

GUÍA BÁSICA

sobre

**PROTECCIÓN DE DATOS,
PROPIEDAD INTELECTUAL Y
*KNOW-HOW***

EN

***DOCENCIA, INVESTIGACIÓN Y
EMPRESARIADO***

DPD-UV

Javier Plaza Penadés

Delegado de Protección de Datos

Universitat de València

Bajo licencia (CC BY)

Debido a las peticiones de información continuas en lopd@uv.es y a la complejidad de la normativa de protección de datos, junto con la complejidad de otras normativas concurrentes, como las de sociedad de la información, propiedad intelectual o Know-How (secreto comercial), tanto en el ámbito de la legalización de tratamientos y ficheros de investigación como en las investigaciones derivadas de las prácticas externas, Trabajos Fin de Master (TFM) y Trabajos Fin de Grado (TFG),

así como a la necesidad de actualizar el “Protocolo de la UV de protección de datos para TFM, TFGs y Prácticas Externas”,

la Delegación de Protección de Datos UV ha elaborado esta breve y sencilla Guía, que pretende orientar y ayudar a los investigadores y estudiantes en su labor de cumplimiento normativo.

OBJETO DE LA GUÍA

Sobre esa base, esta Guía pretende y persigue un **doble objetivo**:

- **Informar de la normativa de protección de datos personales, tanto en la realización de “encuestas” como en la elaboración de “bases de datos” o, en general, ficheros de carácter personal y tratamiento de datos personales por investigadores y estudiantes. (Por tanto, la expresión “ficheros” incluye, a los efectos de esta Guía, documentos informáticos o en papel, encuestas o bases de datos con datos de personas físicas identificadas o identificables).**
- **Informar, además, de los derechos de autor que tienen los investigadores (PDI) y los estudiantes sobre los TFM, TFG e ideas generadas en Programas de emprendimiento, incluidos los derechos de propiedad intelectual o industrial que se puedan derivar de los mismos (principalmente sobre programas de ordenador o software, bases de datos, patentes o secretos empresariales), haciendo hincapié en “la protección de las ideas” y en la evitación del “delito” de plagio.**

Para ello, vamos a estructurar esta Guía en dos partes: Una parte dedicada al Derecho de protección de datos de carácter personal, y otra relativa al Know-How y a la propiedad intelectual e industrial.

ÍNDICE

I. DERECHO DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN INVESTIGACIÓN

1. ¿QUÉ ES LO MÍNIMO QUE SE DEBE SABER SOBRE EL DERECHO DE PROTECCIÓN DE DATOS?
2. ¿CÓMO SE TIENE QUE LEGALIZAR UN FICHERO O TRATAMIENTO DE PROTECCIÓN DE DATOS?
3. ¿QUÉ FICHEROS O TRATAMIENTOS NO NECESITAN UN REGISTRO DE ACTIVIDADES DE TRATAMIENTO?
4. ¿QUÉ MEDIDAS DE SEGURIDAD SE DEBEN ADOPTAR PARA PROTEGER LOS FICHEROS CON DATOS PERSONALES?
5. ¿SE DEBE FIRMAR UN ACUERDO DE CONFIDENCIALIDAD O *NON DISCLOSURE AGREEMENT* “NDA”?

II. CUESTIONES SOBRE PROPIEDAD INTELECTUAL, INDUSTRIAL Y KNOW-HOW

1. ¿DE QUIÉN ES LA AUTORÍA DE UNA OBRA CIENTÍFICA (como el TFM O TFG) Y QUÉ DERECHOS TIENE?
2. ¿QUÉ OCURRE CON LAS IDEAS QUE EL TUTOR FACILITA AL ESTUDIANTE PARA REALIZAR SU TFM/TFG? ¿CÓMO SE PROTEGEN LAS IDEAS?
3. ¿CÓMO EVITO EL PLAGIO?
4. ¿QUÉ OCURRE SI SE TRATA DE UN TFM/TFG O INVESTIGACIÓN QUE GENERA UN SOFTWARE O UNA APP?
5. ¿QUÉ OCURRE SI EL TFM/TFG O LA INVESTIGACIÓN CONTIENE O ES UNA BASE DE DATOS?
6. ¿CÓMO SE DEBE LEER UN TFM O TFG SI CONTIENE UNA POSIBLE PATENTE o UN SECRETO COMERCIAL?
7. ¿QUÉ OCURRE CON LAS IDEAS DE EMPRENDIMIENTO?

II. DERECHO DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN INVESTIGACIÓN

1. ¿QUÉ ES LO MÍNIMO QUE SE DEBE SABER SOBRE EL DERECHO DE PROTECCIÓN DE DATOS?

✓ Que su objeto son los datos únicamente de personas naturales o físicas. Y, por tanto, no afecta al tratamiento de “datos no personales” o al tratamiento de “datos de personas jurídicas (sociedades, asociaciones, fundaciones, Administraciones e Instituciones Públicas, etc.)

✓ **Que dato personal es** “toda información sobre una persona física identificada o identificable”.

Pero dentro de los datos personales hay que tener especial cuidado y atención con:

(a) los datos sensibles o especialmente protegidos (etnia o raza, opinión política, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar unívocamente, salud, vida u orientación sexual). Dichos datos gozan de una protección reforzada y compleja.

(b) Los datos personales relativos a condenas e infracciones penales, que solo podrán tratarse bajo ciertas circunstancias.

(c) El tratamiento de la imagen de las personas y los datos que puedan afectar al honor e intimidad de las personas, especialmente en el caso de menores (porque son derechos fundamentales a los que se aplica otras leyes como la Ley Orgánica de Protección al honor, intimidad y propia imagen o la de protección del menor).

✓ Que **es un derecho fundamental** reconocido tanto en la Constitución Española, como en diversos tratados internacionales (especialmente en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea).

✓ Que este derecho **se encuentra regulado en** el “Reglamento general de protección de datos, 2016/679” (**RGPD**) -norma de la UE- y en nuestra “Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos y garantía de derechos digitales” (**LOPD-GDD**).

