del RGPD:

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:
   a) los fines del tratamiento;
   b) las categorías de datos personales de que se trate;
   c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
   d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
   e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
   f) el derecho a presentar una reclamación ante una autoridad de control;
   g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
   h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.
3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.
4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso **sin especificar si se refiere a todos o a una parte de los datos**, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un **sistema de acceso** remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad.

Se podrá considerar **repetitivo** el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.

### 1.- ¿Qué obligación tienen los centros o las Administraciones educativas de responder a una solicitud de derecho de acceso?

Los responsables del tratamiento, en el **plazo de un mes**, han de facilitar a los interesados la información sobre sus datos personales o, en su caso, respuesta de que no disponen de ellos.

Esta obligación se puede **cumplir de varias maneras**:

- visualización en pantalla,
- escrito,
- copia o fotocopia,
- correo electrónico o cualquier otro sistema de comunicaciones electrónico o que resulte adecuado.

Si la solicitud de acceso se formula por **medios electrónicos**, se facilitará en un formato electrónico de uso común, salvo que se hubiera solicitado recibirla de otro modo.

### 2.- ¿El cumplimiento del derecho de acceso obliga a facilitar copia del expediente escolar?

El derecho de acceso a los datos personales es **independiente** del derecho de acceso al expediente, a la información y documentación, que se rigen por otra normativa. Conforme a la normativa de protección de datos, no hay obligación de facilitar copia del expediente escolar, sin perjuicio del acceso a la información en el marco de la legislación sectorial.

El RGPD establece que el responsable del tratamiento facilitará una copia de los datos personales de los interesados que, en ningún caso, afectará negativamente a los derechos y libertades de otros.

### 3.- ¿Y si en ese expediente hay datos de salud?

La documentación relativa a los datos de salud recibe el tratamiento de información clínica cuya copia hay que facilitar a los interesados, en aplicación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y de las leyes autonómicas.

### 4.- ¿Se puede cobrar por facilitar el derecho de acceso?

No, la información que se facilite tiene que ser gratuita. No obstante, si el centro o la Administración educativa ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido, los gastos derivados de su elección serán por cuenta del afectado.

**EJEMPLO:**

El acceso a sus datos personales ayudará al interesado a determinar si los datos son precisos o no. Por tanto, es esencial que se comuniquen al interesado, de manera inteligible, no solo los datos personales propiamente dichos que son objeto de tratamiento, sino también las categorías de datos que se tratan, como el nombre, la dirección IP, las coordenadas de geolocalización, el número de tarjeta de crédito, etc.

## El DERECHO de RECTIFICACIÓN.

El derecho de rectificación **permite** corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento. La exactitud de los datos personales es esencial para garantizar un alto nivel de protección de datos para los interesados.

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional[90].

IMPORTANTE

Al ejercer el derecho de rectificación el afectado **deberá** indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

### 1.- ¿Pueden los alumnos solicitar la rectificación de los datos de su expediente escolar?

**SÍ**, siempre que se constate un error. El centro o la Administración educativa tendrán que corregirlo siempre que se acredite el error. Se podrá ejercitar tantas veces como errores se adviertan, no obstante si el interesado es un menor de 14 años, lo tienen que ejercer sus padres o tutores.

Este derecho de rectificación **no se aplica** a las calificaciones o al contenido de los informes del expediente escolar que se rigen por su normativa específica.

### 2.- ¿Puede ejercitarse el derecho de rectificación para modificar un informe de evaluación psicopedagógica?

**NO**, el derecho de rectificación permite modificar los datos de carácter personal que sean inexactos o incompletos (p.ej, el cambio de la dirección postal), pero su ejercicio no se puede utilizar para tratar de modificar la opinión realizada por un profesional a través del correspondiente informe al regirse éste por su normativa específica.

**90** RGPD. Artículo 16.

## El **DERECHO** de **SUPRESIÓN** («el derecho al olvido»).

Permite que se supriman los datos que resulten ser inadecuados o excesivos. La revocación del consentimiento da lugar a la cancelación de los datos cuando su tratamiento esté basado en él, pero sin efecto retroactivo.

Es especialmente importante asegurar el derecho de los interesados a la supresión de sus propios datos para la aplicación efectiva de los principios de protección de datos, y en particular del principio de minimización de datos (*los datos personales deben limitarse a lo necesario para los fines del tratamiento de dichos datos*).

El Convenio 108 modernizado reconoce expresamente que todas las personas físicas tienen derecho a que se supriman datos inexactos, falsos o tratados de forma ilícita[91].

IMPORTANTE

### Derecho de SUPRESIÓN, el artículo 17 del RGPD:

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:
   a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
   b) el interesado retire el consentimiento en que se basa el tratamiento (...) y este no se base en otro fundamento jurídico;
   c) el interesado se oponga al tratamiento con arreglo al artículo 21.1 y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21.2;
   d) los datos personales hayan sido tratados ilícitamente;
   e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
   f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información en relación con la oferta directa a niños.
2. [Derecho al olvido] Cuando haya hecho públicos los datos personales (entorno online) y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

**91** Convenio 108 modernizado, artículo 9, apartado 1, letra e).

IMPORTANTE

**LÍMITES al derecho de supresión.**

No se aplicará el derecho a la supresión cuando el tratamiento sea necesario:

- Para ejercer el derecho a la **libertad de expresión e información**;
- 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;
- Por razones de interés público en el ámbito de la salud pública;
- El tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.
- Para la formulación, el ejercicio o la defensa de reclamaciones.

### 1.- ¿Tienen los centros educativos que suprimir la información de los EXPEDIENTES ACADÉMICOS a solicitud de los alumnos, de sus padres o tutores?

Sin perjuicio de lo establecido en la normativa de educación aplicable, la información de los expedientes académicos requiere su conservación en la medida en que puede ser solicitada por los alumnos después de finalizados los estudios.

### 2.- ¿Y de los datos de SALUD obtenidos por el Equipo de Orientación Educativa?

Se suprimirán cuando no sean necesarios para el desarrollo de la función educativa y, en su caso, al finalizar la escolarización del alumno en el centro, por ejemplo, los datos sobre las alergias alimentarias.

### 3.- ¿Qué es el DERECHO AL OLVIDO?

Es un derecho que persigue garantizar al interesado, persona física, un control sobre sus datos de carácter personal, en particular, en el ámbito electrónico. Por tanto, el derecho al olvido habilita a la persona física titular de los datos a instar al responsable del tratamiento a que, cuando concurran los requisitos de aplicables, proceda a la supresión de los enlaces, copias o réplicas de los datos.

El RGPD destaca que *a fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales*[92].

**92** RGPD. Considerando 66.

### 4.- Derecho al olvido en los NIÑOS.

En relación al derecho al olvido on line en los niños, este derecho resulta pertinente y debe ser estimado de conformidad con el considerando 65 del RGPD donde se detallan los supuestos donde el interesado dio su consentimiento siendo un niño y no era consciente de los riesgos que ello implicaba resultando que, más tarde, desea ejercer su derecho de supresión sobre tales datos personales, por tanto, reiteramos que sería procedente la supresión.

En nada afecta al derecho de supresión el hecho de que el interesado ejerza su derecho una vez alcanzada la mayoría de edad que habilita el consentimiento (mayor de 14 años) toda vez que se reconoce a la persona física titular de los datos el derecho a solicitar "el olvido" de sus datos personales (supresión) sobre la base de su consentimiento cuando era un niño y ahora no quiere que se sigan tratando.

### 5.- Derecho al olvido en BÚSQUEDAS por Internet.

Toda persona tiene derecho a que los **motores de búsqueda en Internet** eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre[93] los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen:

- inadecuados,
- inexactos,
- no pertinentes,
- no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo,

lo anterior teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

### 6.- Derecho al olvido en servicios de REDES SOCIALES y servicios equivalentes.

Toda persona tiene derecho a que sean suprimidos, **a su simple solicitud**, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

**93** LOPDGDD. Artículo 93.

Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido **facilitados por terceros** para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información[94].

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se **exceptúan** de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su **minoría de edad**, el prestador deberá proceder sin dilación a su supresión por su simple solicitud.

## El DERECHO de OPOSICIÓN.

El derecho de oposición es el derecho del interesado a que, por motivos relacionados con su situación personal, no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo.

No obstante, debemos destacar que en los supuestos en que el tratamiento se encuentre legitimado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, pueden existir **excepciones** al derecho de oposición.

La Agencia de Protección de Datos destaca sobre este derecho[95] lo siguiente:

Este derecho, como su nombre indica, supone que te puedes oponer a que el responsable realice un tratamiento de los datos personales en los siguientes supuestos:

- Cuando sean objeto de tratamiento basado en una **misión de interés público o en el interés legítimo**, incluido la elaboración de perfiles:

  El responsable dejará de tratar los datos salvo que acredite motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

- Cuando el tratamiento tenga como finalidad la **mercadotecnia directa**, incluida también la **elaboración de perfiles** anteriormente citada:

  Ejercitado este derecho para esta finalidad, los datos personales dejarán de ser tratados para dichos fines.

**94** LOPDGDD. Artículo 94.
**95** https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-oposicion

Es importante destacar que en el supuesto de ejercicio del derecho de oposición y que éste sea estimado, el responsable del tratamiento tendría que buscar otra base de legitimación del tratamiento de los datos.

### 1.- ¿Qué ocurre si el responsable del tratamiento no atiende a la oposición?

La consecuencia de no atender al ejercicio del derecho de oposición implica que *un tratamiento de datos hasta ese momento lícito (...) puede devenir ilícito si no se atiende a las especiales circunstancias invocadas por el interesado al tiempo de ejercitar su derecho*[96].

### 2.- ¿Cuando podrá tratar los datos el responsable del tratamiento a pesar de existir una oposición basada en una situación particular?

El interesado tiene derecho a oponerse al tratamiento de los datos cuando tenga motivos relacionados con su situación particular, no obstante, a pesar de la oposición del titular el responsable del tratamiento podrá tratar los datos cuando:

- Acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o
- para la formulación, el ejercicio o la defensa frente a reclamaciones.

### 3.- ¿Pueden los alumnos o los familiares oponerse a la publicidad de sus datos?

Sí, cuando exista un motivo legítimo y fundado, referido a una concreta situación personal, para oponerse a la publicidad de su información personal.

Por ejemplo, en los casos en los que se ha acordado por los jueces el alejamiento de uno de los progenitores o se le ha privado de la patria potestad y la publicidad de información personal pueda suponer un riesgo para la integridad física y psíquica del alumno o del otro progenitor.

## El DERECHO de LIMITACIÓN al tratamiento.

Es uno de los nuevos derechos que introduce el Reglamento General de Protección de Datos, así, el derecho de limitación al tratamiento es el "*marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro*" según las condiciones establecidas en el artículo 18 del RGPD.

La Agencia de Protección de Datos destaca sobre este derecho[97] lo siguiente:

Este nuevo derecho consiste en que obtengas la limitación del tratamiento de tus datos que realiza el responsable, si bien su ejercicio presenta dos vertientes:

Puedes solicitar la **suspensión** del tratamiento de tus datos:

- Cuando impugnes la exactitud de tus datos personales, durante un plazo que permita al responsable su verificación.

**96** Agencia Española de Protección de Datos -AEPD- Informe jurídico 0389/2009.
**97** https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-la-limitacion-del-tratamiento

- Cuando te hayas opuesto al tratamiento de tus datos personales que el responsable realiza en base al interés legítimo o misión de interés público, mientras aquel verifica si estos motivos prevalecen sobre los tuyos.

Solicitar al responsable la **conservación** tus datos:

- Cuando el tratamiento sea ilícito y te has opuesto a la supresión de tus datos y en su lugar solicitas la limitación de su uso.
- Cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

**IMPORTANTE**

El **derecho de limitación** del tratamiento **habilita al interesado a solicitar del responsable** del tratamiento a que **aplique las medidas necesarias** sobre los datos con la finalidad de **evitar** su **modificación** o, en su caso, que se **borren o supriman**.

Una vez ejercido el derecho de limitación el responsable del tratamiento facilitará que el titular de los datos pueda formular reclamaciones o, llegado el caso, los datos se conserven como prueba de un presunto tratamiento ilícito.

El responsable debe **informar** al interesado **ANTES** de que se **levante** la limitación del tratamiento.

## 1.- ¿Qué medidas debe aplicar el responsable para limitar el tratamiento?

El RGPD nos indica al respecto[98] que *entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema*.

## 2.- ¿Qué condiciones tienen que concurrir para que proceda el derecho a la limitación en el tratamiento de datos de carácter personal?

El RGPD prevé que el interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes[99]:

a. **El interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos**.

   El titular de los datos considera que éstos no son exactos y formula reclamación al responsable quien deberá limitar el tratamiento hasta verificar su exactitud.

**98** RGPD. Considerando 67.
**99** RGPD. Artículo 18, apartado 1º.

**b. El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.**

En ese supuesto el interesado pretende que los datos no sean borrados o suprimidos por el responsable del tratamiento y se conserven con limitación de uso al objeto de servir de prueba, pudiendo utilizarse posteriormente dicha prueba ante un eventual procedimiento ante la Agencia Española de Protección de Datos o los juzgados o tribunales.

**c. El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.**

El responsable del tratamiento deberá conservar los datos del interesado al objeto de dar cumplimiento al derecho de limitación del tratamiento.

**d. El interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.**

Esto es, que el interesado se oponga al tratamiento:

1. Sobre la base de la necesidad del mismo para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, o
2. Interés legítimo, incluida en ambos casos la elaboración de perfiles.

IMPORTANTE

Cuando el tratamiento de datos personales se haya limitado, dichos datos **solo podrán ser objeto de tratamiento** por el responsable, con excepción de su conservación:

- Con el **consentimiento** del interesado,
- Para la formulación, el ejercicio o la defensa de **reclamaciones**,
- Con miras a la **protección** de los derechos de otra persona física o jurídica,
- Por razones de **interés público** importante de la Unión o de un determinado Estado miembro.

## 3.- ¿Tiene alguna OBLIGACIÓN ESPECÍFICA DE INFORMACIÓN el responsable del tratamiento en relación al derecho de limitación del tratamiento?

Sí, tiene dos:

1. **A la finalización de la limitación**: el responsable deberá informar al interesado con carácter previo a que se levante la limitación del tratamiento y, una vez informado, podrá proceder a poner fin a la limitación.

2. **Comunicación de la limitación del tratamiento a los destinatarios**: Es deber del responsable del tratamiento el informar de la limitación del mismo a cada uno de los destinatarios a los que haya comunicado los datos personales, salvo que dicho acto resulte imposible o exija un esfuerzo desproporcionado.

### 4.- ¿Que diferencia existe entre LIMITACIÓN y BLOQUEO de los datos?

Debemos partir de la diferencia existente entre el derecho a la limitación del tratamiento y la obligación de conservación de los datos de carácter personal.

La LOPDGDD nos dice que *el responsable del tratamiento estará obligado a* ***bloquear*** *los datos cuando proceda a su rectificación o supresión. El bloqueo de los datos* ***consiste*** *en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización,* **excepto** *para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas*[100].

Así, en la **limitación se permite el tratamiento** y, por contra, en el **bloqueo** el responsable **debe impedir el tratamiento** toda vez que los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada.

## El DERECHO de PORTABILIDAD.

En virtud del RGPD, los interesados gozan del derecho a la portabilidad de sus datos en circunstancias en que los datos personales que hayan facilitado a un responsable sean objeto de tratamiento por medios automatizados o cuando el tratamiento de los datos personales sea necesario para cumplir un contrato y se lleve a cabo de forma automatizada.

Esto significa que el derecho a la portabilidad de los datos no será de aplicación en situaciones en que el tratamiento de los datos personales tenga un fundamento jurídico que no sea el consentimiento o un contrato.

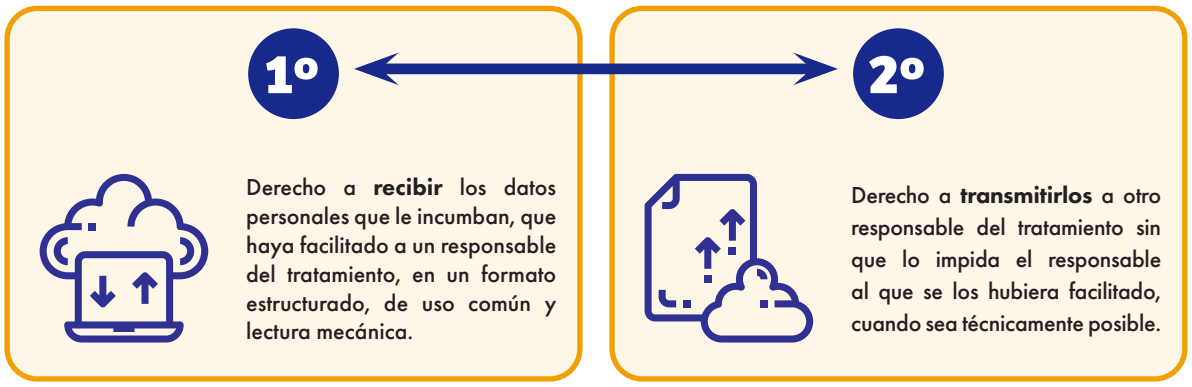
**IMPORTANTE**

La persona física cuyos datos son objeto de tratamiento automatizado, basado en el consentimiento o el cumplimiento de un contrato, y que ejercite su derecho de portabilidad **obtendrá** los mismos del responsable o logrará que se transmitan a otro responsable de su interés.

La portabilidad **otorga** al interesado el derecho a obtener del responsable del tratamiento una parte de sus datos personales o poder reutilizarlos.

