

# Aspectos legales de la seguridad informática

Mikel Egaña Aranguren

[mikel-egana-aranguren.github.io](https://mikel-egana-aranguren.github.io)

[mikel.egana@ehu.eus](mailto:mikel.egana@ehu.eus)



# Aspectos legales de la seguridad informática

<https://doi.org/10.5281/zenodo.4302267>

<https://github.com/mikel-egana-aranguren/EHU-SGSSI-01>



# Delitos informáticos

Convenio sobre ciberdelincuencia de la Unión Europea (2001)

- Delitos relacionados con el contenido
- Delitos relacionados con las infracciones de derechos de autor
- Delitos relacionados con la informática
- Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos

# Delitos relacionados con el contenido

- Pornografía infantil
- Amenazas
- Calumnias
- Difusión de contenidos racistas y xenófobos (Por ejemplo en Alemania contenido nazi o negación del holocausto)

# Calumnia vs injuria

Calumnia: decir que alguien ha cometido un delito

Injuria: atentar contra la dignidad de alguien

# Delitos relacionados con las infracciones de derechos de autor

- Propiedad intelectual e industrial
- Distribución de copias ilegales de películas y canciones
- Reproducción de programas informáticos protegidos

# Delitos relacionados con la informática

Falsificación informática que produzca la alteración, borrado o supresión de datos informáticos que ocasionen datos no auténticos: fraudes, estafas, tráfico de contraseñas, etc.

# Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos

- Acceso ilícito a sistemas informáticos (Delitos contra la intimidad, revelación de secretos de empresa, uso no autorizado de equipos informáticos)
- Interceptación ilícita de datos
- Interferencia de los datos que provoquen daños
- Distribución de virus



# Código penal Español

Ley orgánica 10/1995

- Delitos contra la intimidad y el secreto de las comunicaciones (art. 197.1)
- Estafas electrónicas (art. 248.2)
- Infracción de los derechos de propiedad intelectual (art. 270)
- Delitos de daños (art. 264.2)
- Utilización de ordenadores y de terminales de telecomunicaciones sin consentimiento de su titular (art. 256)

# Código penal Español

Ley orgánica 10/1995

- Descubrimiento y revelación de secretos contenidos en documentos o soportes informáticos (art. 278)
- Falsedad en documentos electrónicos (art. 390)
- Fabricación o tenencia de útiles para la comisión de delitos (art. 400)
- Distribución entre menores de edad de material pornográfico (art. 186)

# Código penal Español

Ley orgánica 10/1995

- Distribución de pornografía infantil (art. 189)
- Publicación de calumnias o injurias

# Protección de datos personales

Derecho a la intimidad y privacidad: derecho de poder excluir a terceros del conocimiento de su vida personal (Sentimientos, datos biográficos, imagen, ...)

# Protección de datos personales

Ley orgánica 15/1999, de 13 de diciembre: LOPD

Declaración de derechos humanos 1948: nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques

# Ley Organica Proteccion de Datos de Caracter Personal (LOPD)

Se aplica a organizaciones públicas, privadas y profesionales independientes que almacenen datos personales para tratamiento, uso o explotación posterior (Con exenciones como el censo electoral o los boletines oficiales)

# LOPD: Responsable de Fichero

- Documento de seguridad: actualizado a las leyes vigentes en materia de seguridad de los datos personales
- Adoptar las medidas necesarias para que el personal conozca las normas en materia de seguridad y consecuencias de su incumplimiento
- Implantar un mecanismo de identificación de usuarios
- Mantener una relación de los usuarios del sistema con los derechos de acceso a los datos y aplicaciones

# LOPD: Responsable de Fichero

- Establecer mecanismos para evitar que los usuarios accedan a recursos con derechos distintos de los autorizados
- Verificar los procedimientos de copia y de recuperación de datos
- Autorizar por escrito la ejecución de procedimientos de recuperación de datos



# LOPD: Responsable de Fichero

- Autorizar expresamente el tratamiento fuera de los locales de la organizaciones
- Autorizar la salida de soportes informáticos fuera de los locales de la organizaciones
- Adoptar las medidas correctoras de las deficiencias detectadas en las auditorías de seguridad

# LOPD: Principios

- **Habeas data** ([Habeas corpus](#)): los datos pertenecen al usuario, no a la organización que los almacena
- Calidad de los datos: los datos tienen que ser pertinentes al fin para el que han sido recogidos, y solo conservados durante el tiempo necesario para ese fin
- Seguridad de los Datos
- Deber de secreto incluso después de haber finalizado la relación
- Información en la recopilación de los datos

# LOPD: Principios

- Consentimiento del afectado para el tratamiento
- Cesión de datos solo con el consentimiento
- Cesión a terceros países: solo a países con el mismo nivel de protección
- Datos especialmente protegidos: salud, ideología, vida sexual, origen racial, religión o creencias

# LOPD: Derechos

- Derecho de información en la recopilación de datos
- Derecho de consulta al Registro General de Protección de Datos
- Derecho de acceso a sus datos de caracter personal
- Derecho de rectificación y cancelación
- Derecho de oposición
- Derecho de una indemnización

# Agencia Vasca de Protección de Datos

<https://www.avpd.euskadi.eus/>

# Reglamento General de Protección de Datos (RGPD)

Reglamento Europeo para unificar los reglamentos de todos los países

25 Mayo 2016

# RGPD: nuevos principios

Principio de responsabilidad (accountability): implementar mecanismos que permitan acreditar que se han adoptando todas las medidas necesarias (responsabilidad proactiva)

Protección de datos por defecto y desde el diseño

Principio de transparencia

# RGPD: nuevas obligaciones para entidades

- Designar un Delegado de Protección de Datos (DPO)
- En algunos casos evaluaciones de impacto sobre la privacidad
- Las empresas multinacionales sólo tendrán como intercolutora a una sola autoridad de control (ventanilla única)
- Las brechas de seguridad deberán ser comunicadas a la autoridad de control en menos de 72h y a los usuarios en brechas graves
- Más datos sensibles: genéticos, biométricos, condenas penales



# RGPD: nuevas obligaciones para entidades

- Garantías adicionales para las transferencias internacionales de datos
- Sellos y acreditaciones para la responsabilidad proactiva
- Desaparece la obligación de inscribir los ficheros
- Sanciones más sustanciales, que pueden llegar a los 20 millones de euros o el 20% de la facturación de una empresa

# RGPD: nuevos derechos para ciudadanos

- Mayor transparencia y información
- Consentimiento inequívoco, libre y revocable, mediante acto afirmativo claro  
(No se admite consentimiento tácito)
- Derecho al olvido
- Derecho a la limitación temporal del tratamiento
- Portabilidad de los datos