



U8. Principios legales en la Inteligencia Artificial



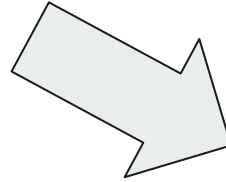
ÍNDICE

1. Contexto legal aplicable a proyectos de IA
2. Agencia Española de Protección de Datos
3. Comité Europeo de Protección de Datos
4. RGPD y LOPDGDD
 - a. Introducción
 - b. Definiciones
 - c. ¿Qué dice la ley?
5. Noticias relacionadas
6. Enlaces para profundizar
7. Caso práctico 1: Transferencias internacionales.
8. Lab 1: Anonimización de datos

1. Contexto legal aplicable a proyectos de IA

Los proyectos de IA están basados en datos

- Se necesitan datos para entrenar y validar modelos
- Se necesita almacenar y analizar esos datos



Los proyectos de IA se ven afectados por la legislación vigente en materia de protección de datos.



1. Contexto legal aplicable a proyectos de IA

1.1 Organismos

- **Ámbito europeo:** **Comité Europeo de Protección de datos** (CEPD), en inglés European Data Protection Board(EDPB). Tiene como objetivo garantizar la aplicación coherente del Reglamento General de Protección de Datos(RGPD) y la Directiva europea sobre protección de datos en el ámbito policial. [Vídeo](#)
- **Ámbito nacional:** **Agencia Española de Protección de Datos** (AEPD) vela por el cumplimiento de la legislación relativa a la protección de datos.



1. Contexto legal aplicable a proyectos de IA

1.2 Principales normas:

- **Ámbito europeo: Reglamento General de Protección de Datos (RGPD-2016)**
- **Ámbito nacional: Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)** que deroga la Ley Orgánica de Protección de Datos de carácter personal (LOPD)



3. Comité Europeo de Protección de Datos

- Es un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de la UE.
- El CEPD está compuesto por representantes de las autoridades nacionales de protección de datos y del Supervisor Europeo de Protección de Datos (SEPD).
 - De entre los representantes de las autoridades nacionales de PD se eligen un presidente y 2 vicepresidentes.
- El CEPD se creó mediante el Reglamento General de Protección de Datos (RGPD) y tiene su sede en Bruselas.
- Funciones:
 - Proporcionar **orientaciones** (incluidas directrices, recomendaciones y buenas prácticas) para clarificar la ley.
 - **Asesorar** a la Comisión Europea sobre cualquier aspecto relacionado con la protección de los datos personales y la nueva legislación que se proponga en la Unión Europea.
 - Adoptar **resultados coherentes** en casos transfronterizos de protección de datos.
 - Promover la **cooperación** y el intercambio efectivo de información y buenas prácticas entre las autoridades nacionales de supervisión.



2. Agencia Española de Protección de Datos.

- AEPD es la autoridad pública independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos. Tiene más de 25 años de vida
- Se relaciona con el Gobierno a través del Ministerio de Justicia
- Funciones:
 - Cooperación con diversos organismos internacionales y con los órganos de la Unión Europea (cepd) en materia de protección de datos.
 - Llevar a cabo investigaciones sobre la aplicación del presente Reglamento,
 - Asesorar en materia de protección de datos
 - Llevar a cabo investigaciones en forma de auditorías de protección de datos.
 - Sancionar a toda persona responsable o encargado del tratamiento con una advertencia, apercibimiento o multa cuando las operaciones de tratamiento previstas puedan infringir o hayan infringido lo dispuesto en la normativa de protección de datos.
 - [Acceso a su Web](#)