**100** LOPDGDD. Artículo 32, apartados 1º y 2º.

**Resumen gráfico del derecho a la portabilidad.**




### 1.- ¿Tiene alguna limitación el derecho a la portabilidad de los datos?

Existen varios supuestos donde no será posible ejercer el derecho a la portabilidad de los datos de carácter personal cuando[101]:

- Los datos personales, siempre que se cumplan los requisitos aplicables en cuanto a la base de legitimación del tratamiento y que dicho tratamiento sea automatizado, no hayan sido proporcionados por el interesado, es decir, han sido inferidos o deducidos por el responsable del tratamiento, a dicho datos no aplicará el derecho a la portabilidad.
- Atendiendo a la base de legitimación del tratamiento, se traten sobre una base de legitimación diferente al consentimiento del interesado o el cumplimiento de un contrato en el que el interesado es parte.
- Los datos personales se refieran a terceros, es decir, a otras personas físicas. Y el ejercicio de este derecho no podrá afectar negativamente a los derechos y libertades de otros.
- La condición que legitima el tratamiento de los datos personales del interesado no sea el consentimiento o el incumplimiento de un contrato.
- En el supuesto de que los datos sean suprimidos o anonimizados, dado que a dichos datos les dejaría de ser aplicable la normativa de protección de datos.

## El **EJERCICIO** de los derechos en materia de Protección de Datos.

La Agencia Española de Protección de Datos -AEPD- nos recuerda como la normativa de protección de datos permite que puedas ejercer ante el responsable del tratamiento tus derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas[102].

**101** Recio, M. *El ejercicio de los derechos de protección de datos y su aplicación práctica.* Ed. Bosch. 1ª. 2019. Pags 61 y 62
**102** AEPD. https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos

Estos derechos se caracterizan por lo siguiente:

- Su ejercicio es gratuito.
- Si las solicitudes son manifiestamente infundadas o excesivas (p. ej., carácter repetitivo) el responsable podrá:
  - Cobrar un canon proporcional a los costes administrativos soportados.
  - Negarse a actuar.
- Las solicitudes deben responderse en el plazo de 1 mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros 2 meses más.
- El responsable está obligado a informarte sobre los medios para ejercitar estos derechos. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que optes por otro medio.
- Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo.
- Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control (Agencia Española de Protección de Datos).
- Cabe la posibilidad de que el encargado sea quien atienda tu solicitud por cuenta del responsable si ambos lo han establecido en el contrato o acto jurídico que les vincule.

## 1.- ¿Quiénes pueden ejercitar estos derechos en educación?

Los derechos en Protección de Datos tienen carácter personalísimo, lo que significa que sólo pueden ser ejercidos por sus titulares o sus representantes legales. En el caso de los menores de 14 años, los padres, cuando ostenten la patria potestad, o los tutores podrán ejercitarlos en su nombre. Si son mayores de esa edad lo podrán ejercitar los propios alumnos o sus representantes legales, que igualmente pueden ser sus padres.

Si se trata de los datos de los padres serán éstos los legitimados para ejercitarlos.

## 2.- ¿Ante quién se ejercitan los derechos?

Se ejercitan ante los responsables del tratamiento: los centros educativos o las Administraciones educativas.

## 3.- ¿Hay obligación de contestar a los interesados?

Sí, siempre, aunque no se disponga de los datos sobre los que verse el derecho ejercitado, en cuyo caso habrá que responder en dicho sentido. También deberá informarle del derecho a presentar, en su caso, una reclamación ante la Agencia Española de Protección de Datos.

**EJERCICIO DEL DERECHO DE ACCESO**

**DATOS DEL RESPONSABLE DEL TRATAMIENTO.**

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

**DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico……..por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

**SOLICITA**

Que se le facilite gratuitamente el derecho de acceso por ese responsable en el plazo de un mes a contar desde la recepción de esta solicitud, y que se remita, a la dirección arriba indicada, la siguiente información:

-Copia de mis datos personales que son objeto de tratamiento por ese responsable.
-Los fines del tratamiento así como las categorías de datos personales que se traten.
-Los destinatarios o categorías de destinarios a los que se han comunicado mis datos personales, o serán comunicados, incluyendo, en su caso, destinatarios en terceros u organizaciones internacionales.
-Información sobre las garantías adecuadas relativas a la transferencia de mis datos a un tercer país o a una organización internacional, en su caso.
-El plazo previsto de conservación, o de no ser posible, los criterios para determinar este plazo.
-Si existen decisiones automatizadas, incluyendo la elaboración de perfiles, información significativa sobre la lógica aplicada, así como la importancia y consecuencias previstas de dicho tratamiento.
-Si mis datos personales no se han obtenido directamente de mí, la información disponible sobre su origen.
-La existencia del derecho a solicitar la rectificación, supresión o limitación del tratamiento de mis datos personales, o a oponerme a dicho tratamiento.
-El derecho a presentar una reclamación ante una autoridad de control.

En .....a.....de.....de 20.....

**INSTRUCCIONES**

**1.** Será necesario aportar fotocopia del D.N.I. o documento equivalente que acredite la identidad y sea considerado válido en derecho, en aquellos supuestos en que el responsable tenga dudas sobre su identidad. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

**2.** Se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.

**3.** La Agencia Española de Protección de Datos no dispone de sus datos personales y sólo puede facilitar los datos de contacto de los Delegados de Protección de Datos de las entidades obligadas a designar uno que hubieren comunicado su nombramiento a la Agencia. También puede facilitar estos datos de contacto respecto a aquellas entidades que hayan designado un Delegado de forma voluntaria y lo hayan comunicado.

**4.** El titular de los datos personales objeto de tratamiento debe dirigirse directamente ante el organismo público o privado, empresa o profesional del que presume o tiene la certeza de que posee sus datos.

**5.** Para que la Agencia Española de Protección de Datos pueda tramitar su reclamación en caso de no haber sido atendida su solicitud de ejercicio del derecho de acceso, resulta necesario que haya transcurrido un mes desde la presentación de la solicitud por la que se ejercita el derecho de acceso, y que se aporte, junto con el escrito que en su caso haya recibido del responsable del tratamiento, alguno de los siguientes documentos:

•copia del modelo de solicitud de acceso sellada por el responsable del tratamiento.

•copia del modelo de solicitud de acceso sellada por la oficina de correos o copia del resguardo del envío por correo certificado.

•cualesquiera otros medios de prueba facilitados por el responsable del tratamiento y de los que se pueda deducir la recepción de la solicitud.

**6.** Este derecho de acceso es independiente del derecho de acceso a la información pública que regula la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno. También es independiente del derecho de acceso a la documentación en un procedimiento administrativo cuando se ostenta la condición de interesado, regulado por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. El acceso a la historia clínica se regula por la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, si bien la AEPD es competente para atender este acceso en caso de que una vez ejercitado, la respuesta no sea satisfactoria para el ciudadano, o no se haya respondido. Además, esta Ley permite el acceso a la historia clínica de los pacientes fallecidos a personas vinculadas con él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite.

**EJERCICIO DERECHO DE RECTIFICACIÓN**

**DATOS DEL RESPONSABLE DEL TRATAMIENTO.**

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de rectificación: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

**DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico……..por medio del presente escrito ejerce el derecho de rectificación, de conformidad con lo previsto en el artículo 16 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

**SOLICITA**

Que se proceda a acordar la rectificación de los datos personales, que se realice en el plazo de un mes a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la rectificación practicada.

Datos sobre los que solicito el derecho de rectificación:

Que en caso de que se acuerde que no procede practicar la rectificación solicitada, se me comunique motivadamente a fin de, en su caso, reclamar ante la Autoridad de control que corresponda.

Asimismo, en caso de que mis datos personales hayan sido comunicados por ese responsable a otros responsables del tratamiento, se comunique esta rectificación a los mismos.

En .....a.....de.....de 20.....

Firmado:

**INSTRUCCIONES**

**1.** Este modelo se utilizará para el caso de que se deban rectificar datos inexactos o incompletos por parte del responsable del tratamiento.

**2.** Para probar el carácter inexacto o incompleto de los datos que se estén tratando resulta necesaria la aportación de la documentación que lo acredite al responsable del tratamiento.

**3.** Será necesario aportar fotocopia del D.N.I. o documento equivalente que acredite la identidad y sea considerado válido en derecho, en aquellos supuestos en que el responsable tenga dudas sobre su identidad. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

**4**. La Agencia Española de Protección de Datos no dispone de sus datos personales y sólo puede facilitar los datos de contacto de los Delegados de Protección de Datos de las entidades obligadas a designar uno que hubieren comunicado su nombramiento a la Agencia. También puede facilitar estos datos de contacto respecto a aquellas entidades que hayan designado un Delegado de forma voluntaria y lo hayan comunicado.

**5.** El titular de los datos personales objeto de tratamiento debe dirigirse directamente ante el organismo público o privado, empresa o profesional del que presume o tiene la certeza que posee sus datos.

**6.** Para que la Agencia Española de Protección de Datos pueda tramitar su reclamación en caso de no haber sido atendida su solicitud de ejercicio del derecho de rectificación, resulta necesario que hayan transcurrido un mes sin que el responsable haya respondido a su petición, y aporte alguno de los siguientes documentos:

• la negativa del responsable del tratamiento a la rectificación de los datos solicitados.

• copia sellada por el responsable del tratamiento del modelo de petición de rectificación.

• copia del modelo de solicitud de rectificación sellada por la oficina de correos o copia del resguardo del envío por correo certificado.

• cualesquiera otros medios de prueba facilitados por el responsable del tratamiento y de los que se pueda deducir la recepción de la solicitud.

**EJERCICIO DEL DERECHO A LA LIMITACIÓN DEL TRATAMIENTO**

**DATOS DEL RESPONSABLE DEL TRATAMIENTO.**

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de limitación: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

**DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ....., Comunidad Autónoma ..... con D.N.I....., con correo electrónico ……..,por medio del presente escrito ejerce el derecho de limitación, de conformidad con lo previsto en el artículo 18 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

SOLICITO

Que se limite el tratamiento de mis datos personales, teniendo en consideración:

☐ Que el tratamiento es ilícito y me opongo a su supresión.

☐ Que el responsable ya no necesita mis datos personales para los fines para los cuales fueron recabados, pero los necesito para la formulación, ejercicio o defensa de mis reclamaciones.

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes, y que se comunique esta limitación a cada uno de los destinatarios que ese responsable del tratamiento haya comunicado mis datos personales.

En .....a.....de.....de 20.....

Firmado:

**INSTRUCCIONES**

**1.** Este modelo se utilizará por el afectado que desee solicitar al responsable que limite el tratamiento de sus datos personales cuando proceda alguna de las siguientes situaciones:

- El tratamiento de sus datos personales es ilícito y el afectado se oponga a la supresión de sus datos personales;

-El responsable ya no necesita los datos personales para los fines del tratamiento, pero el afectado los necesita para la formulación, el ejercicio o defensa de sus reclamaciones.

**2.** Será necesario aportar fotocopia del D.N.I. o documento equivalente que acredite la identidad y sea considerado válido en derecho, en aquellos supuestos en que el responsable tenga dudas sobre su identidad. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

**3.** La Agencia Española de Protección de Datos no dispone de sus datos personales y sólo puede facilitar los datos de contacto de los Delegados de Protección de Datos de las entidades obligadas a designar uno que hubieren comunicado su nombramiento a la Agencia. También puede facilitar estos datos de contacto respecto a aquellas entidades que hayan designado un Delegado de forma voluntaria y lo hayan comunicado.

**4.** El titular de los datos personales objeto de tratamiento debe dirigirse directamente ante el organismo público o privado, empresa o profesional del que presume o tiene la certeza que posee sus datos.

**5.** Para que la Agencia Española de Protección de Datos pueda tramitar su reclamación en caso de no haber sido atendida su solicitud de ejercicio del derecho a la limitación del tratamiento en el plazo máximo de un mes, y aporte alguno de los siguientes documentos:

•la negativa del responsable del tratamiento a la limitación del tratamiento de los datos solicitados.

•copia sellada por el responsable del tratamiento del modelo de petición de limitación del tratamiento.

•copia del modelo de solicitud de limitación del tratamiento sellada por la oficina de correos o copia del resguardo del envío por correo certificado.

•cualesquiera otros medios de prueba facilitados por el responsable del tratamiento y de los que se pueda deducir la recepción de la solicitud.

**EJERCICIO DEL DERECHO DE OPOSICIÓN (Modelo A)**

**DATOS DEL RESPONSABLE DEL TRATAMIENTO.**

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de oposición: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

**DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico……..por medio del presente escrito ejerce el derecho de oposición previsto en el artículo 21 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

**SOLICITO**

La oposición al tratamiento de mis datos personales, teniendo en consideración que:

☐ El tratamiento de mis datos personales se basa en una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, debiendo limitarse el tratamiento de los mismos hasta que obtenga respuesta del ejercicio de este derecho.

☐ El tratamiento de mis datos personales se basa en la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o un tercero, debiendo limitarse el tratamiento de los mismos hasta que se obtenga respuesta del ejercicio de este derecho.

☐ El tratamiento de mis datos personales se está realizando con fines de investigación científica o histórica o fines estadísticos.

Sin perjuicio de que corresponde al responsable del tratamiento acreditar motivos legítimos imperiosos que prevalezcan sobre mis intereses, derechos y libertades (en los dos primeros supuestos), o una misión realizada en interés público (en el tercer supuesto), acredito como situación personal para oponerme al tratamiento de mis datos personales

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes.

En .....a.....de.....de 20.....

Firmado:

**EJERCICIO DEL DERECHO DE OPOSICIÓN (Modelo B)**

**DATOS DEL RESPONSABLE DEL TRATAMIENTO.**

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de oposición: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

**DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico……..por medio del presente escrito ejerce el derecho de oposición previsto en el artículo 21 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

**SOLICITO**

La oposición al tratamiento de mis datos personales con fines de mercadotecnia, incluyendo la elaboración de perfiles sobre mi persona.

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes.

En .....a.....de.....de 20.....

Firmado:

**INSTRUCCIONES**

1. El modelo A se utilizará cuando el afectado desee oponerse al tratamiento de sus datos personales, por motivos relacionados con su situación particular, en cualquiera de las siguientes situaciones:

-El tratamiento de sus datos personales se está realizando en base a una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

-El tratamiento de mis datos personales se está realizando en base a la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o un tercero.

En estos dos primeros supuestos, el mero ejercicio del derecho de oposición conlleva la limitando

-El tratamiento de mis datos personales se está realizando con fines de investigación científica o histórica o fines estadísticos.

El modelo B. se utilizará cuando el afectado desee oponerse al tratamiento de sus datos personales con fines de mercadotécnica directa, incluyendo la elaboración de perfiles.

2. Será necesario aportar fotocopia del D.N.I. o documento equivalente que acredite la identidad y sea considerado válido en derecho, en aquellos supuestos en que el responsable tenga dudas sobre su identidad. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

**3.** La Agencia Española de Protección de Datos no dispone de sus datos personales y sólo puede facilitar los datos de contacto de los Delegados de Protección de Datos de las entidades obligadas a designar uno que hubieren comunicado su nombramiento a la Agencia. También puede facilitar estos datos de contacto respecto a aquellas entidades que hayan designado un Delegado de forma voluntaria y lo hayan comunicado.

**4.** El titular de los datos personales objeto de tratamiento debe dirigirse directamente ante el organismo público o privado, empresa o profesional del que presume o tiene la certeza que posee sus datos.

**5.** Para que la Agencia Española de Protección de Datos pueda tramitar su reclamación en caso de no haber sido atendida su solicitud de ejercicio del derecho de oposición, resulta necesario que hayan transcurrido un mes sin que el responsable haya hecho efectivo el derecho, y aporte alguno de los siguientes documentos:

•la negativa del responsable del tratamiento a la oposición de los datos solicitados.

•copia sellada por el responsable del tratamiento del modelo de petición de oposición.

•copia del modelo de solicitud de oposición sellada por la oficina de correos o copia del resguardo del envío por correo certificado.

•cualesquiera otros medios de prueba facilitados por el responsable del tratamiento y de los que se pueda deducir la recepción de la solicitud.

**EJERCICIO DEL DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS.**

**DATOS DEL RESPONSABLE DEL TRATAMIENTO.**

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho a no ser objeto de decisiones individuales automatizadas C/Pl ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

**DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico……..por medio del presente escrito ejerce el derecho a no ser objeto de decisiones individuales automatizadas previsto en el artículo 22 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

**SOLICITA:**

No ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que me produzca efectos jurídicos o me afecte significativamente de modo similar, en particular en los siguientes aspectos:

Que se adopten las medidas necesarias para salvaguardar mis derechos y libertades, así como mis intereses legítimos, el derecho a la intervención humana y que pueda exponer mi punto de vista e impugnar la decisión, todo ello en el supuesto de que el tratamiento de mis datos personales se fundamente en la celebración o ejecución de un contrato, o bien en mi consentimiento explícito.

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes.

En .....a.....de.....de 20.....

Firmado:

**INSTRUCCIONES**

**1.** Este modelo se utilizará por el afectado cuando no desee ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos o le afecte a uno.

También se utilizará a los efectos de que el tratamiento se fundamente en la celebración o ejecución de un contrato, o en el consentimiento explícito del afectado, con la finalidad de que se adopten las medidas necesarias para salvaguardar sus derechos y libertades así como sus intereses legítimos, el derecho a la intervención humana y que pueda exponer su punto de vista e impugnar la decisión.

**2.** Será necesario aportar fotocopia del D.N.I. o documento equivalente que acredite la identidad y sea considerado válido en derecho, en aquellos supuestos en que el responsable tenga dudas sobre su identidad. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

**3.** La Agencia Española de Protección de Datos no dispone de sus datos personales y sólo puede facilitar los datos de contacto de los Delegados de Protección de Datos de las entidades obligadas a designar uno que hubieren comunicado su nombramiento a la Agencia. También puede facilitar estos datos de contacto respecto a aquellas entidades que hayan designado un Delegado de forma voluntaria y lo hayan comunicado.

