# Ética, Legislación y Profesión

"'Aprender"' a hacer tu trabajo de una fomra ética y legal

Alejandro Barrachina Argudo

*Grado en Ingeniería informática*
*Facultad de Informática*
*Universidad Complutense de Madrid*

2022-2023

# Índice general

# 1 | Introducción a la Ética y la Legislación

## 1.1. Introducción a la Ética

La ética es una parte de la filosofía, la cual implica cuestionarse sobre problemas relativos al bien, al deber, a la virtud o al vicio. Los objetivos de la ética son:

1. Llegar a alguna conclusión acerca de lo que es correcto o no
2. Que la conclusión pueda ser defendida con argumentos.
3. Justificar las normas que regulan el comportamiento en diferentes ámbitos de la vida

La reflexión es la consideración minuciosa de un asunto, esto implica dedicarle tiempo y no quedarse con la primera impresión. Para llevar a cabo esta consideración minuciosa debemos:

- Informarnos: contrastar fuentes y poder citarlas.
- Pros y contrastar.
- Partes afectadas.
- Circunstancias.
- Posibles escenarios futuros.
- Contrastar: comentar, dialogar, escuchar otros puntos de vista diferentes al propio.
- Discernir, analizar

Es importante hacerse muchas preguntas para poder reconocer y tener en cuenta a todas las partes implicadas, dirigir esfuerzos a la hora de buscar información, ampliar nuestra visión del tema y compartir o hacer esas preguntas a otras personas para ampliar nuestra perspectiva. Los elementos claves para una reflexión ética son:

1. Identificar los valores del conflicto.
2. Empatía: personas/colectivos afectados: ponerse en el lugar de los otros, percibir a los demás como seres sintientes.
3. Analizar las circunstancias.
4. Pros, contras y su peso.
5. Alcance de las consecuencias en el espacio y el tiempo.
6. Posibles escenarios futuros partiendo del presente.

Tras una reflexión ética debemos llegar a una conclusión clara, directamente relacionada con los argumentos y ejemplos reales utilizados. Esta conclusión debe ser coherente con los argumentos y ejemplos usados. Si esta conclusión está matizada demostrará un correcto proceso de reflexión.

## 1.2. Introducción a la Legislación

El derecho es la técnica de dar a cada persona lo que le corresponde. También es un conjunto de normas organizadas, escritas o no, cuyo cumplimiento es obligatorio y pueden ser impuestas de forma coactiva, que sirven para asegurar la pacífica convivencia.

El Código Civil en su art. 1.1 señala como fuentes del Derecho:

1. La Ley: norma vigente.
2. La costumbre: conductas repetidas desde tiempos inmemoriales. Solo rige en defecto de ley aplicable y siempre que no contradiga la moral o al orden público y tiene que ser probada.

3. Los PGD (Principios Generales del Derecho): principios fundamentales. Se aplican en defecto de la Ley o costumbre. Además, su contenido está siempre presente en el ordenamiento jurídico.

Estas fuentes de derecho tienen una jerarquía, lo que hace que una disposición no carezca de valor si contradice a una de rango superior. Ley > costumbre > PGD. La legislación refleja una serie de valores (Derechos, protección) y una serie de conflictos (delitos, sanción, penas).

## 1.3. Cuestiones éticas relacionadas con el diseño de aplicaciones informáticas

Tanto el diseño como el software son políticos, ya que podemos considerar que "Los algoritmos son opiniones incrustadas en código".

El diseño de un software no es neutro, ya que se tienen que considerar distintos puntos al hacer el programa:

- Qué función o funciones realiza.
- Qué restricciones ponemos al usuario y cuales no.
- Qué datos vamos a recolectar y/o analizar.
- Qué podemos deducir sobre los usuarios.
- Qué mecanismos se van a utilizar para crear o no adicción entre los usuarios.

Un ejemplo de software político puede ser BOSCO, una aplicación financiada por el Gobierno Español utilizada por las compañías eléctricas para decidir quién tiene derecho a un descuento en la factura de la luz.

Otro ejemplo sería el sistema VeriPol utilizado por la Policía Nacional para detectar denuncias falsas.

### 1.3.1. Manipulación online

Algunos de los casos más conocidos son: Facebook con su publicidad dirigida a adolescentes estresados y deprimidos, Uber con estrategias para conseguir que sus conductores trabajen más horas o en determinadas zonas y Cambrige Analytica y sus mensajes políticos personalizados basados en perfiles de Facebook.

Dentro de la manipulación online podemos ver varios tipos:

- **Persuasión (influencia):** cualquier forma de influencia e influencia a través de la discusión racional.
- **Persuasión en sentido explicito:** es visible, consciente y resistible (hay alternativas).
- **Manipulación:** es oculta, inconsciente y explota vulnerabilidades cognitivas emocionales y estructurales o individuales. La víctima no es consciente de que ha sido dirigida a una decisión determinada. Hay un beneficio para la parte manipuladora.
- **Manipulación + TIC (Tecnologías de la información y la comunicación):** hay grandes cantidades de información personal y algoritmos que analizan estos datos que son invisibles y omnipresentes. Generan campañas individualizadas con anuncios y mensajes a medida.

Estas acciones pueden producir daños materiales como gastar dinero en cosas que no necesitamos o gastar más de lo que queríamos o daños en cuanto a violación de la autonomía, con impacto individual y/o social y político.

Al estudiar un programa tenemos que hacernos las siguientes preguntas:

- Quién decide qué y cómo se diseñan.
- Si tiene mayor o menor potencial manipulador.
- Si está diseñada para ser adictiva.
- Si está diseñada para potenciar el comportamiento impulsivo y disminuir la capacidad analítica.
- Si se da al usuario una falsa sensación de autonomía.

### 1.3.2. El salto a la IA

La evolución de la IA nos ha traído sistemas muy complejos con aprendizajes profundos (encuentran patrones en un conjunto de datos) que sacan conclusiones estadísticas y son fáciles de engañar.

Al ser entrenadas mediante conjuntos de datos, £Pueden sus diseñadores predecir su comportamiento? Algunas arquitecturas de IA funcionan como una caja negra en la que no sabemos el porqué de las decisiones de la máquina, aunque no todas las arquitecturas son tan opacas.

Hay que tener en cuenta el hecho de que el sesgo cognitivo y los prejuicios de los desarrolladores de una IA pueden influir de manera negativa en su toma de decisiones. Estos sesgos pueden ser inconscientes o heredados(por el diseño o por el conjunto de datos que se usa para el entrenamiento) o prejuicios deliberados que nazcan de una determinada política o idea.

Para evitar IAs con este tipo de problema tenemos que buscar siempre que el algoritmo sea explicable.

> Cómo asegurar que el algoritmo es justo, cómo asegurar que el algoritmo es interpretable y explicable: todo eso está todavía bastante lejos.
>
> *Nihar Shah*

Es de interés para las personas que desarrollan el algoritmo, para abogades y jueces y para toda la ciudadanía entender la toma de decisiones de un algoritmo.

