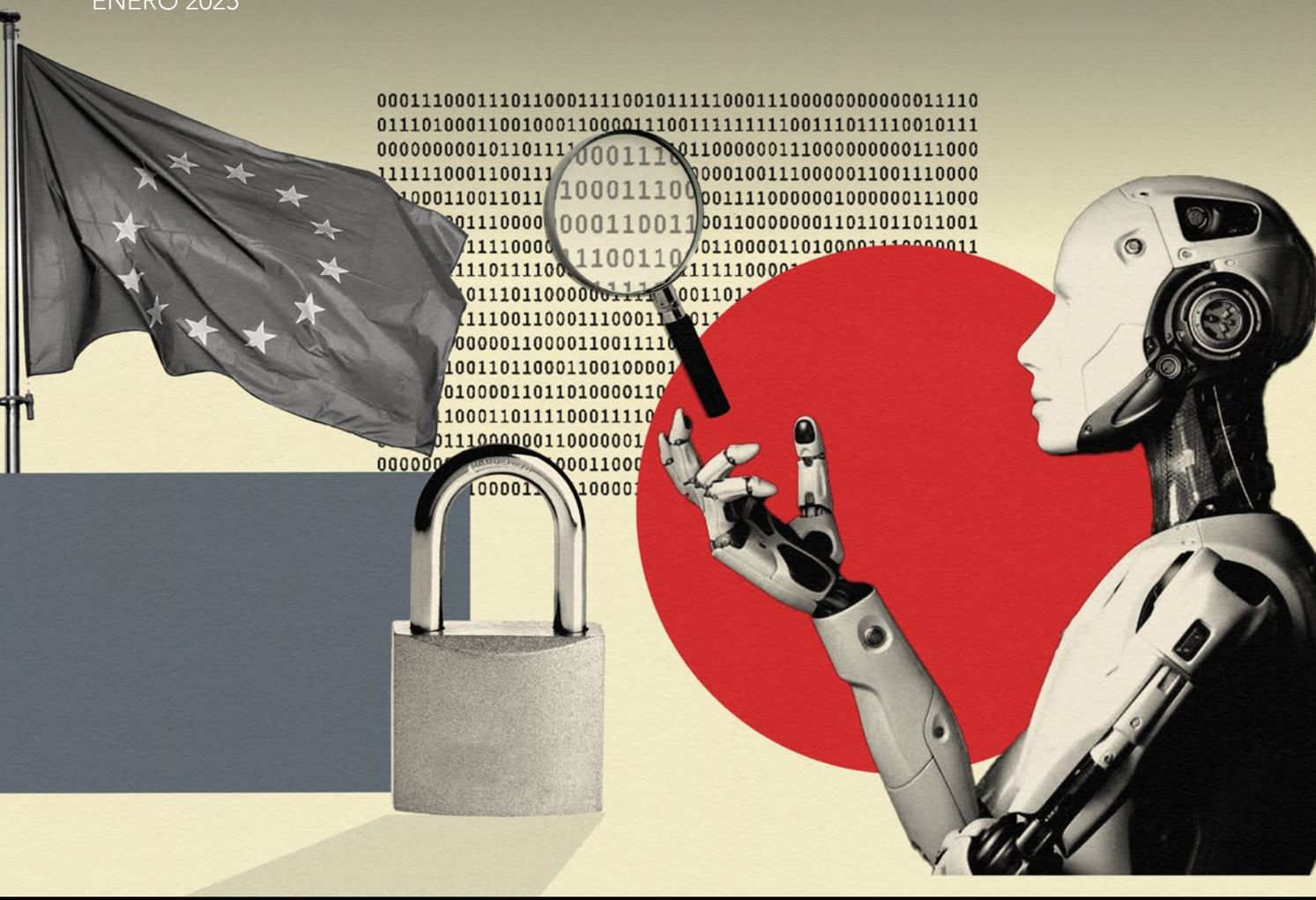
CRITERIO EMITIDO EN LA UNIÓN EUROPEA SOBRE EL USO DE DATOS PERSONALES PARA EL **DESARROLLO E IMPLEMENTACIÓN DE MODELOS DE INTELIGENCIA ARTIFICIAL**