**4.** El titular de los datos personales objeto de tratamiento debe dirigirse directamente ante el organismo público o privado, empresa o profesional del que presume o tiene la certeza que posee sus datos.

**5.** Para que la Agencia Española de Protección de Datos pueda tramitar su reclamación en caso de no haber sido atendida su solicitud de ejercicio del derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles, resulta necesario que el responsable no haya respondido a su solicitud en el plazo de un mes, y aporte alguno de los siguientes documentos:

• la negativa del responsable del tratamiento al derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles.

• copia sellada por el responsable del tratamiento del modelo de petición de no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles.

• copia del modelo de solicitud de ejercicio del derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles, sellada por la oficina de correos o copia del resguardo del envío por correo certificado.

• cualesquiera otros medios de prueba facilitados por el responsable del tratamiento y de los que se pueda deducir la recepción de la solicitud.

**EJERCICIO DEL DERECHO A LA PORTABILIDAD DE LOS DATOS**

**DATOS DEL RESPONSABLE DEL TRATAMIENTO.**

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que ejercita el derecho a la portabilidad de los datos: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

**DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico ……..... por medio del presente escrito ejerce el derecho la la portabilidad de los datos, de conformidad con lo previsto en el artículo 20 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

**SOLICITA**

Que se le faciliten en el plazo de un mes sus datos personales en un formato estructurado, de uso común y lectura mecánica.

En su caso, que los citados datos personales sean transmitidos directamente al responsable ……(especifíquese nombre o razón social), siempre que sea técnicamente posible.

En .....a.....de.....de 20.....

Firmado

**INSTRUCCIONES**

**1**. El Modelo se utilizará por el afectado que desee que se le faciliten sus datos personales en un formato estructurado, de uso común y lectura mecánica.
También podrá emplearse si quisiera que los citados datos personales sean transmitidos directamente de responsable a responsable cuando sea técnicamente posible.

**2.** Será necesario aportar fotocopia del D.N.I. o documento equivalente que acredite la identidad y sea considerado válido en derecho, en aquellos supuestos en que el responsable tenga dudas sobre su identidad. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

**3.** La Agencia Española de Protección de Datos no dispone de sus datos personales y sólo puede facilitar los datos de contacto de los Delegados de Protección de Datos de las entidades obligadas a designar uno que hubieren comunicado su nombramiento a la Agencia. También puede facilitar estos datos de contacto respecto a aquellas entidades que hayan designado un Delegado de forma voluntaria y lo hayan comunicado.

**4.** El titular de los datos personales objeto de tratamiento debe dirigirse directamente ante el organismo público o privado, empresa o profesional del que presume o tiene la certeza que posee sus datos.

**5.** Para que la Agencia Española de Protección de Datos pueda tramitar su reclamación en caso de no haber sido atendida su solicitud de ejercicio del derecho a la portabilidad de datos en el plazo de un mes, y aporte alguno de los siguientes documentos:

•la negativa del responsable del tratamiento a la portabilidad de los datos solicitados.

•copia sellada por el responsable del tratamiento del modelo de petición de portabilidad.

•copia del modelo de solicitud de portabilidad sellada por la oficina de correos o copia del resguardo del envío por correo certificado.

•cualesquiera otros medios de prueba facilitados por el responsable del tratamiento y de los que se pueda deducir la recepción de la solicitud.

**EJERCICIO DEL DERECHO DE SUPRESIÓN**

**DATOS DEL RESPONSABLE DEL TRATAMIENTO.**

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de supresión: C/Plaza ..... nº ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

**DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico……..por medio del presente escrito ejerce el derecho de supresión, de conformidad con lo previsto en el artículo 17 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

**SOLICITA**

Que se proceda a acordar la supresión de sus datos personales en el plazo de un mes a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la supresión practicada.

Que en caso de que se acuerde que no procede practicar total o parcialmente la supresión solicitada, se me comunique motivadamente a fin de, en su caso, reclamar ante la Autoridad de control que corresponda.

Que en caso de que mis datos personales hayan sido comunicados por ese responsable a otros responsables del tratamiento, se comunique esta supresión.

En .....a.....de.....de 20.....

**INSTRUCCIONES**

**1**. Este modelo se utilizará por el afectado cuando desee la supresión de los datos cuando concurra alguno de los supuestos contemplados en el Reglamento General de Protección de Datos. Por ejemplo, tratamiento ilícito de datos, o cuando haya desaparecido la finalidad que motivó el tratamiento o recogida.
No obstante, se prevén ciertas excepciones en las que no procederá acceder a este derecho. Por ejemplo, cuando deba prevalecer el derecho a la libertad de expresión e información.

**2**. Será necesario aportar fotocopia del D.N.I. o documento equivalente que acredite la identidad y sea considerado válido en derecho, en aquellos supuestos en que el responsable tenga dudas sobre su identidad. En caso de que se actúe a través de representación legal deberá aportarse, además, DNI y documento acreditativo de la representación del representante.

**3.** La Agencia Española de Protección de Datos no dispone de sus datos personales y sólo puede facilitar los datos de contacto de los Delegados de Protección de Datos de las entidades obligadas a designar uno que hubieren comunicado su nombramiento a la Agencia. También puede facilitar estos datos de contacto respecto a aquellas entidades que hayan designado un Delegado de forma voluntaria y lo hayan comunicado.

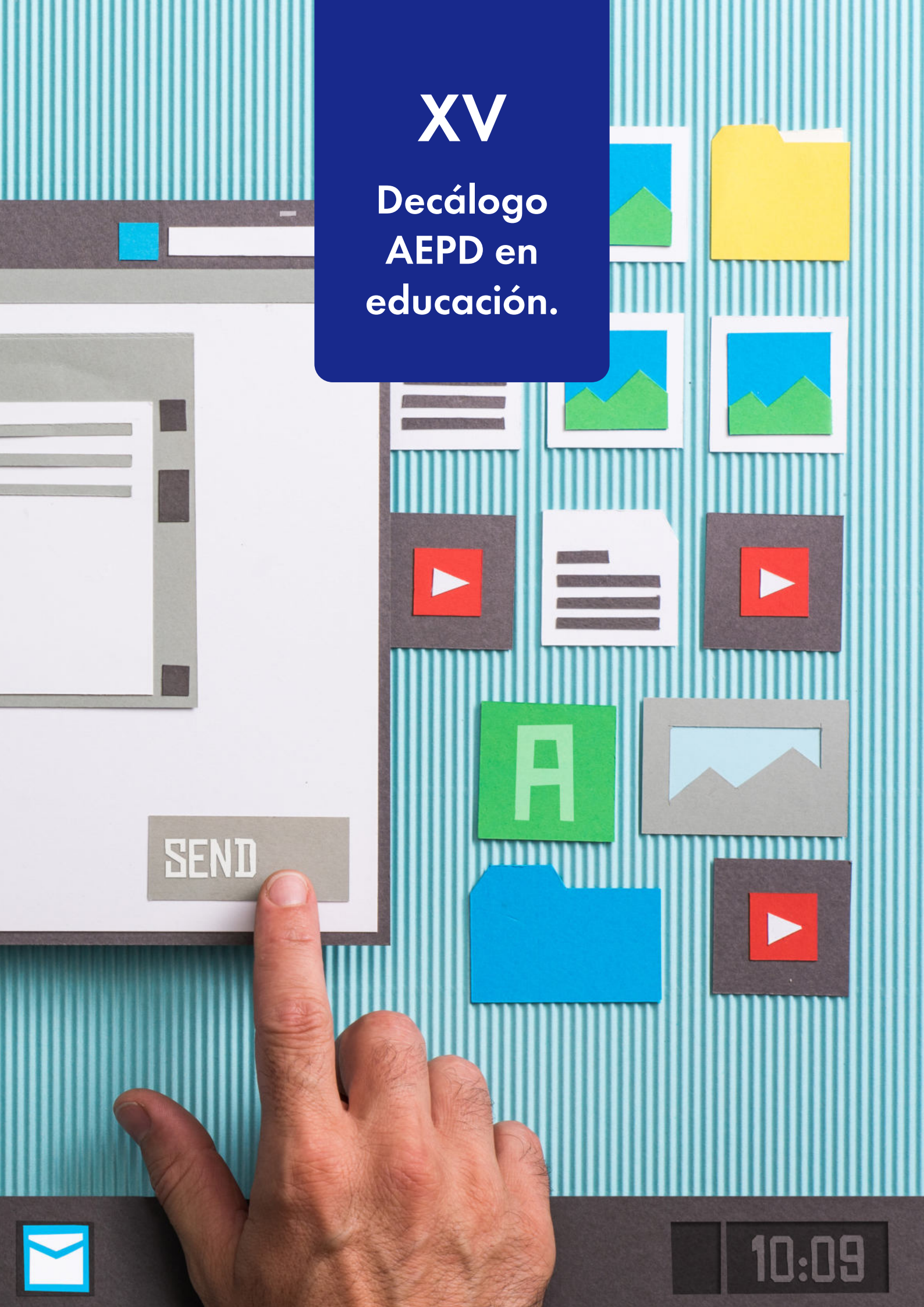
**4.** El titular de los datos personales objeto de tratamiento debe dirigirse directamente ante el organismo público o privado, empresa o profesional del que presume o tiene la certeza que posee sus datos.

**5.** Para que la Agencia Española de Protección de Datos pueda tramitar su reclamación en caso de no haber sido atendida su solicitud de ejercicio del derecho de supresión, resulta necesario que el responsable no haya hecho efectivo el derecho, y aporte alguno de los siguientes documentos:

- la negativa del responsable del tratamiento a la supresión de los datos solicitados.
- copia sellada por el responsable del tratamiento del modelo de petición de supresión.
- copia del modelo de solicitud de supresión sellada por la oficina de correos o copia del resguardo del envío por correo certificado.
- cualesquiera otros medios de prueba facilitados por el responsable del tratamiento y de los que se pueda deducir la recepción de la solicitud.

# XV

## Decálogo AEPD en educación.



Los equipos directivos, profesores, personal administrativo y auxiliar de los centros educativos en el ejercicio de sus funciones y tareas necesitan tratar datos de carácter personal de los alumnos y de sus familiares, lo que deberán realizar con la debida **diligencia y respeto** a su privacidad e intimidad, teniendo presente el interés y la protección de los menores.

DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD -

**2**

Las Administraciones y los centros educativos son los **responsables del tratamiento** de los datos y deben formar sobre sus principios básicos y cómo hacerlo correctamente.

DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD -

**3**

Por regla general, los centros educativos no necesitan el consentimiento de los titulares de los datos para su tratamiento, que estará justificado en el ejercicio de la función educativa y en la relación ocasionada con las matrículas de los alumnos. No obstante, se les debe **informar** de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo, que se puede realizar en el mismo impreso en el que se recojan los datos de:

- la **finalidad** para la que se recaban los datos y su **licitud**, por ejemplo, para el ejercicio de la función educativa, o para difundir y dar a conocer las actividades del centro,
- la obligatoriedad o no de facilitar los datos y las consecuencias de la negativa a facilitarlos,
- los **destinatarios** de los datos,
- los **derechos** de los interesados y dónde ejercitarlos,
- la **identidad** del responsable del tratamiento: la Administración educativa o el centro,

El RGPD amplía, la información que debe facilitarse a los titulares de los datos cuando se recaben de ellos mismos, añadiendo los datos de contacto del delegado de protección de datos y el plazo de conservación o los criterios para determinarlo.

DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD -

Cuando sea preciso **obtener el consentimiento** de los alumnos o de sus padres o tutores para la utilización de sus datos personales por tratarse de **finalidades distintas a la función educativa**, se debe informar con claridad de cada una de ellas, permitiendo a los interesados oponerse a aquellas que así lo consideren.

DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD -

**5**

Las **TIC** son herramientas fundamentales para la gestión y el aprendizaje de los alumnos. Las Administraciones educativas y los centros deben **conocer las aplicaciones que vayan a utilizar**, su política de privacidad y sus condiciones de uso de éstas antes de utilizarlas, debiendo **rechazarse** las que no ofrezcan información sobre el tratamiento de los datos personales que realicen.

DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD -

**6**

Las Administraciones educativas y los centros deben **disponer** de protocolos, instrucciones, guías, directrices o recomendaciones para el uso de las **TIC** por los profesores, que deberán utilizar las que la Administración educativa y/o el centro hayan dispuesto. Su enseñanza y uso deberán **adaptarse** al grado de desarrollo del niño.

DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD -

**7**

Las **comunicaciones** entre profesores y padres de alumnos deben llevarse a cabo, preferentemente, a través de los **medios** puestos a disposición de ambos por el **centro educativo** (plataformas educativas, correo electrónico del centro).

DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD -

**8**

El uso de aplicaciones de mensajería instantánea (como WhatsApp) entre profesores y padres o entre profesores y alumnos **NO SE RECOMIENDA**. No obstante, en aquellos casos en los que el interés superior del menor estuviera comprometido, como en caso de accidente o indisposición en una excursión escolar, y con la finalidad de informar y tranquilizar a los padres, titulares de la patria potestad, se podrían captar imágenes y enviárselas.

DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD -

Los profesores deben tener **cuidado** con los contenidos del trabajo de clase que suben a Internet. Deben enseñar a **valorar la privacidad** de uno mismo y la de los demás, así como enseñar a los alumnos que no pueden sacar fotos ni videos de otros alumnos ni de personal del centro escolar sin su consentimiento y hacerlos circular por las redes sociales, para evitar cualquier forma de violencia (ciberacoso, grooming, sexting o de violencia de género).

DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD -

**10**

Cuando los centros educativos organicen y celebren **eventos** (fiestas de Navidad, fin de curso, eventos deportivos) a los que asistan los familiares de los alumnos, constituye una **buena práctica** informarles, por ejemplo, al solicitarles la autorización para participar o mediante avisos o carteles, de la posibilidad de grabar imágenes exclusivamente para su uso personal y doméstico (actividades privadas, familiares, etc.).

DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD - DECÁLOGO AEPD -

# XVI

## Guías, fichas y recursos.

# FICHA 1

## El dato personal

¿Jugamos? ¿Sabrías decir todos tus datos personales?

### 1. LOS MÁS FÁCILES SON LOS QUE TE IDENTIFICAN DIRECTAMENTE.

Tu nombre, tus apellidos, tu fotografía, tu domicilio, tu número de carnet de identidad o de pasaporte…

Cualquier información que hace posible que alguien pueda identificarte es uno de tus datos personales.

### 2. OTROS DICEN MÁS DE TI DE LO QUE IMAGINAS.

Tu correo electrónico, tu número de teléfono, las webs que visitas, las consultas que haces en los buscadores, los vídeos que consultas por internet, tus cuentas en redes sociales, tus mensajes, tus publicaciones, los comentarios que haces en un blog o un foro, tus «me gusta», el móvil que utilizas...

Todo lo que haces en internet deja un rastro, una huella digital que habla de ti.

¿Sabías que toda la información que dejas cuando te conectas forma lo que se llama tu identidad digital?

### 3. Y ADEMÁS...

Un lunar, una pequeña mancha en la piel, una cicatriz, la forma de tus manos o de cualquier parte de tu cuerpo, un objeto que utilizas como un anillo o un pendiente, tu ropa o incluso la foto de tu colegio o instituto pueden servir para que alguien te identifique.

### 4. TU INFORMACIÓN PERSONAL ES VALIOSA ¿CUIDAS DE TUS DATOS?

- Tú decides quién puede tener tus datos.
- Tú decides para qué pueden utilizarlos.
- Te damos algunas pistas y trucos para cuidar de ellos.

# Trucos para las trampas de internet

FICHA 2
PRIVACIDAD Y SEGURIDAD

## 1. LAS WEBS QUE ENGAÑAN ¿WWW.MOGOLLONDEJUEGOS.COM O WWW. MOGOLONDEJUEGOS.COM?

Comprueba en tu navegador si realmente estás visitando la página que quieres. Mira en la barra de direcciones y decide dónde quieres ir.

Algunos hackers aprovechan nuestros despistes para crear webs casi iguales a las que utilizas habitualmente pero con contenido que puede dañar tus dispositivos (tu tablet, tu móvil, tu ordenador) o para robarte tu cuenta o tus datos personales.

Antes de escribir tu nombre de usuario y contraseña asegúrate de que has entrado en la web correcta. Para ello, revisa la barra de direcciones.

## 2. WEBS CON DEMASIADAS COOKIES.

Las cookies o galletas guardan información sobre ti: dicen qué páginas has visitado, qué te gusta, qué sueles hacer y mucho más.

- Para borrarlas busca la opción en el menú del navegador. Si estás en tu ordenador pulsa las teclas may+ctrl+supr.
- En tu móvil, revisa los ajustes de privacidad.

## 3. WIFI GRATIS Y SIN CLAVE.

Desconfía de las redes wifi gratis o sin clave. No son seguras, otra persona puede ver lo que haces, las contraseñas que utilizas o incluso pueden entrar en tus dispositivos y robarte tu información personal.

Comprueba que la wifi de tu casa tiene contraseña, evitarás que accedan invitados no deseados.

## 4. LOS VIRUS QUE ESTROPEAN TU ORDENADOR TAMBIÉN LO HACEN CON TU TABLET Y TU MÓVIL.

Utiliza un antivirus en tus dispositivos.

## 5. LOS SECUESTRADORES DE TUS CARPETAS.

- Cuando navegues por internet puede que al abrir una imagen, pinchar un enlace o descargar un programa, se te instalen archivos que pueden bloquear tu dispositivo y hacer ilegibles tus ficheros.
- No abras mensajes de desconocidos. No abras ficheros o enlaces a sitios webs que aparezcan en estos mensajes.
- Haz una copia de tus fotos, vídeos, documentos, etc.