✓ Que se materializa en una serie de derechos concretos, cuyo ejercicio es gratuito, los llamados derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) y que comprende el **derecho a acceder** a los datos personales, el **derecho a rectificarlos**, el **derecho a cancelar o suprimirlos (derecho al olvido)** y el **derecho de oposición** al tratamiento o cesión. Pero el RGPD ha añadido el **derecho a limitar el acceso**, el **derecho a la portabilidad** de los datos propios, y el **derecho a no ser objeto de perfiles personales sobre los que se tomen decisiones automatizadas**.

✓ Que los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado; que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (principio de «minimización de datos» o «de protección por defecto»). Que sean exactos y recogidos con fines determinados, explícitos y legítimos, y que no serán tratados ulteriormente de manera incompatible con dichos fines.

✓ Además, se debe tener una **responsabilidad proactiva** y, en ese sentido, la Universitat de València está implicada en el cumplimiento de la compleja normativa de protección de datos y te puede ayudar, a través de la Delegación de datos, **desde el diseño** (velando por el cumplimiento íntegro de la normativa de protección de datos desde antes de poner en marcha cualquier iniciativa docente o investigadora) y **por defecto** (ya que se deben de tratar únicamente los datos que sean imprescindibles).

✓ Que todo “tratamiento de datos” y toda “transferencia o cesión de datos” de datos personales debe tener su base en la “ley” o en un “consentimiento” inequívoco, en el que se informe de la finalidad del tratamiento y/cesión y del uso y destino que se va a hacer de los datos personales.

✓ Por “tratamiento de datos” se entiende cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos automatizados o no, como la recogida, el registro, la organización, la estructuración, etc., lo que afecta tanto a los ficheros informatizados o en soporte electrónico como a los ficheros en papel. Mientas que “la cesión” de datos consiste en la transmisión de los mismos o el acceso no autorizado de terceros.

PARA PODER TRATAR Y/O CEDER DATOS PERSONALES HACE FALTA

✓ O BIEN UNA **LEY** QUE LO AUTORICE

✓ O BIEN UN **CONSENTIMIENTO**,

QUE ADEMÁS, EL CONSENTIMIENTO NO PUEDE SER TÁCITO NI VENIR PREMARCADO, Y QUE TIENE QUE SER “INFORMADO” y “TRANSPARENTE”, PUES TODA PERSONA, DENTRO DE SU “DERECHO A CONTROLAR Y A DECIDIR SOBRE EL USO DE SUS DATOS”, TIENE QUE CONOCER Y COMPRENDER LA FINALIDAD Y UTILIDAD QUE REPORTA EL TRATAMIENTO Y LA CESIÓN DE SUS DATOS. Además, DICHO CONSENTIMIENTO SE PUEDE REVOCAR en cualquier momento.

Y se debe tener especial cuidado con aquellos supuestos en los que la ley permite el tratamiento pero no la cesión. En estos casos, la cesión requiere de consentimiento.

✓ Que los menores, pueden consentir, con carácter general, por sí solos si tienen **14 años**. Por tanto, los menores de 14 años requieren de consentimiento de sus representantes legales. Si solo se puede conseguir el consentimiento de uno de ellos, resulta conveniente que éste se responsabilice del consentimiento del otro representante legal del menor. Y, **excepcionalmente, la edad para consentir el tratamiento o la cesión de datos puede ser superior a 14 años**, cuando el acto o negocio jurídico exigen que el menor tenga una edad mayor para poder realizar válidamente dicho acto o negocio jurídico. Por ejemplo, **en el ámbito sanitario, la edad para que un menor consienta por sí solo es de 16 años**. Y se requiere de **18 años para enajenar o gravar bienes de extraordinario valor** (que no pueden realizar por sí solos ni tan siquiera los menores emancipados).

✓ Pero está prohibido cualquier tratamiento o cesión de datos y/o imágenes de un menor que atente, de manera objetiva, contra su **honor, intimidad y propia imagen**. En tales casos, **la obtención del consentimiento del propio menor o de sus representantes legales no sirve** para legitimar dicha intromisión ilegítima.

✓ Que el “**responsable de un tratamiento**” y titular de los datos (*controller*) es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. Mientras que el “**encargado del tratamiento**” (*processor*) es la persona que trata o cede los datos siguiendo las indicaciones del responsable. Por consiguiente, si un estudiante o investigador determina los fines y medios de un tratamiento de datos personales de su TFG/TFM o investigación, es responsable de ese tratamiento. Del mismo modo, la Universitat Valencia es responsable del tratamiento de los ficheros que realiza y gestiona su personal (como encargado del tratamiento).

✓ Respecto de las **prácticas externas** es habitual que el estudiante (como un investigador más) tenga acceso a los ficheros de datos personales cuya titularidad es de la empresa o de la institución donde se desarrollan las prácticas, por lo que **es necesario respetar la normativa de protección de datos, junto con las de privacidad o confidencialidad y de propiedad intelectual o de Know-How que establezca la empresa o institución**, y pedir siempre la debida autorización para poder utilizar todos o algunos de esos datos personales en la investigación que se pretenda desarrollar (artículos, libros, TFM, TFG...).

✓ En la investigación, y sobre todo **en los proyectos de investigación entre diversos grupos** o “*partners*”, puede haber una titularidad (horizontal) conjunta o compartida del fichero o base de datos (siendo todos “corresponsables o cotitulares del fichero”, *joint controllers*) o puede haber un sistema vertical o piramidal, con un único responsable y varios encargados del tratamiento. En todos estos casos, **resulta conveniente realizar un contrato (artículo 28 RGPD)**, que delimite las titularidades, los ámbitos de gestión, la responsabilidad, el tratamiento y acceso a los datos, los deberes de confidencialidad, los actos ilícitos que pueda cometer y la coordinación en materia de seguridad y de información en caso de brechas de seguridad.

LA AEPD ofrece unas directrices para elaborar, contratos del artículo 28 RGPD en: <https://www.aepd.es/media/guias/guia-directrices-contratos.pdf>

ASIMISMO, LA DELEGACIÓN DE PROTECCIÓN DE DATOS UV TE PUEDE FACILITAR UN “FORMULARIO DE OBTENCIÓN DE CONSENTIMIENTO” Y SUPERVISAR CONTRATOS DEL ART. 28 RGPD, YA SEAS “RESPONSABLE” O “ENCARGADO” DEL TRATAMIENTO.

2. ¿CÓMO SE TIENE QUE LEGALIZAR UN FICHERO O TRATAMIENTO DE PROTECCIÓN DE DATOS?

