Dictamen del Comité (art. 64)

Dictamen 28/2024 sobre determinados aspectos de la protección de datos relacionados con el tratamiento de datos personales en el contexto de los modelos de IA

Adoptado el 17 de diciembre de 2024

Resumen ejecutivo

Las tecnologías de IA crean muchas oportunidades y beneficios en una amplia gama de sectores y actividades sociales.

Al proteger el derecho fundamental a la protección de datos, el RGPD apoya estas oportunidades y promueve otros derechos fundamentales de la UE, como el derecho a la libertad de pensamiento, expresión e información, el derecho a la educación o la libertad de empresa. De este modo, el RGPD es un marco jurídico que fomenta la innovación responsable.

En este contexto, teniendo en cuenta las cuestiones de protección de datos que plantean estas tecnologías, la autoridad de control irlandesa solicitó al CEPD que emitiera un dictamen sobre cuestiones de aplicación general de conformidad con el artículo 64, apartado 2, del RGPD. La solicitud se refiere al tratamiento de datos personales en el contexto de las fases de desarrollo y despliegue de los modelos de inteligencia artificial («**IA**»). En más detalle, en la solicitud se preguntaba lo siguiente: (1) cuándo y cómo un modelo de IA puede considerarse «anónimo»; (2) cómo pueden los responsables del tratamiento demostrar la idoneidad del interés legítimo como base jurídica en las fases de desarrollo y (3) despliegue; y (4) cuáles son las consecuencias del tratamiento ilícito de datos personales en la fase de desarrollo de un modelo de IA sobre el posterior tratamiento o funcionamiento del modelo de IA.

Con respecto a la primera pregunta, el Dictamen menciona que las declaraciones de anonimato de un modelo de IA deben ser evaluadas por las autoridades de control competentes caso por caso, ya que el CEPD considera que los modelos de IA entrenados con datos personales no pueden considerarse siempre anónimos. Para que un modelo de IA se considere anónimo, tanto 1) la probabilidad de extracción directa (incluida la probabilística) de datos personales relativos a personas cuyos datos personales se utilizaron para desarrollar el modelo como 2) la probabilidad de obtener, intencionadamente o no, dichos datos personales a partir de consultas, debe ser insignificante, teniendo en cuenta «*todos los medios que sea razonablemente probable que utilicen*» el responsable del tratamiento u otra persona.

Para llevar a cabo su evaluación, las autoridades de control deben revisar la documentación facilitada por el responsable del tratamiento para demostrar el anonimato del modelo. A este respecto, el Dictamen proporciona una lista no prescriptiva y no exhaustiva de métodos que pueden utilizar los responsables del tratamiento en su demostración del anonimato y que, por tanto, las autoridades de control pueden tener en cuenta al evaluar la alegación de anonimato de un responsable del tratamiento. Esto incluye, por ejemplo, los enfoques adoptados por los responsables del tratamiento durante la fase de desarrollo para prevenir o limitar la recogida de datos personales utilizados para fines de entrenamiento, reducir su identificabilidad, impedir su extracción u ofrecer garantías en relación con las funciones más avanzadas de resistencia frente a los ataques.

Con respecto a las preguntas segunda y tercera, el Dictamen establece consideraciones generales que las autoridades de control deben tener en cuenta a la hora de evaluar si los responsables del tratamiento pueden basarse en el interés legítimo como base jurídica adecuada para el tratamiento llevado a cabo en el contexto del desarrollo y la implantación de modelos de IA.

El Dictamen recuerda que no existe una jerarquía entre las bases jurídicas previstas en el RGPD, y que corresponde a los responsables del tratamiento identificar la base jurídica adecuada para sus actividades de tratamiento. A continuación, el Dictamen recuerda la prueba de tres pasos que debe llevarse a cabo al evaluar el uso del interés legítimo como base jurídica, es decir, 1) identificar el interés

legítimo perseguido por el responsable del tratamiento o un tercero; 2) analizar la necesidad del tratamiento para los fines del interés o los intereses legítimos perseguidos (también denominada «prueba de necesidad»); y 3) evaluar que el interés o los intereses legítimos no se vean anulados por los intereses o los derechos y libertades fundamentales de los interesados (también denominada «prueba de ponderación»).

Con respecto al primer paso, el Dictamen recuerda que un interés puede considerarse legítimo si se cumplen los tres criterios acumulativos siguientes: el interés (1) es lícito; (2) está articulado de forma clara y precisa; y (3) es real y presente (es decir, no especulativo). Ese interés puede abarcar, por ejemplo, el desarrollo de un modelo de IA -desarrollar el servicio de un agente conversacional para ayudar a los usuarios- o su despliegue -mejorar la detección de amenazas en un sistema de información.

Por lo que se refiere a la segunda fase, el Dictamen recuerda que la evaluación de la necesidad implica considerar: 1) si la actividad de tratamiento permitirá la persecución del interés legítimo; y 2) si no existe una forma menos intrusiva de perseguir dicho interés. Al evaluar si se cumple la condición de necesidad, las autoridades de control deberán prestar especial atención a la cantidad de datos personales tratados y si es proporcionado perseguir el interés legítimo en juego, también a la luz del principio de minimización de datos.

Por lo que se refiere a la tercera fase, el Dictamen recuerda que la prueba de ponderación debe llevarse a cabo teniendo en cuenta las circunstancias específicas de cada caso. A continuación, ofrece una visión general de los elementos que las autoridades de control pueden tener en cuenta a la hora de evaluar si el interés de un responsable del tratamiento o de un tercero se ve superado por los intereses, los derechos fundamentales y las libertades de los interesados.

Como parte de la tercera fase, el Dictamen destaca los riesgos específicos para los derechos fundamentales que pueden surgir en las fases de desarrollo o de despliegue de los modelos de IA. También aclara que el tratamiento de datos personales que tiene lugar durante las fases de desarrollo e implantación de los modelos de IA puede afectar a los interesados de diferentes maneras, lo que puede ser positivo o negativo. Para evaluar dicho impacto, las autoridades de control podrán tener en cuenta la naturaleza de los datos tratados por los modelos, el contexto del tratamiento y las posibles consecuencias adicionales del tratamiento.

Además, el Dictamen destaca el papel de las expectativas razonables de los interesados en la prueba de ponderación. Esto puede ser importante debido a la complejidad de las tecnologías utilizadas en los modelos de IA y al hecho de que puede ser difícil para los interesados comprender la variedad de sus usos potenciales, así como las diferentes actividades de tratamiento que implican. En este sentido, tanto la información facilitada a los interesados como el contexto del tratamiento pueden figurar entre los elementos que deben tenerse en cuenta para evaluar si los interesados pueden esperar razonablemente que se traten sus datos personales. Por lo que se refiere al contexto, esto puede incluir: si los datos personales estaban a disposición del público, la naturaleza de la relación entre el interesado y el responsable del tratamiento (y si existe un vínculo entre ambos), la naturaleza del servicio, el contexto en el que se recogieron los datos personales, la fuente a partir de la cual se recogieron los datos (es decir, el sitio web o el servicio en el que se recogieron los datos personales y la configuración de privacidad que ofrecen), los posibles nuevos usos del modelo y si los interesados son realmente conscientes de que sus datos personales están en línea.