Parte de evitar problemas de bias viene en forma de auditorías, para las cuales hay que tener acceso a:

- Diseño: explicabilidad, trazabilidad y reproducibilidad.
- Datos de entrenamiento o conjunto de datos para probar el sistema.
- Código fuente

### 1.3.3. Guía ética para una IA confiable (UE)

> To everyone who shapes technology today
> We live in a world where technology is consuming society, ethics, and our core existence. It is time to take responsibility for the world we are creating. Time to put humans before business. Time to replace the empty rhetoric of building a better world with a commitment to real action. It is time to organize, and to hold each other accountable.
>
> *The Copenhagen Letter, 2017*

La UE define una IA fiable como una que es lícita, ética y robusta. Una IA fiable debe respetar cuatro principios éticos (a parte de respetar los derechos fundamentales):

- Respeto de la autonomía humana.
- Prevención del daño.
- Equidad.
- Explicabilidad.

Una IA fiable debe cumplir también siete requisitos clave:

- Acción y supervisión humanas.
- Solidez técnica y seguridad.

- Transparencia.
- Diversidad, no discriminación y equidad.
- Bienestar social y ambiental.
- Rendición de cuentas.

Para aplicar estos principios hay que hacerlo desde el propio diseño del algoritmo: poniendo el respeto al ser humano por encima de cualquier otro tipo de interés como centro del diseño, respetar la autonomía individual y colectiva, no discriminar, revisar los sesgos, hacer un algoritmo explicable y transparente, respetar la privacidad y los DDAA (derechos de autor) (licencia y opciones de protección de los DDAA) y prever y tratar de evitar posibles usos fraudulentos y/o delictivos del algoritmo.

# 2 | Privacidad

## 2.1. Derecho fundamental

La privacidad es un derecho fundamental recogido en la Constitución Española de 1978 en el Articulo 18:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
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.

## 2.2. Redes sociales

Las redes sociales tienen diseños basados en crear adicción (modelo "Hooked" de Mil Eyal), con técnicas de persuasión/ manipulación / coacción y extracción de datos del usuario para su monetización.

Los términos y condiciones de una red social recogen datos importantes como:

- Copyright
- Información que recogen y cómo la almacenan:
  - Qué información.
  - Donde (transferencia de datos fuera de la UE).
  - Durante cuánto tiempo.
  - Con quién la comparten.
  - Para qué la utilizan.
- Cambios, notificaciones.
- Como cerrar una cuenta y que pasa con ella después de cerrarla,
- Cookies de rastreo
- Censura de contenido

Pero normalmente la gente no las lee, ya que son largas y complicadas con mucho texto jurídico. Es importante leer estos términos de servicio para ser conscientes de lo que hace la aplicación con nuestros datos.

Es importante también saber que una clausula o termino ilegal no tiene validez aunque aparezca en los términos de servicio y que toda empresa que opere en la UE debe cumplir con el RGPD

El auge de las redes sociales a traído también el ciberacoso, que tiene un mayor impacto y difusión que el acoso "tradicional". Podemos decir que hay tres tipos de ciberacoso: exclusión, manipulación y hostigamiento, también podemos diferenciar tres partes: persona que acosa, persona que es acosada y persona observadora.

El ciberacoso puede causar una reacción en cadena, ocasionando un efecto de bola de nieve. No hay violencia física pero causa un perjuicio muy grande en la víctima.

Al usar las redes sociales es importante pensar en qué uso damos de ellas, cuánto las usamos y si las usamos de manera correcta. Es importante el impacto de nuestros actos en las redes sociales.

## 2.3. LOPD y RGPD

El RGPD se define en el Reglamento (UE) **2026/679** del Parlamento Europeo y del Consejo de 27 de abril de 2016 y es relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

La LOPD es una adaptación de este reglamento en nuestro país, cada país miembro tiene su propia adaptación.

El RGPD define su entrada en vigor y aplicación en el **Artículo 99**:

- El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.
- Será aplicable a partir del 25 de mayo de 2018.

El presente reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

El esquema del RGPD es:

1. 173 consideraciones (28 páginas): por qué, para qué (preámbulo).
2. Disposiciones Generales.
3. Ámbito de aplicación: actividades realizadas en la UE independientemente de donde realices el tratamiento.
4. Definiciones
5. Principios: relativos al tratamiento, al consentimiento, definir categorías especiales de datos personales etc.
6. Derechos: transparencia, información y acceso, rectificación, oposición + art. 17 → Derecho al olvido.
7. Limitaciones: casos judiciales etc.
8. Obligaciones de responsables del tratamiento.

### 2.3.1. Consideraciones

**1.-** La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El Artículo 8, apartado 1, de la Carta de los Derechos fundamentales de la UE y el Artículo 16, apartado 1, del TFUE (Tratado de funcionamiento de la Unión Europea) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

**6.-** La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial.

**58.-** El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea mas difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea.

**83.-** A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado.

Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuanta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse.

**101.-** En todo caso, la transferencia a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento.

Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales.

### 2.3.2. AEPD

La AEPD es el organismo público encargado de velar por el cumplimiento de la LOPD en España.

La AEPD lista los siguientes derechos del ciudadano sobre sus datos:

- Derecho a conocer: para qué se usan tus datos, plazo de conservación, derecho a presentar una reclamación ante la AEPD y la existencia de decisiones automatizadas, elaboración de perfiles y sus consecuencias.
- Derecho a solicitar al/la responsable: suspensión del tratamiento de tus datos, conservación de tus datos, portabilidad de tus datos a otros proveedores de servicios.
- Derecho a rectificar tus datos: cuando sean inexactos o cuando estén incompletos.
- Derecho a suprimir tus datos: por tratamiento ilícito, por desaparición de la finalidad que motivó el tratamiento o recogida, cuando revocas tu consentimiento o cuando te opones a que se traten.
- Derecho a oposición al tratamiento de tus datos: Por motivos personales, salvo que quien trata tus datos acredite un interés legítimo, cuando el tratamiento tenga por objeto el marketing directo.

La AEPD también ofrece una "Guía para responsables de tratamiento de datos" en la cual se establecen unos principios a seguridad

**El principio de responsabilidad proactiva.** Este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que se lleven a cabo. Este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en la que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión. Podemos distinguir seis medidas de responsabilidad activa:

- Análisis de riesgos
- Registro de actividades de tratamiento
- Protección de datos desde el diseño y por defecto
- Medidas de seguridad
- Notificaciones de "violaciones de seguridad de los datos"
- Evaluaciones de impacto sobre la Protección de datos

Todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo. El tipo de análisis variará en función de: el tipo de tratamiento, la naturaleza de los datos, el número de interesados afectados y la cantidad y variedad de tratamientos que una misma organización lleve a cabo.