✓ Si, para nuestra investigación, se necesita desarrollar un fichero o base de datos (digitalizado o en papel) con datos personales o preparar un tratamiento de datos mediante formularios, encuestas..., con datos de personas identificadas directa o indirectamente, la **“legalización” de dicho fichero o tratamiento de datos personales ya no se produce mediante la “inscripción en el registro de la AEPD”** (Agencia Española de Protección de Datos).

✓ De hecho, **el Registro de la AEPD ya no existe** y, por ello, conviene que todos los que tuvieran inscritos sus ficheros en el Registro AEPD los legalicen adaptándolos al nuevo modelo.

✓ **AHORA, EL SISTEMA DE LEGALIZACIÓN DE FICHEROS Y TRATAMIENTOS EXIGE QUE CADA “RESPONSABLE DEL FICHERO” (CONTROLLER)**

DEBA TENER Y LLEVE UN “REGISTRO DE ACTIVIDADES DE TRATAMIENTO” (“RAT”) DE CADA FICHERO O TRATAMIENTO.

(puedes solicitar un RAT en lopd@uv.es, donde te informaremos y te ayudaremos en su llevanza y gestión) PUESTO QUE ADEMÁS LA UV TIENE UN “RAT” MÁS COMPLETO QUE EL DE LA AEPD, en el que contiene diversos tratamientos.

✓ Incluso el **“encargado de tratamiento” (processor)** también tiene que llevar su propio RAT cuando sea necesario por la estructura o características del fichero o cuando lo exija el responsable (especialmente en virtud del contrato entre responsable y encargado del artículo 28 RGPD).

✓ De todos modos, si tienes curiosidad sobre cuál es el contenido y diseño de un registro de actividades de tratamiento, lo puedes ver en <https://www.aepd.es/agencia/transparencia/inventario-actividades-tratamiento/index.html>

✓ **ADEMÁS, ALGUNOS FICHEROS**

CREADOS DESPUÉS DEL 25 DE MAYO DEL 2018 CON DATOS ESPECIALES O SENSIBLES, REQUIEREN DE UN

“INFORME DE EVALUACIÓN DE IMPACTO”

QUE TIENE QUE SUPERVISAR EL

(DELEGADO DE PROTECCIÓN DE DATOS) DPD o DPO (en inglés)

Cuya función únicamente es asesorar, informar y orientar.

✓ EN CONCRETO, **REQUIEREN DE INFORME DE EVALUACIÓN DE IMPACTO, SEGÚN LISTADO DE LA AEPD, COMO UNA “LISTA NO EXHAUSTIVA”**, LOS SIGUIENTES FICHEROS O TRATAMIENTOS:

✓ **Tratamientos que impliquen perfilado o valoración de sujetos**, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sus hábitos.

✓ **Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de decisiones**, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.

✓ Tratamientos que impliquen la **observación, monitorización, supervisión, geolocalización o control del interesado** de forma sistemática y exhaustiva, incluida la **recogida de datos y metadatos a través de redes**, aplicaciones o en zonas de acceso público, así como el **procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, tv interactiva, aplicaciones móviles**, etc.

✓ Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD (**datos de salud física y psíquica, orientación sexual, ideología**), **datos relativos a condenas o infracciones penales** a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la **situación financiera o de solvencia patrimonial** o deducir información sobre las personas relacionada con categorías especiales de datos.

✓ Tratamientos que impliquen el uso de **datos biométricos** con el propósito de identificar de manera única a una persona física.

✓ Tratamientos que impliquen el uso de **datos genéticos** para cualquier fin.

✓ Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 “Directrices sobre los delegados de protección de datos (DPD)” del Grupo de Trabajo del Artículo 29.

✓ Tratamientos que impliquen la **asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes** o por responsables distintos.

✓ Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo **datos de menores de 14 años, mayores con algún**

grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.

✓ **tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas**, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.

✓ **Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato**, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b, c, d) del RGPD.

✓ **El Contenido del Informe de Evaluación de impacto (IEI), artículo 35.7 RGPD deberá incluir como mínimo:**

✓ Una **descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento**, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento.

✓ Una **evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento** con respecto a su finalidad.

✓ Una **evaluación de los riesgos para los derechos y libertades de los interesados** y

✓ Las **medidas previstas para afrontar los riesgos**, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

RESUMIENDO

TODO FICHERO DE INVESTIGACIÓN DEBE TENER SIEMPRE:

✓ **«RAT-REGISTRO DE ACTIVIDADES DE TRATAMIENTO»**

Y, EN ALGUNOS CASOS,

✓ **«INFORME DE EVALUACIÓN DE IMPACTO» O**

✓ **«CONTRATO DEL ART. 28 RGPD**

ENTRE RESPONSABLE/S Y ENCARGADO/S».

3. ¿QUÉ FICHEROS O TRATAMIENTOS NO NECESITAN UN RAT?

✓ Obviamente **no todos los ficheros de protección de datos tienen que ser legalizados** con el nuevo sistema, que consiste en la llevanza de un “registro de actividades de tratamiento” individualizado.

✓ Están **excluidos todos los ficheros (de investigación) de datos de personas jurídicas**, ya que el derecho de protección de datos se proyecta únicamente sobre personas físicas, y están excluidos aunque dichos ficheros contengan también datos de personas físicas, pero siempre que dichos datos se incluyan a los meros efectos de poder contactar con las personas jurídicas.

✓ Tampoco requieren de legalización **los ficheros (de investigación) de datos no personales**, como, por ejemplo, los ficheros con datos medioambientales sobre el tiempo o el clima en las ciudades y poblaciones. **Los ficheros de datos no personales se rigen además por el principio de libre circulación de datos**, por lo que, si el responsable de dicho fichero decide compartirlos en la red, dichos datos engrosarían el llamado **big data**.

✓ Por último, tampoco requieren de legalización los **ficheros (de investigación) de uso exclusivamente personal o doméstico**, que no serán compartidos ni accesibles a terceros. Ni los **ficheros o tratamiento datos de personas anonimizados**, porque la protección de datos se proyecta sobre las “personas identificadas o identificables”. En consecuencia, si los datos de las personas incluidos en los ficheros no permiten su identificación individual, directa o indirecta (esto es, mediante un sencillo proceso de reidentificación o con datos como el “cargo” o “la fecha de nacimiento” que permitan identificar a las personas) **únicamente hay que informar de que los datos serán anonimizados y el uso y destino que se va a hacer con dichos datos anónimos**; pero no es necesario tener un RAT.