El Dictamen también recuerda que, cuando los intereses, los derechos y las libertades de los interesados parecen prevalecer sobre el interés o intereses legítimos que persigue el responsable del tratamiento o un tercero, el responsable del tratamiento puede considerar la posibilidad de introducir

medidas de mitigación para limitar el impacto que el tratamiento puede tener en dichos interesados. Las medidas de mitigación no deben confundirse con las medidas que el responsable del tratamiento está legalmente obligado a adoptar en cualquier caso para garantizar el cumplimiento del RGPD. Además, las medidas deben adaptarse a las circunstancias del caso y a las características del modelo de IA, incluido su uso previsto. A este respecto, el dictamen ofrece una lista no exhaustiva de ejemplos de medidas paliativas en relación con la fase de desarrollo (también en lo que respecta a la extracción de información de sitios web o *web scraping*) y la fase de despliegue. Las medidas paliativas pueden estar sujetas a una rápida evolución y deben adaptarse a las circunstancias del caso. Por lo tanto, corresponde a las autoridades de control evaluar la idoneidad de las medidas de mitigación aplicadas caso por caso.

Con respecto a la cuarta pregunta, el Dictamen recuerda en general que las autoridades de control disponen de facultades discrecionales para evaluar la posible infracción o infracciones y elegir medidas adecuadas, necesarias y proporcionadas, teniendo en cuenta las circunstancias de cada caso concreto. A continuación, el Dictamen examina tres supuestos.

En el supuesto 1, los datos personales se conservan en el modelo de IA (lo que significa que el modelo no puede considerarse anónimo, como se detalla en la primera pregunta) y posteriormente son tratados por el mismo responsable del tratamiento (por ejemplo, en el contexto del despliegue del modelo). El Dictamen señala que la cuestión de si las fases de desarrollo y despliegue implican fines distintos (constituyendo así actividades de tratamiento separadas) y la medida en que la falta de base jurídica para la actividad de tratamiento inicial afecta a la licitud del tratamiento posterior, deben evaluarse caso por caso, en función del contexto del asunto.

En el supuesto 2, los datos personales se conservan en el modelo y son tratados por otro responsable del tratamiento en el contexto de la implantación del modelo. A este respecto, el Dictamen establece que las autoridades de control deberán tener en cuenta si el responsable del tratamiento que despliegue el modelo llevó a cabo una evaluación adecuada, como parte de sus obligaciones de rendición de cuentas para demostrar el cumplimiento del artículo 5, apartado 1, letra a), y del artículo 6 del RGPD, para garantizar que el modelo de IA no se desarrolló mediante el tratamiento ilícito de datos personales. Esta evaluación debe tener en cuenta, por ejemplo, la fuente de los datos personales y si el tratamiento en la fase de desarrollo fue objeto de la constatación de una infracción, en particular si dicha infracción fue determinada por una autoridad de control o un tribunal, y deberá ser más o menos detallada en función de los riesgos que plantee el tratamiento en la fase de despliegue.

En el supuesto 3, un responsable del tratamiento trata ilícitamente datos personales para desarrollar el modelo de IA y, a continuación, se asegura de que sean anonimizados antes de que el mismo responsable o cualquier otro responsable del tratamiento inicie otro tratamiento de datos personales en el contexto del despliegue. A este respecto, el Dictamen afirma que si puede demostrarse que el funcionamiento posterior del modelo de IA no implica el tratamiento de datos personales, el CEPD considera que el RGPD no sería aplicable. Por lo tanto, la ilicitud del tratamiento inicial no debería afectar al funcionamiento posterior del modelo. Además, el CEPD considera que, cuando los responsables del tratamiento traten posteriormente los datos personales recogidos durante la fase de despliegue, una vez anonimizado el modelo, el RGPD se aplicaría en relación con estas operaciones de tratamiento. En estos casos, el Dictamen considera que, en lo que respecta al RGPD, la licitud del tratamiento llevado a cabo en la fase de despliegue no debe verse afectada por la ilicitud del tratamiento inicial.

Índice

El Comité Europeo de Protección de Datos

Vistos el artículo 63 y el artículo 64, apartado 2, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en lo sucesivo, el «Reglamento general de protección de datos»),

Visto el Acuerdo sobre el Espacio Económico Europeo y, en particular, su anexo XI y su Protocolo 37, modificado por la Decisión del Comité Mixto del EEE n.º 154/2018, de 6 de julio de 2018[1],

Vistos el artículo 10 y el artículo 22 de su Reglamento interno,

Considerando lo siguiente:

1) El principal cometido del Comité Europeo de Protección de Datos (en lo sucesivo, el **Comité** o el **CEPD**) es responsable de garantizar la aplicación coherente del RGPD en todo el Espacio Económico Europeo (**EEE**). El artículo 64, apartado 2, del RGPD establece que cualquier autoridad de control, el presidente del Comité o la Comisión podrán solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro del EEE sea examinado por el Comité a efectos de dictamen El objetivo de este Dictamen es examinar un asunto de aplicación general o que surta efecto en más de un Estado miembro del EEE.

2) El dictamen del Comité se adoptará de conformidad con el artículo 64, apartado 3, del RGPD en relación con el artículo 10, apartado 2, del Reglamento interno del CEPD en un plazo de ocho semanas posterior al momento en que el presidente y la autoridad de control competente hayan decidido que el expediente está completo. Por decisión de la presidenta, dicho plazo podrá ampliarse otras seis semanas atendiendo a la complejidad del asunto.

HA ADOPTADO EL SIGUIENTE DICTAMEN

1 Introducción

1.1 Resumen de los hechos

1. El 4 de septiembre de 2024, la autoridad de control irlandesa (la **IE SA** o **autoridad de control solicitante**) solicitó al CEPD que emitiera un dictamen de conformidad con el artículo 64, apartado 2, del RGPD en relación con los modelos de IA y el tratamiento de datos personales (**la Solicitud**).

2. La presidenta del Comité y la IE SA consideraron completo el expediente el 13 de septiembre de 2024. El siguiente día laborable, el 16 de septiembre de 2024, la Secretaría del CEPD difundió el expediente. La presidenta del Comité, teniendo en cuenta la complejidad del asunto, decidió ampliar el plazo legal de conformidad con el artículo 64, apartado 3, del RGPD y el artículo 10, apartado 4, del Reglamento interno del CEPD.

[1] Las referencias a los «Estados miembros» realizadas en el presente Dictamen deben entenderse como referencias a los «Estados miembros del EEE». Las referencias a la «Unión» realizadas en el presente Dictamen deben entenderse como referencias al «EEE».

3. La solicitud aborda determinados elementos del entrenamiento, la actualización, el desarrollo y el funcionamiento de los modelos de IA en los que los datos personales forman parte del conjunto de datos pertinente. La IE SA destaca que la solicitud se refiere a cuestiones clave que tienen un gran impacto en los interesados y responsables del tratamiento en el EEE, y que no existe una posición armonizada en esta fase entre las autoridades de control nacionales[2]. La terminología que se utilizará a efectos del presente Dictamen figura abajo en las secciones 2.2 y 2.3 abajo.