ENERO 2025



I. **¿Cuándo y cómo un modelo de IA puede considerarse «anónimo»?**

II. **¿Cómo pueden demostrar los responsables del tratamiento la idoneidad del interés legítimo como base jurídica en las fases de desarrollo, conforme el Reglamento General de Protección de Datos ("RGPD") ?**

III. **¿Cómo pueden demostrar los responsables del tratamiento la idoneidad del interés legítimo como base jurídica en las fases de implementación, conforme el RGPD?**

IV. **¿Cuáles son las consecuencias del tratamiento ilícito de datos personales en la fase de desarrollo de un modelo de IA sobre el posterior procesamiento o funcionamiento del modelo de IA?**

En el contexto de los modelos de inteligencia artificial ("IA") y su relación con la protección de datos personales, en Europa se ha emitido un nuevo criterio sobre sus implicaciones legales. En septiembre del año anterior, la Comisión Irlandesa de Protección de Datos solicitó al Comité Europeo de Protección de Datos ("CEPD") que emitiera una opinión sobre cuestiones de aplicación general, de conformidad con el artículo 64, apartado 2, del RGPD. Estas opiniones emitidas por el CEPD son vinculantes para una, varias o todas las autoridades públicas e independientes establecidas por los Estados miembro de la Unión Europea ("Autoridades de Control"), según se indique en la opinión correspondiente.

La solicitud referida anteriormente versó sobre al tratamiento de datos personales en el contexto de las fases de desarrollo e implementación de modelos de IA, en específico se plantearon las siguientes preguntas:

1. ¿Cuándo y cómo un modelo de IA puede considerarse «anónimo»?
2. ¿Cómo pueden demostrar los responsables del tratamiento la idoneidad del interés legítimo como base jurídica en las fases de desarrollo, conforme el RGPD?
3. ¿Cómo pueden demostrar los responsables del tratamiento la idoneidad del interés legítimo como base jurídica en las fases de implementación, conforme el RGPD?
4. ¿Cuáles son las consecuencias del tratamiento ilícito de datos personales en la fase de desarrollo de un modelo de IA sobre el posterior procesamiento o funcionamiento del modelo de IA?

Atendiendo lo anterior, el 17 de diciembre de 2024, el CEPD emitió la Opinión 28/2024 sobre ciertos aspectos de protección relacionados con el tratamiento de datos personales en el contexto de modelos de IA, misma que es de cumplimiento y observancia obligatoria para todas las Autoridades de Control (la "Opinión"), mediante la cual el CEPD proporcionó las siguientes respuestas:

I. Respuesta a la primera pregunta:

Se establece en la Opinión que las declaraciones de anonimización de un modelo de IA deben ser evaluadas por las Autoridades de Control, ya que el CEPD considera que los modelos de IA entrenados con datos personales no pueden, en todos los casos, considerarse anónimos.

Para tales efectos, a fin de que un modelo de IA se considere anónimo deben ser insignificantes tanto la probabilidad de extracción directa (incluida la probabilística) de datos personales relativos a los titulares cuyos datos personales se utilizaron para desarrollar el modelo, como la probabilidad de obtener, intencionalmente o no, dichos datos personales a partir de consultas.

Para llevar a cabo su evaluación, las Autoridades de Control revisarán la documentación facilitada por el responsable para demostrar la anonimización del modelo de IA. Para probar lo anterior, algunos elementos que los responsables podrán utilizar son: (i) las fuentes que se utilizaron para recabar la información a fin de entrenar los modelos de IA; (ii) la preparación y minimización que se le dé a los datos personales que se utilizaron para entrenar los modelos de IA; (iii) las auditorías llevadas a cabo para estimar y prever la probabilidad de identificación de los datos personales; y (iv) las pruebas que se realizaron al modelo de IA contra ataques externos, entre otros.