✓ Por ello la **Unión Europea recomienda que los ficheros de datos personales destinados a investigación sean principalmente ficheros anonimizados**, con un doble fin: evitar la compleja gestión en materia de protección de datos y favorecer la libre circulación de datos anonimizados en el ámbito del Big Data.

✓ Pero es **muy importante distinguir correctamente entre “ANONIMIZACIÓN” y “SEUDONIMIZACIÓN”**.

✓ La **anonimización** existe cuando los datos personales se tratan (o se ceden) de modo que no es posible identificar, ni directa ni indirectamente (ni tan siquiera

mediante un procedimiento de reidentificación) a las personas físicas titulares de los datos tratados.

✓ La **seudonimización**, según la RAE, es todo tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. (la palabra “seudoanonimización” es incorrecta).

✓ Por tanto, lo que diferencia la “anonimización” de la “seudonimización” es que ésta última permite excepcionalmente la reidentificación, mientras que en la anonimización resultará absolutamente imposible reidentificar a las personas.

✓ La LOPD-GDD ha previsto que sea lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.

✓ Es muy importante recordar que **el uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido siempre al informe previo del comité de ética de la investigación previsto en la normativa sectorial**, para comprobar las medidas de seguridad y confidencialidad respecto de los datos que permiten la reidentificación, y que dicha reidentificación se realice únicamente cuando se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos, o sea necesaria para garantizar una adecuada asistencia sanitaria.

✓ **La praxis habitual en Medicina es que la historia clínica del paciente tenga dos tipos de accesos. Un primer acceso a la historia clínica con los datos personales de identificación del paciente**, que es el que utiliza el médico que debe de prestar asistencia sanitaria personalizada. **Y un segundo acceso, al conjunto de historias clínicas anonimizadas, para que puedan ser consultadas por los servicios de salud pública y por los grupos de investigación**, respetando la intimidad y el honor del paciente y resultando imposible que el investigador pueda identificar a ningún paciente, salvo que utilice un proceso de “reidentificación”, controlado por una persona o grupo limitado de personas, que tienen que comprobar además si existe causa justificada para la reidentificación.

✓ El **acceso a la historia clínica** está regulado en el artículo 16 de ley 41/2002, de derechos del paciente. Así, por ejemplo, cuando sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, **las Administraciones competentes en salud pública podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública**, pero el acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos, a no ser que sea

para proteger la vida o integridad física del titular de los datos o personas próximas, en cuyo caso está permitido el acceso, tratamiento y la cesión de datos sin consentimiento.

✓ **La LOPD-GDD ha previsto la posibilidad de “reutilizar” los datos de investigación con fines de salud** (física o mental) sin necesidad de obtener un nuevo consentimiento. En concreto, se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomedicina cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial. Para ello es absolutamente **imprescindible contar con el informe previo favorable del Comité de ética.**

✓ La normativa de investigación y, en especial, la Ley 14/2007, de 3 de julio, de Investigación biomédica, han previsto la existencia de **“Comités de ética de la investigación”** como los que tiene la UV. Dichos comités tienen como misión garantizar el respeto a la dignidad, integridad e identidad del ser humano en lo que se refiere a la investigación con humanos, con muestras biológicas o con “datos” de origen humano, así como promover un comportamiento ético en la investigación. Por tanto, entre sus competencias está el velar por el cumplimiento de la normativa vigente aplicable en materia de protección de datos y de investigación cuando se vayan a utilizar datos personales de personas físicas identificadas o identificables, datos seudonimizados o datos anonimizados, por lo que **cualquier investigación que contenga datos personales deberá contar con la autorización del comité de ética competente en investigación sobre personas (es la llamada “ética de los datos”, que exige que se cumpla la normativa de protección de datos, como derecho fundamental, en toda investigación con datos de personas físicas identificadas o seudonimizadas).**

✓ **CONVIENE RECORDAR QUE:**

**TODO PROCESO DE SEUDONIMIZACIÓN
PARA ELABORAR FICHEROS DE DATOS PERSONALES,
ESPECIALMENTE**

en el ámbito de la biomedicina

**REQUIERE SIEMPRE DEL CONTROL Y LA APROBACIÓN DEL “COMITÉ
DE ÉTICA DE LA UV”**

**Y lo mismo ocurre si se quieren “REUTILIZAR” los datos para otros fines
distintos pero relacionados con el fin para que obtuvieron.**

**Dicha reutilización no requiere de nuevo consentimiento, pero sí de su
aprobación por el Comité de ética de investigación.**

4. ¿QUÉ MEDIDAS DE SEGURIDAD SE DEBEN ADOPTAR PARA PROTEGER LOS FICHEROS CON DATOS PERSONALES?

✓ **Los datos tienen que estar alojados en servidores seguros.** Todas las páginas web y servicios de almacenamiento que dependen de la Universitat de València están en servidores seguros, y además están plenamente adaptados al Esquema Nacional de Seguridad.

✓ Además, hemos diseñado unas medidas de seguridad de carácter personal, para ser observadas y aplicadas por cualquier estudiante o investigador con sus ficheros y documentos, que conviene que SEA CONOCIDO Y CUMPLIDO por todos los miembros del equipo o grupo de investigación; dichas normas deben ser cumplidas por:

<https://www.uv.es/ensuv/es/uvstic-seguridad-tecnologias-informacion-comunicaciones.html>

✓ Una de las novedades más relevante que tiene el nuevo marco normativo de protección de datos es que **hay que informar inmediatamente**, en caso de “**brecha de seguridad**” sobre los ficheros propios, **al delegado de protección de datos** de la institución, a fin de que éste pueda evaluar los riesgos, y decida si se tiene que comunicar a la Agencia Española de Protección de Datos y a los interesados afectados.