4. La IE SA planteó las siguientes preguntas:

Pregunta 1: ¿Se considera que un modelo de IA final que ha sido entrenado utilizando datos personales no cumple en ningún caso lo establecido en la definición de datos personales (tal como se establece en el artículo 4, apartado 1, del RGPD)?

Si la respuesta a la primera pregunta es afirmativa:

i. ¿En qué fase de las operaciones de tratamiento que dan lugar a un modelo de IA ya no se tratan los datos personales?
   a) ¿Cómo puede demostrarse que el modelo de IA no trata datos personales?

ii. ¿Existen factores que hagan que el funcionamiento del modelo de IA final deje de considerarse anónimo?
   a) En caso afirmativo, ¿cómo pueden demostrarse las medidas adoptadas para mitigar, prevenir o proteger contra estos factores (a fin de garantizar que el modelo de IA no trate datos personales)?

Si la respuesta a la primera pregunta es negativa:

i. ¿Cuáles son las circunstancias en las que esto podría ocurrir?
   a) En caso afirmativo, ¿cómo pueden demostrarse las medidas que se han tomado para garantizar que el modelo de IA no está tratando datos personales?

Pregunta 2: Cuando un responsable del tratamiento se base en intereses legítimos como base jurídica para el tratamiento de datos personales con el fin de crear, actualizar o desarrollar un modelo de IA, ¿cómo debe demostrar dicho responsable la adecuación de los intereses legítimos como base jurídica, tanto en relación con el tratamiento de datos de terceros y de datos propios?

i. ¿Qué consideraciones debe tener en cuenta dicho responsable del tratamiento para garantizar que los intereses de los interesados, cuyos datos personales están siendo tratados, se ponderan adecuadamente con los intereses de dicho responsable en el contexto de:
   a) datos de terceros

   b) datos propios

Pregunta 3: Después del entrenamiento, cuando un responsable del tratamiento de datos se base en intereses legítimos como base jurídica para el tratamiento de datos personales que tiene lugar dentro de un modelo de IA, o de un sistema de IA del que forma parte un modelo de IA, ¿cómo debe demostrar dicho responsable la idoneidad de los intereses legítimos como base jurídica?

[2] Solicitud, p. 1.

Pregunta 4: Si se descubre que un modelo de inteligencia artificial ha sido creado, actualizado o desarrollado utilizando datos personales tratados ilícitamente, ¿cuál es el impacto de ello, en su caso, sobre la licitud del tratamiento o explotación continuados o subsiguientes del modelo de inteligencia artificial, ya sea por sí solo o como parte de un sistema de inteligencia artificial, cuando:

i. el modelo de IA, ya sea por sí solo o como parte de un sistema de IA, está tratando datos personales?
ii. ni el modelo de inteligencia artificial, ni el modelo de inteligencia artificial como parte de un sistema de inteligencia artificial, está tratando datos personales?

1.2 Admisibilidad de la solicitud de dictamen en virtud del artículo 64, apartado 2, del RGPD

5. El artículo 64, apartado 2, del RGPD establece que, en particular, cualquier autoridad de control podrá solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro sea examinado por el Comité a efectos de dictamen.

6. La autoridad de control solicitante planteó preguntas al CEPD en relación con aspectos relacionados con la protección de datos en el contexto de los modelos de IA. La autoridad especificó en su solicitud que, si bien muchas organizaciones utilizan ahora modelos de IA, incluidos grandes modelos de lenguaje (“**LLMs”**), sus operaciones, entrenamiento y uso plantean «*una serie de problemas de gran alcance en materia de protección de datos*»[3], que «*afectan a los interesados en toda la UE/el EEE*»[4].

7. La solicitud plantea, en esencia, preguntas sobre i) la aplicación del concepto de datos personales; ii) el principio de licitud, con especial atención a la base jurídica del interés legítimo, en el contexto de los modelos de IA; así como, sobre iii) las consecuencias del tratamiento ilícito de datos personales en la fase de desarrollo de los modelos de IA, sobre el posterior tratamiento o funcionamiento del modelo.

8. Por lo tanto, el Comité considera que la solicitud se refiere a una «*cuestión de aplicación general*» en el sentido del artículo 64, apartado 2, del RGPD. En particular, el asunto se refiere a la interpretación y aplicación del artículo 4, apartado 1, del artículo 5, apartado 1, letra a), y del artículo 6 del RGPD en relación con el tratamiento de datos personales en el desarrollo y la implantación de modelos de IA. Como subraya la autoridad de control solicitante, la aplicación de estas disposiciones a los modelos de IA plantea cuestiones sistémicas, abstractas y novedosas[5]. El rápido desarrollo y despliegue de modelos de IA por parte de un número cada vez mayor de organizaciones plantea cuestiones específicas y, como se señala en la solicitud, *«el CEPD se beneficiará en gran medida de alcanzar una posición común sobre las cuestiones planteadas en la presente solicitud, ya que estas cuestiones son fundamentales para el trabajo previsto del CEPD a corto y medio plazo»*[6]. Además, las tecnologías de IA crean muchas oportunidades y beneficios en una amplia gama de sectores y actividades sociales. Por su parte, el RGPD es un marco jurídico que fomenta la innovación responsable. De ello se deduce que existe un interés general en realizar esta evaluación en forma de dictamen del CEPD, a fin de garantizar la aplicación coherente de determinadas disposiciones del RGPD en el contexto de los modelos de IA.

[3] Solicitud, p. 1.
[4] Ibíd.
[5] Solicitud, p. 2.
[6] Solicitud, p. 1. Como se menciona en el Programa de Trabajo del CEPD para 2024-2025, adoptado el 8 de octubre de 2024, disponible en https://www.edpb.europa.eu/system/files/2024-10/edpb_work_programme_2024-2025_en.pdf, el CEPD tiene previsto publicar, entre otras cosas, directrices sobre anonimización, seudonimización y extracción de información en el contexto de la IA generativa.

9. La segunda condición mencionada en el artículo 64, apartado 2, del RGPD se refiere a los asuntos «*que surtan efecto en más de un Estado miembro*». El CEPD recuerda que el término «efectos» debe interpretarse *lato sensu*, por lo que no se limita simplemente a los efectos jurídicos[7]. Dado que cada vez más modelos de IA están siendo entrenados y utilizados por un número cada vez mayor de organizaciones del EEE, sí afectan a un gran número de interesados en todo el EEE, algunos de los cuales ya han expresado su preocupación a su autoridad de control competente[8]. Por lo tanto, el CEPD considera que la cuestión planteada por la autoridad de control solicitante también cumple esta condición.

10. La solicitud incluye un razonamiento escrito sobre los antecedentes y las motivaciones para presentar las preguntas al Comité, en particular sobre el marco jurídico pertinente. Por consiguiente, el Comité considera que la solicitud está motivada de conformidad con el artículo 10, apartado 3, del Reglamento interno del CEPD.

11. De conformidad con el artículo 64, apartado 3, del RGPD[9], el CEPD no emitirá un dictamen si ya ha emitido un dictamen sobre el asunto. El CEPD no ha emitido un dictamen sobre el mismo asunto y todavía no ha respondido a las preguntas contenidas en la solicitud.

