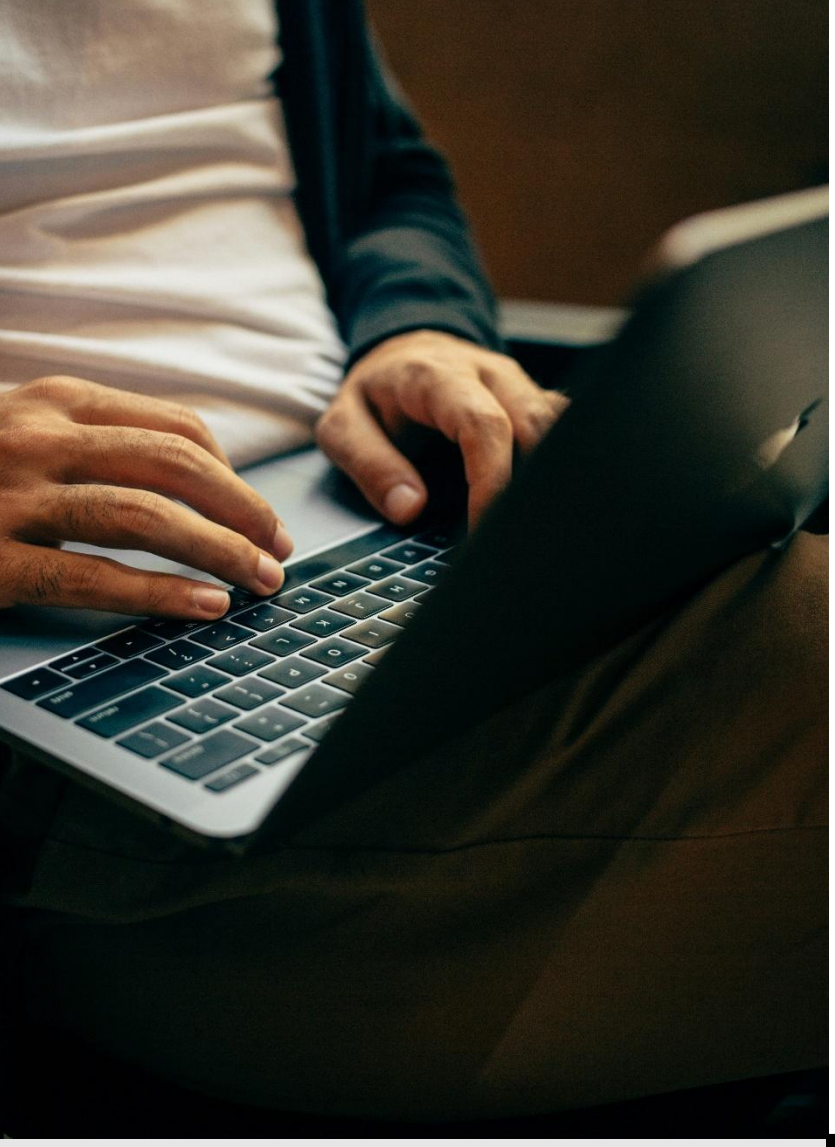

ECIJA

NOTA INFORMATIVA

Dictamen del CEPD, sobre el tratamiento de datos personales en el desarrollo y uso de modelos de IA

El Dictamen 28/2024 del CEPD aborda cuestiones clave relacionadas con el tratamiento de datos personales en el desarrollo y uso de modelos de IA, proporcionando directrices relevantes para la aplicación del RGPD.

Lo que debes saber

- Aunque el modelo no esté diseñado para proporcionar datos personales, la información del conjunto de datos de entrenamiento puede ser extraíble o inferible, por lo que deberán aplicarse medidas para evitar la identificación de los interesados y realizar pruebas regulares para evaluar la resistencia del modelo frente a posibles ataques.

- Es fundamental realizar una evaluación exhaustiva de la licitud del tratamiento de datos personales en todas las fases del desarrollo e implementación de modelos de IA.

- El interés legítimo puede ser una base de legitimación adecuada para el tratamiento de datos en los modelos de IA, si bien deberá evaluarse caso por caso, realizando y documentado el ejercicio de ponderación de los intereses perseguidos y los derechos de los interesados.

