



1

Régimen jurídico superposición

Ya hay mucha regulación:

- Privacidad-datos
- Datos, RISP
- Propiedad intelectual
- Ciberseguridad (ENS...)
- Responsabilidad
- Plataformas (DSA, DMA...)
- NORMALIZACIÓN Y ESTÁNDARES...

2

...privacidad y protección de datos



Lorenzo Cotino

3



**Adecuación al RGPD de
tratamientos que
incorporan Inteligencia
Artificial.
Una introducción**

Lorenzo Cotino

4

III. CUMPLIMIENTO	20
A. Legitimación y limitación del tratamiento	20
Interés legítimo	22
Categorías especiales	22
Tratamientos con fines compatibles	23
B. Información	23
Información significativa sobre la lógica aplicada	24
C. Generalidades sobre los ejercicios de derechos	24
D. Derecho de Acceso	25
E. Derechos de Supresión	25
Limitaciones a la supresión.	26
F. Bloqueo de los datos	26
G. Derecho de Rectificación	27
H. Portabilidad	27
I. Toma de decisiones basadas únicamente en un tratamiento automatizado	28
IV. GESTIÓN DEL RIESGO PARA LOS DERECHOS Y LIBERTADES	30
A. Evaluación del Nivel de Riesgo	30
B. La Evaluación de Impacto de la Privacidad - EIPD	31
C. Transparencia	33
Durante la etapa de entrenamiento	33

Lorenzo Cotino

5

Certificación	34
Decisiones automatizadas y elaboración de perfiles	34
Personal del responsable	34
El Delegado de Protección de Datos como herramienta de transparencia	35
D. Exactitud	35
Factores que influyen en la exactitud	36
Información biométrica	37
Combinación de perfilados	37
Verificación vs. Validación	38
Garantía de exactitud como un proceso continuo	38
E. Minimización	38
Datos de entrenamiento	39
Técnicas de minimización	39
Extensión de las categorías de datos en la solución IA	40
Extensión del conjunto de entrenamiento	41
Datos personales en la solución IA	41
F. Seguridad	42
Amenazas específicas en componentes IA	42
Logs o registros de actividad	43
G. Evaluación de la proporcionalidad y necesidad de dichos tratamiento	44
H. Auditoria	45
V. TRANSFERENCIAS INTERNACIONALES	48

Lorenzo Cotino

6



Requisitos para Auditorías de Tratamientos que incluyan IA



v. enero 2021

Lorenzo Cotino

7

ÍNDICE

I. INTRODUCCIÓN	7
II. METODOLOGÍA DE AUDITORÍA Y TRATAMIENTOS QUE INCORPORAN COMPONENTES DE IA	11
A. Objetivos generales de la auditoría de un componente IA en PD	11
B. Características singulares de la metodología de la auditoría de un componente IA en PD	12
III. OBJETIVOS DE CONTROL Y CONTROLES	14
A. Identificación y transparencia del componente	14
Objetivo: Inventario del componente IA auditado	14
Objetivo: Identificación de responsabilidades	14
Objetivo: Transparencia	15
B. Propósito del componente IA	16
Objetivo: Identificación de las finalidades y usos previstos	16
Objetivo: Identificación del contexto de uso del componente IA	16
Objetivo: Análisis de la proporcionalidad y necesidad	17
Objetivo: Determinación de los destinatarios de los datos	18
Objetivo: Limitación de la conservación de datos	18
Objetivo: Análisis de las categorías de interesados	19

Lorenzo Cotino

8

C. Fundamentos del componente IA	20
Objetivo: Identificación de la política de desarrollo del componente IA	20
Objetivo: Implicación del DPD	20
Objetivo: Adecuación de los modelos teóricos base	21
Objetivo: Adecuación del marco metodológico	21
Objetivo: Identificación de la arquitectura básica del componente	21
D. Gestión de los datos	23
Objetivo: Aseguramiento de la calidad de los datos	23
Objetivo: Determinación del origen de las fuentes de datos	23
Objetivo: Preparación de los datos personales	24
Objetivo: Control del sesgo	25
E. Verificación y validación	26
Objetivo: Adecuación del proceso de verificación y validación del componente IA	26
Objetivo: Verificación y Validación del componente IA	26
Objetivo: Rendimiento	27
Objetivo: Coherencia	28
Objetivo: Estabilidad y robustez	29
Objetivo: Trazabilidad	30
Objetivo: Seguridad	31

Lorenzo Cotino

9

¿Cuándo se aplica RGPD a IA?

