LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS EMITIÓ LA GUÍA "REQUISITOS PARA AUDITORÍAS DE TRATAMIENTOS QUE INCLUYAN INTELIGENCIA ARTIFICIAL"

El 12 de enero de 2021, la Agencia Española de Protección de Datos (en adelante, "AEPD") publicó la guía sobre "Requisitos para Auditorías de Tratamientos que incluyan Inteligencia Artificial"[1] (en adelante, la "Guía"), con el propósito de ofrecer una lista de controles que se podrían incorporar a las auditorías de tratamientos de datos personales que hacen uso de componentes basados en inteligencia artificial (en adelante, "AI"), orientados desde la perspectiva de protección de datos personales.

La Guía está dirigida tanto a los encargados de auditar este tipo de tratamientos de datos personales, a los desarrolladores que quieran ofrecer garantías sobre sus productos y soluciones, a los Delegados de Protección de Datos encargados de supervisar estos tratamientos y de asesorar a los responsables; y, a los equipos de auditores cuando realicen la evaluación de este tipo de tratamiento de datos.

En base a ello, a continuación, se desarrolla la lista de los principales objetivos de control propuestos por la AEPD para tener en cuenta en este tipo de auditoría,:

1. Identificación y transparencia del componente de IA

De acuerdo con la Guía, en cumplimiento del principio de responsabilidad proactiva y principio de transparencia, en estas auditorías se debe cumplir con tres objetivos:

- Identificar el componente de IA parte del tratamiento auditado para que exista trazabilidad.
- Identificar los roles con relación al tratamiento auditado que incluye el componente de IA y las responsabilidades de las partes implicadas
- Verificar que el origen de los datos, las propiedades y la lógica del componente IA es accesible, comprensible y puede ser explicada.

2. Propósito del componente IA

La Guía resalta la importancia de cumplir con identificar los fines para los que son procesados los datos por y para el componente IA y sus usos previos, los cuales deben ser determinados, explícitos y legítimos sin ser utilizados de manera incompatible con esos fines. Todo esto en cumplimiento del principio de limitación de finalidad.

En este aspecto, en virtud de cumplir la obligación de analizar el contexto del tratamiento en el que se integra el componente IA, también se busca conocer las circunstancias en las que tiene lugar el tratamiento y otros factores que puedan condicionar las expectativas de las partes involucradas y puedan tener impacto en los derechos de los interesados.

Adicionalmente, se señala que se debe analizar la necesidad y proporcionalidad del empleo del componente IA respecto a la finalidad perseguida con el tratamiento de datos.

Otro objetivo a tener en cuenta en la auditoría es la identificación de los destinatarios o categorías de destinatarios de los datos personales procesados por el componente IA, en cumplimiento de los derechos de los

[1] Disponible en: https://cutt.ly/Kj28SA0

interesados, especialmente a la transparencia e información facilitada. En este aspecto se debe incluir también los destinatarios en otros países u organizaciones internacionales.

Se debe tomar atención a la limitación de la conservación de datos utilizados por el componente IA, los cuales solo deben mantenerse durante el tiempo necesario para los fines que se pretende alcanzar.

Por último, se debe identificar las categorías de interesados a los que afecta el tratamiento y evaluar si corresponde incluirlos, o a sus representantes, en el proceso de evaluación.

3. Fundamentos del Componente IA

Otro de los objetivos de control que debe guiar la evaluación de las auditorías de tratamientos de datos que incluyan componente de IA, se relaciona con los fundamentos del componente IA, referida a:

- **Identificar la política de desarrollo del componente IA**, la cual debe ser coherente con la política de protección de datos de la organización, estar alineada con el Reglamento General de Protección de Datos, Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales y demás normativa sectorial de aplicación española.
- Se debe prestar atención a que el responsable o encargado del tratamiento de datos personales cuente con un Delegado de Protección de Datos, como figura que cumpla con asesorar y participar activamente en la selección, diseño y/o desarrollo del componente IA en el que se apoya el tratamiento de los datos personales.
- **Adecuación de los modelos teóricos base y adecuación del marco metodológico,** para que el tratamiento pueda ser considerado leal, debe ser idóneo respecto a su propósito declarado, en lo relacionado a los modelos teóricos base y el marco metodológico que fundamenten el desarrollo y creación del componente IA.
- **Identificación de la arquitectura básica del componente**, debe estar documentado el desarrollo del componente IA de manera que permita comprender su implementación, contexto de funcionamiento y las interrelaciones que mantiene con otros elementos integrantes del tratamiento.