## 6. LAS DESCARGAS GRATIS.

Descarga aplicaciones sólo de sitios de confianza.

# FICHA 3

**PROTECCIÓN DE DATOS PERSONALES (SEGURIDAD, DERECHOS, POLÍTICA DE PRIVACIDAD)**

# Trucos para apuntarme y borrarme de una web

## 1. DOY TODA LA INFORMACIÓN QUE PIDAN: RELLENO MIS DATOS, LOS DE MIS PADRES, HERMANOS, AMIGOS, PROFESORES, LOS DE MI COLEGIO... ¿ESTÁS SEGUR@?

Nunca des información de tu familia o de otras personas. Desconfía de las webs que te piden demasiada información.

Evita que tu usuario o tu *login* tengan tu nombre, fecha de nacimiento o edad.

## 2. TUS CLAVES SECRETAS.

- No utilices como contraseñas palabras que se puedan asociar fácilmente a ti, como el nombre de tu mascota, el nombre de tu calle, tu fecha de nacimiento...
- Utiliza contraseñas de un mínimo de 8 caracteres y mezcla mayúsculas, minúsculas, caracteres especiales (@ # *) y números.
- Evita utilizar palabras que vengan en los diccionarios.
- Nunca des a otra persona tus claves y utiliza siempre el botón de salir o cerrar sesión. Así evitas que alguien robe tu sesión, tu cuenta o tus datos personales.

## 3. ¡EN ESTE SITIO WEB SOMOS MUY GUAYS, SIEMPRE DE BUEN ROLLO!

Si es «guay» tienen que decirte quiénes son, para qué van a utilizar tus datos y cómo puedes borrarte.

Esto es lo que se llama la «política de privacidad».

Todos los sitios web que utilicen tus datos personales deben tener una política de privacidad.

## 4. CUANDO TE DICEN QUE NO PUEDEN BORRARTE DE UNA WEB.

¡Es falso!

Cuando te apuntas a una web das tus datos y tú decides cuándo borrarlos. Tienes derecho a decidir sobre tus datos.

## 5. LAS FOTOS O VÍDEOS DONDE APAREZCO Y OTRAS COSAS QUE HABLAN DE MÍ.

Piensa bien si quieres compartir una imagen o vídeo con los demás.

Si lo haces, fíjate en quién puede verlo.

## 6. PARA QUITAR LAS FOTOS Y VÍDEOS DONDE APAREZCO Y OTRAS COSAS QUE HABLAN DE MÍ.

Dirígete, en primer lugar, a quien subió esa información y dile que quieres que la borre.

Si no te hace caso, pídeselo al responsable de la web. Si tampoco la quita, habla con tus padres o con alguien de confianza. Podéis recurrir a la Agencia Española de Protección de Datos para que os ayude a borrarla.

# Trucos para evitar malos rollos

**FICHA 4**
**ACOSO Y CONVIVENCIA EN LA RED**

## 1. ALGUIEN QUE NO CONOCES QUIERE CONTACTAR CONTIGO.

- Cuando un desconocido te pide tu número de teléfono o te escribe un mensaje, ignóralo.
- Nunca facilites tu teléfono, tu nombre, o cualquier información tuya a un desconocido y menos aún una fotografía tuya o de alguna parte de tu cuerpo.

## 2. ESCRIBIR Y GRITAR.

- Cuando escribes mensajes en mayúsculas alguien puede entender que le gritas.

## 3. RESPETA A LOS DEMÁS.

- No hagas en internet algo que no harías en la vida real.
- Evita gestos o conductas que puedan ofender a otras personas.

## 4. CUANDO NO TE DEJAN EN PAZ.

Si recibes mensajes o comentarios que te molestan, si recibes incluso durante la noche toques o mensajes en tu teléfono o tablet, si alguien te molesta aunque sea con número oculto…

Se llama acoso. No lo permitas. Cuéntalo. No tengas miedo. Pide ayuda a tus padres o a alguien de tu confianza.

## 5. NO ACOSES A OTRAS PERSONAS.

- No participes en el acoso de otras personas y, si conoces algún caso, cuéntaselo a tus padres o a alguien de tu confianza.
- No utilices datos personales de otras personas para acosar.
- No reenvíes mensajes, fotos o vídeos humillantes o pensados para dañar a otra persona. Además podrías estar cometiendo un delito.

# FICHA 5

## REDES SOCIALES

# Con los amig@s en la red

## 1. SI TODO LO PONES EN LA RED SOCIAL.

- Elige a tus amig@s de la red social entre las personas que conoces.
- Rechaza solicitudes de amistad de desconocidos.
- No cuentes cosas de otras personas.
- Revisa la configuración o los ajustes de tu cuenta en la red social y decide quién puede ver tus cosas (Facebook, Twitter, Instagram, Youtube, Tuenti, Google+). Visita nuestros vídeos.
- Piensa antes de publicar algo si lo que dices o pones en tu perfil puede molestar a otras personas.
- Te aconsejamos que lo que publicas sólo puedan verlo tus amig@s.
- No compartas tu ubicación, la información de dónde te encuentras (Facebook, Twitter, Instagram, Youtube, Tuenti, Google+) podría ser conocida por extraños.

## 2. SI SUBES A LA RED SOCIAL INFORMACIÓN DE OTRAS PERSONAS.

- Si vas a publicar fotos o vídeos en los que aparecen otras personas, asegúrate de que no les va a molestar.
- No etiquetes.

## 3. LOS AMIG@S DE MIS AMIG@S EN LAS REDES.

- Los amig@s de tus amig@s también pueden llegar a ver lo que compartes.
- Evita compartir con otras personas lo que tus amig@s comparten contigo.

## 4. BLOGS Y FOROS.

- No facilites información que permita que desconocidos te puedan localizar o identificar. Podrías tener problemas.
- Utiliza siempre un pseudónimo y nunca digas tu nombre real o el nombre real de tus amig@s.
- No publiques tu domicilio, tu colegio o instituto, tu correo, tu número de teléfono y, en general, tus datos personales o los de otras personas.

# Mensajes sin parar

## FICHA 6

**MENSAJERÍA INSTANTÁNEA**

### 1. REENVÍO TODO LO QUE RECIBO.

- Muchos mensajes contienen datos personales de otras personas.
- Consulta antes con quien te envía un mensaje para saber si lo puedes pasar a otra persona.
- Cuando escribas un mensaje o mandes fotos o vídeos, piensa que las personas a las que se lo envías siempre pueden reenviarlos a otras personas.
- Nunca reenvíes imágenes y vídeos que puedan molestar a otras personas. Puedes causar muchos problemas y a veces estarás cometiendo un delito.
- No participes en las cadenas de mensajes.

### 2. SI ENVÍAS UN CORREO A MUCHAS PERSONAS.

- Utiliza la opción de tu correo con copia oculta (cco).
- Evitarás que todos vean la dirección de correo de los demás.
- Algunas personas no quieren que se facilite su correo a otros. Es un dato suyo y ellos deciden. Respeta sus deseos.

### 3. MENSAJES Y COMENTARIOS EN REDES SOCIALES.

- Si haces un comentario o publicas un mensaje en una red social piensa si quieres que todo el mundo pueda verlo o prefieres enviar un mensaje privado.
- Si crees que a la otra persona le puede molestar que el mensaje o comentario sea visible utiliza la opción del mensaje privado.
- No reveles tus datos personales o los de otras personas en mensajes y comentarios que no sean privados.

### 4. DESCARGAS AUTOMÁTICAS.

- Algunos virus llegan a tu móvil o tablet dentro de vídeos y pueden robar tus datos personales.
- Revisa los ajustes para mensajes multimedia (MMS) y apps de mensajes (Whatsapp, Snapchat, Telegram…) para evitar que los vídeos se descarguen automáticamente.
- Evitarás recibir contenido multimedia de desconocidos que puede dañar tu tablet o móvil.
- También ahorrarás megas de tu contrato del móvil.

### 5. GRUPOS.

- Si te incluyen en un grupo y no te interesa, bórrate.
- No vuelvas a incluir en un grupo a alguien que se ha borrado salvo que te lo pida él.
- El número de teléfono o el usuario de otras personas son datos personales que no puedes utilizar si ellos no lo desean. Cuenta con ellos antes de incluirlos en un grupo o una lista para el envío de mensajes.

# FICHA 7

## AJUSTES DE PRIVACIDAD

# Trucos para el tablet, móvil y ordenador

## 1. ¿ESTÁS EN LAS NUBES?

- Tu móvil y tu tablet almacenan mucha información tuya, de tus amig@s y de tu familia.
- Decide si te interesa guardar tus cosas en la nube o si prefieres tenerlas en tu dispositivo móvil.
- Si utilizas la nube, comprueba quién tiene acceso a tus cosas.

## 2. GPS, WIFI Y BLUETOOTH EN TU TABLET O MÓVIL.

- Apaga tu GPS, wifi y Bluetooth cuando no los necesites.
- Evitarás que otras personas puedan saber dónde estás.
- Además la batería te durará más tiempo.

## 3. PARA QUE NO TE VEAN.

- Un hacker puede observarte a través de la cámara de tu dispositivo sin que lo sepas.
- Utiliza una pegatina y tapa tu cámara cuando no la utilices.

# Bloquea y desconecta

## FICHA 8

### SEXTING Y ADICCIÓN

### 1. DESNUD@S POR LA RED.

- No te hagas o hagas a otros fotos comprometidas.
- No envíes fotos de nadie desnudo. Podría llegar a ser un delito.
- Bloquea al remitente para que no te envíe este tipo de imágenes y evitar que te acose.
- Enviar o reenviar imágenes comprometidas puede ser acoso. No lo permitas. Pide ayuda a tus padres o a alguien de tu confianza.

### 2. NO DUERMO, NO ESTUDIO, NO PUEDO DEJAR DE MIRAR MENSAJES...

- Tú controlas tu móvil, tu tablet, tu ordenador. No permitas que él te controle a ti.
- No permitas que nadie te acose con mensajes constantes.

### 3. DESCONECTA.

- Cuando duermes no necesitas estar conectad@.
- Apaga tu tablet, tu móvil o tu ordenador cuando descansas.

### 4. CONSULTA CON TUS PADRES, PROFESORES O CON ALGUIEN DE TU CONFIANZA.

- Cuando tengas dudas.
- Cuando te sientas acosado.
- Cuando creas que se está acosando a otra persona.

# Ficha 1

## Los datos personales que compartes

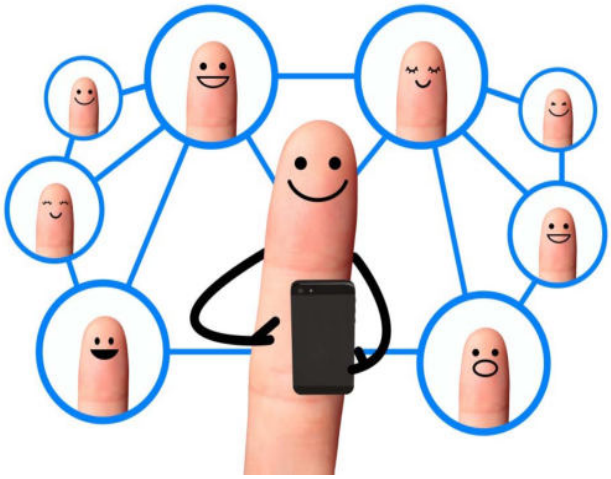
### 1. ¿Sabrías decir cuáles son los datos personales que compartes con otras personas desde tu terminal móvil, tu tablet y desde una red social?

Tu nombre, tus apellidos, tu fotografía tu domicilio, tu correo electrónico, tu número de teléfono, tu número de carnet de identidad o de pasaporte… Cualquier información que hace posible que alguien pueda identificarte es uno de tus datos personales. Un lunar, una pequeña mancha en la piel, una cicatriz, la forma de tus manos o de cualquier parte de tu cuerpo, un objeto que utilizas como un anillo o un pendiente, tu ropa o incluso la foto de tu colegio o instituto pueden servir para que alguien te identifique.

Por ejemplo tu imagen, que es un dato personal. Si tu foto aparece en el perfil de una red social o en un perfil de una aplicación de mensajería, como puede ser WhatsApp, estás compartiendo tu imagen con otras personas.

Si compartes tu ubicación con otras personas ¿sabes exactamente quiénes tienen acceso a tu ubicación? El lugar en el que te encuentras es un dato personal que habla de ti. Dice a otras personas dónde pueden encontrarte y, probablemente, lo que haces en un momento determinado o conocer tus hábitos, gustos o aficiones, (si estas en el colegio, en casa, en el cine, haciendo deporte, etc.).

Si lo necesitas puedes revisar la primera ficha de nuestra guía "No te enredes en internet", donde explicamos el significado de "dato personal".



# Ficha 1

## Los datos personales que compartes

## 2. ¿Serías capaz de identificar las personas que acceden a los datos personales que compartes?

Trata de averiguar los datos personales que puedes compartir en internet y luego intenta identificar a las personas que tienen acceso a estos datos, como, por ejemplo, a tu fotografía de perfil de WhatsApp o de otra aplicación de mensajería instantánea. (LINE, Hangouts, etc.).

Comprueba los datos personales que puedes compartir en una red social. Revisa las opciones de configuración de tu red social e identifica a las personas que tienen acceso a tu información personal, recuerda que a veces los amigos de tus amigos también pueden ver los datos personales que compartes.

¿Estás completamente seguro de quiénes pueden ver lo que compartes en internet?

¿Qué ocurriría si un amigo tuyo pierde o le roban el móvil?

¿Quién podría acceder a tus datos personales si un amigo se deja una sesión de tu red social sin cerrar en un ordenador al que acceden otras personas?

# Ficha 2

## Cosas que no te gustaría que hicieran con tus datos personales

### 1. ¿Qué esperas cuando das tus datos personales a otras personas?

Cuando facilitas información sobre ti a otras personas hay algunas cosas que no te gustaría que hicieran, principalmente cosas que te molestan, te hacen sentir mal o te entristecen.

Recuerda que eres tú quien decide y elige quién puede utilizar tus datos personales y para qué los puede utilizar. No permitas que otras personas te puedan hacer daño utilizando tus datos personales a través de internet o del teléfono móvil ni permitas que se haga daño a otras personas, consulta siempre con tus familiares, profesores o un adulto de tu confianza cuando creas que alguien puede estar sufriendo algún daño por lo que se sube a internet o lo que recibes, sea lo que sea: comentarios, etiquetas, videos, imágenes, etc.

Ahora intentaremos darte algunas ideas sobre aquellas cosas que seguro que podrían molestarte o incluso hacerte daño para que puedas identificarlas. Tienes que tener en cuenta que estas mismas acciones que a ti te molestan, o incluso que te hacen daño, pueden molestar o hacer daño a otras personas en igual o mayor grado que a ti.

### 2. A continuación piensa como podría sentirse una persona en cada uno de los supuestos siguientes. Elige entre triste, ridículo, feliz o indica otra forma en la que creas podría sentirse alguien:

- @ Que recibe un mensaje en el que se le llama torpe porque se ha caído en clase de educación física.
- @ Que recibe por WhatsApp una imagen suya manipulada en la que se le ha reducido su estatura y su aspecto es cómico o parecido a un elefante.
- @ Que recibe un vídeo en el que aparece cambiándose en el vestuario del cole.
- @ Que es etiquetado en una imagen en una red social y alguien añade un comentario diciendo que es el mejor jugador de tenis del cole.
- @ Al que le han etiquetado en una fotografía de otra persona desnuda.
- @ Del que han comentado detalles de su enfermedad en una red social .

# Ficha 2

## Cosas que no te gustaría que hicieran con tus datos personales

@ Que ha sido añadido a un grupo de WhatsApp que tiene el nombre "KK" y aunque se sale del grupo alguien le vuelve a añadir constantemente.

@ Del que han subido a internet fotos suyas en las que se le llama "robot" porque tiene un aparato de ortopedia en las piernas.

@ Al que se le ha etiquetado en una red social como mejor compañer@ y delegado de clase.

@ De quien se habla sobre la religión que practica y la de su familia en un foro de internet.

@ De quien por el grupo de WhatsApp del cole comentan que es una seguidor del Barça, del Madrid, del Depor o cualquier otro equipo que acaba de ganar la liga de futbol.

@ Que recibe un WhatsApp con una imagen de un personaje famoso que es gay y sobre la que alguien ha escrito el nombre de la persona a quien se dirige el mensaje.

@ Que recibe más de cien llamadas diarias desde números desconocidos.

@ Que recibe un mensaje por WhatsApp que dice: "al salir al patio te vas a caer, ya lo verás".

@ Que se va a apuntar en una red social y ya existe otra persona con su nombre y su fotografía que alguien ha cogido de su perfil de WhatsApp.

@ Que es insultado en un foro porque es de una "raza" distinta o por cualquier otra razón.

# Ficha 2

## Cosas que no te gustaría que hicieran con tus datos personales

@ Cuyo número de teléfono y su dirección de correo electrónico aparecen en una página web junto a la foto de una persona adulta desnuda.

@ Al que sus compañeros han mirado su teléfono móvil mientras iba al aseo y han leído sus mensajes.

@ Que recibe una fotografía en la que se ridiculiza a uno de sus profesores y se le insulta pero dicen que es una broma.

@ Que recibe un mensaje con amenazas que prometen cumplir si no facilita los números de las tarjetas de crédito de sus familiares.

@ Que olvidó desconectar la webcam y alguien ha subido a internet un video en el que aparece en su habitación vistiéndose antes de ir a dormir y le piden dinero si quiere que quiten el video de internet.

@ Al que por Skype un amigo le pide que se quite la ropa delante de la cámara.

@ Que está siempre controlado a través de mensajes y llamadas al móvil.

Protégete

# Ficha 3

## 1. ¿Qué harías tú en cada uno de los casos anteriores?

Algunas de estas conductas pueden ser lo que se llama acoso y puede ser un delito.