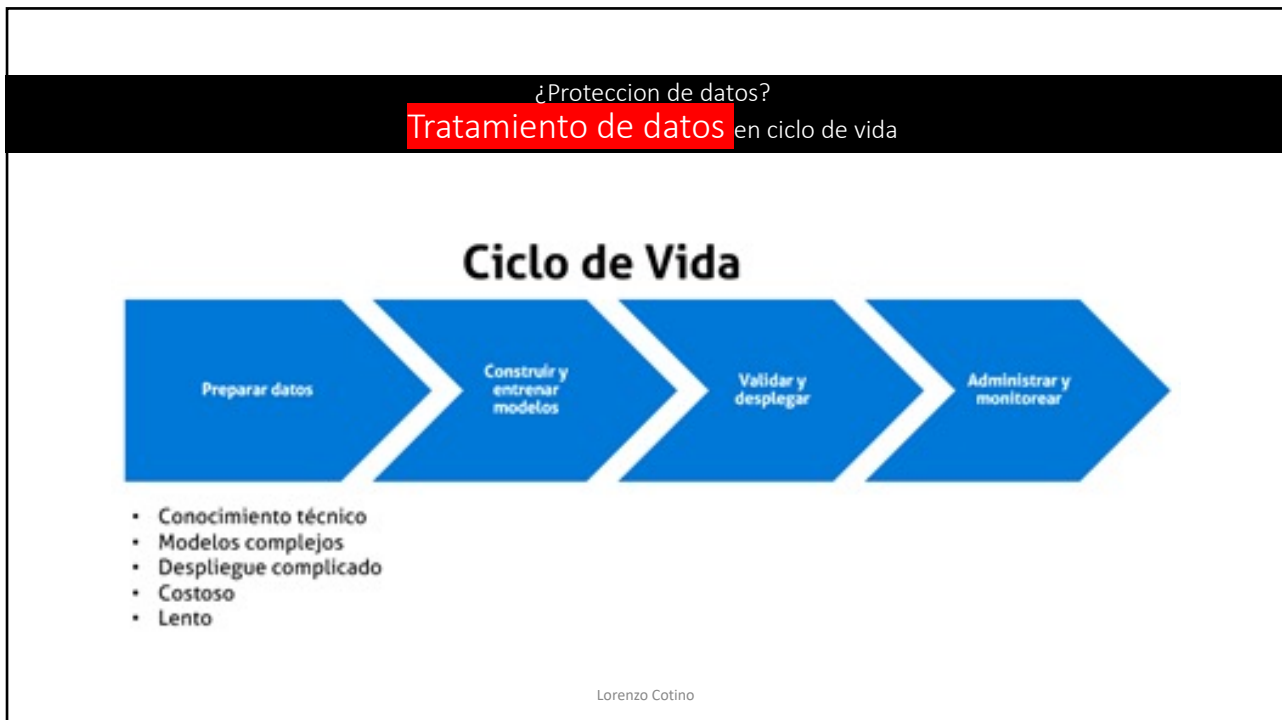
¿Protección de datos?

Tratamiento de datos **personales**



Lorenzo Cotino

10



11

datos en un sistema IA

- **datos de entrenamiento** los datos utilizados para entrenar un sistema de IA mediante el ajuste de sus parámetros entrenables.
- los **datos de validación** los datos usados para proporcionar una evaluación del sistema de IA entrenado y adaptar sus parámetros no entrenables y su proceso de aprendizaje para, entre otras cosas, evitar el ajuste insuficiente o el sobreajuste.
- los **datos de prueba** los datos usados para proporcionar una evaluación independiente del sistema de IA, con el fin de confirmar el funcionamiento previsto de dicho sistema antes de su introducción en el mercado o su puesta en servicio;
- **datos de entrada** proporcionados al SIA o adquiridos por este, a partir de los cuales el SIA produce la información de salida
- **-DATOS DE SALIDA O INFERIDOS...**

12

Cadena de valor de la IA y tratamiento de datos



- . Modelos de acceso y uso de datos por parte de fabricantes y proveedores.
- . Continuidad del aprendizaje de sistemas IA con datos de usuarios y políticas de acceso de fabricantes.