Responsables y encargados deberán mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD y que contenga cuestiones como:

- Nombre y datos de contacto del responsable o corresponsable y del Delegado de Protección de Datos si existiese.
- Finalidades del tratamiento.
- Descripción de categorías de interesados y categorías de datos personales tratados.
- Transferencias internacionales de datos.

Están exentas las organizaciones que empleen a menos de 250 trabajadores, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

**Protección de Datos desde el Diseño y por Defecto.** Estas medidas se incluyen dentro de las que debe aplicar el responsable con anterioridad al inicio del tratamiento y también cuando se esté desarrollando.

Este tipo de medidas reflejan muy directamente el enfoque de responsabilidad proactiva. Se trata de pensar en términos de protección de datos desde el mismo momento en que se diseña un tratamiento, un producto o servicio que implica el tratamiento de datos personales.

Cuando se produzca una violación de seguridad de los datos, el responsable debe notificar a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

La notificación de la quiebra a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella. Los responsables del tratamiento deberán realizar una EIPD (Evaluación de Impacto sobre la Proteccin de Datos) con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un riesgo alto para los derechos y libertades de los interesados.

# 3 | Derechos Digitales

Los avances digitales tales como la IA, realidad virtual y aumentada o la robótica suponen nuevos retos para la legislación:

- Protección de datos personales.
- Procesamiento de *big data* justo y respetuoso.
- Internet de las cosas.
- Robótica.
- Sistemas de IA.

El derecho al respeto por la vida privada es una preocupación, ya que muchas aplicaciones TIC intentan influir en las actitudes y comportamientos de las personas. Dichas actividades persuasivas afectan a la autonomía de la persona, a su capacidad de autodeterminación y a si libertad de pensamiento y de conciencia.

Los derechos digitales surgen por las limitaciones de los derechos fundamentales "tradicionales" en el ámbito digital, son medidas necesarias para garantizar el respeto de los derechos fundamentales en este ámbito. Algunos de estos derechos son el derecho a que "me dejen en paz", el derecho al olvido y el derecho al acceso a Internet(no es lo mismo que acceso gratuito) entre otros.

## 3.1. Libertad de expresión

La **libertad de expresión** se recoge en el Artículo 20 de la constitución y es un derecho fundamental. La libertad de expresión en Internet se mantiene igual, pero con un carácter más global. Cualquier persona puede hacer públicas sus opiniones, puntos de vista etc. con una mayor posibilidad de impacto y difusión que por otros medios. Se mantienen los mismos límites establecidos por la constitución:

- Respeto al honor.
- Respeto a la intimidad.
- Respeto a la propia imagen.
- Respeto a la juventud y a la infancia.

En internet hay filtros en las distintas para plataformas para proteger el copyright, aunque podrían utilizarse para retirar contenidos que "no interesen". Son muchos los ejemplos de plataformas que usan estos filtros para imponer su ideología y estándares.

El **anonimato** garantiza poder expresar opiniones sin temor a las represalias. En internet garantiza la libertad de expresión y también el libre intercambio de información y la privacidad y derecho a no ser espiados. El anonimato se declara como parte del derecho a la libertad de expresión (art. 20 CE (Constitución Española)) y como parte del secreto de las comunicaciones (art 18 CE) Así, la extensión del secreto de las comunicaciones a las comunicaciones electrónicas, la garantía de un cierto derecho al anonimato cuando se navegue por Internet, se hagan transacciones económicas o se participe políticamente a través de la Red, aparece como uno de los más importantes derechos, a la vez que más discutido, en la actualidad.

La suma de la IP, mas las cookies, más la minería de datos, puede resultar en la identificación de una persona. Para identificar a una persona(por ejemplo al investigar un delito cometido desde una IP) es necesaria la IP y "medios que pueden ser razonablemente utilizados" para asegurar la correspondencia IP-persona. La protección otorgada a las direcciones IP constituye, por lo tanto, un elemento esencial para mantener el anonimato en Internet. Grandes empresas de Internet (como Google) han cuestionado que la IP sea un dato de carácter personal. Una misma IP puede ser compartida por diferentes usuarios de un mismo ISP (Internet Service Provider) (IPs dinámicas).

## 3.2. Transparencia

La relación entre publicidad y privacidad o los derechos de acceso a la información, a la intimidad y a la protección de datos es potencialmente conflictiva. Convergen en un punto de conexión, la divulgación por las autoridades públicas de información que contienen datos personales, lo que quiere dilucidar cuál es la normativa aplicable y las determinaciones sustantivas, procedimentales, de garantías y organizativas que permitan maximizar la eficacia de ambos derechos. Y, a demás, hacerlo de forma adaptar al mundo digital en que actualmente vivimos.

Sobre esta problemática particular se presenta el conflicto entre publicidad y privacidad de la información pública en Internet, y a falta de Autoridades de transparencia y acceso a la información, el protagonismo lo está ejerciendo la AEPD, que ha dictado resoluciones y recomendaciones del mayor interés sobre esta materia.

## 3.3. Neutralidad de la red

Todos los paquetes que viajan por la red deben recibir el mismo tratamiento por parte de los ISP y los gobiernos, no se privilegia a ningún participante por encima de otro. No se debe cobrar diferente en función del contenido al que se acceda, plataforma, aplicación o tipo de equipamiento utilizado para el acceso. Esto es muy importante porque garantiza la igualdad de acceso a contenidos de Internet y porque garantiza la privacidad de la información que viaja por la red (que tendría que ser examinada para ser tratada de diferente forma).

## 3.4. Criptografía: derecho fundamental

Para mantener la privacidad y el anonimato es importante encriptar ciertos tipos de información:

- Comunicaciones personales.
- Transacciones monetarias.
- Contraseñas, números de tarjetas de crédito etc.
- Información empresarial.

Hay un debate sobre si los gobiernos deberían tener acceso a datos encriptados (Estados Unidos contra Apple, Rusia contra Telegram).

Las leyes sobre criptografía tienen algunas restricciones:

- **Control de exportaciones:** que es la restricción a exportar métodos de criptografía desde un país a otro país o entidad comercial. Hay acuerdos de exportación internacionales, siendo el principal el Acuerdo de Wassenaar.
- **Control de importaciones:** este punto se refiere a las restricciones de usar ciertos métodos de encriptado en un país.
- **Problemas con patentes.**
- En algunas ocasiones una persona puede ser obligada a desencriptar archivos o revelar una clave de encriptado.

En EEUU (Estados Unidos) es necesario pedir permiso antes de publicar un algoritmo o software de cifrado y tienen una regulación de algoritmos criptográficos fuera de su país, el EAR (Export Administration Regulations) parte del International Traffic in Arms Regulation.

## 3.5. Comunidades online / virtuales

Se denomina comunidad virtual a aquella cuyos vínculos, interacciones y relaciones tienen lugar, no en un espacio físico sino en un espacio como Internet. Las comunidades online se forman a partir de intereses similares entre grupos de personas. Se organizan y se llevan a cabo a partir de objetivos específicos. Las comunidades saben que son redes, evolucionan de este modo, ampliando los miembros, diversificándose entre sí, nacen en el ciberespacio.