2. Agencia Española de Protección de Datos.

- Funciones (cont)
 - **Ayuda a la ciudadanía:**
 - protege tus derechos de acceso, rectificación, limitación, oposición, supresión (“derecho al olvido”), portabilidad y oposición al tratamiento de decisiones automatizadas.
 - antes de reclamar ante la AEPD debes exigir tu derecho ante la entidad responsable y solo si no te responde o no consideras adecuada la respuesta interponer una reclamación frente a AEPD
 - **Ayuda al responsable :**
 - si vas a tratar datos de carácter personal la AEPD pone a disposición la herramienta RGPD para ayudar en la adecuación al Reglamento General de Protección de Datos (RGPD)
 - orienta cómo proceder si vas a realizar una transferencia internacional de datos a un país que ofrece un nivel adecuado de protección
 - **Ayuda específica a menores**
 - Puede ser utilizada por menores, madres, padres y personal docente.
 - Trata cuestiones relativa al tratamiento de datos personales de menores



4. RGPD(2016) y LOPDGDD(2018)

La RGPD

- Unifica todas las normativas europeas relativas a protección de datos
- De aplicación directa en 2018
- A quién afecta:
 1. Deben cumplirla todas las empresas independientemente de su país de origen o de actividad, deberán cumplirla si recogen, guardan, tratan, usan o gestionan algún tipo de dato de los ciudadanos de la Unión Europea.
 2. Protege a todos los ciudadanos de UE



4. RGPD(2016) y LOPDGDD(2018)

No se aplica:

1. al tratamiento de datos personales efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.
2. al tratamiento por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.



4. RGPD(2016) y LOPDGDD(2018)

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



4. RGPD(2016) y LOPDGDD(2018)

- Ámbito(Artículo 2):
 - El presente Reglamento se aplica **al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado** de datos personales contenidos o destinados a ser incluidos en **un fichero**.



4. RGPD(2016) y LOPDGDD(2018)

- Definiciones
 - **Datos personales:** toda información sobre una persona física identificada o identificable (el interesado).
 - datos personales: nombre, teléfono, la dirección de correo electrónico, dirección IP, información financiera...
 - datos personales sensibles: origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos relativos a la vida sexual o la orientación sexual, antecedentes penales, datos genéticos, biométricos (imagen del rostro, huellas dactilares), datos relativos a la salud física o mental,



4. RGPD(2016) y LOPDGDD(2018)

- Definiciones
 - **Tratamiento:** operación o cjto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no. Ej: recogida, registro, organización, conservación, modificación, consulta, transmisión, cotejo, difusión, destrucción..
 - **Elaboración de perfiles:** tratamiento automatizado de datos para evaluar determinados aspectos: rendimiento profesional, situación económica, salud, preferencias personales, intereses, comportamiento, ubicación...



4. RGPD(2016) y LOPDGDD(2018)

- Definiciones
 - **Seudonimización:** el 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
 - **Fichero:** todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;



4. RGPD(2016) y LOPDGDD(2018)

- Definiciones

- **Responsable del tratamiento:**» la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento
- **Encargado del tratamiento:** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento
- **Destinatario:** la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.

4. RGPD(2016) y LOPDGDD(2018)

Perfil y funciones de un DPD-DPO profesional

- ✓ Amplios conocimientos en derecho, concretamente en todo lo referente a protección de datos.
- ✓ Conocimientos en informática. Seguridad en la Red, sistemas operativos, aplicaciones, Esquema Nacional de Seguridad - ENS (para Organismos Públicos)



- Delegado de protección de datos

El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

- el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
- las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
- las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales
CE Inteligencia Artificial y Big Data/ Modelos de Inteligencia Artificial

4. RGPD(2016) y LOPDGDD(2018)



- Delegado de protección de datos (cont)

La LOPDGDD detalla más los casos donde es obligado el nombramiento de un delegado de protección de datos(art 34). Algunos de ellos son

- Los centros docentes y universidades públicas y privadas
- Las entidades que exploten redes y presten servicios de comunicaciones electrónicas cuando traten dat. per. a gran escala
- Los establecimientos financieros de crédito.
- Las entidades aseguradoras y reaseguradoras.
- Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
- Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
- Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
- Las empresas de seguridad privada.
- Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.
- Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.
- Las federaciones deportivas cuando traten datos de menores de edad



4. RGPD(2016) y LOPDGDD(2018)

- Definiciones
 - **Tercero:** persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;
 - **Consentimiento del interesado:** toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;