✓ Las BRECHAS DE SEGURIDAD

especialmente las consistentes en la sustracción o robo de datos de ficheros de investigadores o grupos de investigación vinculados a la Universitat de València,

CUYA INVESTIGACIÓN NO TENGA DPD PROPIO,

DEBEN DE COMUNICARSE AL DELEGADO DE PROTECCIÓN DE DATOS de la UV

como ocurre también con los ficheros de protección de datos de naturaleza administrativa de nuestra Universidad, ENVIANDO UN E-MAIL a lopd@uv.es indicando como asunto “posible brecha de seguridad”

5. ¿SE DEBE FIRMAR UN ACUERDO DE CONFIDENCIALIDAD O *NON DISCLOSURE AGREEMENT* “NDA”?

✓ Los acuerdos de confidencialidad (en inglés *NDA*) son documentos o contratos en los que una concreta persona se obliga a guardar secreto sobre ideas, sobre el desarrollo de nuevos productos y procedimientos o sobre cualquier información personal e íntima que se derive de los datos personales y a los que tenga acceso legítimo.

✓ Por ello, cualquier investigador o tercero que pueda tener acceso legítimo a los datos debería tener firmado un compromiso de confidencialidad respecto de las informaciones y circunstancias que pueda conocer con ocasión de dicho acceso legítimo a datos personales, sobre todo si se están tratando datos especialmente protegidos o íntimos.

✓ Se recomienda que todo investigador conozca las diferentes conductas que pueden ser constitutivas de delito en materia de protección de datos, especialmente las previstas en el **artículo 197 del Código Penal**, y

✓ **Para garantizar o reforzar el cumplimiento de la normativa de protección de datos, conviene que también firme un “compromiso de confidencialidad”**, más allá de sus deberes de secreto profesional, **la persona responsable del proceso seudonimización**, (esto es, la persona que tiene acceso al proceso o variables que permiten la reidentificación de aquellos datos personales seudonimizados y que se ofrecen de forma anonimizada al resto de investigadores).

✓ Del mismo modo, es conveniente redactar y firmar un compromiso o acuerdo específico de confidencialidad en el caso de secretos comerciales (Know-How) desarrollados por un equipo de investigadores, en el que solo unos pocos tienen acceso a esas ideas protegidas.

II. CUESTIONES SOBRE PROPIEDAD INTELECTUAL, INDUSTRIAL Y KNOW-HOW

1. ¿DE QUIÉN ES LA AUTORÍA DE UNA OBRA CIENTÍFICA (como el TFM O TFG) Y QUÉ DERECHOS TIENE?

✓ Los derechos de autor de un “artículo o *paper*, libro, manual, tratado, panel... *científico*” son del autor por el mero hecho de escribirlo y, del mismo modo, **los derechos de autor del artículo o libro escrito exclusivamente por un estudiante, como puede ser el TFG o TFM, son del estudiante**, puesto que los derechos de propiedad intelectual nacen para el autor por el “hecho de crear” una obra literaria, artística o científica original y propia (artículos 1 y 10 del Texto Refundido de la Ley de Propiedad Intelectual, a partir de ahora, **TRLPI**).

✓ Obviamente, **esta regla general puede tener excepciones o singularidades**, especialmente en los casos de “coautoría” o en aquellos en los que el TFM se realice con los materiales del profesor-tutor y bajo su dirección científica (más habitual en TFM’s realizados en laboratorio, como física, química, biomedicina).

✓ Así, la Ley de propiedad intelectual prevé **tres tipos básicos de cotitularidad** sobre obras intelectuales:

- Las **obras en colaboración** son una obra conjunta, que es la suma de aportaciones individuales, y donde el autor de cada concreta aportación la puede divulgar o comercializar por separado, siempre que no cause perjuicio a la obra en colaboración o no se hay restringido tal posibilidad por un acuerdo o contrato. (**artículo 7 TRLPI**)
- Las **obras colectivas** son aquellas en las que la autoría es de la persona (física o jurídica) que coordina y dirige la obra, especialmente cuando en dicha obra colectiva ya no existen aportaciones separables cuya autoría se pueda individualizar (artículo 8 TRLPI). Este supuesto, permite que exista un único titular de los derechos de autor (la persona física o jurídica que dirige la obra) aunque participen varias personas.
- Las **obras compuestas** son aquellas que son iniciadas por un autor y concluidas por otro (artículo 9 TRLPI)
- Por ello, **cuando el profesor, que dirige un TFM o TFG, entienda que él es el autor**, deberá ver qué clase de coautoría de las previstas en el TRLPI es el que se adecúa a su caso.

**En caso de COAUTORÍA, cuando todo o parte de la autoría sea del director del TFM o TFG,
CONVIENE
QUE SE DELIMITE DICHA AUTORÍA CON CARÁCTER PREVIO
EN UN DOCUMENTO O CONTRATO
clarificando la titularidad del profesor y el modo en que el estudiante puede ejercitar los derechos de propiedad intelectual.**

✓ Los derechos de autor comprenden tanto el “derecho moral de autor” como los “derechos de explotación”.

✓ El derecho moral contiene a su vez siete derechos (artículo 14 TRLPI), de los que merece destacarse *el derecho a ser reconocido como autor de la obra y el derecho de respeto a la integridad de la obra*, decidiendo además cuándo y cómo se debe publicar. Lo más destacable es que los **derechos morales son irrenunciables, intransmisibles e indisponibles**. Por tanto, es nula la renuncia a la condición de autor sobre una obra cuya verdadera autoría se puede probar.

✓ Los **derechos de explotación** (artículos 17 y ss. TRLPI), como son el de *reproducción, distribución, transformación, comunicación pública, incluida la puesta a disposición en Internet, la traducción o transformación...* **son derechos renunciables y disponibles**.

POR TANTO, LAS OBRAS INTELECTUALES (LIBROS, ARTÍCULOS, GRABACIONES AUDIOVISUALES...) PUEDEN EXPLOTARSE MEDIANTE CESIÓN DE DERECHOS o MEDIANTE SISTEMAS “OPEN ACCESS”, COMO LAS LICENCIAS “CREATIVE COMMONS”

https://creativecommons.org/licenses/?lang=es_ES

Las cuales se basan precisamente en ese principio de disponibilidad de los derechos de explotación, y de respeto al derecho moral irrenunciable a ser reconocido como autor.