Podemos ver comunidades centralizadas y distribuidas, gobernadas por Empresas, gobiernos o autogestionadas.

# 4 | Brecha Digital y Privilegios

## 4.1. Privilegios y desigualdad

> Los españoles son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social
>
> *Artículo 14 CE*

En la sociedad podemos ver una igualdad de derechos, pero una desigualdad de oportunidades.

Debemos ver los privilegios de dos maneras:

- Con relación a la ética: con la capacidad de tener en cuenta a todas las partes implicadas en un conflicto y ponerse en su lugar.
- En relación con la brecha digital: plantearse si el acceso a la tecnología es o no un privilegio y si tendría que considerarse un Derecho Fundamental.

## 4.2. Brecha Digital

El DESI (Digital Economy and Society Index) es un informe anual publicado por la Comisión Europea que supervisa los avances de los Estados Miembros de la UE en el ámbito digital. En este ranking España supera la media europea de personas con capacidades digitales básicas (64 % frente a un 54 %), pero está por debajo de la media en la proporción de especialistas y titulados en TIC.

Se consideran competencias digitales básicas saber que existe el correo electrónico y nivel medio al saber utilizarlo.

En España, según datos del INE (Instituto Nacional de Estadística), hay un $1,6$ % de personas sin habilidades digitales, un $31,4$ % con habilidad baja y un $19,1$ % con habilidades básicas, lo que implica que más de la mitad de la población no sepa usar el correo electrónico.

Tenemos que plantearnos si es un verdadero avance estar más conectados sin resolver los problemas éticos relacionados con el diseño como con el uso de la tecnología digital, como si es ético a cada vez obligar a realizar más trámites administrativos por internet.

## 4.3. Brecha de género

Podemos ver esta brecha de género en las TIC extrapolando datos de nuestra propia facultad:

- **Curso 2018/2019**:
  - $15,3$ % mujeres(total)
  - Nuevos ingresos: 14 %
- **Curso 2020/2021**:
  - $19,4$ % mujeres(total)
  - Nuevos ingresos: n/s
- **Curso 2021/2022**:

- 19,3 % mujeres(total)
- Nuevos ingresos: 18 %

Algunas de las posibles causas de esta brecha cuantitativa son:

- Falta de referentes femeninos en la profesión.
- Percepción de menor capacidad de las mujeres.
- Falta de interés natural de las mujeres.
- Programas educativos / diseño de entorno muy masculino que no resulta atrayente.
- Estereotipos.
- Publicidad relacionada con la informática dirigida a público masculino.

Las primeras programadoras eran mujeres("Top secret rosies":Kathleen McNulty Mauchly, Marlyn Wescoff Meltzer, Betty Snyder Holberton, Jean Jennings Bartik, Frances Bilas Spencer y Ruth Lichterman Teitelbaum ), los primeros avances en el software los realizaron mujeres: el primer compilador, primeros lenguajes de alto nivel, primer procesador de texto y el propio termino "bug".

A finales de los años 60 y principios de los 70 el software comienza a tener un valor económico y se empiezan a cotizar más los puestos de programación ya que estaban mejor pagados. Esto llevó a que la presencia de las mujeres en la profesión disminuyese al 25 %.

La falta de presencia de mujeres en las TIC tiene como consecuencia que un 51 % de la población esté infra-representada en el diseño de la sociedad actual y futura. La falta de diversidad conlleva una peor calidad, menor innovación, menos ingresos y diseños que reproducen estereotipos y discriminaciones, manteniendo así los sesgos.

En 1997 un estudio demuestra que en Suecia una mujer necesita hasta 2,4 veces más méritos que un hombre para recibir una beca pos-doctoral (`https://www.nature.com/articles/387341a0`). En 2012 un experimento demuestra que el mismo currículum atribuido a un hombre recibe mayor valoración que cuando es atribuido a una mujer (`http://www.pnas.org/content/early/2012/09/14/1211286109`)

Estos son solo dos ejemplos de decenas que demuestran que en las profesiones relacionadas con las ciencias hay una clara preferencia hacia los hombres, dejando en una injusta desventaja a las mujeres.

También son muchos los casos de empresas que han sido llevadas a juicio por pagar menos a empleadas frente a sus compañeros masculinos con el mismo puesto:

- `https://eu.usatoday.com/story/tech/2017/09/29/oracle-yet-another-tech-firm-hit-suit-allegedly-pay`
  `718471001/`
- `https://eu.usatoday.com/story/tech/2017/09/14/google-hit-gender-pay-gap-lawsuit-seeking-class-act`
  `666944001/`
- `https://www.mercurynews.com/2019/09/19/google-paid-female-engineering-director-less-demoted-her-f`

# 5 | Derechos de autor

## 5.1. Propiedad intelectual, derechos de autor, LPI

### 5.1.1. Productos objeto y derechos del autor

El Artículo 10 de la LPI define que productos son objeto de propiedad intelectual:

**1.** Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas:

**a)** Los libros, folletos, impresos, epistolarios, escritos, discursos, alocuciones, conferencias, informes forenses, explicaciones de cátedra y cualesquiera otras obras de la misma naturaleza.

**b)** Las composiciones musicales, con o sin letra.

**c)** Las obras dramáticas y dramático-musicales, las coreografías, las pantomimas y, en general, las obras teatrales.

**d)** Las obras cinematográficas y cualesquiera otras obras audiovisuales.

**e)** Las esculturas y las obras de pintura, dibujo, grabado, litografía y las historietas gráficas, tebeos o cómics, así como sus ensayos o bocetos y las demás obras plásticas, sean o no aplicadas.

**f)** Los proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería.

**g)** Los gráficos, mapas, diseños relativos a la topografía, la geografía y, en general, a la ciencia.

**h)** Las obras fotográficas y las expresadas por procedimiento análogo a la fotografía.

**i)** Los programas de ordenador

**2.** El titulo de una obra, cuando sea original, quedará protegido como parte de ella.

El Capítulo III de la LPI define los derechos morales del autor (resumen):

Pertenecen al autor, no pueden cederse:

- Decidir si su obra ha de ser divulgada y en qué forma.
- Exigir el reconocimiento de su condición de autor de la obra.
- Retirar la obra del comercio, por cambio de sus convicciones intelectuales o morales, previa indemnización de daños y prejuicios a los titulares de derechos de explotación.

Pueden cederse:

- Obtención de beneficios
- Reproducción, distribución, comunicación pública y transformación.

### 5.1.2. Dominio público

En los Artículos 26 y 30 se define el tiempo que una obra está amparada bajo la LPI:

**Artículo 26: Duración y cómputo**
Los derechos de explotación de la obra durarán toda la vida del autor y setenta años después de su muerte o declaración de fallecimiento.

**Artículo 30: Cómputo del plazo de protección**
Los plazos de protección establecidos en esta Ley se computarán desde el día 1 de enero del año siguiente al de la muerte o declaración de fallecimiento del autor o a la de la divulgación lícita de la obra, según proceda.