12. Por estas razones, el Comité considera que la solicitud es admisible y que las cuestiones que se plantean a partir de la solicitud deben analizarse en el presente Dictamen (**el Dictamen**) adoptado de conformidad con el artículo 64, apartado 2, del RGPD.

2 Ámbito de aplicación y conceptos clave

2.1 Alcance del Dictamen

13. El Comité está de acuerdo con la autoridad de control solicitante en que, desde la perspectiva de la protección de datos, el desarrollo y la implantación de modelos de IA plantean cuestiones fundamentales en materia de protección de datos. Las cuestiones se refieren, en particular, a: I) cuándo y cómo un modelo de IA puede considerarse «anónimo» (pregunta 1 de la solicitud); ii) cómo pueden los responsables del tratamiento demostrar la idoneidad del interés legítimo como base jurídica en las fases de desarrollo (pregunta 2 de la solicitud) y despliegue (pregunta 3 de la solicitud), y iii) si la ilicitud del tratamiento de datos personales en la fase de desarrollo tiene consecuencias sobre la licitud del posterior tratamiento u operación del modelo de IA (pregunta 4 de la solicitud).

14. El CEPD recuerda que las autoridades de control son responsables de supervisar la aplicación del RGPD y deben contribuir a su aplicación coherente en toda la Unión[10]. Por lo tanto, es competencia de las autoridades de control investigar modelos de IA específicos y, al hacerlo, llevar a cabo evaluaciones caso por caso.

15. El presente Dictamen proporciona un marco para que las autoridades de control competentes evalúen los casos específicos en los que pueden surgir (algunas de) las preguntas planteadas en la solicitud. El presente Dictamen no pretende ser exhaustivo, sino más bien ofrecer consideraciones generales sobre la interpretación de las disposiciones pertinentes que las autoridades de control competentes

[7] Documento interno 3/2019 del CEPD sobre orientaciones internas en relación con el artículo 64, apartado 2, del RGPD, adoptado el 8 de octubre de 2019, apartado 15, disponible en https://www.edpb.europa.eu/system/files/2022-07/internaledpb_document_201903_art64.2_en.pdf.
[8] Solicitud, pp. 1-2.
[9] Artículo 64, apartado 3, del RGPD y artículo 10, apartado 4, del Reglamento interno del CEPD.
[10] Artículo 51, apartados 1 y 2, del RGPD.

deberían tener muy en cuenta a la hora de utilizar sus potestades de investigación. Si bien el presente Dictamen se dirige a las autoridades de control competentes y se refiere a sus actividades y competencias, se entiende sin perjuicio de las obligaciones de los responsables y encargados del tratamiento en virtud del RGPD. En particular, de conformidad con el principio de rendición de cuentas consagrado en el artículo 5, apartado 2, del RGPD, los responsables del tratamiento serán responsables de todos los principios relativos a su tratamiento de datos personales y deberán ser capaces de demostrar su cumplimiento.

16. En algunos casos, pueden facilitarse algunos ejemplos en el Dictamen, pero teniendo en cuenta el amplio alcance de las preguntas incluidas en la solicitud, así como los diferentes tipos de modelos de IA cubiertos en ella, en el presente Dictamen no se tendrán en cuenta todos los supuestos posibles. Las tecnologías asociadas a los modelos de IA están sujetas a una rápida evolución; en consecuencia, las consideraciones del CEPD en el presente Dictamen deben interpretarse a la luz de ello.

17. **El presente Dictamen no analiza las siguientes disposiciones, que pueden seguir desempeñando un papel importante a la hora de evaluar los requisitos de protección de datos aplicables a los modelos de IA:**

- **Tratamiento de categorías especiales de datos:** El CEPD recuerda la prohibición del artículo 9, apartado 1, del RGPD en relación con el tratamiento de categorías especiales de datos y las limitadas excepciones del artículo 9, apartado 2, del RGPD[11]. A este respecto, el Tribunal de Justicia de la Unión Europea (**TJUE**) aclaró además que «*en el supuesto de que un conjunto de datos que contiene a la vez datos sensibles y datos no sensibles [...] se recoja en bloque, sin que unos datos puedan disociarse de otros en el momento de esa recogida, el tratamiento de ese conjunto de datos debe considerarse prohibido, en el sentido del artículo 9, apartado 1, del RGPD, cuando incluya al menos un dato sensible sin que sea aplicable ninguna de las excepciones previstas en el artículo 9, apartado 2, del citado Reglamento*»[12]. Además, el TJUE también destacó que «*a efectos de la aplicación de la excepción prevista en el artículo 9, apartado 2, letra e), del RGPD, es preciso comprobar si el interesado ha pretendido, de manera explícita y mediante un acto positivo claro, hacer accesibles al público en general los datos personales en cuestión*»[13]. Estas consideraciones deben tenerse en cuenta cuando el tratamiento de datos personales en el contexto de los modelos de IA implique categorías especiales de datos.
- **Toma de decisiones automatizada, incluida la elaboración de perfiles**: Las operaciones de tratamiento realizadas en el contexto de los modelos de IA pueden entrar en el ámbito de aplicación del artículo 22 del RGPD, que impone obligaciones adicionales a los responsables del tratamiento y proporciona garantías adicionales a los interesados. El CEPD recuerda, a este

[11] Véase también el Informe del CEPD sobre el trabajo realizado por el Grupo de Trabajo de ChatGPT, adoptado el 23 de mayo de 2024, apartado 18: «Por lo que respecta al tratamiento de categorías especiales de datos personales, debe aplicarse además una de las excepciones del artículo 9, apartado 2, para que el tratamiento sea lícito. *En principio, una de estas excepciones puede ser el artículo 9, apartado 2, letra e), del RGPD. Sin embargo, el mero hecho de que los datos personales sean de acceso público no implica que "el interesado haya hecho manifiestamente públicos dichos datos" [...]*».

[12] Sentencia del TJUE de 4 de julio de 2023, asunto C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), apartado 89.

[13] Sentencia del TJUE de 4 de julio de 2023, asunto C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), apartado 77.

respecto, sus Directrices sobre la toma de decisiones individuales automatizadas y la elaboración de perfiles a efectos del Reglamento 2016/679[14].

- **Compatibilidad de propósitos**: El artículo 6, apartado 4, del RGPD establece, para determinadas bases jurídicas, los criterios que un responsable del tratamiento debe tener en cuenta para determinar si el tratamiento para otro fin es compatible con el fin para el que se recogen inicialmente los datos personales. Esta disposición puede ser pertinente en el contexto del desarrollo y la implantación de modelos de IA, y su aplicabilidad debe ser evaluada por las autoridades de control.

- **Evaluaciones de impacto relativas a la protección de datos** («**DPIA**») (artículo 35 del RGPD): Las DPIA son un elemento importante de la rendición de cuentas, cuando es probable que el tratamiento en el contexto de los modelos de IA suponga un alto riesgo para los derechos y libertades de las personas físicas[15].

- **Principio de protección de datos por diseño** (artículo 25, apartado 1, del RGPD): La protección de datos desde el diseño es una salvaguardia esencial que deben evaluar las autoridades de control en el contexto del desarrollo y la implantación de un modelo de IA.