✓ La **forma básica de advertir** que una obra literaria, **artística o científica tiene derechos de autor es con una “c” (de Copyright) con un circulito (©)**, siendo conveniente que se indique la fecha exacta de publicación. Del mismo modo, se puede proteger inscribiendo las obras en el **Registro de Propiedad Intelectual**.

✓ Las licencias *Creative Commons* son variadas y diversas. La más básica, como la que utiliza esta guía, es la licencia (CC BY), que permite a terceros usar la obra, incluso con fines comerciales, pero siempre que se reconozca y respete la autoría. Pero también hay licencias *Creative Commons* que prohíben los usos comerciales (NC de *non commercial*) o usos derivados (ND *non derivative*) o restringir el uso a los que explotan sus obras con licencias CC (con la mención SA, *share a like* o compartir entre iguales o con la misma licencia). Ver https://creativecommons.org/licenses/?lang=es_ES

✓ Por último, el Director del TFM o TFG no puede publicar como suyo todo o parte de un TFM o TFG del que sea autor un estudiante, aunque haya aportado ideas originales al mismo, pues **“la propiedad intelectual nunca protege las ideas en sí mismas”**, si bien protege la forma en que se ordenan y expresan dichas ideas en un documento o soporte que permite su publicación o difusión.

2. ¿QUÉ OCURRE CON LAS IDEAS QUE EL TUTOR FACILITA AL ESTUDIANTE PARA REALIZAR SU TFM/TFG? ¿CÓMO SE PROTEGEN LAS IDEAS?

Es muy Sencillo: el **Tribunal Supremo ha declarado** en reiteradas ocasiones que:

“LAS IDEAS NO SE PROTEGEN POR PROPIEDAD INTELECTUAL”

✓ Por tanto, si un Profesor tiene ideas nuevas y las comparte con un estudiante, que las incluye en su TFM o TFG, dichas ideas no son propiedad del Profesor, ni puede reclamar ningún derecho de propiedad intelectual sobre las mismas ideas que transmitió al estudiante.

✓ Así pues, **las ideas, como los descubrimientos científicos, solo se protegen manteniéndolas en secreto**, hasta que se divulguen por primera vez en un libro, tratado o artículo científico o aplicación práctica de la idea, pero no porque se proteja la idea en sí misma, sino porque va implícita en los derechos de autor sobre la forma en que se ha divulgado o publicado dicha idea (en un libro, tratado, artículo, etc.).

✓ Además, si se **trata de una idea que tiene aplicación o valor comercial, la Ley 1/2019 de secretos empresariales**, que incorpora la normativa europea sobre secretos comerciales, **exige dos requisitos básicos**, a parte de su valor comercial, para que exista protección:

- **Que se trate de una IDEA (INFORMACIÓN O CONOCIMIENTO) REALMENTE NUEVA Y DESCONOCIDA EN EL SECTOR.**
- Que exista un **ACCESO RESTRINGIDO A DICHAS IDEAS, CON LOS CORRESPONDIENTES COMPROMISOS DE CONFIDENCIALIDAD**, si son varias las personas que tienen acceso al desarrollo de una idea que se mantiene como secreto.

Por ello, en la práctica, va a resultar casi imposible proteger una idea como secreto comercial y ejercitar acciones legales contra los que han divulgado indebidamente o ilícitamente dicho secreto si previamente no hay un **“compromiso de confidencialidad”**.

Pero es más, **LA INFRACCIÓN DEL COMPROMISO DE CONFIDENCIALIDAD ES LA BASE PARA EL EJERCICIO DE ACCIONES CIVILES Y PENALES POR VULNERACIÓN DEL SECRETO.**

Como novedad legal: **UN SECRETO COMERCIAL, delimitado, y con sus compromisos de confidencialidad, SE PUEDE TRANSMITIR a un tercero que tenga interés en continuar con su desarrollo o que pueda beneficiarse del mismo.**

3. ¿CÓMO EVITO EL PLAGIO?

CUMPLIENDO ESTAS TRES REGLAS:

- 1^a.- **NO COPIAR A TERCEROS.**
- 2^a.- **RESPETAR EL “DERECHO DE CITA”, Y, SOBRE TODO,**
- 3^a.- **UTILIZANDO SIEMPRE PALABRAS E IDEAS PROPIAS, BUSCANDO LA ORIGINALIDAD Y, SI ES POSIBLE, LA NOVEDAD, Y LA EXCELENCIA**

✓ El **plagio siempre es un acto ilícito**, porque genera un daño moral en el autor plagiado al lesionarse su derecho moral a ser reconocido como autor y, según los casos, se deben indemnizar los daños económicos derivados de la explotación por obra ajena.

✓ Pero además, el plagio puede ser constitutivo de un **delito contra la propiedad intelectual**, conforme al artículo 270 del Código Penal, si se obtiene un “*beneficio económico* aunque sea *indirecto*”. Por ejemplo, obtener el título de doctor y concurrir a una plaza de profesor titular.

✓ En concreto, el **artículo 270 del Código Penal** establece que: «Será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero,... plagie..., en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio...»

Además, **el plagio es el acto de mayor desprestigio profesional que puede cometer un investigador.**

Pero, ¿qué es el plagio?

✓ Es verdad que, aunque la **RAE define plagio** como «**COPIAR EN LO SUSTANCIAL OBRAS AJENAS**, dándolas como propias», **lo cierto es que jurídicamente EL TEMA ES MÁS COMPLEJO**, por lo que nos podemos acercar al concepto de plagio a través de sus modalidades.

✓ El plagio más simple consiste en copiar todo o parte de una obra (literaria, artística o científica) y atribuirse la autoría. Los métodos habituales de copia son:

- El popular “corta y pega”,
- El “copiado indirecto”, amanuense o mecanografiado.

✓ Pero, como modalidad de plagio, también hay **un método un poco más sofisticado de plagio (“el maquillaje de párrafos”)** que consiste en copiar un número importante de páginas ajenas e ir cambiando burdamente el texto párrafo a párrafo. p.e, si el texto original dice: «En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocín flaco y galgo corredor....» el plagiarlo corrige los párrafos uno a uno, más o menos de esta forma: «En un sitio de La Mancha, cuyo nombre no recuerdo, no hace mucho que vivía un caballero con un caballo flaco y un veloz galgo ...».