Pasados los 70 años las obras pasan al dominio público.

### 5.1.3. Límites y excepciones

Algunos artículos ponen excepciones y límites a los derechos del autor:

- **Artículo 31** Reproducciones provisionales y copia privada.
- **Artículo 31 bis** Seguridad, procedimientos oficiales y discapacidades.
- **Artículo 32** Cita e ilustración de la enseñanza.
- **Artículo 33** Trabajos sobre temas de actualidad.
- **Artículo 34** Utilización de bases de datos por el usuario legítimo y limitaciones a los derechos de explotación del titular de una base de datos.
- **Artículo 35** Utilización de las obras con ocasión de informaciones de actualidad y de las situadas en vías públicas.
- **Artículo 36** Cable, satélite y grabaciones técnicas.
- **Artículo 37** Reproducción, préstamo y consulta de obras mediante terminales especializados en determinados establecimientos.
- **Artículo 38** Actos oficiales y ceremonias religiosas.
- **Artículo 39** Parodia.

### 5.1.4. Sobre la copia privada

**Artículo 31. Reproducciones provisionales y copia privada**

**1.** No requerirán autorización del autor los actos de reproducción provisional a los que se refiere el artículo 18 que, además de carecer por si mismos de una significación económica independiente, sean transitorios o accesorios y formen parte integrante y esencial de un proceso tecnológico y cuya única finalidad consista en facilitar bien una transmisión en red entre terceras partes por un intermediario, bien una autorización lícita, entendiendo por tal la autorizada por el autor o por la ley.

**2.** Sin perjuicio de la compensación equitativa prevista en el artículo 25, no necesita autorización del autor la reproducción, en cualquier soporte, sin asistencia de terceros, de obras ya divulgadas cuando ocurran simultáneamente las siguientes circunstancias, constitutivas del límite legal de la copia privada:

**a)** Que se lleve a cabo por una persona física exclusivamente para su uso privado, no profesional ni empresarial, y sin fines directa ni indirectamente comerciales.

**b)** Que la reproducción se realice a partir de una fuente lícita y que no se vulnere las condiciones de acceso a la obra o presentación.

**c)** Que la copia obtenida no sea objeto de una utilización colectiva ni lucrativa, ni de distribución mediante precio.

**3.** Quedan excluidas de lo dispuesto en el anterior apartado:

**a)** Las reproducciones de obras que se hayan puesto a disposición del público conforme al artículo 20.2.i), de tal forma que cualquier persona pueda acceder a ellas desde el lugar y momento que elija autorizándose, con arreglo a lo convenido por contrato y, en su caso, mediante pago de precio, la reproducción de la obra.

**b)** Las bases de datos electrónicas.

**c)** Los programas de ordenador, en aplicación de la letra a) del artículo 99.

**Artículo 25. Compensación equitativa por copia privada**

**1.** Las reproducciones de obras divulgadas en forma de libros o publicaciones que a estos efectos se asimilen mediante real decreto, así como de fonogramas, videogramas o de otros soportes sonoros, visuales o audiovisuales, realizada mediante aparatos o instrumentos técnicos no tipográficos, exclusivamente para uso privado, no profesional ni empresarial, sin fines directa o indirectamente comerciales, de conformidad con el artículo 31, apartados 2 y 3, originará una compensación equitativa y única para cada una de las tres modalidades de reproducción mencionadas dirigidas a compensar adecuadamente el perjuicio causado

a los sujetos acreedores como consecuencia de las reproducciones realizadas al amparo del límite legal de copia privada.

**2.** Serán sujetos acreedores de esta compensación equitativa y única los autores de las obras señaladas en el apartado anterior, explotadas públicamente en alguna de las formas mencionadas en dicho apartado, conjuntamente y, en los casos y modalidades de reproducción en que corresponda, con los editores, los productores de fonogramas y videogramas y los artistas intérpretes o ejecutantes cuyas actuaciones hayan sido fijadas en dichos fonogramas y videogramas. Este derecho será irrenunciable para los autores y los artistas intérpretes o ejecutantes.

## 5.2. Protección legal del software

### 5.2.1. Referencia histórica

Se proponen dos vías para la protección del software, o bien por patente de invención o bien por derechos de autor. Se optó finalmente por derechos de autor dado que las patentes no ofrecían la suficiente protección para el software. Un software no puede reunir información suficiente para conocer el "estado de la técnica" del mismo, imposibilitando el hacer el examen de novedad y actividad inventiva. La Propiedad Intelectual ofrece protección con un mínimo de formalidades y costos y es la más adecuada para la cantidad de software que se genera.

Un programa de ordenador sería patentable como componente de un procedimiento de fabricación o de un aparato protegido por patente o por modelo de utilidad, y exclusivamente para la aplicación del mismo.

## 5.3. ¿Qué se puede proteger?

Se pueden proteger programas como sistemas operativos, controladores y utilidades, compiladores, bibliotecas y entornos de desarrollo y utilidades, guiones y procedimientos almacenados, servidores web y de aplicaciones y código empotrado, firmware y microcódigo.

También se puede proteger la documentación de dichos programas: documentos de análisis de requisitos y de diseño del sistema, planes de pruebas, manuales de instalación y usuario, manuales de referencia, y ayuda interactiva.

No se puede proteger ni ideas, ni algoritmos, ni fórmulas matemáticas, ni principios generales ni interfaces de usuario o de aplicación.

## 5.4. ¿A quién pertenece el software?

**Artículo 96. Objeto de la protección**

**1.** A los efectos de la presente Ley se entenderá por programa de ordenador toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.
A los mismos efectos, la expresión programas de ordenador comprenderá también su documentación preparatoria. La documentación técnica y los manuales de uso de un programa gozaran de la misma protección que este Título dispensa a los programas de ordenador.

**4.** No estarán protegidos mediante los derechos de autor con arreglo a la presente Ley las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador, incluidos los que sirven de fundamento a sus interfaces.

**Artículo 97. Titularidad de los derechos**

**1.** Será considerado autor del programa de ordenador la persona o grupo de personas naturales que lo hayan creado, o la persona jurídica que sea contemplada como titular de los derechos de autor en los casos expresamente previstos por esta Ley.

**2.** Cuando se trate de una obra colectiva tendrá la consideración de autor, salvo pacto de lo contrario, la persona natural o jurídica que la edite y divulgue bajo su nombre.

**3.** Los derechos de autor sobre un programa de ordenador que sea resultado unitario de la colaboración entre varios autores serán propiedad común y corresponderán a todos éstos en la proporción que determinen.

**4.** Cuando un trabajador asalariado cree un programa de ordenador, en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación correspondientes al programa de ordenador así creado, tanto el programa fuente como el programa objeto, corresponderán, exclusivamente, al empresario, salvo pacto en contrario.