2.2 Nociones esenciales

18. Como observación preliminar, el CEPD desea aportar aclaraciones sobre la terminología y los conceptos que utiliza a lo largo del presente Dictamen, y solo a efectos del presente Dictamen:

- Los «**datos propios**» se refieren a los datos personales que el responsable del tratamiento ha recabado de los interesados.

- Los «**datos de terceros**» se refieren a los datos personales que los responsables del tratamiento no han obtenido de los interesados, sino que han recopilado o recibido de un tercero, por ejemplo de un intermediario de datos o recopilados mediante extracción de información (web scraping).

- «**Web scraping**» es una técnica comúnmente utilizada para recopilar información de fuentes en línea de acceso público. La información que se extrae, por ejemplo, de servicios como los medios de comunicación, las redes sociales, los debates en foros y los sitios web personales, puede contener datos personales.

- La solicitud se refiere al **«ciclo de vida» de los modelos de IA**, así como a diversas fases relativas, entre otras cosas, a la «creación», el «desarrollo», el «entrenamiento», la «actualización», el «ajuste», el «funcionamiento» o la «fase posterior al entrenamiento» de los modelos de IA. El CEPD reconoce que, dependiendo de las circunstancias, tales etapas pueden tener lugar en el desarrollo y despliegue de modelos de IA y pueden incluir el tratamiento de datos personales para diversos fines de tratamiento. No obstante, a efectos del presente Dictamen, el CEPD considera importante racionalizar la categorización de las fases que es probable que se produzcan. Por lo tanto, a efectos del presente Dictamen, el CEPD se refiere a la «**fase de desarrollo**» y a la «**fase**

[14] Directrices del Grupo de Trabajo del artículo 29 («**WP29**») sobre la toma de decisiones individuales automatizadas y la presentación de perfiles a efectos del Reglamento 2016/679, revisadas por última vez y adoptadas el 6 de febrero de 2018, refrendadas por el CEPD el 25 de mayo de 2018. Véase también la sentencia del TJUE de 7 de diciembre de 2023, asunto C-634/21, *SCHUFA Holding y otros* (ECLI:EU:C:2023:957).

[15] WP29 Directrices sobre la evaluación de impacto relativa a la protección de datos (DPIA) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento 2016/679, revisado y adoptado el 4 de abril de 2017, refrendado por el CEPD el 25 de mayo de 2018.

de despliegue». El desarrollo de un modelo de IA abarca todas las etapas previas a cualquier despliegue del modelo de IA, e incluye, entre otras cosas, el desarrollo del código, la recogida de datos personales para el entrenamiento, el tratamiento previo de los datos personales para el entrenamiento y el entrenamiento propiamente dicho. El despliegue de un modelo de IA abarca todas las etapas relacionadas con el uso de un modelo de IA y puede incluir cualquier operación realizada después de la fase de desarrollo. El CEPD sigue siendo consciente de la variedad de casos de uso y de sus posibles consecuencias en términos de tratamiento de datos personales; por lo tanto, las autoridades de control deben considerar si las observaciones formuladas en el presente Dictamen son pertinentes para el tratamiento que evalúan.

- El CEPD también subraya que, cuando sea necesario, el término «**entrenamiento**» se refiere a la parte de la fase de desarrollo en la que los modelos de IA aprenden de los datos para realizar la tarea prevista (como se explica en la siguiente sección del presente Dictamen).
- La noción y el alcance de **modelos de IA**, tal como la entiende el CEPD a efectos del presente Dictamen, se especifican con más detalle en la siguiente sección específica.

2.3 Modelos de IA en el contexto del Dictamen

19. La Ley de Inteligencia Artificial de la UE (en lo sucesivo, «**Ley de IA**»)[16] define *un «sistema de IA» como «un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales*»[17]. El considerando (12) de la Ley de IA explica además el concepto de «sistema de IA». Según esto, una característica principal de los sistemas de IA es su capacidad de inferencia. Las técnicas que permiten la inferencia al construir un sistema de IA incluyen el aprendizaje automático y enfoques basados en la lógica y el conocimiento.

20. Por otra parte, los «modelos de IA» solo se definen indirectamente en el Reglamento de IA: «*Aunque los modelos de IA son componentes esenciales de los sistemas de IA, no constituyen por sí mismos sistemas de IA. Los modelos de IA requieren que se les añadan otros componentes, como, por ejemplo, una interfaz de usuario, para convertirse en sistemas de IA. Los modelos de IA suelen estar integrados en los sistemas de IA y formar parte de dichos sistemas*»[18].

21. El CEPD entiende que la definición de modelo de IA propuesta en la solicitud es más restringida que la de la Ley de IA, ya que se refiere a «modelo de IA» «*para englobar el producto resultante de los mecanismos de entrenamiento que se aplican a un conjunto de datos de entrenamiento, en el contexto de la inteligencia artificial, el aprendizaje automático, el aprendizaje profundo u otros contextos de procesamiento relacionados*» y además especifica que «*El término se aplica a los modelos de IA que están destinados a someterse a un entrenamiento adicional, puesta a punto o desarrollo, así como a los modelos de IA que no lo están*.»[19]

[16] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).
[17] Artículo 3, apartado 1, del Reglamento de IA.
[18] Considerando 97 de la Ley de IA.
[19] Solicitud, p. 3.

22. Sobre esta base, el CEPD adoptó este Dictamen entendiendo que un sistema de IA se basará en un modelo de IA para llevar a cabo su objetivo previsto mediante la incorporación del modelo en un marco más amplio (por ejemplo, un sistema de IA para la atención al cliente podría utilizar un modelo de IA entrenado con datos históricos de conversaciones para proporcionar respuestas a las consultas de los usuarios).

23. Además, los modelos de IA (o «**modelos**») pertinentes para el presente Dictamen son los desarrollados a través de un proceso de entrenamiento. Este proceso de entrenamiento forma parte de la fase de desarrollo, en la que los modelos aprenden de los datos para realizar la tarea prevista. Por lo tanto, el proceso de entrenamiento requiere un conjunto de datos a partir del cual el modelo identificará y «aprenderá» patrones. En estos casos, el modelo utilizará diferentes técnicas para construir una representación del conocimiento extraído del conjunto de datos de entrenamiento. Este es el caso, en particular, del aprendizaje automático.

24. En la práctica, cualquier modelo de IA es un algoritmo, cuyo funcionamiento está determinado por un conjunto de elementos. Por ejemplo, los modelos de aprendizaje profundos suelen adoptar la forma de una red neural con múltiples capas compuestas de nodos conectados por bordes que tienen ponderaciones, que se ajustan durante el entrenamiento para aprender las relaciones entre los insumos y los resultados. Las características de un modelo simple de aprendizaje profundo serían: I) el tipo y el tamaño de cada capa, ii) la ponderación atribuida a cada borde (a veces denominado «parámetros»), iii) las funciones de activación[20] entre capas y, posiblemente, iv) otras operaciones que pueden producirse entre capas. Por ejemplo, cuando se forme un modelo sencillo de aprendizaje profundo para la clasificación de imágenes, las entradas (los «**píxeles de imagen**») se asociarán a los resultados, y las ponderaciones podrán ajustarse para producir el resultado adecuado la mayor parte del tiempo.