13

modelos de cadena de valor , a efectos de protección de datos



- desarrollo o implementación de un **SIA interno**, coincidiendo proveedor y usuario
- una entidad escribe el código y entrena el sistema, y lo comercializa a través de un acceso restringido al SIA, de modo que **el usuario no puede hacer cambios, solo enviar datos de entrada y recibir resultados**;
- una entidad vende **modelos pre-entrenados** y la entidad que adquiere el modelo incorpora datos de entrenamiento;
- proveedor vende un **SIA actualizable** cuando los responsables del despliegue introducen nuevos datos;
- un desarrollador de un SIA lo vende a otro desarrollador SIA, para continuar entrenando, para mejorarlo, o para adaptarlo tareas más específicas – trabajan por tanto diferentes conjuntos de datos-;
- una entidad integra diferentes SIAs (p.e. el SIA decide a qué SIA se derivan los datos de entradas)

14

• **Aplicación en bloque de la normativa de datos si hay tratamiento de datos por IA**



- por regla general el uso de IA respecto de personas supone un tratamiento de datos y, por tanto, sometido a la normativa general
- PRINCIPIOS (proactiva, por defecto, idoneidad, minimización, finalidad, información CÓMO?)
- LEGITIMACIÓN (consentimiento, ley, interés legítimo...)
- DATOS ESPECIALMENTE PROTEGIDOS- , Nuevas perspectivas: proxies, datos afines, tratamientos sensibles con datos ordinarios.
- a mayor impacto de los tratamientos, mayores han de ser sus garantías compensatorias; *casi por defecto* será exigible un estudio de impacto

Lorenzo Cotino

15



• **Principios:**

- Licitud del tratamiento
- Lealtad y transparencia
- Limitación de la finalidad
- Minimización de datos
- Exactitud
- proactividad

Lorenzo Cotino

16

Evaluación del riesgo y Nuevo modelo de cumplimiento normativo, **responsabilidad proactiva** y demostrada, impacto social, diseño, defecto, DPOs...

Más vale prevenir que curar...



Lorenzo Cotino

17

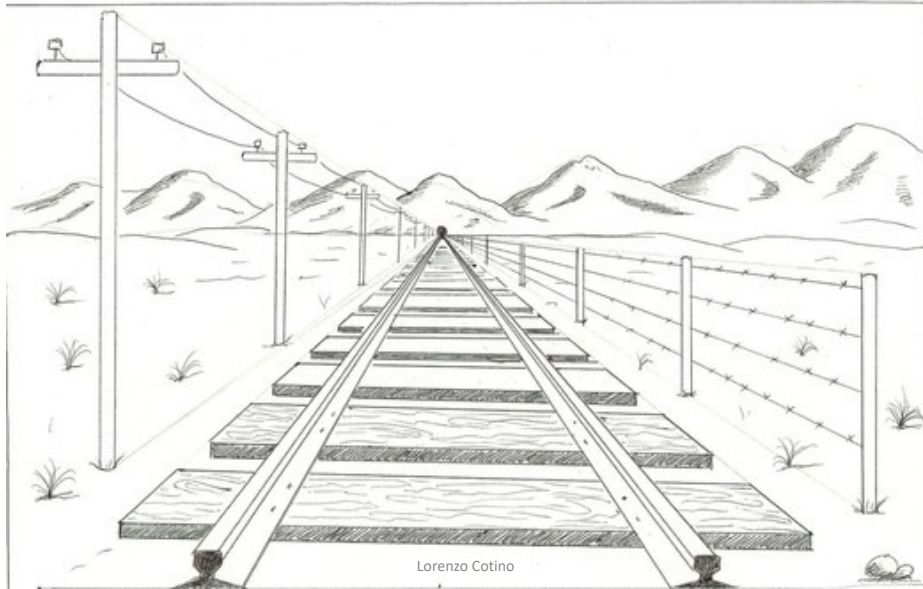
Legitimación del tratamiento



Lorenzo Cotino

18

la capa de IA es tratamiento o finalidad nueva (incompatible?)