II. Respuesta a la segunda y tercera preguntas:

En la Opinión se indican consideraciones generales que las Autoridades de Control deberán tener en cuenta a la hora de evaluar si los responsables pueden invocar el interés legítimo como base jurídica idónea para el tratamiento realizado en el contexto del desarrollo y de implementación de modelos de IA.

En la Opinión se señalaron los tres procesos que deben realizarse al evaluar la aplicación del interés legítimo como base jurídica del tratamiento de datos personales, a saber: (1) identificar el interés legítimo perseguido por el responsable; (2) analizar la necesidad del tratamiento para los fines del interés o intereses legítimos perseguidos (prueba de necesidad); y (3) evaluar que el interés o intereses legítimos no prevalezcan sobre los intereses o los derechos y libertades fundamentales de los titulares de los datos personales (prueba de ponderación). Asimismo, será importante analizar las expectativas razonables de los titulares en la prueba de ponderación, ya que, debido a la complejidad de las tecnologías utilizadas en los modelos de IA, puede ser difícil para los titulares comprender la variedad de distintas actividades de tratamiento implicadas.

En la Opinión también se recalca que, cuando los intereses, derechos y libertades de los titulares parezcan prevalecer sobre el interés o intereses legítimos perseguidos por el responsable, éste podrá considerar la introducción de medidas de mitigación para limitar el impacto del tratamiento sobre dichos titulares; por ejemplo, medidas técnicas, medidas de pseudonimización, medidas para facilitar el ejercicio de derechos, medidas de transparencia, medidas contra raspado web (*web scraping*), entre otras.

III. Respuesta a la cuarta pregunta:

En la Opinión se indica que las Autoridades de Control gozan de facultades discrecionales para evaluar la posible infracción derivada del tratamiento ilícito de datos personales para estos efectos, así como imponer las medidas correctivas que sean adecuadas, necesarias y proporcionales, teniendo en cuenta las circunstancias de cada caso. En la Opinión se analizan tres hipótesis sobre el tratamiento de datos personales en modelos de IA:

- En la primera hipótesis, se evalúa el tratamiento posterior de datos personales realizado por el mismo responsable que desarrolló e implementó el modelo de IA, y sus implicaciones dependiendo si las fases de desarrollo e implementación tienen fines distintos.

- En la segunda hipótesis, se analiza que el responsable de la fase de implementación del modelo haya realizado una evaluación adecuada para garantizar que en la fase de desarrollo no se haya llevado a cabo un tratamiento ilícito de los datos personales conservados en el modelo de IA, mismo que fue desarrollado por un tercero.

- En la tercera hipótesis, se estudian los casos en que el tratamiento de datos personales en el desarrollo del modelo de IA es ilegal, pero se anonimizan antes de la implementación y posterior uso del modelo en la fase de implementación, por lo que, el modelo de IA podría operar sin que el RGPD sea aplicable siempre que no se traten datos personales adicionales posteriormente. Sin embargo, el RGPD sí aplicaría cuando, tras la anonimización del modelo de IA, se traten datos personales adicionales en la fase de implementación. Por lo tanto, la ilegalidad del tratamiento inicial en la fase de desarrollo no debería afectar la legalidad del tratamiento efectuado en la fase de implementación del modelo de IA.

Finalmente, a pesar de que esta Opinión solamente surta sus efectos y sea aplicable en los Estados miembro de la Unión Europea, es posible que llegue a tener injerencia de manera colateral como criterio no vinculante en otras jurisdicciones, incluyendo a México, tal y como ha sucedido con el contenido establecido en el RGPD. Por ello, será importante conocer el impacto práctico que la Opinión vaya alcanzando en la Unión Europea. +