25. Otros ejemplos de modelos de aprendizaje profundo son los LLM y la IA generativa, que se utilizan, por ejemplo, para generar contenidos similares a los humanos y crear nuevos datos.

26. **Sobre la base de las consideraciones anteriores, en consonancia con la solicitud, el ámbito de aplicación del presente Dictamen solo abarca el subconjunto de modelos de IA que son el resultado de un entrenamiento de dichos modelos con datos personales.**

3 Sobre el fondo de la solicitud

3.1 Sobre la naturaleza de los modelos de IA en relación con la definición de datos personales

27. El artículo 4, apartado 1, del RGPD define los datos personales como «*toda información sobre una persona física identificada o identificable*» (es decir, el interesado). Además, el considerando 26 del RGPD establece que los principios de protección de datos no deben aplicarse a la información anónima, es decir, a la información que no se refiera a una persona física identificada o identificable, teniendo en cuenta «*todos los medios que [...] razonablemente pueda utilizar*» el responsable del tratamiento o cualquier otra persona. Esto incluye: i) los datos que nunca hayan estado relacionados con una persona física identificada o identificable, y ii) los datos personales que se hayan anonimizado de tal manera que el interesado no sea identificable o haya dejado de serlo.

[20] Es decir, funciones que calculan, sobre la base de las entradas y ponderaciones, la producción de un nodo neural que se enviará a continuación a la siguiente capa de la red neuronal.

28. En consecuencia, la pregunta 1[21] de la Solicitud puede responderse analizando si un modelo de IA resultante de un entrenamiento que implique el tratamiento de datos personales debe considerarse, en todos los casos, anónimo. Basándose en el enunciado de la pregunta, el CEPD se referirá en esta sección al proceso de «entrenamiento» de un modelo de IA.

29. En primer lugar y, ante todo, el CEPD desea presentar las siguientes consideraciones generales. Los modelos de IA, independientemente de si se entrenan con datos personales o no, suelen estar diseñados para hacer predicciones o sacar conclusiones, es decir, están diseñados para inferir. Además, los modelos de IA entrenados con datos personales suelen estar diseñados para hacer inferencias sobre personas distintas de aquellas cuyos datos personales se utilizaron para entrenar el modelo de IA. Sin embargo, algunos modelos de IA están diseñados específicamente para proporcionar datos personales relativos a las personas cuyos datos personales se utilizaron para entrenar el modelo, o de alguna manera para que dichos datos estén disponibles. En estos casos, dichos modelos de IA incluirán intrínsecamente (y normalmente necesariamente) información relativa a una persona física identificada o identificable, por lo que implicarán el tratamiento de datos personales. Por lo tanto, estos tipos de modelos de IA no pueden considerarse anónimos. Este sería el caso, por ejemplo, (i) de un modelo generativo afinado a partir de las grabaciones de voz de una persona para imitar su voz; o (ii) de cualquier modelo diseñado para responder con datos personales procedentes del entrenamiento cuando se le solicite información relativa a una persona concreta.

30. Sobre la base de las consideraciones anteriores, al responder a la pregunta 1 de la solicitud, el CEPD se centra en la situación de los modelos de IA que no están diseñados para proporcionar datos personales relacionados con los datos de entrenamiento.

31. El CEPD considera que, incluso cuando un modelo de IA no se ha diseñado intencionadamente para producir información relativa a una persona física identificada o identificable a partir de los datos de entrenamiento, la información procedente del conjunto de datos de entrenamiento, incluidos los datos personales, puede seguir siendo «absorbida» en los parámetros del modelo, a saber, representada a través de objetos matemáticos. Pueden diferir de los puntos de datos de entrenamiento originales, pero pueden conservar la información original de esos datos, que en última instancia puede ser extraída u obtenida de otro modo, directa o indirectamente, del modelo. Siempre que la información relativa a personas identificadas o identificables cuyos datos personales se utilizaron para entrenar el modelo pueda obtenerse de un modelo de IA con medios que sea razonablemente probable que se utilicen, puede concluirse que dicho modelo no es anónimo.

32. A este respecto, la solicitud afirma que «*Las publicaciones de investigación existentes ponen de relieve algunas posibles vulnerabilidades que pueden existir en los modelos de IA y que podrían dar lugar al tratamiento de datos personales*[22]*, así como el tratamiento de datos personales que puede continuar cuando los modelos se despliegan para su uso con otros datos, ya sea a través de interfaces de programación de aplicaciones (**«APIs»**) o interfaces de comandos»*[23].

[21] «*¿Se considera que el modelo de IA final, que ha sido entrenado utilizando datos personales, en todos los casos, no se ajusta a la definición de datos personales (tal como se establece en el artículo 4, apartado 1, del RGPD*)?»
[22] Como los ataques de inferencia de los miembros (OWASP), y los ataques de inversión de modelo (OWASP y Veale et al, 2018).
[23] Solicitud, pp. 1-2.

33. En la misma línea, la investigación sobre la extracción de datos de entrenamiento es especialmente dinámica[24]. Demuestra que es posible, en algunos casos, utilizar medios razonablemente probables para extraer datos personales de algunos modelos de IA, o simplemente obtener accidentalmente datos personales a través de interacciones con un modelo de IA (por ejemplo, como parte de un sistema de IA). Los continuos esfuerzos de investigación en este ámbito ayudarán a evaluar más a fondo los riesgos residuales de la regurgitación[25] y la extracción de datos personales en cualquier caso concreto.

34. **Basándose en las consideraciones anteriores, el CEPD considera que los modelos de IA entrenados con datos personales no pueden, en todos los casos, considerarse anónimos. En su lugar, la determinación de si un modelo de IA es anónimo debe evaluarse, sobre la base de criterios específicos, caso por caso.**

3.2 Sobre las circunstancias en las que los modelos de IA podrían considerarse anónimos y la demostración correspondiente

35. Por lo que respecta a la pregunta 1 de la solicitud[26], se pide al CEPD que aclare las circunstancias en las que un modelo de IA, que ha sido entrenado utilizando datos personales, puede considerarse anónimo. Por lo que se refiere a la pregunta 1, inciso i), letra a), [27]de la solicitud, se pide al CEPD que aclare qué pruebas o documentación deben tener en cuenta las autoridades de control a la hora de evaluar si un modelo de IA es anónimo.

3.2.1 Consideraciones generales sobre la anonimización en el contexto que nos ocupa

36. El uso de la expresión «*cualquier información*» en la definición de «*datos personales*» en el artículo 4, apartado 1, del RGPD refleja el objetivo de asignar un ámbito de aplicación amplio a este concepto, que abarca todo tipo de información, siempre que «*se refiera*» al interesado, que se identifique o pueda identificarse directa o indirectamente.

