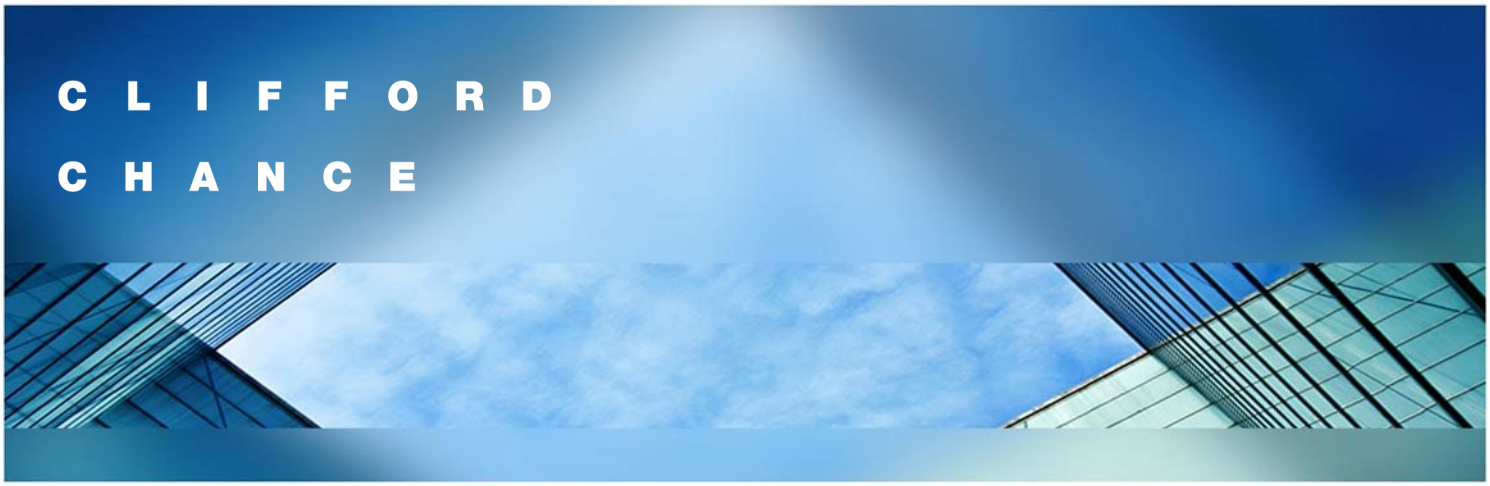

PROTECCIÓN DE DATOS E INTELIGENCIA ARTIFICIAL: LA NUEVA GUÍA DE LA AEPD

La Agencia Española de Protección de Datos ("**AEPD**") ha publicado una guía sobre la adecuación al Reglamento General de Protección de Datos ("**RGPD**") de aquellos tratamientos que incorporan inteligencia artificial, en la que la AEPD pretende señalar los aspectos más relevantes en la relación entre la inteligencia artificial y la protección de datos personales.

El pasado mes de febrero, la AEPD publicó la guía titulada "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción" (la "**Guía**"), que es accesible en su integridad en el siguiente enlace: Guía

La Guía está dirigida a responsables del tratamiento que incorporen componentes de inteligencia artificial ("**IA**") en sus tratamientos, así como a desarrolladores y encargados del tratamiento que les den soporte.

La Guía se centra en los tratamientos que incorporan componentes de la conocida como IA-débil (aquella relativa a soluciones capaces de resolver un problema concreto y acotado), dejando fuera a las soluciones de IA-fuerte e IA-generales (las que van más allá de las capacidades humanas – o superinteligencia – y las capaces de resolver cualquier tarea intelectual resoluble por un ser humano, respectivamente).

Como reconoce la AEPD, pese a su extensión, la Guía no pretende hacer un análisis exhaustivo de las relaciones entre la protección de datos y la IA.

A continuación se exponen algunos de los aspectos de la Guía que, a nuestro entender, son de mayor interés.

1. VISIÓN EXTENSIVA DE LOS TRATAMIENTOS EN UNA SOLUCIÓN IA

La Guía adopta una visión extensiva de los posibles tratamientos de datos personales en una solución IA, destacando que podrá haber tratamiento de datos personales en todas las etapas del ciclo de vida de la solución IA, comenzando por la fase de "entrenamiento" del sistema, pasando por las fases de "validación", "despliegue" y "explotación", y acabando por la fase de "retirada" del servicio (las "**Etapas**").

Si bien no todas las soluciones IA tratarán datos personales en alguna (o todas) de las Etapas de su ciclo de vida, será necesario – en línea con el principio de protección de datos desde el diseño y por defecto – realizar un análisis y determinar con carácter previo qué concretos tratamientos de datos personales se van a llevar a cabo.

Aspectos clave

- **La IA ha venido para quedarse**: además de la Guía, en el mes de enero de 2020 se celebró en Bruselas la Conferencia internacional sobre protección de datos e IA organizada por *Computers, Privacy & Data Protection*; y, hace tan solo unos días, la Comisión Europea publicó su Libro Blanco sobre IA, que contiene numerosas referencias a la protección de datos.
- Se **refuerzan los deberes de información** al deberse incluir en la primera "capa" "*información significativa sobre la lógica aplicada*" y "*la importancia y las consecuencias previstas*".
- **En ningún caso se aceptará la traslación de la responsabilidad del tratamiento de datos al propio sistema IA**.
- La Guía incluye un Anexo con una lista no exhaustiva de **servicios que actualmente se están prestando basándose en IA**: recomendación de productos basándose en el perfil del cliente y en el análisis de sus compras; asistentes y electrodomésticos inteligentes (IoT); monitorización de transacciones bancarias para detectar actividades fraudulentas basándose en los hábitos de consumo.