- Si la fase de desarrollo carece de una base legal adecuada para el tratamiento de los datos, ello podría invalidar el tratamiento posterior en la fase de implementación del modelo. En estos casos, si se detecta una vulneración de los derechos de los interesados, las autoridades de control pueden llevar a cabo acciones correctivas, tales como imponer una sanción, una limitación del uso de manera temporal, o incluso requerir el borrado de parte o del total de la base de datos utilizada durante la fase de desarrollo del modelo de IA.

I. Contexto y objetivos

El Dictamen del EDPB atiende a las consultas trasladadas por la Autoridad de Control Irlandesa acerca del tratamiento de datos en el desarrollo e implementación de modelos de Inteligencia Artificial (IA) y aborda tres aspectos principales: (i) la anonimización de los modelos de IA, (ii) el uso del interés legítimo como base legal para el tratamiento de los datos personales utilizados, y (iii) las consecuencias legales de un tratamiento de datos personales ilícito en fases previas al desarrollo del modelo de IA.

Siendo consciente de la importancia que tienen las cuestiones planteadas por la Comisión de Protección de Datos de Irlanda ("DPC" por sus siglas en inglés) en el marco de la protección de datos personales, el organismo europeo adoptó el pasado 17 de diciembre el **Dictamen 28/2024** sobre determinados aspectos de la protección de datos relacionados con el tratamiento de datos personales en el contexto de modelos de IA.

El texto incluye una serie de consideraciones generales destinadas, no solo a promover una aplicación uniforme de la normativa, **sino también a recordar a responsables y encargados del tratamiento la obligación de cumplir con los principios del Reglamento General de Protección de Datos (RGPD), en especial el de responsabilidad proactiva**.

II. Consideraciones sobre la anonimización de modelos de IA

Con respecto a la primera de las preguntas planteadas por la DPC relativa a las circunstancias en las que un modelo de IA entrenado con datos personales puede considerarse anónimo, el CEPD subraya que **debe realizarse una valoración caso por caso**, dado que no todos los modelos que utilizan datos personales pueden ser clasificados automáticamente como anónimos.

Para determinar si un modelo de IA cumple con los **estándares de anonimización**, el CEPD establece dos criterios fundamentales:

- La probabilidad de que datos personales relacionados con los individuos del conjunto de datos de entrenamiento puedan ser extraídos de forma directa o indirecta debe ser insignificante.

- La información generada a través de interacciones o consultas al modelo no debe permitir la identificación de personas específicas.

Los responsables del tratamiento deben adoptar **medidas técnicas y organizativas** destinadas a garantizar la **anonimización** efectiva de los modelos. Entre estas medidas se incluyen el **cifrado**, el uso de técnicas de privacidad diferencial y la aplicación del **principio de minimización de datos**. Adicionalmente, se hace hincapié en la necesidad de realizar pruebas regulares para evaluar la resistencia del modelo frente a los posibles ataques, como los ataques de inferencia de membresía o inversión de modelos, los cuales podrían comprometer la privacidad de los datos tratados.

En este contexto, se advierte sobre riesgos específicos como el fenómeno de **regurgitación**, donde el modelo reproduce fragmentos del conjunto de datos de entrenamiento en sus salidas. Aunque este riesgo es más común en modelos generativos, su presencia subraya la necesidad de controles rigurosos en el diseño y funcionamiento del modelo.

Finalmente, el CEPD recuerda que los responsables deben **documentar adecuadamente** las medidas adoptadas para garantizar la anonimización, incluidas auditorías internas, análisis de riesgos y resultados de las pruebas realizadas. La ausencia de medidas suficientes, o la incapacidad de demostrar que se han llevado a cabo, podría implicar el incumplimiento del principio de responsabilidad proactiva y otras disposiciones del RGPD.

III. Uso del interés legítimo como base legal

En relación con la segunda cuestión planteada por la DPC, el CEPD destaca que, aunque el interés legítimo puede ser una base jurídica válida, su aplicación requiere una **evaluación rigurosa y documentada** conforme a la normativa europea en materia de protección de datos.