37. La información puede referirse a una persona física aun cuando esté técnicamente organizada o codificada (por ejemplo, en un formato legible únicamente por máquina, ya sea propio o abierto) de un modo que no haga inmediatamente evidente la relación con dicha persona física. En tales casos, las

[24] Véase, a este respecto, por ejemplo: (i) Veale Michael, Binns R. y Edwards L. 2018, *Algorithms that remember: model inversion attacks and data protection law* Phil. Trans. R. Soc. A 376: 20180083, disponible en http://dx.doi.org/10.1098/rsta.2018.0083; (ii) Brown H., Lee K., Mireshghallah F., Shokri R., y Tramèr F., *What Does it Mean for a Language Model to Preserve Privacy?*, 2022, ACM Digital Library, FAccT '22, 20 de junio de 2022, Seul, República de Corea, disponible en https://dl.acm.org/doi/abs/10.1145/3531146.3534642; (iii) Vassilev A., Oprea A., Fordyce A., Anderson H., *Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations*, enero de 2024, National Institute of Standards and Technology, disponible en https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf; (iv) Carlini N., Tramèr F., Wallace E., Jagielski M., Herbert-Voss A., Lee K., Roberts A., Brown T., Song D., Erlingsson U., Oprea A., Raffel C., *Extracting Training Data from Large Language Models*, arXiv:2012.07805v2 [cs.CR] 15 de junio de 2021, disponible en https://arxiv.org/pdf/2012.07805; (v) Fredrikson M., Jha S., Ristenpart T., *Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures*, ACM Digital Library, 12 de octubre de 2015, disponible en https://dl.acm.org/doi/abs/10.1145/2810103.2813677; (vi) Zhang Y., Jia R., Pei H., Wang W., Li B., Song D., *The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks*, arXiv:1911.07135v2 [cs.LG] 18 de abril de 2020, disponible en https://arxiv.org/pdf/1911.07135.

[25] En el caso de un sistema de IA basado en IA generativa, la regurgitación corresponde a la situación en la que los resultados se relacionarían directamente con los datos de entrenamiento.

[26] «*¿Cuáles son las circunstancias en las que esto podría ocurrir?*»

[27] «*En caso afirmativo, ¿cómo pueden demostrarse las medidas que se han tomado para garantizar que el modelo de IA no está tratando datos personales?*»

aplicaciones de software pueden utilizarse para identificar, reconocer y extraer fácilmente datos específicos. Esto es especialmente cierto en el caso de los modelos de IA en los que los parámetros representan relaciones estadísticas entre los datos de entrenamiento, y en los que puede ser posible extraer datos personales exactos o inexactos (porque se deducen estadísticamente), ya sea directamente de las relaciones entre los datos incluidos en el modelo, o consultando dicho modelo.

38. Dado que los modelos de IA no suelen contener registros que puedan estar directamente aislados o vinculados, sino parámetros que representan relaciones probabilísticas entre los datos contenidos en el modelo, en supuestos realistas puede ser posible deducir[28] información del modelo, como la inferencia de la afiliación. Por lo tanto, para que una autoridad de control acuerde con el responsable del tratamiento que un determinado modelo de IA pueda considerarse anónimo, deberá comprobar al menos si ha recibido pruebas suficientes de que, con medios razonables: I) los datos personales, relacionados con los datos de entrenamiento, no pueden extraerse[29] del modelo, y ii) los resultados obtenidos al consultar el modelo no se refieren a los interesados cuyos datos personales se utilizaron para entrenar el modelo.

39. Las autoridades de control deben tener en cuenta tres elementos a la hora de evaluar si se cumplen estas condiciones.

40. En primer lugar, las autoridades de control deben tener en cuenta los elementos identificados en los dictámenes más recientes del Grupo de Trabajo del Artículo 29 (WP29) o en las directrices del CEPD sobre el asunto. En lo que respecta a la anonimización a la fecha del presente Dictamen, las autoridades de control deberán considerar los elementos incluidos en el Dictamen 05/2014 del WP29 sobre Técnicas de Anonimización (el **«Dictamen 05/2014 del WP29»**), que establece que, si no es

[28] (i) Carlini N., Chien S., Nasr M., Song S., Terzis A., Tramer F., *Membership Inference Attacks From First Principles,* arXiv:2112.03570, disponible en https://arxiv.org/abs/2112.03570;
(ii) Creţu A.M, Guépin F., y De Montjoye Y.A, *Correlation inference attacks against machine learning models*. Health, B19, pp. Adv.10, eadj9260(2024). DOI:10.1126/sciadv.adj9260 disponible en https://www.science.org/doi/10.1126/sciadv.adj9260;
(iii) Dana L., Pydi M. S., Chevaleyre Y., *Memorization in Attention-only Transformers* arXiv:2411.10115v1 [cs.AI], 15 de noviembre de 2024, disponible en: https://arxiv.org/abs/2411.10115;
(iv) Gehrke M., Liebenow J., Mohammadi E. & Braun T. et al. *Lifting in Support of Privacy-Preserving Probabilistic Inference*. Künstl Intell, 13 de junio de 2024, disponible en https://doi.org/10.1007/s13218-024-00851-y:
(v) Hu H., *Membership Inference Attacks and Defenses on Machine Learning Models Literature*, disponible en: https://github.com/HongshengHu/membership-inference-machine-learning-literature;
(vi) Nasr M., Carlini N., Hayase J., Jagielski M., Cooper A. F., Ippolito D., Choquette-Choo C. A., Wallace E., Tramèr F., y Lee K., *Scalable Extraction of Training Data from (Production) Language Models*, arXiv:2311.17035 28 de noviembre de 2023, disponible en: https://arxiv.org/abs/2311.17035;
(vii) Shokri R., Stronati M., Song C., Shmatikov V., *Membership Inference Attacks against Machine Learning Models* arXiv:1610.05820v2 [cs.CR], 31 de marzo de 2017, disponible en https://arxiv.org/abs/1610.05820;
(viii) Staab R., Vero M., Mislav Balunović, Martin Vechev, 2024, *Beyond Memorization: Violating Privacy Via Inference with Large Language Models*, arXiv:2310.07298v2, 6 de mayo de 2024, disponible en https://arxiv.org/abs/2310.07298;
(ix) Wu F., Cui L., Yao S., Yu S., *InferenceAttacks in Machine Learning as a Service: A Taxonomy, Review, and Promising Directions* arXiv:2406.02027v1 [cs.LG], 27 de junio de 2024, disponible en https://arxiv.org/abs/2406.02027v1;
(x) Zhang J., Das D., Kamath G., Tramèr F., *Membership Inference Attacks Cannot Prove that a Model Was Trained On Your Data* arXiv:2409.19798v1, [cs.LG], 29 de septiembre de 2024, disponible en https://arxiv.org/abs/2409.19798;
(xi) Zhou Z., Xiang J., Chen C., and Su S., *Quantifying and Analyzing Entity-Level Memorization in Large Language Models*, arXiv:2308.15727v2 [cs.CL], 5 de noviembre de 2023, disponible en: https://arxiv.org/abs/2308.15727.