4. RGPD(2016) y LOPDGDD(2018)

- Definiciones
 - **Representante:** persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones
 - **Empresa:** persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;



4. RGPD(2016) y LOPDGDD(2018)

- Definiciones
 - **Violación de la seguridad de los datos personales:** toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
 - **Autoridad de control:** la autoridad pública independiente establecida por un Estado miembro que supervisa la aplicación del RGPD



4. RGPD(2016) y LOPDGDD(2018)

- Definiciones
 - **Tratamiento transfronterizo:**
 - el tratamiento realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o
 - el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

4. RGPD(2016) y LOPDGDD(2018)



- Definiciones
 - **Transferencias internacionales:**
 - Las transferencias internacionales de datos suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega)
 - Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica

4. RGPD(2016) y LOPDGDD(2018)

- Definiciones
 - **Transferencias internacionales:**
 - Países que han sido declarados de nivel de protección adecuado por la Comisión Europea: Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Japón, Reino Unido, República de Corea, US (leer [Nota informativa del Comité Europeo de Protección de Datos sobre transferencias internacionales a los Estados Unidos de América tras la adopción de la Decisión de adecuación del 10 de julio de 2023, lista de organizaciones: https://www.dataprivacyframework.gov/](#))



4. RGPD(2016) y LOPDGDD(2018)

- Definiciones
 - **Objeción pertinente y motivada:** la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;



4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?

- **Todo tratamiento de datos personales debe ser lícito y leal.**
 - **el consentimiento debe ser inequívoco, claro y distinguible de otros asuntos.**
 - **Identificación del responsable del tratamiento de los datos y de los derechos sobre la cesión**
 - **el destinatario está obligado a informar sobre cada finalidad del tratamiento de los datos**



4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?

- **Derechos del interesado.**
 - **Acceso**
 - **Oposición**
 - **Rectificación**
 - **Limitación del tratamiento**
 - **Supresión(olvido)**



4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?

- **Sobre el responsable del tratamiento**

- aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD
- garantizará que solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Delimitará la cantidad de datos personales recogidos, la extensión de su tratamiento, su plazo de conservación y a su accesibilidad



4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?

- **Sobre encargado del tratamiento**
 - tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable
 - garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;



4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?

- **Registro de las actividades**
 - Los responsables llevarán un registro de actividades de tratamiento, que contendrá entre otras informaciones:
 - fines del tratamiento, categorías de datos personales, destinatarios, plazos previstos para la supresión, medidas de seguridad



4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?

- **Registro de las actividades**

- Los encargados de tratamiento llevarán un registro de actividades de tratamiento, que contendrá entre otras informaciones:
 - categorías de tratamientos efectuados por cuenta de cada responsable
 - transferencias realizadas
 - descripción de medidas técnicas y organizativas de seguridad



4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?

- **Registro de las actividades**
 - **Estos registros constaran por escrito, incluso en formato electrónico.**
 - **Se pondrán a disposición de la autoridad de control que lo solicite**
 - **No serán necesarios cuando una empresa u organización emplee a menos de 250 personas.**



4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?

- **Seguridad del tratamiento**
 - Responsables y encargados aplicarán las medidas necesarias para garantizar un nivel de seguridad adecuado al riesgo:
 - seudonimización y cifrado de datos personales,
 - garantía de confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
 - capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
 - verificación, evaluación y valoración regulares de la eficacia de las medidas para garantizar la seguridad del tratamiento.



4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?

Notificación de una violación de seguridad a la autoridad de control

- el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas física



4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?

Notificación de una violación de seguridad al interesado

- Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.
- no será necesaria
 - la información estuviera cifrada
 - se hayan tomado medidas ulteriores que garanticen que ya no exista alto riesgo para los derechos y libertades del interesado



4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?

Decisiones Automatizadas y Derecho a Explicación

- Todo interesado tendrá **derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado**, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.



4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?