Acosar a una persona es no dejarla en paz, perseguirla o molestarla con insultos, bromas de mal gusto, de forma insistente y continuada, incluso cuando ni siquiera sabes quién es la persona que te está haciendo daño.

El acoso puede realizarse utilizando tus datos personales a través de internet o de tu terminal móvil, y entonces se llama ciberacoso o ciberbullying.

Cuida de tus datos personales y de los datos personales de otras personas, nunca facilites información tuya, de tu familia, tus amigos o tus profesores a personas desconocidas. Cuando tengas que facilitar información sobre ti procura que sea la mínima información posible.

Si te sientes acosado habla con un adulto de tu confianza, entre tus familiares o profesores, es posible que tengas que acudir a la Policía o a la Guardia Civil.

Cuando creas que tienes problemas, no elimines mensajes o el registro de llamadas, aprende a capturar las pantallas en las que aparecen imágenes o mensajes que te hacen sentir acosado.

Los mensajes y las pantallas que captures serán de utilidad para que los adultos de tu confianza puedan entender lo que está ocurriendo y, en su caso, la Policía pueda identificar a la persona o personas que realmente realizan las llamadas o envían los mensajes.

¿Crees que nadie puede ver lo que hacemos en internet? Algunas personas creen que lo que hacen por internet nadie puede verlo pero están equivocadas: todo lo que hacemos por internet o por teléfono deja huella, la Policía pueden acceder a consultar estas huellas para averiguar quién es la persona que te está haciendo daño.

## 2. ¿Sabías que cada persona tiene derecho a decidir sobre sus datos personales?

Existen normas o reglas escritas a las que llamamos leyes y seguro que todos habéis oído alguna vez hablar de ellas.

Algunas leyes tratan de tus derechos y nadie puede negarte los derechos que una ley te ha dado. Tienes derecho a decidir sobre tus datos personales pero

# Ficha 3

## Protégete

no tienes derecho a decidir sobre los datos personales de otras personas, antes tienes que pedirles permiso para que no se molesten o se enfaden contigo y para actuar siempre como dicen las leyes, respetando tus derechos y los de los demás.

La ley de Protección de Datos es la que te da derecho a decidir sobre tus datos evitando que otra persona pueda utilizar tu información personal sin tu permiso.

Cuando alguien utiliza los datos de otras personas, sin tener en cuenta sus derechos, lo puede hacer sabiendo lo que se hace o por error; ambas conductas se contemplan en la ley y tienen sus consecuencias, tanto si se hace conscientemente como por error se puede estar cometiendo un delito.

Cuando cometemos un delito hacemos daño a otras personas. Además, los delitos también suponen problemas para las personas que los cometen, para sus familiares y sus amigos.

Cuando alguien comete un delito y hace daño a otras personas puede ocurrir que tenga que pagar dinero por los daños que haya causado o que sea castigado para evitar que lo vuelva a hacer.

Aunque seas menor de edad la ley también se te aplica, te pueden castigar. Si eres mayor de 14 años el Juez te puede imponer diferentes castigos, por ejemplo, que no salgas a la calle los fines de semana, o realizar tareas o trabajos en beneficio de la comunidad. En el peor de los casos un Juez podría decidir que fueras internado en un centro de reforma. Si hubiera que pagar dinero a las personas que hiciste daño serían tus familiares o tutores quienes tendrían que pagar con su dinero.

# Ficha 4

## Ciberbullying

### 1. ¿Sabrías decir qué significa acosar a una persona?

Intenta identificar entre los supuestos que aparecen en la ficha 2 (punto 2) los que podríamos decir que constituyen situación de acoso.

Cuando los que te molestan son compañeros tuyos (del colegio, del instituto, del gimnasio, de tu equipo, etc.) se llama "bullying" y cuando lo hacen por internet se llama ciberbullying.

El acoso en cualquiera de sus formas es un delito, no permitas que nadie te acose. No participes en el acoso hacia otras personas, no consientas que se acose a otras personas.

Si crees que se está produciendo una situación de acoso habla con un adulto de tu confianza.

A continuación vamos a darte más pistas que te ayudarán a identificar situaciones de acoso en las que una persona podría verse involucrada, como víctima o como acosador.

### 2. ¿Sabes lo que significa ciberbullying?

Seguramente has oído hablar de acoso en la red o de compañeros que dicen que sufren persecución cuando manejan aplicaciones porque otros compañeros:

- @ Leen los mensajes de sus móviles sin su permiso y luego emplean lo que saben para descalificarles, humillarles, amenazarles o insultarles en las redes sociales.
- @ Les hacen fotos sin permiso y luego las envían a otros para reírse de ellos.
- @ Entran en sus móviles, tablets u ordenadores y les roban fotos o información que almacenan y les amenazan porque saben cosas sobre ellos.
- @ Quieren obligarles a hacer cosas porque tienen fotos de ellos u otras informaciones de su vida.
- @ Les roban los móviles para enviar mensajes haciéndose pasar por ellos.

Tienes que saber que cuando alguien te amenaza con enseñar a otro una foto tuya, quiere obligarte a hacer algo en contra de tu voluntad empleando tu

Ficha 4

## Ciberbullying

imagen o cualquier otra información sobre ti, está cometiendo un delito.

Si uno o varios compañeros envían información sobre ti y te hacen sentir mal o sin ganas de ir a clase puede que estén cometiendo un delito de acoso.

Debes recordar que cada persona es dueña de su información y sólo esa persona puede decidir sobre su información.

Hay ciberbullying cuando constantemente una o más personas envían a otra persona mensajes con el fin de hacerle sentir mal valiéndose de su información personal.

### 3. ¿Crees que puedes reenviar la información personal que recibes de otras personas?

Uno no debe reenviar información de otras personas porque cada uno es dueño de su información.

Cuando se reenvía información de otros se debe estar seguro de que la persona a la que pertenece esa información está de acuerdo.

Puede suceder que un grupo en WhatsApp esté manejando fotos o información sobre ti que te esté haciendo sentir mal. Puede ser que no quieras verlos y prefieras quedarte en casa. Esto nunca debería llegar a ocurrir, pero si alguna vez te ocurre a ti o a un compañero o amigo deberías de ponerlo en conocimiento de tus familiares, tus profesores o un adulto en el que confíes. Si te da vergüenza puedes decírselo a la Policía, o a la Guardia Civil, o llamar al teléfono de ANAR, 900 20 20 10, que es una asociación que ayuda a los niños y adolescentes, y es anónimo, gratuito y confidencial.

# Ficha 4

## Ciberbullying

¿Te has sentido obligado a hacer cosas que tus compañeros querían porque tenían fotos o información sobre ti?

Hacer sentir mal a un compañero reenviando información suya sin su permiso puede llegar a provocarle daños muy graves y es un delito.

Recuerda que amenazar o querer que otro haga algo en contra de su voluntad se llama acoso o bullying y si se hace a través de internet (redes sociales, WhatsApp, etc.) se llama ciberbullying y tienes que reconocerlo cuándo se produzca.

# Ficha 5

## Ciberbaiting

### 1. ¿Sabes lo que significa ciberbaiting? ¿Sabes qué es acosar a un profesor?

A veces un grupo del colegio o del instituto decide tomarla con un profesor, meterse con él y hacerle sentir mal: publicando datos sobre él que no son ciertos, o haciendo fotos y vídeos que luego suben a la Red para que haga el ridículo y reírse de él, o creándole un perfil falso en las redes sociales, buscando en su móvil, en su tablet, o en su ordenador, información sobre él.

Debes saber que acosar a un profesor a través de Internet, WhatsApp o las redes sociales, se denomina ciberbaiting y, además de que te pueden expulsar del colegio, también se puede estar cometiendo un delito.

# Ficha 6

## Grooming

### 1. ¿Te has sentido obligado por un adulto a hacer cosas que te molestaban porque decía que tenía fotos o vídeos sobre ti que iba a publicar o subir a internet?

Por ejemplo, ¿algún amigo te ha obligado a encender la webcam de tu ordenador para poder verte?

Y si no es un amigo y ¿es un adulto?

A veces también utilizan tu información para hacerse amigo tuyo, por ejemplo, ven tu foto de las vacaciones y te dicen que ellos también estuvieron allí de vacaciones y que ya te conocían.

En otras ocasiones un adulto se puede acercar a ti, por ejemplo para enseñarte un cachorro en el parque, y pedirte que le digas tu teléfono, tu identificador en la red social, etc., para enviarte fotos del cachorro que seguro que te van a gustar.

### 2. ¿Sabes lo que significa grooming?

Cuando un adulto, a través de internet, WhatsApp, el ordenador, el teléfono móvil… se hace pasar por tu amigo y te pide imágenes o grabaciones tuyas íntimas o de contenido sexual se llama grooming.

En estos casos es un adulto el que se hace pasar por una persona de tu edad, en ocasiones porque ha accedido a tu información personal y sabe tus gustos y aficiones que utiliza para ganarse tu amistad y confianza.

Cuando ya han ganado tu confianza te piden que les cuentes cosas o que le envíes fotos que sólo se las dirías o enviarías a un amigo.

Entonces te acosan y te piden que hagas cosas de contenido sexual, por ejemplo que les envíes fotos o vídeos en los que estés desnudo o cosas más graves, y te amenazan con contarles a todos lo que le has dicho o mandarles las fotos que le enviaste.

# Ficha 6

## Grooming

Tienes que estar atento para poder reconocer estas situaciones, no fiarte de desconocidos que por internet te dicen que son amigos tuyos o que quieren serlo y tú no los conoces de nada.

El grooming es un delito y si te pasa a ti, o conoces a algún amigo o compañero al que se lo estén haciendo, debes decírselo a tus familiares, profesores o un adulto de tu confianza. Si te da vergüenza puedes decírselo a la Policía o a la Guardia Civil. También puedes llamar al teléfono de ANAR, 900 20 20 10, que es una asociación que ayuda a los niños y adolescentes, y es anónimo, gratuito y confidencial.

Sexting

# Ficha 7

## 1. ¿Sabes lo que significa sexting?

Es posible que hayas utilizado esta palabra cuando hablas con tus amigos sobre determinadas fotografías o vídeos que hayas recibido en tu smartphone, en tu email, o por mensajes en tu red social.

El sexting consiste en hacerse fotografías o grabarse en un vídeo o dejar que otros te las hagan o graben en una situación comprometida o pose íntima que no te gustaría que las viera todo el mundo, sobre todo tus familiares. Por ejemplo, desnudo, o parcialmente desnudo, o en una posición insinuante, y se las envías voluntariamente a alguien que puede que luego las reenvíe o difunda sin tu consentimiento.

## 2. ¿Es malo el sexting?

El enviar fotos de esta forma es muy arriesgado. Cuando envías una fotografía tuya a otra persona puede ser reenviada a otras personas sin tu permiso.

Puede terminar en internet y no podrás controlar quién puede ver tu fotografía. Las consecuencias pueden ser que te sientas mal y te avergüences delante de tú familia, amigos y compañeros, al saber que te han visto de esa manera, o que otra persona te acose, te humille, te amenace o te coaccione.

Incluso si ahora no te importa que te puedan ver sin ropa, tal vez, cuando crezcas te moleste que los demás tengan tu fotografía en estas condiciones.

## 3. ¿Qué hacer si recibes una fotografía de sexting?

Nunca reenvíes fotos de personas desnudas o semidesnudas, recuerda que la imagen de una persona es un dato personal y no puedes decidir sobre los datos personales de otra persona sin su permiso. El reenvío de imágenes de sexting es un delito.

# Ficha 8

## Recuerda que:

Recuerda que:

- @ Acoso es cuando alguien te molesta constantemente, cuando alguien no te deja en paz.
- @ Ciberbullying, ciberbaiting, grooming y sexting son acoso.
- @ El acoso es un delito.
- @ Algunas personas adultas pueden engañarte haciéndose pasar por una persona de tu edad, a veces utilizan un perfil falso o fotos de otras personas, a veces haciéndote creer que es alguien famoso para confundirte, ir ganando tu confianza y engañarte.
- @ Cuando te relacionas con un adulto conocido o desconocido nunca puede obligarte a hacer algo que te haga sentir mal.
- @ Cuando tratas con desconocidos puedes pensar que sólo pretenden hacerte sentir bien y quieren que te diviertas, pero no siempre es así. Ten cuidado.
- @ Debes ser prudente y no enviar a nadie fotos ni vídeos tuyos, ni los datos de tu familia, de dónde vives, de dónde estudias porque pueden emplearlas para hacerte daño.
- @ No puedes facilitar información de otras personas que conoces sin pedirles permiso (familiares, profesores, amigos, vecinos, etc.). Son sus datos personales y sólo ellos pueden decidir a quiénes facilitan sus datos personales.
- @ Si piensas que un adulto te está proponiendo algo que no está bien y te quiere obligar a hacerlo puede estar cometiendo un delito y debes hablar con tus familiares o tus profesores.

GUÍA
*para*
PADRES Y
PROFESORES

# Guíales en internet

## Ayúdales a construir su futuro

Los más pequeños manejan pantallas táctiles de forma natural y han crecido conociendo como parte de su entorno los dispositivos electrónicos e internet. Resulta casi imposible separar la convivencia del menor de la conexión con la Red. Su vida social ha pasado a tener un componente online en el que de forma casi instintiva sus datos personales son compartidos en red y la conciencia sobre la importancia de sus datos personales en ocasiones se acaba adquiriendo como resultado de una mala experiencia propia o de las personas próximas al menor. El niñ@ no es consciente de los riesgos a los que su actitud puede exponerle.

Esta guía sirve como complemento a la guía para jóvenes de la Agencia Española de Protección de Datos y pretende ofrecer a padres y educadores un texto orientador acerca de algunas consideraciones que pueden ser de utilidad en el buen uso de los datos personales, favoreciendo una convivencia saludable del menor con las nuevas tecnologías.

En la Agencia Española de Protección de Datos hemos diseñado una serie de elementos didácticos destinados a los menores pero, además, queremos facilitar una serie de reflexiones y recomendaciones que ayuden a los padres y profesores a comprender mejor estos riesgos y, así favorecer la tarea educacional en hábitos responsables para el adecuado uso de sus datos personales y los de terceros a través de cualquiera de los elementos electrónicos que tienen a su alcance.

FICHA 1

# Los datos personales del menor

Ha llegado el momento de la adquisición de su primer móvil. Posiblemente sea una oportunidad para decidir juntos aquel que mejor se adecúa a su edad y al uso que se le pretende dar. El teléfono ofrece a los padres la gran ventaja de estar en contacto con el menor, pero también es la puerta de entrada de algunos riesgos para la seguridad y la privacidad de los datos personales del niñ@ e incluso de su propia integridad física y psicológica.

Es posible que ya manejara una tablet en casa, también es posible que jugara con el ordenador en tu presencia o incluso que navegara, pero el teléfono abre una nueva etapa en la convivencia del niñ@ con la Red. Es un dispositivo que siempre le acompañará, que almacenará sus datos e información personal a la que podrán acceder terceros y que irá acumulando datos de otras personas como amigos, profesores, familiares, etc. A esta situación hay que añadir que no siempre podrá contar con la supervisión de un adulto.

Hasta ahora los datos de navegación del niñ@ estaban asociados a la identidad de un adulto, ahora será el propio menor quien utilizará su dirección de correo electrónico y número de teléfono para identificarse en su terminal y acceder a determinados servicios[1]. Esta información puede identificarle y estar a disposición de terceros para diferentes fines, que pueden incluir, por ejemplo, el envío de publicidad personalizada. Por ello, tal vez, interese añadir la información del niñ@ en un fichero de exclusión[2] para el envío de comunicaciones comerciales, evitaremos en gran medida que personas desconocidas puedan dirigirse al menor para ofrecerle productos u ofertas a través de llamadas telefónicas o mensajes de cualquier tipo.

Cuando hablamos de los datos personales del niñ@ hay que tener en cuenta que no se trata únicamente de su nombre, apellidos, correo electrónico, número de teléfono, etc. Además, entre sus datos personales se encuentran también los que son recogidos por las cookies[3] de los sitios web por los que navega, la información de las búsquedas, el historial de navegación que genera, sus perfiles en las redes sociales, sus datos de ubicación, etc. En definitiva es el momento en el que su identidad digital empieza a perfilarse a la vez que desarrolla su personalidad.

Un dato personal es cualquier información que haga posible la identificación de una persona. A menudo internet proporciona una falsa sensación de anonimato y nula sensación de riesgo.

Por ejemplo, el envío de una parte desnuda de su cuerpo a un tercero les puede hacer pensar en la imposibilidad de que alguien descubra

1 La instalación de aplicaciones y el uso de servicios exige la existencia de una dirección de correo electrónico.

2 Los ficheros de exclusión para el envío de comunicaciones comerciales son listas de usuarios que han manifestado su derecho de oposición al envío de comunicaciones comerciales. La inclusión del usuario en estas listas es gratuita, como las Listas Robinson de Exclusión Publicitaria.

3 Cookies: o «galletas» son ficheros que utilizan los sitios web en los que se almacena información de la sesión (usuario y contraseña) que se utiliza para acceder a un portal (correo electrónico, red social, etc.), también son ficheros que utilizan los sitios web por los que navegamos con el fin de almacenar información acerca de nuestras preferencias de navegación para adecuar la publicidad de estos sitios webs a nuestros hábitos de navegación.

# IDENTIDAD DIGITAL

su identidad. Sin embargo, en ocasiones, es tan fácil de descubrir su identidad como abrir en un ordenador las propiedades de la imagen y leer los metadatos[4]. También puede ocurrir que una marca en la piel (la forma del bronceado, un lunar, una cicatriz, etc.) que inicialmente no era perceptible aparece al ampliar la imagen y haga posible su identificación, o puede ocurrir que posteriormente, incluso años después, un determinado comentario del menor en una red social permita su identificación.