4. Gestión de los datos

Según lo propuesto en la Guía, otro objetivo de control que podría considerarse en las auditorías de tratamientos que incluyen componentes de IA, es el referido a la gestión de los datos personales.

Considerando ello, se propone realizar la evaluación tomando en cuenta los siguientes aspectos:

- **Aseguramiento de la calidad de datos:** los datos personales tratados deben ser exactos y actualizados en relación la finalidad de su tratamiento.
- **Determinación del origen de las fuentes de datos:** los datos deben ser tratados con licitud, lealtad y transparencia; y tener fines determinados, explícitos y legítimos. Está prohibido tratar categorías especiales de datos, salvo las excepciones previstas.
- **Preparación de los datos personales:** deben ser tratados aplicando el principio de minimización.

- **Control del sesgo:** los datos personales tratados deben ser exactos y actualizados con relación a los fines para los que son tratados.

5. Verificación y validación

Respecto a este último objetivo, la Guía desarrolla una lista de objetivos a tener en cuenta respesto a la verificación y validación del componente IA respecto al tratamiento de los datos personales:

- **Adecuación del proceso de verificación y validación del componente IA:** que se pueda demostrar que la metodología empleada en la incorporación del componente IA en el tratamiento o en su desarrollo, cumple con los principios relativos al tratamiento y el resto de las obligaciones impuestas por la normativa española en materia de protección de datos.
- **Verificación y validación del componente IA:** se debe demostrar que el componente IA trata los datos de manera correcta, respetando el principio de exactitud.
- **Rendimiento**: referido a la eficacia respecto a la protección de datos, el componente IA debe tratar los datos personales respetando el principio de exactitud.
- **Coherencia:** respecto a la concordancia entre los resultados obtenidos de los esperados ante los datos de entrada similares o idénticos. Se debe tratar los datos personales respetando el principio de exactitud.
- **Estabilidad y robustez:** como consecuencia de cambios de contexto internos y externos al tratamiento, el componente IA está sometido a procesos de supervisión continua para adaptarse a las modificaciones del entorno y detectar necesidades de reajuste.
- **Trazabilidad:** el comportamiento en el tratamiento del componente IA debe poder supervisarse a través de mecanismos de trazabilidad, incluidos los medios humanos. Esto en atención a los principios de protección de datos y del derecho del interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, que produzca en éste efectos jurídicos o le afecte significativamente en modo similar.
- **Seguridad:** el componente IA debe tratar los datos personales aplicando los principios de protección de datos de manera eficaz y efectiva; así como, integrando las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad de la información adecuado al riesgo y en lo que se refiere a la confidencialidad, integridad, disponibilidad y resiliencia del tratamiento.

La Guía precisa que la enumeración de este conjunto de controles no implica una obligación de aplicarlos sistemáticamente todos ellos; sino, que será el auditor quien seleccionará los que se adecuen a la auditoría en concreto y añadirá los que crea oportunos.

En esa misma línea, se señala que la selección de los controles a auditar, la extensión de su análisis y la formalidad requerida en su implementación dependerá del objetivo y alcance definido para la auditoría: así como del análisis de riesgos realizados.

En el caso del Perú, no contamos con normativa nacional que regule el

tratamiento de datos personales que incluyan componentes de IA; sin embargo, al formar parte de la Red Iberoamericana de Protección de Datos Personales, se aplican las "Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial" y "Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de Datos Personales en los Proyectos de Inteligencia Artificial", aprobados en el 2019.

Si bien el listado de objetivos de control propuestos por la AEPD se fundamentan en el cumplimiento de los principios de protección de datos y los principios relativos al tratamiento propios del ordenamiento español, en Perú, la Guía deberá ser tratada cumpliéndose los principios rectores establecidos en la Ley N° 29733, Ley de Protección de Datos Personales, siendo el principio de legalidad, de consentimiento, de finalidad, de proporcionalidad, de calidad, de seguridad; y, de protección adecuado, los de observancia indispensable para realizar el control del tratamiento de datos personales en el marco de las auditorías.

En ese sentido, la Guía es una buena referencia para las auditorías a tratamientos de datos personales que incluyan componentes de IA, porque permitirá un mayor control del cumplimiento de la normativa de protección de datos personales, tanto por parte de los encargados de realizar las auditorías, como de los responsables de los tratamientos que incluyan componentes de IA. Además, con estos objetivos de control propuestos, se generaría mayor seguridad para los titulares de los datos personales, respecto a su tratamiento.