**5.** La protección se concederá a todas las personas naturales y jurídicas que cumplan los requisitos establecidos en esta Ley para la protección de los derechos de autor.

## 5.5. Límites a los derechos de explotación

**Artículo 100. Límites a los derechos de explotación**

**1.** No necesitarán autorización del titular, salvo disposición contractual en contrario, la reproducción o transformación de un programa de ordenador incluida la corrección de errores, cuando dichos actos sean necesarios para la utilización del mismo por parte del usuario legítimo, con arreglo a su finalidad propuesta.

**2.** La realización de una copia de seguridad por parte de quien tiene derecho a utilizar el programa no podrá impedirse por contrato en cuanto resulte necesaria para dicha utilización.

**3.** El usuario legítimo de la copia de un programa estará facultado para observar, estudiar o verificar su funcionamiento sin autorización previa del titular, con el fin de determinar las ideas y principios implícitos en cualquier elemento del programa, siempre que lo haga durante cualquiera de las operaciones de carga, visualización, ejecución, transmisión o almacenamiento del programa que tiene derecho a hacer.

**5.** No será necesaria la autorización del titular del derecho cuando la reproducción del código y la traducción de su forma en el sentido de los párrafos a) y b) del artículo 99 de la presente LEy, sea indispensable para obtener la información necesaria para la interoperabilidad de un programa creado de forma independiente con otros programas, siempre que se cumplan los siguientes requisitos:

**a)** Que tales actos sean realizados por el usuario legítimo o por cualquier otra persona facultada para utilizar una copia del programa, o, en su nombre, por parte de una persona debidamente autorizada.

**b)** Que la información necesaria para conseguir la interoperabilidad haya sido puesta previamente y de manera fácil y rápida, a disposición de las personas a que se refiere el párrafo anterior.

**c)** Que dichos actos se limiten a aquellas partes del programa original que resulten necesarias para conseguir la interoperabilidad.

## 5.6. Protección "sui generis" de las Bases de Datos

**Artículo 12. Colecciones. Bases de datos.**

**1.** También son objeto de propiedad intelectual, en los términos del libro I de la presente Ley, las colecciones de obras ajenas, de datos o de otros elementos independientes como las antologías y las bases de datos que por la sección o disposición de sus contenidos construyan creaciones intelectuales, sin perjuicio, en su caso, de los derechos que pudieran subsistir sobre dichos contenidos.
La protección reconocida en el presente artículo a estas colecciones se refiere únicamente a su estructura en cuanto forma de expresión de la selección o disposición de sus contenidos, no siendo extensiva a estos.

**2.** A efectos de la presente LEy, y sin perjuicio de lo dispuesto en el apartado anterior, se consideran bases de datos las colecciones de obras, de datos o de otros elementos independientemente dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma.

**3.** La protección reconocida a las ases de datos en virtud del presente artículo no se aplicará a los programas de ordenador utilizados en la fabricación o en el funcionamiento de bases de datos accesibles por medios electrónicos.

## 5.7. Copyright

Cuando una obra está protegida bajo copyright no está permitida la reproducción total o parcial de la misma, ni su tratamiento informático, ni la transmisión de ninguna forma o cualquier medio, ya sea electrónico, mecánico, por fotocopia, por registro u otros métodos, sin el permiso previo y por escrito de los titulares del copyright. Reserva también todos los derechos, incluido el derecho a venta, alquiler, préstamo o cualquier otra forma de cesión del uso del ejemplar.

## 5.8. Patentes

Una patente es un título que reconoce el derecho de explotar en exclusiva la invención patentada, impidiendo a otros su fabricación, venta o utilización sin consentimiento del titular. Como contrapartida, la patente se pone a disposición del público para generar conocimiento.

La patente puede referirse a un procedimiento nuevo, un apartado nuevo, un producto nuevo o un perfeccionamiento o mejora de los mismos. La duración de una patente es de veinte años a contar desde la fecha de presentación de la solicitud. Para mantenerla en vigor es preciso pagar tasas anuales a partir de su concesión.

# 6 | Cultura libre

> Free software is a matter of liberty, not price. To understand the concept you should think of free as in free speech, not as in free beer
>
> Richard Stallman

## 6.1. Software libre, de código abierto y gratuito

Software libre y software gratuito no son lo mismo. En ingles *Free software* se refiere a software libre.

Según `gnu.org` las libertades del software son las siguientes:

**0.** La libertad de ejecutar el programa para cualquier propósito.

**1.** La liberta de estudiar cómo funciona el programa , y cambiarlo para que haga lo que usted quiera. El acceso al código fuente es una condición necesaria para ello.

**2.** La libertad de redistribuir copias para ayudar a su prójimo.

**3.** La libertad de distribuir copias de sus versiones modificadas a terceros. Esto le permite ofrecer a toda la comunidad la oportunidad de beneficiarse de beneficiarse de las modificaciones. El acceso al código fuente es una condición necesaria para ello.

**Copyleft:** mantenimiento de las condiciones de la licencia en toda la cadena de distribución. No permite que legalmente se puedan cerrar creaciones puestas a disposición del público de forma libre.

**Código abierto:** no se exige la distribución libre del código modificado. Permite que creaciones puestas a disposición del público libre se puedan cerrar.

## 6.2. Historia

En 1938 empieza el proyecto GNU (GNU is Not Unix) y en 1985 se funda la FSF (Free Software Foundation). El movimiento de software libre es un movimiento ético y político, ya que se fundamenta en que tener el control de la tecnología que usamos para que trabaje para nosotros y no para corporaciones o gobiernos que busquen restringirnos y monitorearnos.

El concepto de software libre ya existía, a finales de los 60 había software gratuito y empezaba a aparecer software (licencias de uso) de pago y con restricciones de uso.

A principios de los 70 AT&T distribuyó copias gratuitas de Unix y conforme se fue extendiendo su uso, a principios de los 80 empezó a cobrar por ellas. En los 80, en paralelo al desarrollo comercial del software existían comunidades que compartían software libre online.

El término Software de Código Abierto lo adoptó un grupo de dentro del movimiento de software libre en 1998 que querían desmarcarse de la posición más radical y poco comercial del término software libre.

Raymond fundó la Open Source Initiative en 1998 junto a otras personas, Stallman y más miembros de la FSF se opusieron al término y concepto dividiendo el movimiento.

En recientes años han aparecido los llamados *hacktivistas* como Aaron Swartz "Internet's own boy' que luchó por la privacidad en internet hasta que le impusieron una multa astronómica y 35 años de prisión, terminando él por suicidarse.

## 6.3. Licencias

Algunas licencias populares son GPL (General Public License) y BSD (Berkeley Software Distribution).

Las características principales de GPL son:

1. Copia y distribución del código fuente original.
2. Modificación.
3. Distribución de las modificaciones, siempre que se hagan bajo la misma licencia y sin cobrar por ellas.
4. Copia y distribución del ejecutable, siempre que se ponga a disposición el código fuente sin cobrar un extra por ello.