Es fundamental hablar con nuestros hijos o alumnos para concienciarles de la importancia de sus datos personales y de los del resto de personas con las que intercambian información. Una adecuada convivencia digital redundará en lo que podríamos denominar «salud digital», evitando problemas que puedan repercutir en su normal desarrollo.


«El paso por internet deja un rastro fácil de seguir»

4 Metadatos: muchos archivos digitales contienen información adicional a su contenido. Información relativa al terminal telefónico o cámara fotográfica utilizada, identidad de la persona que ha creado el archivo, fecha de captura, ubicación, etc.

4

FICHA 2

# Privacidad y seguridad: trucos para las trampas de internet

Cada vez son más frecuentes los intentos de engañar a los usuarios de internet mediante la utilización de webs que suplantan la identidad de sitios conocidos como bancos, redes sociales, webs de comercio electrónico, etc.

El engaño a veces se basa en la similitud tipográfica del nombre del sitio real al que se suplanta. En la guía para jóvenes se ha utilizado el ejemplo «www.mogollondejuegos.com» como supuesto nombre real de un sitio web frente al de nombre«www.mogolondejuegos.com», un supuesto sitio web que intenta engañar al menor, un pequeño error al teclear la dirección le llevaría a un sitio web con una posible identidad falsa.

Es necesario hacer entender al niñ@ la necesidad de verificar la dirección de internet en el navegador, especialmente cuando se va a introducir su nombre de usuario y contraseña o cuando intenta registrarse en una web con sus datos personales.

Otra vía frecuente para este engaño son los correos electrónicos o la mensajería instantánea[5]. Es frecuente la realización de campañas de «phishing»[6] en las que se remiten masivas oleadas de mensajes electrónicos que le invitan a enviar, actualizar o revisar sus códigos de usuario, contraseña o sus datos personales, y que contienen enlaces a sitios web fraudulentos o ficheros que al abrir dañan el dispositivo o el ordenador.

Conviene que el niñ@ entienda esta situación para no poner en riesgo sus datos personales. En algunos casos los mensajes contienen un archivo adjunto que al abrirlo ocasiona el bloqueo del ordenador o del dispositivo. En la Guía para Jóvenes nos referimos a esta situación como el robo o el secuestro de las carpetas porque la información que contenga el dispositivo o el ordenador dejará de ser accesible. Además, el pago de la cantidad reclamada por el delincuente no garantiza el desbloqueo del ordenador o dispositivo.

Determinadas descargas de programas o apps pueden poner en riesgo los datos personales del menor, por lo que es preciso concienciarle para evitar la instalación de programas o apps de origen desconocido. Suele ser habitual la descarga de contenido multimedia o programas informáticos que por su nombre crean en el niñ@ la expectativa de disponer de determinados contenidos que en última instancia pueden resultar inapropiados.

Es indispensable disponer de un antivirus tanto en el ordenador como en el resto de dispositivos, ya que el antivirus realiza un análisis de los programas, apps y archivos que se cargan en el ordenador y en los dispositivos del menor. Sin olvidar que los antivirus no realizan un análisis del contenido temático, por ejemplo, de las webs que visita el menor por lo que no ofrecen

5 Mensajería instantánea: cualquier herramienta, app, o aplicación informática que permite el envío de mensajes en tiempo real como por ejemplo: WhatssApp, Hangouts, Line, etc. En este apartado se incluyen los medios de mensajería de las redes sociales que permiten el «chat» o diálogo en tiempo real entre varios usuarios.

6 Phishing: envío de mensajes electrónicos con enlaces que conducen a sitios web que suplantan la identidad digital de sitios webs habituales (bancos, redes sociales, correo electrónico, etc.) para el usuario con el fin de robar claves de acceso a cuentas bancarias, datos personales o bloquear el ordenador o dispositivo electrónico reclamando dinero a cambio de una contraseña para el desbloqueo del mismo. Algunas de estas campañas utilizan direcciones de correo electrónico aparentemente reales como por ejemplo «**envios@correos.es**» o «**policia@policia.es**».

«¿www.mogollondejuegos.com o www.mogolondejuegos.com? Enséñales a verificar los direcciones de internet»

protección frente a contenidos inadecuados.

Si se desea controlar el acceso del menor a determinados contenidos es necesario disponer de un programa para el control parental que permita controles y opciones sobre el uso del dispositivo por parte del menor, como impedir el acceso a contenido inapropiado[7], limitar el tiempo de uso del terminal o de los juegos, evitar el uso de determinado vocabulario, restringir los resultados de las búsquedas en internet o conocer los sitios que ha visitado, limitar el acceso de aplicaciones a los datos personales del menor, conocer la ubicación del niñ@, etc. En cualquier caso, si se decide usar este tipo de herramientas, habría que considerar la posibilidad de llegar a acuerdos con el menor de forma que sea consciente de que se ha instalado una herramienta de este tipo y los motivos por los que es necesaria.

La Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad pone a su disposición abundante información y herramientas gratuitas que podrían ser útiles para garantizar la seguridad de los dispositivos electrónicos en general.

En la Guía para Jóvenes se recomienda no utilizar ninguna wifi sin clave: un canal wifi que no disponga de clave envía nuestros datos (incluyendo nombre de usuario y contraseña) sin ningún cifrado ni protección y los hace accesibles a cualquier persona con ciertos conocimientos informáticos.

Con relación a las «galletas» o «cookies», que se mencionan en la Guía para Jóvenes, es ya habitual que al entrar en una web se nos informe acerca del uso de cookies que guardan nuestra información personal. Sería interesante ayudar al menor a entender que la finalidad de esta información es la publicidad y explicarle la forma de eliminar las las cookies[8].

7 Contenido pornográfico, webs de compras, suicidio, anorexia, etc. conocido también como «internet tóxico».

8 En el navegador del ordenador (Google Chrome, Internet Explorer, Mozilla) el menú para eliminar los datos de navegación se obtiene a través de los menús del propio navegador o con la combinación del teclado «Mayús + Ctrl + Supr». En smartphones y tabletas se accede a través de las opciones de configuración de privacidad.

# Protección de datos personales. Seguridad, derechos.

FICHA 3

En este apartado de la Guía para Jóvenes se facilitan al menor unas nociones sobre sus derechos[9], que siempre podrá ejercer cuando se registra en un sitio web, junto a algunas recomendaciones que debe tener en cuenta.

El menor de catorce años debe de contar con el consentimiento de sus padres o tutores legales para registrarse y, a su vez, la información que se le puede pedir debe ser proporcional a la finalidad o uso que se pretende. Para el caso de un registro web no sería proporcional que le pidan al menor datos de su entorno familiar salvo que se solicite con el fin de otorgar el consentimiento[10] de padres o tutores.

Es muy probable que al menor le cueste decidir su nombre de usuario: puede que le guste un nombre que permita a sus amigos reconocerle fácil y rápidamente. Como es probable que ese nombre ya haya sido utilizado, la solución suele ser que el menor añada a continuación su edad o su fecha de nacimiento para poder utilizar el nombre que haya elegido. El nombre de usuario es un identificador personal que no debe de facilitar a extraños información acerca de la fecha de nacimiento o de la edad del usuario. Se evitará encarecidamente que se pueda obtener información partiendo de su nombre de usuario, ya que esta información del niñ@ puede funcionar como reclamo para actividades como el acoso o la pederastia.

Otra de las recomendaciones que se hacen al menor trata de la elección de sus claves, que siempre deberían ser de más de ocho caracteres incluyendo mayúsculas minúsculas y caracteres especiales. Se puede recomendar al niñ@ que utilice recursos nemotécnicos para recordar la contraseña usando, por ejemplo, parte de una canción que le guste o de un texto que recuerde y que sobre el mismo haga variaciones de carácter tipográfico.

Se recomienda también al menor no elegir palabras que ya existan en un diccionario, pues suele ocurrir que los delincuentes utilizan bases de datos de diccionarios para acceder a cuentas de otros usuarios y obtener sus datos personales o la cuenta o la identidad digital del niñ@.

En ningún caso se deben utilizar contraseñas del entorno del menor, por ejemplo, el nombre de la mascota, la marca o modelo del vehículo de la madre o del padre, el barrio donde se vive, el equipo de fútbol en el que juega el niñ@, etc.

También es importante que el menor conozca que siempre debe utilizar el botón de «cerrar sesión» o «salir». Cerrar el navegador no siempre equivale a cerrar sesión, y puede permitir que otro usuario abra el navegador y tenga acceso a su información personal o utilice la identidad digital del menor.

Antes de proceder al registro de los datos personales del menor se recomienda leer la política de privacidad[11] de la página web. En la política de privacidad nos deben informar sobre la fina-

**9** Derechos ARCO: derecho de acceso: a solicitar y obtener información de nuestros datos de carácter personal sometidos a tratamiento, derecho a rectificarlos, derecho a cancelarlos y derecho a oponernos a su tratamiento.

**10** En cualquier caso la información ofrecida al menor deberá expresarse en un lenguaje que le sea fácilmente comprensible.

**11** La política de privacidad describe como se recoge, guarda y utiliza la información que facilitamos a través de los diferentes servicios, redes sociales o páginas webs que visitamos. Es importante que el niño entienda qué información se recoge y cómo se utiliza ya que el acceso a este sitio implica la aceptación de esas condiciones.

# política de privacidad): trucos para apuntarme y borrarme en un sitio web

lidad de los datos que aportamos, la identidad del responsable de tratar los datos y la forma de ejercer los derechos de acceso, rectificación, cancelación y oposición (ARCO).

Para el ejercicio de los derechos del menor de 14 años en relación con sus datos personales, los padres o tutores legales deberán solicitarlo ante el responsable del fichero o del tratamiento de datos personales, acreditando su condición de madre, padre o tutor legal.

La información para ejercer estos derechos debe aparecer dentro de la política de privacidad de cualquier sitio web que utilice datos personales de sus usuarios. Si no fuera así, siempre se puede consultar el Registro General de Protección de Datos en la web de la Agencia Española de Protección de Datos donde se encuentra a disposición de los interesados la información relativa a los titulares de ficheros de datos personales ante quienes ejercer los derechos de acceso, rectificación, cancelación y oposición. Finalmente, si los derechos del menor no fueran atendidos, los padres o tutores legales pueden solicitar la Tutela del Derecho ante la Agencia Española de Protección de Datos, que instará al responsable del fichero para que atienda los derechos del menor.

También es posible que el niñ@ ejerza sus derechos frente a los buscadores de internet, solicitando la cancelación de los resultados de búsqueda en los que aparezca. Es lo que se denomina «derecho al olvido», derecho que puede ser ejercido por cualquier persona afectada y, en el caso de menores de 14 años, siempre a través de sus padres o tutores legales.

8

FICHA 4

# Acoso y convivencia en la red: trucos para evitar malos rollos

En este apartado intentamos dar al joven la noción de respeto y convivencia en la Red. La convivencia digital no se distingue de la convivencia de la vida real y el niñ@ debe ser consciente de que sus palabras o sus hechos pueden ofender o dañar a otras personas y que en ningún caso en la Red se debe de hacer algo que no se haría en la vida real. Detalles como evitar escribir mensajes en mayúsculas[12] o evitar palabras malsonantes, que no se utilizarían en presencia del interlocutor, pueden ayudar a mantener un clima de convivencia entre los menores.

También intentamos dar al menor la noción de acoso, que puede resultar un término abstracto que conviene concretarlo de alguna manera con algunos ejemplos específicos, como el hecho de recibir constantes llamadas o mensajes a cualquier hora. Si el niñ@ no es capaz de identificar una situación de acoso podría verse involucrado en ella por el simple desconocimiento y verse envuelto en un posible delito.

Otra medida preventiva es la concienciación del menor para que ignore mensajes de personas desconocidas, mensajes de correo electrónico, mensajería instantánea, redes sociales, buzón de voz o de cualquier otra índole. El menor nunca debe enviar fotografías a un desconocido porque podría dar información de su edad, vivienda, entorno social o sobre su ubicación.

Finalmente, además de ayudar al menor a identificar una situación de acoso, se le recomienda que evite acosar a otras personas. El menor debe ser consciente del uso respetuoso de los datos personales de los demás y no utilizarlos para ofender o ridiculizar a otros.

12 En los mensajes electrónicos las mayúsculas pueden ser entendidas como gritos por la persona a la que se dirige el mensaje.

# FICHA 5

# Redes sociales: con los amigos en la red

El objetivo de este apartado es proporcionar algunas pautas encaminadas a facilitar la convivencia y el buen uso de los datos personales del joven y de los de sus amigos y conocidos.

En primer lugar es conveniente que el menor entienda que el término «amigos» en las redes sociales no es lo mismo que en la vida real, donde la amistad se forja compartiendo experiencias. En las redes sociales un simple clic se utiliza para designar a un«amigo». En algunas redes se utiliza el término «seguidor[13]» para designar a las personas con las que compartes contenidos en la red. La semántica utilizada en las redes sociales puede crear cierta confusión en el niñ@.

Una vez que el menor se registra en una red social, deberemos ayudarle a revisar su configuración de privacidad, evitando que sus publicaciones puedan ser visibles por todo el mundo o indexadas por los buscadores. Un detalle que se debe tener en cuenta es evitar en todo momento facilitar las opciones de ubicación que posibiliten a terceros identificar el lugar donde se encuentra el menor.

Es recomendable compartir con el niñ@ sus primeras publicaciones para que vea cómo ven los demás lo que publica. Mostrando al menor el resultado de sus publicaciones, etiquetados y comentarios puede entender que no gusten o molesten.

La información personal que el menor comparte con sus amigos podría, a su vez, ser vista por los amigos de sus amigos. El menor no debe compartir la información personal que sus amigos comparten con él, antes debería considerar si esto podría molestarles.

Si el menor utiliza blogs o foros es importante proteger su identidad con un alias o pseudónimo y evitar cualquier información que permita que sea identificado o que proporcione pistas acerca de su edad.

**13** Redes Sociales como por ejemplo Twitter o Instagram utilizan el término «seguir», en otros casos, como por ejemplo Facebook, se utiliza el término «amigos» o «mejores amigos» y, en ocasiones, se utiliza la palabra «seguir» para designar a las personas de entre sus «amigos» cuyas publicaciones tiene interés en seguir.

FICHA 6

# Mensajería instantánea: mensajes sin parar

Los mensajes que intercambiamos contienen información personal nuestra o de otras personas. En este apartado intentamos que el niñ@ sea consciente de esta situación proporcionándole algunas recomendaciones para evitar el mal uso de la mensajería o la información personal que se intercambia en los mensajes.

El smartphone o la tablet facilitan el envío o reenvío de cualquier información de forma intuitiva, lo que puede empujar al menor al reenvío de mensajes que podrían ofender a otras personas, como podría ser el caso de imágenes o vídeos que pudieran resultar ofensivos para otro menor o formar parte de una cadena de acoso.

En el correo electrónico es importante hacerle ver la conveniencia de utilizar la opción de envío con copia oculta, evitando que un mensaje que vaya dirigido a múltiples personas revele las direcciones de correo de todos los destinatarios: las direcciones de correo electrónico son un dato personal que puede aportar información de otra persona (trabajo, colegio, etc.) por lo que antes de enviar un correo electrónico a múltiples destinatarios el menor deberá ser capaz de entender esta situación.

En las redes sociales, debe distinguir entre publicar un mensaje que sea visible a todos sus amigos de la red social o utilizar la opción de mensaje privado que solamente sea visible para su destinatario. Habitualmente los comentarios en las redes sociales son públicos y si no se desea que sea visible públicamente es preciso recurrir a un mensaje privado[14].

Las aplicaciones de mensajería instantánea y mensajes multimedia (MMS) pueden permitir la posibilidad de descargar automáticamente el contenido multimedia o descargarlo a petición del usuario. Una buena medida para limitar el acceso del menor a posibles contenidos no deseados o software malicioso podría ser configurar la aplicación para que vídeos y fotografías no se descarguen sin el control del usuario.

La inclusión forzada del menor en un grupo de intercambio de mensajes puede hacer que se sienta acosado. Por este motivo debemos concienciarle para que no permanezca en un grupo del que no desea formar parte y que debe respetar la decisión de otra persona que no desee pertenecer a un determinado grupo.

**14** Mensaje Privado: a veces se representa con su acrónimo MP.

# FICHA 7

## Ajustes de privacidad: trucos para la tablet, móvil y ordenador

La mayor parte de los fabricantes de dispositivos móviles incluyen una cuota de espacio para el almacenamiento de archivos en la nube. Este espacio suele venir configurado por defecto, de forma que fotografías, archivos y copias de seguridad se suben directamente a la nube.

En este apartado intentamos que el menor sea consciente de esta circunstancia y de que existe la posibilidad de no guardar información en la nube si no lo desea. También puede ocurrir que el espacio de almacenamiento en la nube pudiera ser accesible a otras personas. Por ello es importante leer las condiciones de uso y de acceso a la información del menor en la nube con el fin de determinar quién podría tener acceso a sus cosas. Si se optara por no utilizar la nube se recomienda que se guarde una copia del contenido de la tablet o móvil en otro soporte (ordenador, pendrive, disco duro).

Otra de las cuestiones importantes de este apartado son las opciones de los terminales móviles que permiten a un tercero realizar un seguimiento del menor como la interfaz wifi, bluetooth y GPS. Se recomienda que cuando no los utilice procure desconectarlos.

Finalmente, en esta sección prevenimos al menor acerca de la posibilidad de que un virus permita que otra persona pueda observarle a través de la cámara de su ordenador, recomendándole que procure utilizar una pegatina sobre el objetivo de la cámara cuando no la necesite. Se debe evitar disponer de una webcam siempre en disposición de captar el espacio en el que se encuentra el niñ@. El mismo riesgo puede existir con las cámaras del smartphone o la tablet.