Para valorar la adecuación del interés legítimo el CEPD, basándose en las Directrices 1/2024, se remite al ejercicio de ponderación compuesto por tres etapas:

1. **Identificación del interés legítimo**. El interés debe cumplir tres requisitos acumulativos: ser **lícito, estar claramente definido y ser real y actual (no especulativo)**. El EDPB expone ejemplos de intereses legítimos en este contexto, entre los que se incluiría el desarrollo de un modelo de IA para mejorar la detección de amenazas en sistemas de información o el uso de un agente conversacional que facilite la interacción con usuarios.
2. **Evaluación de la necesidad del tratamiento**: este análisis exige demostrar que el tratamiento de datos es necesario para alcanzar el interés legítimo identificado. Además, debe considerarse si existen alternativas menos intrusivas para lograr el mismo objetivo, atendiendo al principio de minimización de datos.
3. **Equilibrio entre los intereses del responsable y los intereses, derechos fundamentales y libertades de los interesados**: esta evaluación debe tener en cuenta el tipo de datos tratados, la naturaleza de la relación entre el interesado y el responsable, las consecuencias que pueda tener para los interesados el tratamiento así como las expectativas de los usuarios sobre el tratamiento de sus datos.

El Dictamen también menciona la importancia de implementar **medidas de mitigación** para limitar el impacto del tratamiento en los derechos y libertades de los interesados. Estas medidas, que deben adaptarse al contexto y características del modelo de IA, no deben confundirse con las medidas que el responsable del tratamiento está obligado a adoptar para garantizar el cumplimiento del RGPD, sino que actúan como **garantías adicionales**.

IV. Consecuencias del tratamiento ilícito de datos personales durante la fase de desarrollo y la posterior fase de implementación del modelo de IA

En respuesta a la tercera cuestión, el CEPD destaca que, cuando se constata una infracción, las autoridades de control, atendiendo al principio de proporcionalidad, **pueden imponer medidas correctivas**, como ordenar a los responsables del tratamiento que adopten medidas para subsanar la ilicitud del tratamiento inicial. Estas medidas pueden incluir, por ejemplo, la imposición de una multa, una limitación del uso de manera temporal, o incluso borrar parte o el total de la base de datos utilizada durante la fase de desarrollo del modelo de IA.

El tratamiento ilícito de datos personales durante la fase de desarrollo de un modelo de IA puede afectar, no solo la validez del modelo en sí, sino también su posterior uso y despliegue. El CEPD identifica **tres posibles escenarios** que ejemplifican las consecuencias de un tratamiento ilícito en la fase de desarrollo:

- **Escenario 1: Retención de datos personales en el modelo de IA y tratamiento posterior por el mismo responsable**

El CEPD señala que las autoridades de control deben evaluar si las finalidades de las fases de desarrollo e implementación son distintas y, por tanto, constituyen actividades de tratamiento separadas. Si la fase de desarrollo carece de una base legal adecuada, ello podría invalidar el tratamiento posterior, dependiendo de las circunstancias del caso concreto.

- **Escenario 2: Retención de datos personales en el modelo de IA y tratamiento posterior por un tercero**

Cuando un modelo desarrollado con datos personales tratados de manera ilícita se pone a disposición de un tercero para su implementación, el responsable del tratamiento en la fase de implementación debe realizar una evaluación adecuada, de conformidad con el principio de responsabilidad proactiva, para cerciorarse de que el modelo de IA no se desarrolló mediante el tratamiento ilícito de datos personales. Esto incluye verificar si el modelo fue desarrollado respetando la normativa y adoptar medidas correctivas cuando existan indicios de irregularidades.

- **Escenario 3: Anonimización del modelo tras un tratamiento ilícito en la fase de desarrollo**

Si, después de un tratamiento ilícito en la fase de desarrollo, el modelo es completamente anonimizado, el CEPD indica que las operaciones posteriores no estarían sujetas al RGPD siempre que no impliquen el tratamiento de datos personales. Sin embargo, si se tratan nuevos datos personales en la fase de implementación, estos tratamientos deben cumplir con el RGPD independientemente de la licitud del desarrollo inicial.

V. Observaciones finales

El CEPD recalca la importancia de adoptar un **enfoque proactivo y preventivo** en la protección de datos en el ámbito de la IA. Asimismo, pese a no ser objeto del presente

dictamen, se menciona la relevancia de las Evaluaciones de impacto sobre la protección de datos y los principios de privacidad desde el diseño y por defecto a la hora de evaluar los requisitos de protección de datos aplicables a los modelos de IA.

La documentación detallada de todas las medidas adoptadas no solo es un requisito legal bajo el principio de responsabilidad proactiva del RGPD, sino que también constituye una herramienta fundamental para demostrar el cumplimiento y garantizar la confianza de los usuarios en las tecnologías emergentes.

Área de Protección de Datos de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60