✓ Se debe tener en cuenta que la prueba del plagio, en estos casos, consiste en contrastar las páginas copiadas una a una y ver si “la ordenación de párrafos e ideas” es la misma, con ligeras variaciones en la forma de “expresar ideas”.

Del mismo modo, es ilícito el uso abusivo del “derecho de cita”.

✓ El “derecho de cita”, en principio, es un acto lícito, concebido como excepción a los derechos de reproducción de la obra, y se regula en el artículo 32 TRLPI, según el cual:

«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*».

✓ Destacamos en cursiva, el fin docente e investigador y, sobre todo, el modo de realizarla lícitamente la cita:

- Incluyendo “fragmentos” de la obra ajena para su cita o análisis,
- E indicando la fuente y el nombre del autor.

✓ Por tanto, **no es lícito incluir fragmentos de obras ajenas sin indicar fuente y nombre del autor**, como **tampoco lo es el “uso abusivo” de la cita, que consiste en disfrazar como cita la copia de páginas enteras, copia que**

excede de lo que comúnmente se entiende como “fragmento” (esto es, un párrafo, a lo sumo dos o tres...)

✓ Es cierto que el concepto “fragmento” es un concepto jurídico indeterminado, pero también es verdad que **incluir en la obra propia “siete u ocho páginas...” de una obra ajena, aunque se cite al autor en varias ocasiones, supone una infracción al derecho de cita** porque dicha praxis no puede quedar amparada ni encontrar justificación en la finalidad de “inclusión a título de cita o para su análisis”.

**Una OBRA QUE haya pasado
EL CONTROL ANTIPLAGIO DE UN PROGRAMA INFORMÁTICO,
puede contener PLAGIO DESDE EL PUNTO DE VISTA JURÍDICO**

por ejemplo, una tesis doctoral de 500 páginas, en la que se incluyen 7 páginas ajenas sin citar, representa, en términos porcentuales, el 1,4 por ciento de la obra; pero existe plagio.

**La mayoría de los programas anti-plagio detectan únicamente
“coincidencias”.**

Aunque, si esas “coincidencias” son

- de textos que no tienen propiedad intelectual, p. ej. leyes o sentencias,
- o de textos que son muy básicos o simples y nada originales,
- o de obras que se difunden como *Open Access*, conforme a licencia que permite su copia en toda la extensión citando al autor...

no existe plagio, pero tampoco originalidad.

✓ Por último, hay que tener **especial cuidado con las fotografías, y con las grabaciones audiovisuales y musicales ajenas**. De momento, y a la espera de que se reforme la normativa de propiedad intelectual en materia de usos permitidos en el ámbito docente e investigador (donde el derecho español, a diferencia del italiano o el portugués, es muy restrictivo y muy costoso para las Universidades Públicas), la inclusión de obras fotográficas ajenas, salvo que se trate de una “obra aislada fotográfica figurativa” y lo mismo con las grabaciones, tienen propiedad intelectual (ya sea como fotografía artística, con una protección de 70 años *p.m.a.*, ya sea como mera fotografía, con una protección de 25 años), y su infracción se puede sustanciar en reclamaciones judiciales de diverso tipo.

✓ Actualmente solo se pueden utilizar libremente fotografías caídas en dominio público o que estén libres de derechos (de explotación), como sería el caso de las obras difundidas como *Open Access* y con una licencia que permita su uso. Por ejemplo, una licencia “(CC BY)”. Pero cuidado, porque una licencia “(CC BY NC)” no permite su inclusión en un libro destinado a la venta, y lo mismo ocurre con licencia “(CC SA)” que permite el uso de obra derivada bajo licencia idéntica o similar.

**Por tanto, recomendamos, en la medida de lo posible,
hacer tus propias fotografías y grabaciones,**

con el pertinente consentimiento informado si fotografías o grabas a personas físicas, especialmente si pretendes difundirlas o compartirlas con tercero, ya que con ello también generas tu propia “propiedad intelectual” respetando los derechos fundamentales de las personas fotografiadas.

4. ¿QUÉ OCURRE SI SE TRATA DE UN TFM/TFG O INVESTIGACIÓN QUE GENERA UN SOFTWARE O UNA APP?

✓ Los programas de ordenador y las aplicaciones (apps) están protegidas por la ley de propiedad intelectual de la misma forma que si fuesen una obra literaria. Pertenecen al autor por el mero hecho de la creación.

¿Pero? ¿Cuándo se entiende creado un programa de ordenador? La respuesta es que **un programa de ordenador existe desde que está escrito en “código fuente”**.

✓ Por tanto, la **adecuada protección del código fuente** y de los algoritmos que se integran en el programa **durante su desarrollo, es básica, a través del “secreto comercial”**. E incluso, una vez creado el software, se puede limitar el acceso al código fuente para impedir su copiado. Lo que no se puede impedir es que un programador, visualizando la apariencia externa del programa, desarrolle un software idéntico o similar, pero siempre que no sea con un “corta y pega” del código fuente.

✓ También **es importante, cuando son varias las personas que participan en el desarrollo de un software, que quede claro, a través de contratos y documentos de confidencialidad, la autoría conjunta**, ya sea como obra colectiva o en colaboración, o **la autoría individual**, así como la titularidad o cesión de los derechos de explotación sobre el programa de ordenador.

RESULTA SIEMPRE CONVENIENTE

**UN ASESORAMIENTO LEGAL PREVIO Y POSTERIOR A SU CREACIÓN
EN EL DESARROLLO Y EXPLOTACIÓN DE CUALQUIER SOFTWARE,
VIDEOJUEGO O APLICACIÓN PARA TELÉFONO MÓVIL (APP)**

5. ¿QUÉ OCURRE SI EL TFM/TFG O LA INVESTIGACIÓN CONTIENE O ES UNA BASE DE DATOS?

✓ Ya hemos visto como **las bases de datos que tratan datos personales tienen que respetar la normativa de protección de datos** (obteniendo los datos mediante un consentimiento libre e informado y llevando un registro de actividades de tratamiento y, en su caso, con solicitud de informe de evaluación de impacto o de formalización de un contrato entre el titular del fichero y los encargados del tratamiento).