12

FICHA 8

# Sexting y adicción: bloquea y desconecta

Comprobar si ha llegado un mensaje en las redes sociales, en el correo electrónico o en cualquier aplicación de mensajería electrónica puede ocasionar adicción.

En algunos casos esta situación tiene repercusión sobre el descanso del niñ@ y en consecuencia sobre su rendimiento y desarrollo como persona. Si fuera necesario, se recomienda en primer lugar que exista un diálogo entre padres, tutores, profesores y el niñ@ con el fin de ayudarle a ser consciente de la situación. El diálogo es una herramienta fundamental para, por una parte, racionalizar el uso de los dispositivos y, por otra, si fuera necesario, acordar horarios y formas de uso.

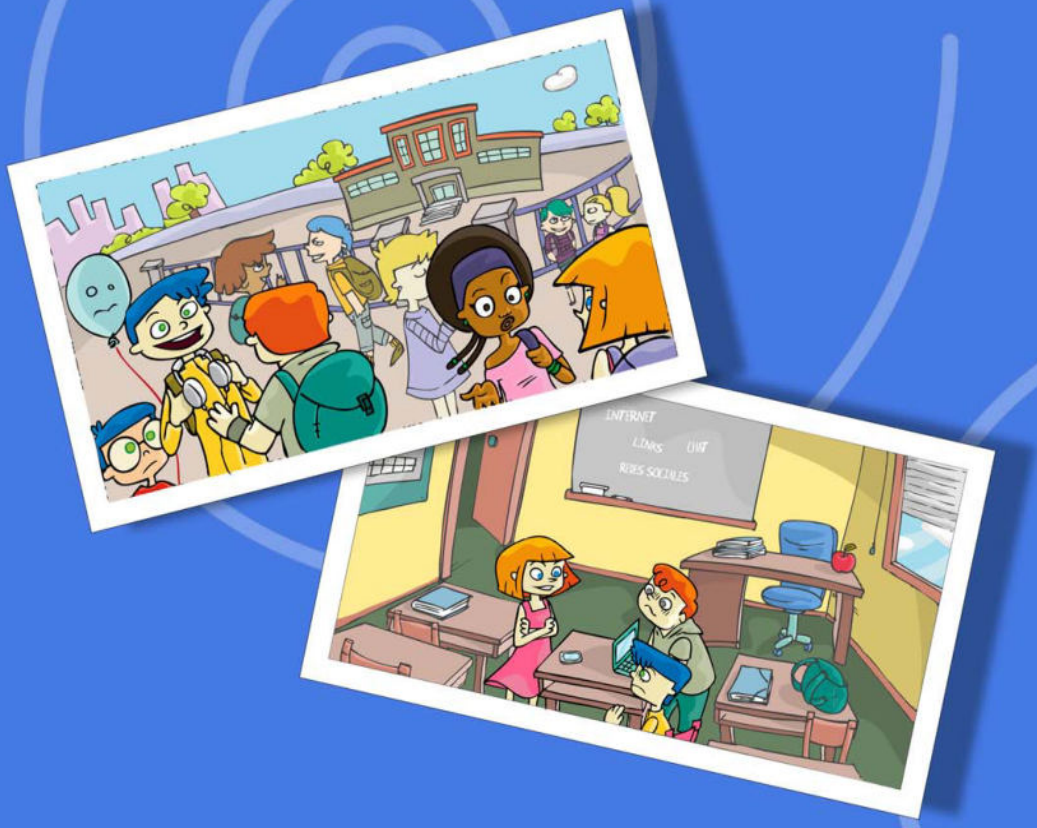
El sexting[15] no es ajeno a los menores. En algunos casos se utiliza el teléfono móvil para capturar imágenes parciales del cuerpo, suyas o de otras personas, para lanzar una cadena de reenvíos desafiando a los demás a averiguar la identidad de la persona que aparece en la imagen o bien como una forma de acoso. El sexting es un delito. El menor debe ser conocedor de este extremo con el fin de no participar en ningún juego de este tipo y de advertir a sus padres, profesores o personas de su confianza acerca de esta situación.

«El sexting es un delito. El menor debe ser conocedor de este extremo»

**15** Visita nuestra **Ficha Didáctica** sobre «Suplantación de Identidad, Ciberbullying, Grooming, Sexting».

GUÍA
para
FAMILIARES Y
PROFESORES

# Enséñales a ser legales en internet






Colegio Concertado
*Ruta de la Plata*
*Almendralejo.*

# Introducción

El uso de internet por los menores de edad, niños y adolescentes, es una constante que comienza a edades cada vez más tempranas. Según la Comisión Europea la edad de comienzo a navegar por internet es de 7 años. Desde que los menores comienzan su andadura en la Red su uso se va incrementando progresivamente. La encuesta sobre hábitos de uso y seguridad de internet de menores y jóvenes en España realizada por el Ministerio del Interior en junio de 2014, recoge que el 60% de los niños entrevistados usa internet todos los días y la frecuencia más habitual es entre 1 y 2 horas, aunque estos porcentajes y tiempos aumentan a medida que van creciendo, así el 83% de los mayores de 15 años usa internet todos los días y su frecuencia de uso es de más de 2 horas y media. Según el VI estudio de IAB Spain el 97% de los menores de 14 a 17 años usan las redes sociales.

En cuanto al uso que hacen de internet, aunque la mayoría lo utiliza para realizar trabajos escolares, el uso de la mensajería instantánea, el intercambio de mensajes con amigos y contactos, la visita de perfiles tanto propios como de terceros están muy extendidos.

Con carácter general, las actividades que realizan en internet proporcionan beneficios, satisfacción y distracción a los usuarios menores de edad y no causan perjuicios a terceros, pero en ocasiones esto no es así y el uso de internet puede implicar ciertos riesgos, más o menos graves, e incluso llegar a constituir una conducta delictiva que origina graves consecuencias a las víctimas y también a sus autores y familiares. El origen de estas conductas puede obedecer a varias causas, como el desconocimiento de que lo que se esté haciendo sea malo, o que llegue a ser un delito, la sensación de anonimato e impunidad que proporciona internet, o también la creencia de que por ser menores no les va a pasar nada.

Cuando en el uso de los servicios de internet se recaba o difunde información de carácter personal de manera inadecuada se puede poner en riesgo al menor e incluso suponer infracciones penales con las graves consecuencias que esas conductas implican.

La Agencia Española de Protección de Datos, en el marco de sus funciones, quiere contribuir a evitar y reducir estas situaciones mediante actuaciones preventivas dirigidas a informar y sensibilizar sobre las consecuencias negativas de determinadas conductas, educando y formando a los menores en privacidad y protección de datos para que dispongan de recursos que les ayuden a prevenirlas.

Junto a la formación de los menores en materia de protección de datos, un aspecto importante es el su sensibilización sobre las consecuencias de conductas que pueden

llegar a constituir delitos, o que pueden facilitar a terceras personas, sobre todo adultas, su comisión y resultar ellos las víctimas.

El catálogo de delitos que se pueden cometer a través de internet por los menores, al igual que por los adultos, es variado e incluiría delitos relativos a la intromisión en la intimidad, contra la propiedad intelectual, industrial, apología del terrorismo, incitación al odio y a la violencia, delitos de odio, etc. pero ahora vamos a centrarnos en aquellos que están directamente vinculados a la utilización de la información personal como elemento que los generan o propician y que pueden afectar de manera significativa al desarrollo natural de los menores.

Los expertos han vienen advirtiendo del incremento de los delitos cometidos por menores a través de internet, especialmente de aquellos que tienen vinculación con el uso de la información personal.

Con esta guía se quiere dotar a familiares, profesores y personas próximas al menor de un complemento a las fichas sobre ciberbullying, ciberbaiting, grooming y sexting dirigidas a los menores, que les proporcionen orientaciones, consideraciones y pautas que les sirvan de ayuda en su labor de educación y formación.

Bajo estas denominaciones, que no aparecen en el Código Penal, se integran unas conductas que pueden dar lugar a varias figuras delictivas, cuyas consecuencias, además de las producidas por las concretas acciones que se realicen, van a depender de la edad de los menores.

A los menores de 14 años no se les va a exigir responsabilidad penal por los posibles delitos que cometan, son inimputables, pero ello no excluye que puedan producirse otras consecuencias, por ejemplo podrían dar lugar a la responsabilidad civil de los padres o tutores por todos los perjuicios que se hayan podido causar a otras personas.
De 14 a 18 años los menores tienen responsabilidad penal por la comisión de todos los delitos tipificados en el Código Penal, en los términos establecidos en la Ley Orgánica 5/2000, de 12 de enero, de responsabilidad penal de los menores, que establece las medidas que pueden imponérseles por la comisión de delitos como amonestaciones, prestaciones en beneficio de la comunidad, realización de tareas socioeducativas, permanencia en el domicilio durante el fin de semana, el internamiento..., además de la responsabilidad civil que pueda exigírsele por daños y perjuicios causados y de la que responden solidariamente sus padres y tutores.

La Ley Orgánica 1/2015, de 30 de marzo, que modifica de manera importante el Código Penal, ha reforzado el principio del interés superior del menor y dispensa una mayor protección a las víctimas de estos delitos, especialmente si se trata de menores, y ha introducido algunas novedades que afectan a la tipificación de los delitos en los que se puede incurrir en los casos de ciberbullying, ciberbaiting

grooming y sexting que conviene tener presente.

Para ello tenemos que conocer qué se entiende por ciberbullying, ciberbaiting grooming y sexting y a qué figuras delictivas pueden dar lugar.

Con la denominación de **ciberbullying** se hace referencia a las situaciones de acoso realizadas a través de Internet y entre menores, ya sea entre dos menores o, como comúnmente ocurre, de un grupo de menores hacia un menor determinado. Podemos decir que es una versión online, una evolución del acoso escolar, que se lleva a cabo a través de medios digitales o electrónicos. Cuando el acosado es el profesor y se realiza por los alumnos se denomina **ciberbaiting**.

El **grooming** se viene definiendo como el embaucamiento y acoso al que se ve sometido un menor por un adulto mediante acciones a través de medios digitales que buscan ganarse la confianza del menor haciéndose pasar por otro menor con fines de abuso sexual o pornografía infantil, sin descartar otros tipos de chantaje o extorsión. Los autores son los adultos, pero en ocasiones la información personal proporcionada por los menores facilita estas conductas al permitir al adulto obtenerla, por ejemplo, a través de las redes sociales donde los menores suelen colocar información personal, como fotografías o el número de teléfono. A partir de ahí, el resto de información necesaria para acosar a un menor el adulto la obtiene del propio menor mediante engaño.

Con la expresión **sexting** nos referimos a la práctica cada vez más extendida de mandar imágenes propias, fotografías y vídeos íntimos, o con contenido sexual, que son tomadas y grabadas por los protagonistas de las imágenes o, con su consentimiento, por terceras personas y posteriormente difundidas de manera no consentida. El origen se encuentra por tanto en una acción voluntaria y confiada por parte de quien toma sus imágenes y las envía, pues sus destinatarios suelen ser personas de su confianza, como la pareja o los amigos íntimos.

Lo que ocurre es que a partir de aquí se pierde el control sobre las imágenes, sobre los datos de carácter personal, y se pierde privacidad, pues pueden llegar a tener una difusión ilimitada. Constituye un delito la difusión o cesión a terceros de estas imágenes o grabaciones, sin autorización de la persona afectada, cuando menoscabe gravemente su intimidad.

Estas figuras pueden suponer la comisión de diversos tipos de **actividades delictivas**, entre otras, las siguientes:

- Delitos de amenazas: cuando se amenaza a una persona o a alguien de su familia o con el que esté íntimamente relacionado con causarle un mal, constituya delito o no, por ejemplo, de revelar o difundir hechos referentes a la vida privada del amenazado o relaciones familiares que no sean públicamente conocidos y puedan afectar a su fama, crédito o interés.

  Puede implicar una pena de privación de libertad que oscila entre los tres

meses y los cinco años, dependiendo de las circunstancias de la amenaza.

@ Delitos de **acoso** (coacciones). El artículo 172 ter del Código Penal castiga con prisión de tres meses a dos años o multa de seis a veinticuatro meses al que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, de manera que altere gravemente el desarrollo de su vida cotidiana, entre otras las siguientes acciones:

  @ La vigilancia, la persecución o la búsqueda de cercanía física.
  @ El establecimiento o el intento de establecer contacto con la persona acosada a través de cualquier medio de comunicación.
  @ La adquisición de productos o mercancías, o la contratación de servicios, o hacer que terceras personas se pongan en contacto con la persona acosada mediante el uso indebido de sus datos personales.
  @ Atentar contra su libertad.

Cuando la víctima sea una persona especialmente vulnerable por razón de edad, enfermedad o situación se impondrá la pena de prisión de seis meses a dos años.

@ Delito **contra la integridad moral:** el artículo 173.1, párrafo primero, del CP: el que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral, será castigado con la pena de prisión de seis meses a dos años.

@ Delito de **calumnias:** achacar a una persona la comisión de un delito, sabiendo que no es cierto. Está castigado con pena de prisión de seis meses a dos años o multa de doce a veinticuatro meses si es con publicidad y, en otro caso multa, de seis a doce meses e indemnización por daños y perjuicios.

@ Delito de **injurias**: consiste en humillar, insultar, ofender a un tercero de manera que lesione su dignidad, menoscabando su fama o atentando contra la propia estima. Se castiga con multa de tres a siete meses y de seis a catorce si se realiza con publicidad.

@ Delitos de **descubrimiento y revelación de secretos**: Se castiga con la pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. Pena que se impondrá en su mitad superior cuando la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección o los hechos se hubieran cometido con una finalidad lucrativa (sexting).

@ Delito de **inducción al suicidio,** castigado con pena de prisión de cuatro a ocho años.

Sin olvidar los **delitos contra la libertad y la identidad sexual** que se pueden cometer utilizando internet y la información personal como medios para consumarlos.

Merece hacer mención especial a la modificación introducida con la reforma del **Código Penal en el artículo 183 ter**, que establece que:

"1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189 (abusos y agresiones sexuales a menores de 16 años), siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño. 2. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años".

En estas conductas son relevantes las modificaciones del Código Penal que se han llevado a cabo por la Ley Orgánica 1/2015, de 30 de marzo, elevando la edad del consentimiento sexual de 13 a 16 años.

Las consecuencias de un uso inadecuado o inconsciente de la información personal en internet por los menores pueden llegar a ser extremadamente graves, por lo que se requiere que se les eduque en un uso sostenible de los servicios que ofrece internet, haciéndoles ver, sin alarmarles, que pueden acabar cometiendo un delito, las consecuencias que ocasiona en las víctimas, y las responsabilidades que se pueden derivar para ellos, así como para sus padres y tutores.

Del mismo modo: es importante sensibilizarles de que pueden llegar a ser ellos las víctimas de los delitos si no son cuidadosos con la información personal que transmiten.

Desde el punto de vista de la privacidad y la protección de datos, determinados comportamientos a la hora de utilizar la información personal en internet propician estas situaciones, como los que se exponen en las fichas orientadas al menor y que se comentan a continuación.

Se recomienda la lectura y el trabajo ordenado de forma secuencial de las fichas para menores.

# Ficha 1

## Los datos personales que compartes

Cuando el menor facilita datos personales suyos o de su entorno familiar, existe la posibilidad de que estos datos sean utilizados con **fines ilícitos** en perjuicio de su propia intimidad, generando posibles situaciones de acoso y que podrían materializarse en determinados delitos como por ejemplo en el delito de acoso previsto en el artículo 172 ter del Código Penal y al que se ha hecho referencia en la introducción. Hay que tener en cuenta que el menor entra dentro de la consideración de persona especialmente vulnerable por razón de su edad y además, cuando concurra, por razón de enfermedad o discapacidad.

Los adultos que participan en la educación menor (familiares, educadores, etc.) deben tener en cuenta que tal vez el menor no haya alcanzado el grado de madurez intelectual necesario para poder valorar la **intimidad y la privacidad** de su familia, la suya propia o la de otras personas. Intimidad y privacidad son términos abstractos que incluso a un adulto le puede resultar difícil de convertir en hechos concretos o tangibles en determinadas situaciones. Para prevenir al menor frente a acciones de terceros que puedan perjudicar su intimidad y privacidad es necesario que el menor identifique "privacidad" e "intimidad" como algo que le pertenece y que sus datos personales son la llave que permite acceder a otras personas a compartir parte de su intimidad.

Para empezar es necesario que el menor sea consciente de aquellos **datos personales** suyos o de otras personas que está compartiendo en internet (dispositivos móviles, mensajería instantánea o redes sociales, etc.) y reflexione también acerca de quiénes pueden tener acceso a su información personal y la forma de comprobarlo (contactos, seguidores, amigos, etc.). Conviene concienciar al menor acerca de los posibles riesgos. Puede, por ejemplo, ocurrir que alguien le robe el terminal a un amigo o que un compañero de clase se deje una sesión abierta en una red social, en estas y otras circunstancias un tercero podría acceder a sus datos personales o los de sus amigos y hacer un uso indebido de los sus datos personales. Un ejercicio que puede resultar interesante es reflexionar con el menor, o con un grupo de menores, acerca de estos tres aspectos: los datos personales que comparten, quiénes tienen acceso y qué situaciones no previstas podrían dar acceso a sus datos a otras personas a las que no se les hubiera autorizado.

Es preciso hacer ver al menor que cuando las personas intercambian su número de teléfono, su dirección de email, o cualquier dato personal, lo hacen con la finalidad de mantener contacto mutuo y nunca deben utilizar estos datos para dañar a otra persona. El menor debe tener en cuenta que **cada persona decide sobre sus datos personales** y nunca debe tomar

decisiones sobre los datos personales de otras personas, nunca deberá ceder datos personales a terceros y en especial a los que le sean desconocidos, esta cuestión es especialmente relevante en el contexto de las redes sociales donde un simple click basta para compartir información personal de terceros.