Las características principales de BSD son:

- Uso, modificación, copia y redistribución sin restricción del código objeto o el fuente.
- Aviso de copyright, negación de cualquier garantía o responsabilidad y prohibición de usar el nombre del autor con fines de promoción de obras derivadas sin su permiso.
- No se otorga ninguna garantía sobre el producto ni se asume ninguna responsabilidad.
- Si el software es modificado, se puede distribuir bajo otro tipo de licencia y no es necesario proveer al usuario final del código fuente.

Otro conjunto de licencias es Creative Commons. Estas licencias tienen categorías:

- **BY:** atribución
- **SA:** compartir igual (copyleft)
- **ND:** sin derivados
- **NC:** sin re-uso comercial

En una escala de libre a libre tendríamos:

**Libre** :

- CC0 (DP)
- CC-by (BSD)
- CC-by-sa (GPL) (copyleft)

**No libre**

- CC by-nc-sa (copyleft)
- CC by-nd
- CC by-nc
- Derechos de autor (CC by-nc-nd)

## 6.4. Hardware libre

Aplicando los mismos conceptos del software libre al hardware llegamos a que los usuarios debería poder distribuir copias del hardware, pero en el hardware no hay algo como las “copias”.

Lo que si se puede liberar es el diseño del propio hardware, esto implica que el diseño debe cumplir las mismas libertades que el software libre. Entonces el hardware hecho con diseños libres se podrá considerar hardware libre.

Una de las ventajas del diseño libre de hardware es que varias empresas pueden hacer el mismo producto y así no depender de un solo distribuidor. Tener los diagramas de circuito o código en HDL nos permite estudiar el diseño para buscar errores en el diseño o funcionalidades maliciosas.

GPL a partir de su versión 3 se diseña con el diseño libre de hardware en mente. Un circuito como topología no puede tener copyright (tampoco copyleft). Definiciones de circuitos escritas en HDL pueden tener copyright y por tanto copyleft, pero la topología que este código genera no. Un dibujo de un circuito puede tener copyright (no voy a repetir lo que esto implica), pero solo cubre el dibujo o la distribución, pero no la topología. Cualquiera podría copiar esa misma topología de forma que se vea distinta, o escribir un código HDL distinto que produzca el mismo circuito.

# 7 | Delitos Informáticos

## 7.1. Definición

Hay una falta de acuerdo sobre la definición jurídica de delitos informáticos. No están reflejados como al en el Código Penal español, sino que se han añadido aspectos relacionados en delitos ya existentes y se ha añadido algún artículo relativo al daño causado a bienes informáticos.

Algunes juristas consideran necesario diferenciar intrusismo informático de delincuencia informática. Para Esther Morón el intrusismo son"comportamientos de acceso o interferencia no autorizados, de forma subrepticia, a un sistema informático o red de comunicación electrónica de datos y utilización de los mismos sin autorización o más allá de lo autorizado".

Los equipos informáticos son nuevos bienes jurídicos, se vela por la integridad de la información y del propio equipo, y a demás los bienes jurídicos que pueden ser accedidos y vulnerados por medios informáticos: patrimonio, intimidad, identidad, material con copyright, etc.

## 7.2. Código Penal Español

**Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal**

**Exposición de Motivos**

Si se ha llegado a definir el organismo jurídico como conjunto de normal que regulan el uso de la fuerza, puede entenderse fácilmente la importancia del Código Penal en cualquier sociedad civilizada.

El código penal define los delitos y faltas que constituyen los presupuestos de la aplicación de la forma suprema que puede revestir el poder coactivo del Estado: la pena criminal. En consecuencia, ocupa un lugar preeminente en el conjunto del ordenamiento, hasta el punto que, no sin razón, se ha considerado como una especie de "Constitución negativa".

El Código Penal ha de tutelar los valores y principios básicos de la convivencia social.

### 7.2.1. Tipos de delitos informáticos

**Delitos informáticos "puros"**

- Delitos contra la intimidad: descubrimiento y revelación de secretos (art. 197, art. 197 bis, art. 197 ter).
- Delito de daños, con especial referencia al sabotaje informático (art. 264, art. 264 bis, art. 264 ter y art. 560).
- Tecnología destinada a la comisión de delitos: art. 400.
- De la consideración de terrorismo: art. 573.2.
- Utilización abusiva dde equipos terminales de comunicaciones: art. 256.

**Delitos "tradicionales" que se ven agravados por el uso de las TIC**:

- Delitos relativos a la propiedad intelectual e industrial: art.270 y art. 278.
- Uso de las TIC para realizar estafas: art. 248
- Uso de las TIC en delitos relacionados con abuso a menores: art. 187 y art. 189.
- Uso de las TIC para amenazar: art. 169.
- Uso de las TIC para calumniar e injuriar: art. 205.

### 7.2.2. TÍTULO X. Delitos contra la intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio: CAPÍTULO PRIMERO. Del descubrimiento y revelación de secretos.

**Articulo 197**

**1.** El qie, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

**2.** Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en prejuicio de terceros, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos de un tercero.

**3.** Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

**Artículo 197 bis**

**1.** El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte del sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

**Artículo 197 ter**

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

**a)** Un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

**b)** Una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

### 7.2.3. TÍTULO XIII. Delitos contra el patrimonio y el orden socioeconómico: CAPÍTULO IX. De los daños

**Artículo 264**

**1.** El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.

**2.** Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1.a Se hubiese cometido en el marco de una organización criminal.

2.a Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.

3.a El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

4.a Los hechos hayan afectado al sistema informático de una estructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la UE o de un Estado Miembro de la UE. A estos efectos se considerará infraestructura crítica a un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado.

**3.** Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de terceros

**Artículo 264 bis**

**1.** Serán castigados con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:

**a)** Realizando alguna de las conductas a que se refiere el articulo anterior;

**b)** Introduciendo o transmitiendo datos; o

**c)** Destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

**Artículo 264 ter**

Será castigado con una pena de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que refiere los dos artículos anteriores:

**a)** Un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o

**b)** Una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

**Artículo 573**

**1.** Se considerará delito de terrorismo la comisión de cualquier delito grave contra la vida o la integridad física, la libertad, la integridad moral, la libertad e indemnidad sexuales, el patrimonio, los recursos naturales o el medio ambiente, la salud pública, de riesgo catastrófico, incendio, contra la Corona, de atentado y tenencia, trafico y depósito de armas, municiones o explosivos, previstos en el presente Código, y el apoderamiento de aeronaves, buques u otros medios de transporte colectivo o de mercancías, cuando se llevaran a cabo con cualquiera de las siguientes finalidades:

1.a Subvenir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.

2.a Alterar gravemente la paz pública.

3.a Desestabilizar gravemente el funcionamiento de una organización internacional.

4.a Provocar un estado de terror en la población o en una parte de ella.

**2.** Se considerarán igualmente delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter y 264 a 264 quater cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior.