19



20

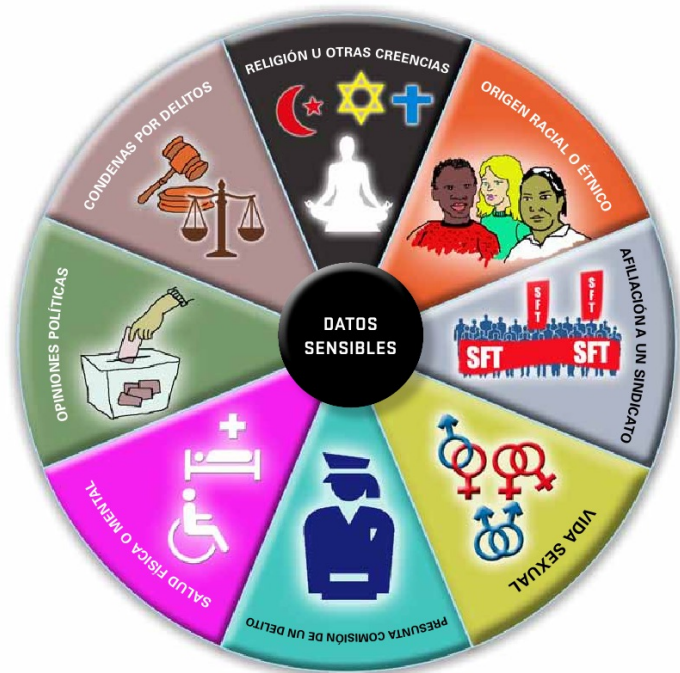


21



22

Datos y
tratamientos
sensibles



Lorenzo Cotino

23

• ESPECÍFICO art. 22 RGPD “sólo automatizadas” y error generalizado

- decisiones automatizadas del artículo 22 RGPD, así como y los deberes de transparencia e información, (art. 13. 2º f y 14. 2º g).



Lorenzo Cotino

24

• QUÉ TRANSPARENCIA (art. 22 –AEPD)



AEPD: un ejemplo de información que podría tener relevancia de cara al interesado, sería:

- El detalle de los datos empleados para la toma de decisión, más allá de la categoría, y en particular información sobre los plazos de uso de los datos (su antigüedad).
- La importancia relativa que cada uno de ellos tiene en la toma de decisión.
- La calidad de los datos de entrenamiento y el tipo de patrones utilizados.
- Los perfilados realizados y sus implicaciones.
- Valores de precisión o error según la métrica adecuada para medir la bondad de la inferencia.
- La existencia o no de supervisión humana cualificada.
- La referencia a auditorías, especialmente sobre las posibles desviaciones de los resultados de las inferencias, así como la certificación o certificaciones realizadas sobre el sistema de IA. En el caso de sistemas adaptativos o evolutivos, la última auditoría realizada.
- En el caso de que el sistema IA contenga información de terceros identificables, la prohibición de tratar esa información sin legitimación y de las consecuencias de realizarlo.

25

Privacidad de rebaño, datos "en su conjunto" y datos inferidos



26

Lorenzo Cotino

Catedrático de Derecho Constitucional

INICIOCURRÍCULUMPUBLICACIONESACTUACIONESBLOG-ACTUALIDADCONTACTO

VNIVERSITAT DE VALÈNCIA

LORENZO COTINO

Catedrático de Derecho Constitucional de la Universitat de València

SOBRE MÍ

Bienvenido a www.cotino.es

Política de Cookies

Lorenzo Cotino Hueso, U. Valencia

www.Odiseia.org
www.derechotics.com