# Ficha 2

## Cosas que no te gustaría que hicieran con tus datos personales

En esta ficha se realiza una aproximación circunstancial en la que el propio menor o algún compañero podría verse involucrado. Se trata de ubicar al menor en hipotéticas circunstancias haciéndole consciente de la distinta **carga emocional** que puede suponer cada uno de estos casos. Algunos de los casos que se plantean pueden ser matizables dando lugar a situaciones que podrían resultar inocuas para la privacidad del menor o con algún matiz o variación pueden dar lugar a una situación de acoso. Conviene hacer reflexionar al menor sobre los sentimientos que estas o similares circunstancias pueden producir en otra persona, se trata de un ejercicio de empatía personal de reflexión y de diálogo entre los menores y entre menores y educadores. El diálogo con el menor debería resultar motivador para animarles a expresar sentimientos o emociones que determinadas conductas o uso indebido de los datos personales pueden suponer sobre otras personas. En definitiva, el objeto de esta ficha es permitir al menor asociar una carga emocional negativa a un posible uso ilícito de sus datos personales o los de otra persona.

# Ficha 3

## Protégete

Algunos conceptos como acoso, leyes, derechos y delitos pueden presentar cierta dificultad para el menor en cuanto a su comprensión. En esta ficha intentamos ayudar al menor a identificar situaciones de acoso y mostrar al menor el significado de estos términos.

Es preciso tener en cuenta que la Ley Orgánica de Protección de Datos de Carácter Personal garantiza los derechos de las personas a decidir sobre sus datos personales. Una infracción de los términos que fija esta Ley Orgánica es una infracción administrativa mientras que, cuando hablamos de acoso, nos referimos a una infracción que puede tener consecuencias penales para el menor.

El menor debe ser consciente de la existencia de sus derechos y de los derechos de los demás, también debe ser conocedor de que algunas actitudes implican infracciones que pueden tener consecuencias para él y su entorno personal.

# Ficha 4

## Ciberbullying

**¿Qué es el Bullying?**

El concepto refiere al acoso escolar y a toda forma de maltrato físico, verbal o psicológico que se produce entre escolares, de forma reiterada y a lo largo del tiempo.

**¿Qué significa Ciberbullying o Ciberacoso escolar?**

Es la utilización de redes de comunicaciones (internet, telefonía móvil, videojuegos online, etc.) para humillar, vejar, difamar o acosar a otras personas, lo que supone ya un delito.

Se trata de un acoso entre iguales y cuando se produce entre menores reviste especial gravedad por las consecuencias que puede ocasionar.

**¿Qué posibles acciones se incluyen bajo este concepto?**

Entre los ejemplos que aparecen en la segunda ficha de la guía "Sé legal en Internet", recomendamos que se trabaje con los menores para averiguar cuándo podría decirse que son casos de ciberbullying.

Las consecuencias del acoso siempre tienen impacto en el desarrollo del menor por lo que conviene estar alerta para identificar cualquier situación que impida al menor vivir con normalidad su etapa infantil y adolescente o que pueda finalmente suponer un anclaje psicológico negativo en su vida como adulto. La ayuda de expertos en el ámbito docente, psicológico, etc. puede ser necesaria para minimizar el impacto de la situación de acoso vivida por un menor.

Las situaciones de acoso pueden producirse en cualquier entorno en el que se desenvuelve la vida del menor, entorno tanto físico como virtual o electrónico. El acosador puede pertenecer a cualquier círculo de personas en el que se desarrolla la vida del menor.

Pero, a diferencia de una situación de acoso físico, el **ciberbullying** o acoso entre menores mediante el uso de medios electrónicos permite al acosador causar daño al menor sin restricciones de horarios ni de situación, ya que al tener lugar a través de las TIC también alcanza al menor en su espacio más íntimo, como es su domicilio. El estrés al que puede estar sometido un menor objeto de ciberacoso puede llegar a impedir el normal desarrollo de su personalidad al sentirse constantemente hostigado o vigilado.

La utilización de medios electrónicos para hacer daño a otra persona puede, en ocasiones, dar al menor la **sensación de impunidad o anonimato** tanto para cometer un delito como cuando el propio menor es la víctima. El menor debe ser consciente de que todo lo que hace con su dispositivo móvil (teléfono, tablet) o con el

ordenador a través de internet deja huellas y que esas huellas son herramientas valiosas que pueden utilizar las Fuerzas y Cuerpos de Seguridad para identificar a las personas que cometen o han cometido un delito.

Cuando el menor es víctima de una situación de acoso es muy importante que **no elimine información.** El registro de llamadas de un terminal móvil (incluyendo las llamadas con número oculto), los mensajes de correo electrónico, SMS, MMS, etc., son evidencias que facilitan información a los especialistas a la hora de identificar a un acosador y, en su caso, perseguirlo. Es necesario concienciar al menor para que conserve toda la información que permita acreditar ante las Fuerzas y Cuerpos de Seguridad los hechos que causan daño al menor. Los mensajes o cualquier evidencia que pueda ayudar a identificar al causante de un delito se deben de conservar tal y como fueron recibidos. Así mismo, el reenvío de los mensajes o las copias de los mismos puede suponer la pérdida de valiosa información[3] para la identificación del acosador, lo que dificultaría la labor de los investigadores al realizar análisis de las posibles pruebas o evidencias que acreditan una situación de acoso.

Puede ocurrir que el acosador publique en un foro, web o red social mensajes con la intención de acosar al menor y que dichos mensajes sean eliminados por el acosador pasados unos minutos o cuando el acosador tiene constancia de que su víctima ha leído el mensaje. En estos casos, recomendamos que se realice una captura de pantalla o una fotografía de la pantalla y se conserve para facilitarla a los Jueces y a las Fuerzas y Cuerpos de Seguridad cuando sea necesario.

Desde la Agencia Española de Protección de Datos también podemos ayudar cuando los hechos no son constitutivos de delito. Por ejemplo, una cuestión que puede denunciarse ante esta Agencia es la aparición de imágenes de los menores en internet sin el consentimiento de los padres, que como se ha indicado, no sería delito sino una infracción administrativa.

Recomendamos que se realice como actividad la revisión por el menor revise de las opciones de configuración de sus perfiles (WhatsApp o redes sociales) con el fin de identificar quiénes tienen acceso a su información personal y que intenten utilizar las opciones existentes para permitir que únicamente sus amigos, contactos y conocidos tengan acceso a esta información. Si fuera necesario, revisar el concepto de dato personal que se encuentra en la ficha número uno de nuestra guía “No te enredes en internet”.

También, en la guía “Sé legal en internet”, facilitamos a los menores información acerca de algunas de las variantes existentes del ciberacoso para profundizar en las siguientes fichas en aquellas en las que el menor podría verse involucrado.

---

3. Por ejemplo, un mensaje de correo electrónico reenviado pierde información que podría permitir identificar a la persona que lo ha enviado.

# Ficha 5

## Ciberbaiting

**¿Qué es el Ciberbaiting?**

Se conoce con este término el acoso al que los menores someten a un profesor.

La actuación contra el docente suele comenzar con situaciones que en las que se produce una pérdida de control por parte del profesor con sus alumnos; pudiendo los alumnos grabarlas y emplearlas en su contra. En otras ocasiones se falsean los perfiles de los profesores en las redes sociales con imágenes y manifestaciones degradantes y humillantes.

¿Es el acoso a profesores un delito si lo realizan los menores o es una travesura?

El acoso siempre es delito y puede tener consecuencias penales. Además, el menor podría ser expulsado del centro.

# Ficha 6

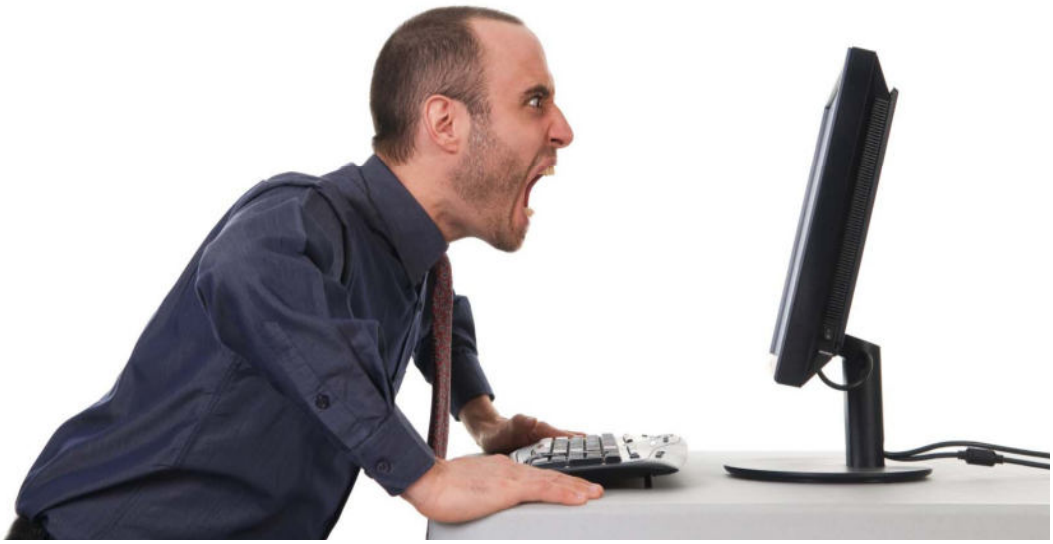
## Grooming

Con esta ficha se intenta explicar a los menores que es el grooming y el sexting y las consecuencias que tienen o pueden llegar a tener.

**¿Qué es el Grooming?**

Acciones llevadas a cabo por adultos para ganarse la confianza o establecer amistad con un menor de edad a través de cualquier servicio de internet para obtener una satisfacción sexual mediante la consecución de imágenes eróticas o pornográficas del menor y, en muchos casos, para preparar una cita con el menor para hacerle objeto de abusos sexuales. Es habitual que el adulto se haga pasar por un menor para ganarse la confianza de la víctima.

El acercamiento del adulto al menor puede ser a través de internet o del teléfono móvil pero también puede ser un acercamiento físico mediante cualquier artimaña que permita obtener cualquier información del menor que luego puede llegar a ser ciberacoso en cualquiera de sus formas.



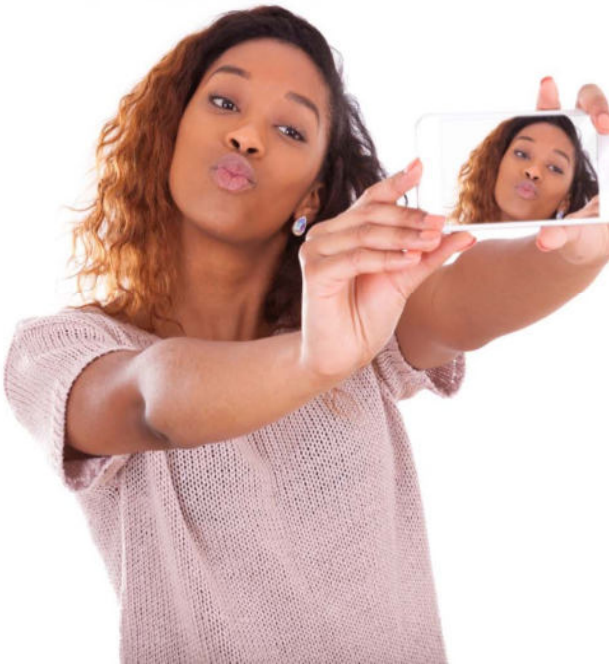
# Ficha 7

## Sexting

El sexting consiste en el envío voluntario de fotografías o grabaciones íntimas, por ejemplo de partes del cuerpo desnudas, o de desnudo total, a una persona de confianza que posteriormente las reenvía o difunde a terceros sin el consentimiento de la persona afectada. El sexting no es exclusivo de personas adultas, también ocurre entre menores.

A menudo el menor piensa que nadie puede reconocerle porque en la fotografía únicamente aparece una parte de su cuerpo en la que aparentemente no es posible identificarle, pero su identificación podría realizarse buscando información en los datos que contiene la fotografía (los metadatos[4]) , o por un simple detalle, como el tipo de terminal o de cámara con el que se ha hecho la fotografía, o por su geolocalización.

Una consecuencia del sexting es lo que a veces se está denominando como "sextorsion", que es el uso de las imágenes utilizadas en el sexting con la finalidad de chantajear al menor obligándole a realizar actos, de cualquier naturaleza, en contra de su voluntad y en perjuicio de su dignidad.



4. Metadatos: muchos archivos digitales contienen información adicional a su contenido, basta con abrir el archivo en el ordenador y revisar las propiedades para averiguar información relativa al terminal telefónico o cámara fotográfica utilizada, identidad de la persona que ha creado el archivo, identidad de la persona que ha revisado el documento, etc.

# Ficha 8

## Recuerda que

Para terminar se proporciona al menor las recomendaciones que podríamos considerar más importantes a la hora de entender, identificar y prevenir situaciones de acoso. Una de las herramientas claves de las que dispone el menor son sus propias sensaciones y emociones, racionalizar con el menor el impacto que determinadas situaciones producen en él o en sus semejantes son clave para identificar posibles situaciones de acoso en su fase más temprana. En este sentido el diálogo y la confianza del menor en familiares y profesores se convierten en el hilo conductor de la convivencia digital de los menores.

### Conclusión:

Las medidas de seguridad a tener en cuenta para proteger los datos personales del menor son importantes, el antivirus o un firewall pueden evitar que un intruso desconocido acceda a su información personal o incluso que pueda contactar con el menor.

La vida digital del menor se puede proteger con medios técnicos pero de nada sirve la tecnología cuando el menor no es consciente de la información que proporciona a terceros.


**Colegio Concertado**
***Ruta de la Plata***
***Almendralejo.***

# XVII

## Bibliografía.

# XVII. Bibliografía.

## 1.- Manuales y Guías.

*Manual de legislación europea en materia de protección de datos*. Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2019.

*Guías sectoriales AEPD. Guía para centros educativos*. Agencia Española de Protección de Datos. Licencia CC BY SA.

*Guía AEPD. Guía para jóvenes. No te enredes en Internet.* Agencia Española de Protección de Datos. Licencia CC BY SA.

*Guía AEPD. Guíales en internet - Ayúdales a construir su futuro.* Agencia Española de Protección de Datos. Licencia CC BY SA.

*Guía AEPD. Enséñales a ser legales en internet*. Agencia Española de Protección de Datos. Licencia CC BY SA.

## 2.- Fotografías.

Samuel Warren, Louis Brandeis, J. Thompson, Alan Westin y Willis Ware de Wikipedia.

Resto de fotografías: Envato Elements©.

## 3.- Bibliografía.

Agustinoy, *A; Monclús, J. Aspectos legale*s de las redes sociales. Ed. Bosch Wolster Kluwer. 2ª. *2019.*

Aparicio, J; Vidal, M. *Estudio* sobre la Protección de Datos. Ed. Aranzadi. 5ª. *2019.*

Arenas, M; Ortega, A. Comentarios a la ley orgánica de p*rotección de datos y garantía de derechos d*igitales (en relación con el RGPD). Ed. Sepin. 1ª. *2019.*

Baz, J. *Privacidad y protección de da*tos de los trabajadores en el entorno dig*ital. Ed. Bosch Wolster Kluwer. 1ª. 2019.*

Blazquez, E.M. *Aplicació*n práctica de la protección de datos en las *relaciones laborales. Ed. Wolster Kluwer - CISS. 1ª. 2018.*

Durán, B. *El delegado de protección de* datos en el RGPD y la nueva LOPDGDD. E*d. LA LEY Wolster Kluwer. 1ª. 2019.*

Ferrer, R.L. Guía de protección de datos de los traba*jadores. Ed. Tirant lo Blanch. 1ª. 2019.*

Gil, C. *Videovigilancia y protecció*n de datos. Ed. LA LEY Wolster Kluwer. 1ª. 2019.

González, C. *GDPR Guía práctica sobre protección de* datos: ámbito laboral. Ed. Aranzadi. 1ª. 2019.

López, J. *Comentarios al Reglamento Europeo de Protección de Datos. Ed. Sepin*. 1ª. 2018.

Martínez, L. Internet y los derechos *de la personalidad. Ed. Tirant lo Blanch. 1ª. 2019.*

Orellana, A.M. El derecho a la protección de datos personales *como garantía de la privacidad de l*os trabajadores. Ed. Aranzadi. 1ª. 2019.

Puyol*, J. Delegado de Protección de Datos (DPO). Ed. Tirant lo Bla*nch. 1ª. 2019.

Rallo, A. Tratado *de protección de datos. Ed. Tirant lo Blanch. 1ª. 2019.*

Rallo, A; Martínez, R. Derecho y redes *sociales. Ed. Civitas. 2ª. 2013.*

Recio, M. El ejercicio de los derechos de protección *de datos y su aplicación práctica. Ed. Bosch Wolster* Kluwer. 1ª. 2019.

Recuerda, M.A. *Tecnologías disruptivas. Re*gulando el futuro. Ed. Aranzadi. 1ª. 2019.

Rodríguez, J.F. *Figuras y responsabilidades en el tratam*iento de datos personales. Ed. Bosch Editor. *1ª. 2019.*

VV.AA. *GDPR Guía práctica sobre protección de datos: ámbito sanitario. Ed. Aranzadi. 1ª. 2019.*

VV.AA. Memento Práctico Francis Lefebvre Pro*tección de datos. Ed. EFL. 1ª. 2019.*

VV.AA. *Practicum Protección de Datos* 2018. Ed. Aranzadi Thomson. 1ª. 2017.


Colegio Concertado

*Ruta de la Plata*

*Almendralejo.*