**Artículo 400**

La fabricación, recepción, obtención o tenencia de útiles, materiales, instrumentos, sustancias, datos y programas informáticos, aparatos, elementos de seguridad u otros medios específicamente destinados a la comisión de delitos descritos en los Capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

### 7.2.4. TÍTULO XIII. Delitos contra el patrimonio y contra el orden socioeconómico, Capítulo VI de las defraudaciones: Sección 3 de las defraudaciones del fluido eléctrico y análogas

**Artículo 256** El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a 400 euros, será castigado con la pena de multa de tres a doce meses.

**Artículo 560**

1. Los que causaren daños que interrumpan, obstaculicen o destruyan líneas o instalaciones de telecomunicaciones o correspondencia posta, serán castigados con la pena de prisión de uno a cinco años.

### 7.2.5. CAPÍTULO XI. De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores: SECCIÓN 1. De los delitos relativos a la propiedad intelectual

**Artículo 270**

1. 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, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o presentación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.
2. La misma pena se impondrá a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o presentaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios.
3. En estos casos, el juez o tribunal ordenará la retirada de las obras o presentaciones objeto de la infracción. Cuando a través de un portal de acceso a internet o servicio de la sociedad de la información, se difundan exclusiva o temporalmente los contenidos objeto de la propiedad intelectual a que se refiere lo.s apartados anteriores, se ordenará la interrupción de la prestación del mismo, y el juez podrá acordar cualquier medida cautelar que tenga por objeto la protección de los derechos de propiedad intelectual.

Excepcionalmente, cuando exista reiteración de las conductas y cuando resulta una medida proporcionada, eficiente y eficaz, se podrá ordenar el bloqueo del acceso correspondiente.

### 7.2.6. CAPÍTULO XI. De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores: SECCIÓN 3. De los delitos relativos al mercado y a los consumidores

**Artículo 278**

1. El que, para descubrir un secreto de empresa se apoderase por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las personas que consideran corresponder por el apoderamiento o destrucción de los soportes informáticos.

**Artículo 510**

3. Las penas previstas en los apartados anteriores se impondrán en su mitad superior cuando lo hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información de modo que, aquel se hiciera accesible a un número elevado de personas

**Artículo 578**

2. Las penas previstas en el apartado anterior se impondrán en su mitad superior cuando los hechos se hubieran llevado a cabo mediante la difusión de servicios o contenidos accesibles al público a través de los medios de comunicación, internet, o por medios de servicios de comunicaciones electrónicas mediante el uso de tecnologías de la información.

## 7.3. Ética hacker

El término hacker lo acuña un "grupo de apasionados programadores" del MIT a principios de los años 60. A mediados de los 80 los medios de comunicación asocian la palabra hacker a criminal informático. El diccionario del argot hacker es "The Jargon File"originalmente creado en el MIT y Standford.

La palabra hacker originalmente se refería a alguien que hacía muebles con un hacha, a día de hoy tiene distintos siginificados:

**hacker** n.

1. Una persona que disfruta explorando los detalles de sistemas programables y como extender sus capacidades, al contrario que la mayoría de usuarios que prefieren aprender el mínimo imprescindible.
2. Una persona que programa con entusiasmo (o incluso de manera obsesiva) o que disfruta la programación en vez de solo teorizar sobre programación.
3. Una persona capaz de apreciar el valor del hack.
4. Una persona que es buena en programar rápido.
5. Un experto en un programa particular, o que trabaje frecuentemente con él o en él.
6. Un experto o entusiasta de cualquier tipo. Alguien puede ser hacker de astronomía, por ejemplo.
7. Alguien que disfruta del desafío intelectual de superar o eludir limitaciones de manera creativa.

deprecado Una persona maliciosa que intenta descubrir información sensible hurgando por ahí. El termino correcto para esto es cracker.

**cracker** n.

- Alguien que rompe la seguridad de un sistema. Acuñado por hackers en 1985 en defensa el uso incorrecto de hacker por la prensa. Anteriormente se intentó usar 'gusano' para este termino pero no tuvo éxito.
- El uso de estos dos términos refleja una repulsa hacia el robo y vandalismo perpetrado por los círculos de crackers. Es esperable que cualquier hacker real haya hecho algo de cracking y conozca algunas de las técnicas básicas, pero también se espera que cualquiera que no sea un principiante haya superado el deseo de usarlas excepto por razones prácticas, inmediatas y benignas.

**Ética hacker** n.

1. La creencia de que compartir información es un poderoso bien positivo, y que es el deber ético de los hackers el compartir su habilidad escribiendo código abierto y facilitando acceso a información y recursos computacionales cuando sea posible.
2. La creencia de que crackear sistemas por diversión y exploración es éticamente correcto siempre y cuando el cracker no cometa ningún robo, vandalismo o brecha de confidencialidad.

## 7.4. Sistemas distribuidos y descentralizados

La descentralización es el proceso de dispersar o distribuir funciones, poderes, personas o cosas fuera de una localización o autoridad central.

Mientras que la centralización, sobretodo en esferas de gobierno, está muy estudiada y practicada, no hay una definición común o entendimiento de la descentralización.

Los agentes o partes toman decisiones en el mismo nivel y se les llama *peers*. Las decisiones locales pueden entrar en conflicto unas con otras. Los *peers* interaccionan entre ellos y pueden entrar en la red y abandonarla en cualquier momento. El objetivo de la descentralización es la participación, la diversidad, resolver inferencias derivadas de la falta de recursos en la centralización de servicios y la resolución de conflictos por reducción de desigualdades.

Hay distintos modelos de plataformas descentralizadas:

- **Federadas:** varios nodos centrales que se comunican entre sí y les usuaries pueden elegir con cuál interaccionan.
- **Distribuidas:** redes donde no existe el clásico servidor y que se forman a través de ordenadores corrientes.

- **Blockchain:** nacido a partir de la primera moneda digital Bitcoin.

# Glosario

**AEPD** Agencia Española de Protección de Datos

**BSD** Berkeley Software Distribution

**CE** Constitución Española

**DDAA** derechos de autor

**DESI** Digital Economy and Society Index

**EAR** Export Administration Regulations

**EEUU** Estados Unidos

**EIPD** Evaluación de Impacto sobre la Proteccin de Datos

**FSF** Free Software Foundation

**GPL** General Public License

**IA** Inteligencia Artificial

**INE** Instituto Nacional de Estadística

**ISP** Internet Service Provider

**LOPD** Ley Orgánica de Protección de Datos

**LPI** Ley de Propiedad Intelectual

**PGD** Principios Generales del Derecho

**RGPD** Reglamento General de Potección de Datos

**TFUE** Tratado de funcionamiento de la Unión Europea

**TIC** Tecnologías de la información y la comunicación

**UE** Unión Europea

# Índice de figuras

# Índice de cuadros

# Licencia de uso del documento

# Licencia de uso del código fuente

Los archivos de código fuente para generar este documento se encuentran en `https://github.com/alk222/ELP` bajo la licencia GPL-3.0