Decisiones Automatizadas y Derecho a Explicación

- el responsable del tratamiento informará al interesado de la existencia de decisiones automatizadas, **información significativa sobre la lógica aplicada**, e importancia y las consecuencias previstas de dicho tratamiento para el interesado

4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?

Decisiones Automatizadas y Derecho a Explicación

- Explicabilidad
 - Las decisiones automáticas basadas en ML o DL no son transparentes, no sabemos como se ha llegado a ellas
 - Esto es un grave problema en algunos casos, donde queremos supervisar la decisión automática:
 - decisiones médicas, jurídicas, de crédito se debe entender la decisión antes de llevarla a cabo



4. RGPD(2016) y LOPDGDD(2018)

¿Qué dice la ley?

Cómo resolver el problema de la explicabilidad

- Los sistemas de IA deberían ser capaces de **explicar de una forma coherente cómo llegan a conclusiones.**
- La XAI (IA explicable) es un **campo en investigación y exploración** donde puede haber muchas ideas, muchos pilotos y muchas técnicas y probablemente vayan inicialmente creciendo y diversificando en técnicas y algoritmos para luego ir consolidando en lo que obtienen mejores resultados.

5. Noticias relacionadas

La AEPD sanciona a Whatsapp y Facebook por ceder y tratar, respectivamente, datos personales sin consentimiento

La resolución de la Agencia concluye que la comunicación de datos realizada por Whatsapp a Facebook no se ajusta a lo exigido por la normativa española y europea de protección de datos.

- Además, sanciona también a Facebook por tratar esos datos cedidos para sus propios fines sin haber obtenido un consentimiento válido por parte de los usuarios
- El marco normativo establece que el consentimiento debe ser “libre, específico e informado”, algo que no se cumple ni en la comunicación de datos realizada por Whatsapp ni en el tratamiento posterior que lleva a cabo Facebook
- La Agencia declara la existencia de dos infracciones graves de la Ley Orgánica de Protección de Datos, sancionando con 300.000 euros a Whatsapp y 300.000 a Facebook

(Madrid, 15 de marzo de 2018). La Agencia Española de Protección de Datos (AEPD) ha dictado [resolución](#) en el procedimiento sancionador iniciado a las empresas Whatsapp y Facebook. La Agencia ha declarado la existencia de **dos infracciones graves de la Ley Orgánica de Protección de Datos**, sancionadas cada una con 300.000 euros: una de ellas a Whatsapp por comunicar datos a Facebook sin haber obtenido un consentimiento válido de los usuarios y otra a Facebook por tratar esos datos para sus propios fines sin consentimiento.

La **Universidad de Valladolid** comunica que ha sido víctima de un **ataque y robo de datos personales** alojados en la página web del Servicio de Relaciones Internacionales, hecho del que se ha tenido constancia en la madrugada del 10 al 11 de enero de 2019.

Hackeo a Twitter verano 2020



Caso práctico con intervención de un país no comunitario



Una empresa española para optimizar costos quiere que parte de la atención al cliente no presencial se realice desde Bogotá.

La empresa tiene centros en Bogotá y Madrid, con relación a la RGPD qué implicaciones tendría ubicar los datos en

- Madrid
- Bogotá

6. Enlaces interesantes para consultar

Visitando www.aepd.es

- Guías de la agencia española de protección de datos:
 - [10 malentendidos relacionados con la anonimización](#)
 - [Requisitos para Auditorías de Tratamientos que incluyan IA](#)
 - [Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial](#)
 - [Introducción al Hash como técnica de seudonimización de datos personales](#)
 - [Código de buenas prácticas en protección de datos para proyectos Big Data.](#)
 - [Orientaciones y garantías en los procedimientos de anonimización de datos personales](#)
 - <https://www.aepd.es/documento/guia-basica-anonimizacion.pdf>

Artículo a modo de conclusión:

<https://protecciondatos-lopd.com/empresas/inteligencia-artificial-rgpd/>

Multas impuestas por la AEPD

https://cincodias.elpais.com/cincodias/2023/01/13/legal/1673615065_683359.html