2. EL ROL DE CADA UNO DE LOS ACTORES INVOLUCRADOS EN LA SOLUCIÓN IA

La Guía identifica a título de ejemplo los diferentes roles (responsable/encargado) entre los actores intervinientes en cada una de las Etapas. Así, en la fase de entrenamiento, el rol de responsable corresponderá a la entidad que defina los fines del componente IA y decida qué datos personales se van a emplear para entrenar el sistema, mientras que la entidad contratada para ayudar en el entrenamiento será considerada generalmente encargada.

3. LAS BASES LEGITIMADORAS DEL TRATAMIENTO

Al igual que sucede con cualquier tratamiento, el primer paso consistirá en establecer una base jurídica legitimadora, que podrá variar en función de la Etapa de que se trate, siendo las más habituales (i) la ejecución de un contrato, (ii) el interés legítimo (en cuyo caso deberá llevarse a cabo el preceptivo ejercicio de ponderación previo, que según la Guía "*reclama del responsable un mayor grado de compromiso, formalidad y competencia*"), o (iii) el consentimiento de los interesados.

Deberá prestarse especial atención a las categorías especiales de datos, así como a las decisiones individuales automatizadas basadas únicamente en un tratamiento automatizado (sin intervención humana), como la elaboración de perfiles.

4. EL DEBER DE INFORMACIÓN REFORZADO

Respecto del deber de información, la Guía sigue el patrón en dos capas (artículo 11 de la LOPDyGDD), pero con mayores exigencias ya en la primera capa. Además, no será suficiente una referencia técnica a la implementación del algoritmo en cuestión, sino que deberá facilitarse información que permita entender el comportamiento del tratamiento mediante la inclusión, por ejemplo, de (i) el detalle de los datos empleados y su antigüedad; (ii) su importancia respectiva para la toma de la decisión: (iii) su calidad y el tipo de patrones utilizados: (iv) los perfilados realizados y sus implicaciones; (v) si existe o no supervisión humana cualificada; (vi) una referencia a auditorías realizadas al sistema IA; (vii) así como si el sistema IA contiene información de terceros identificables, la prohibición de tratar esa información sin legitimación y las consecuencias de realizarlo.

5. EL BLOQUEO DE DATOS: PARTICULARIDADES

La Guía señala que hay una obligación específica de bloqueo de los datos relativos al proceso de inferencia ("*al menos entradas y resultados obtenidos*") cuando se seleccione o desarrolle una solución IA.

6. LA TOMA DE DECISIONES BASADAS ÚNICAMENTE EN UN TRATAMIENTO AUTOMATIZADO

En las soluciones IA será frecuente que se puedan tomar decisiones que afecten a individuos y que estén basadas únicamente en un tratamiento automatizado, pero será preceptivo que concurra alguna de las excepciones previstas en el artículo 22.2 del RGPD (entre ellas, el consentimiento explícito del interesado).

En caso de optar por el consentimiento explícito, la Guía recomienda diseñar el tratamiento de tal forma que proteja la libertad de elección de los usuarios (y por tanto, pueda considerarse que se ha otorgado libremente).

La Guía recomienda encarecidamente que los tratamientos basados en IA siempre sean objeto de supervisión humana, dando la opción de que un operador humano pueda ignorar el algoritmo en un momento dado.

7. EL PERSONAL DEL RESPONSABLE DEL TRATAMIENTO

La Guía también prevé que los responsables tendrán la obligación de proporcionar a su personal "*información precisa y formación específica*" sobre las limitaciones del sistema de IA.

Será necesario evitar que el personal (elemento humano) se comporte como una "mera correa de transmisión" de las inferencias realizadas por la solución IA, así como prevenir errores de interpretabilidad por parte de los operadores. La información y formación son manifestación del principio de responsabilidad proactiva en el que se basa el RGPD.

8. SESGOS Y EXACTITUD

La exactitud de los datos es esencial cuando se utilizan soluciones IA, lo que exige del responsable asegurar que los datos tratados y, sobre todo, los generados y vinculados con el interesado, son exactos.

A fin de evitar estos riesgos, el responsable deberá implementar técnicas orientadas a examinar y determinar la posible existencia de sesgos en los algoritmos utilizados (*Algorithmic Impact Assessment*).

9. AMENAZAS ESPECÍFICAS DE SEGURIDAD

Al igual que sucede con cualquier tratamiento, responsable y encargado estarán obligados a adoptar las medidas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

No obstante, las medidas deberán ser las adecuadas para los sistemas IA, que tienen riesgos específicos y "*tipologías estudiadas de ataque y defensa*" (técnicas de envenenamiento de patrones adversos, inclusión de puertas traseras durante el proceso de desarrollo de la IA, ataques por "*adversarial machine learning*" etcétera).

10. AUDITORÍA

Por último, también en línea con el principio de responsabilidad proactiva, será necesario que responsables y encargados realicen una auditoría para determinar la adecuación de la solución IA a las exigencias del RGPD y comprobar la validez del tratamiento basado en estas soluciones.

En suma, la Guía supone una aproximación gradual a uno de los retos jurídicos más importantes de nuestros días: cómo hacer compatibles los beneficios asociados al uso de la IA con el respeto de los derechos fundamentales.

CONTACTOS

Josep Montefusco
Socio
T +34 93 344 22 25
E josep.montefusco@cliffordchance.com

Fernando Irurzun
Counsel
T +34 91 590 41 20
E fernando.irurzun@cliffordchance.com

Manel Santilari
Asociado
T +34 93 344 22 84
E manel.santilari@cliffordchance.com