✓ **Si el contenido de la base de datos está conformado por materiales protegidos por la propiedad intelectual** (base de datos de obras literarias, científicas, artísticas, audiovisuales...) **también se requiere el consentimiento de los titulares de los derechos de propiedad intelectual cuyas obras conforman la base de datos.**

✓ Obviamente, si la base de datos no contiene datos personales y no contiene material protegido por la propiedad intelectual, no se requiere de consentimiento para ir conformando o desarrollando su contenido, pero **toda base de datos que para su elaboración requiere de un importante esfuerzo en tiempo o de muchos recursos económicos, y es en sí misma valiosa, tiene un “derecho sui de generis de propiedad intelectual sobre dicha base de datos” reconocido por el derecho de la Unión Europea, frente a los actos de extracción o reutilización de su contenido.**

EL TITULAR DE LA BASE DE DATOS ES EL QUE DECIDIRÁ CÓMO SE UTILIZA ésta, COMERCIAL O NO COMERCIALMENTE, PERO SI LA B.D. TIENE DATOS PERSONALES TAMBIÉN ES EL RESPONSABLE DE LA OBTENCIÓN DE UN CONSENTIMIENTO LÍCITO Y DE CUMPLIR CON LA NORMATIVA DE PROTECCIÓN DE DATOS

✓ Obviamente, el titular de una base de datos no puede impedir que otras personas elaboren una base de datos idéntica o similar, pero tiene que ser una creación propia, no siendo válido el método de extracción o copiado de toda la base de datos y explotación de dicha base con otro nombre comercial.

✓ Para poder acreditar en juicio que una base de datos (plagiaría) se ha elaborado copiando todos los contenidos de una base de datos (originaria), lo que se debe hacer, en todos y cada uno de los documentos que integran la base de datos originaria es incluir **“alteraciones o marcas de agua”**. P.e. en una base de datos de leyes, extraídas de BOE, se debe incluir en cada documento que integra la base “dobles espacios” que no existen en el documento original del BOE. De tal suerte, que si una persona copia sin consentimiento todas las leyes contenidas en la base de datos, el titular originario pueda acreditar la extracción y reutilización ilícita (plagio de la base de datos) a través de las marcas de agua que ha introducido en todos los documentos de su base de datos, y que aparecen también en los documentos de la base de datos plagiaría.

6. ¿CÓMO SE DEBE LEER UN TFM O TFG SI CONTIENE UNA POSIBLE PATENTE o UN SECRETO COMERCIAL?

✓ En el supuesto muy excepcional de que un TFM o TFG contenga o describa un producto o un procedimiento nuevo para obtener un producto que pueda ser objeto de patente (nacional o comunitaria) por tratarse de una invención nueva (esto es, desconocida para el estado de la ciencia y de la técnica), es necesario y conveniente, mantenerlo en secreto y protegerlo como secreto, de conformidad con la ley 1/2019 y buscar un modo para que el trabajo pueda:

- leerse, sin acto público y sin público (salvo que se autorice la presencia de personas concretas por el inventor y siempre con un “NDA”).
- sin publicarse en ningún sitio, y menos en internet.
- y con la firma de los correspondientes compromisos de confidencialidad (NDA) por parte de quienes vayan a formar, en su caso, el Tribunal del TFM o TFG.

Obviamente,

- **Después del proceso de obtención o denegación de la patente, o una vez el secreto se ha materializado en una obra o prestación protegida por propiedad intelectual e industrial, el TFM/TFG debe ser publicado en la forma establecida por la Universitat para cada concreto Grado o Máster.**
- **Si la investigación es del personal investigador (funcionario o contratado) de una Universidad Pública (como es la Universitat de València) o está integrada en un equipo, estructura o instituto de investigación de la UV, SE DEBE CUMPLIR CON LA OBLIGACIÓN LEGAL de la Ley de Patentes (art. 21) de comunicar, con la debida confidencialidad, la invención a <patentes.otri@uv.es> para que en el plazo de tres meses la Universidad decida si es ella o no quien patenta, de conformidad con su normativa interna.**

7. ¿QUÉ OCURRE CON LAS IDEAS DE EMPRENDIMIENTO?

✓ La Universitat de València fomenta el espíritu emprendedor de sus estudiantes a través de iniciativas y programas como, por ejemplo, los premios Motivem, en el que se expone ideas básicas y se graba un video de un minuto sobre los beneficios que reportaría dicha idea.

✓ **En principio, cuando la descripción de la idea es muy básica no atribuye ningún título de exclusividad ni impide que otros puedan desarrollar dicha idea.**

✓ Uno de los casos más importantes de emprendimiento fue el de dos hermanos Tyler y Cameron Winklevoss, cuando ambos estudiaban en la Universidad de Harvard, y pensaron en crear una red social para la universidad (Harvard Connection, después conocido como ConnectU) y para ello contactaron con Zuckerberg, que parece materializó la idea, desarrollando la red social Facebook. (El caso se resolvió por acuerdo extrajudicial).

✓ Dicho caso ilustra muy bien las divergencias que pueden surgir en el seno de los equipos, entre los que tienen una idea y quienes luego finalmente la materializan, por lo que (sí realmente se trata de una idea novedosa y desconocida en un sector especializado) **resulta conveniente tener en cuenta todos los mecanismo de protección del Know-How y de la propiedad intelectual que se han esbozado en esta breve guía**, además de no perjudicar con su publicidad la posible patentabilidad del producto o procedimiento resultante.

✓ En nuestro Derecho, **tener la idea no atribuye un monopolio o derecho exclusivo sobre la misma, salvo que se proteja como Know-How con los pertinentes compromisos de confidencialidad.** Y las obras literarias, artísticas o los programas de ordenador son de la persona que los crea y materializa. Por tanto, entre “tener una idea para desarrollar un programa de ordenador que sirva de base a una red social” y “crear el concreto software y la red social” hay una “gran tech”, cuya titularidad es de quien la materializa, ya que nuestro derecho solo protege a quien “desarrolla el concreto software y crea la red social”, salvo que la idea se haya protegido como secreto comercial (con la actual ley 1/2019 de secretos empresariales) o el “proyecto de idea” se haya inscrito de una forma más detallada en el Registro de la Propiedad Intelectual como obra protegida y ya materializada.

Esperamos que esta Guía te haya sido de utilidad.

Estamos, como siempre, a tu disposición en la

Delegación de Protección de Datos de la UV

lopd@uv.es