[29] La extracción incluye, en particular, el caso en que los datos personales se deducen del propio modelo de IA, con escasa o nula utilización de las interfaces de consulta.

posible identificar, vincular e inferir información del conjunto de datos supuestamente anónimos, los datos pueden considerarse anónimos[30]. También establece que «*siempre que una propuesta no cumpla uno de los criterios, deberá realizarse una evaluación exhaustiva de los riesgos de identificación*»[31]. **Dada la probabilidad de extracción e inferencia antes mencionada, el CEPD considera que es muy probable que los modelos de IA requieran una evaluación tan exhaustiva de los riesgos de identificación.**

41. En segundo lugar, esta evaluación deberá realizarse teniendo en cuenta «*todos los medios razonablemente susceptibles de ser utilizados*» por el responsable del tratamiento u otra persona para identificar a las personas[32], y la determinación de dichos medios deberá basarse en factores objetivos, como se explica en el considerando 26 del RGPD, que pueden incluir:
    a. las características de los propios datos de entrenamiento, el modelo de IA y el procedimiento de entrenamiento[33];
    b. el contexto en el que el modelo de IA se pone en servicio o se trata[34];
    c. la información adicional que permitiría la identificación y podría estar a disposición de la persona determinada;
    d. los costes y el tiempo que la persona necesitaría para obtener dicha información adicional (en caso de que no esté ya a su disposición)[35]; y
    e. la tecnología disponible en el momento del tratamiento, así como los avances tecnológicos[36].

42. En tercer lugar, las autoridades de control deberán considerar si los responsables del tratamiento han evaluado el riesgo de identificación por parte del responsable del tratamiento y por parte de diferentes tipos de *«otras personas»*, incluidos los terceros no deseados que acceden al modelo de IA, teniendo también en cuenta si puede considerarse razonablemente que pueden acceder a los datos en cuestión o tratarlos.

43. **En resumen, el CEPD considera que, para que un modelo de IA se considere anónimo, utilizando medios razonables, tanto (i) la probabilidad de extracción directa (incluida la probabilística) de datos personales relativos a las personas cuyos datos personales se utilizaron para entrenar el modelo; como (ii) la probabilidad de obtener, intencionadamente o no, dichos datos personales a partir de consultas, deberían ser insignificantes[37] para cualquier interesado**. **Por defecto, las autoridades de control deberán considerar que es probable que los modelos de IA requieran una evaluación exhaustiva de la probabilidad de identificación para llegar a una conclusión sobre su posible carácter anónimo. Esta probabilidad deberá evaluarse teniendo en cuenta «*todos los medios que sea***

[30] Dictamen 5/2014 del WP29, p. 24.
[31] Dictamen 5/2014 del WP29, p. 24.
[32] Sentencia del TJUE de 19 de octubre de 2016, asunto C-582/14, *Breyer/Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), apartado 43.
[33] Esto incluye características como la unicidad de los registros en los datos de entrenamiento, la precisión de la información, la agregación, la aleatorización y, en particular, cómo estas afectan a la vulnerabilidad a la identificación.
[34] Esto incluye elementos contextuales, como la limitación del acceso solo a determinadas personas y garantías jurídicas.
[35] Sentencia del TJUE de 7 de marzo de 2024, asunto C-479/22 P, *OC/Comisión Europea* (ECLI:EU:C:2024:215), apartado 50.
[36] Sentencia del TJUE de 7 de marzo de 2024, asunto C-479/22 P, *OC/Comisión Europea* (ECLI:EU:C:2024:215), apartado 50.
[37] Sentencia del TJUE de 19 de octubre de 2016, asunto C-582/14, *Breyer/Bundesrepublik Deutschland* (ECLI:EU:C:2016:779), apartado 46, y sentencia del TJUE de 7 de marzo de 2024, asunto C-479/22 P, *OC/Comisión Europea* (ECLI:EU:C:2024:215), apartado 51.

***razonablemente probable que sean utilizados*» por el responsable del tratamiento u otra persona, y también deberá considerarse la (re)utilización o divulgación no deseadas del modelo.**

3.2.2 Elementos para evaluar la probabilidad residual de identificación

44. Si bien podrían adoptarse medidas tanto en las fases de desarrollo como de despliegue para reducir la probabilidad de obtener datos personales de un modelo de IA, la evaluación del anonimato de un modelo de IA también deberá considerar el acceso directo al modelo.

45. Además, las autoridades de control deberán evaluar, caso por caso, si las medidas aplicadas por el responsable del tratamiento para garantizar y demostrar que un modelo de IA es anónimo son adecuadas y eficaces.

46. En particular, la conclusión de la evaluación de una autoridad de control podría diferir entre un modelo de IA públicamente disponible, al que puede acceder un número desconocido de personas con una gama desconocida de métodos para tratar y extraer datos personales, y un modelo interno de IA al que solo pueden acceder los empleados. Si bien en ambos casos las autoridades de control deben verificar que los responsables del tratamiento han cumplido su obligación de rendición de cuentas en virtud del artículo 5, apartado 2, y del artículo 24 del RGPD los «*medios razonablemente probables de ser utilizados*» por otras personas pueden repercutir en el alcance y la naturaleza de los posibles supuestos que deben tenerse en cuenta. Por lo tanto, en función del contexto del desarrollo y la implantación del modelo, las autoridades de control pueden considerar diferentes niveles de pruebas y resistencia a los ataques.

47. A este respecto, el CEPD proporciona a continuación una lista no prescriptiva y no exhaustiva de posibles elementos que pueden tener en cuenta las autoridades de control a la hora de evaluar la invocación de anonimato de un responsable del tratamiento. Otros enfoques pueden ser posibles si ofrecen un nivel de protección equivalente, en particular teniendo en cuenta el estado de la técnica.

48. La presencia o ausencia de los elementos enumerados a continuación no es un criterio concluyente para evaluar el anonimato de un modelo de IA.

3.2.2.1 Diseño de modelos de IA

49. En lo que respecta al diseño de modelos de IA, las autoridades de control deberán evaluar los enfoques adoptados por los responsables del tratamiento durante la fase de desarrollo. A este respecto, deberá tenerse en cuenta la aplicación y la eficacia de cuatro ámbitos clave (que se indican a continuación).

Selección de fuentes

50. La primera área de evaluación consiste en examinar la selección de fuentes utilizadas para entrenar el modelo de IA. Esto incluye una evaluación, por parte de las autoridades de control, de cualquier medida adoptada para evitar o limitar la recogida de datos personales, incluyendo, entre otras cosas, i) la idoneidad de los criterios de selección; ii) la pertinencia y adecuación de las fuentes elegidas teniendo en cuenta la finalidad o finalidades previstas; y iii) si se han excluido fuentes inadecuadas.

Preparación y minimización de datos

51. El segundo ámbito de evaluación se refiere a la preparación de los datos para la fase de entrenamiento. Las autoridades de control deberán examinar, en particular: (i) si se ha considerado el uso de datos anónimos o personales que hayan sido objeto de seudonimización; y (ii) en caso de que se haya decidido no utilizar tales medidas, los motivos de esta decisión, teniendo en cuenta la finalidad prevista; (iii) las estrategias y técnicas de minimización de datos empleadas para restringir el volumen de datos personales incluidos en el proceso de entrenamiento; y (iv) cualquier proceso de filtrado de

datos aplicado antes del entrenamiento de modelos con el fin de eliminar datos personales irrelevantes.

Opciones metodológicas en relación con el entrenamiento

52. El tercer ámbito de evaluación se refiere a la selección de métodos robustos en el desarrollo de modelos de IA. Las autoridades de control deberán evaluar las opciones metodológicas que puedan reducir o eliminar significativamente la identificabilidad, en particular, entre otras: (i) si dicha metodología utiliza métodos de regularización para mejorar la generalización de los modelos y reducir el exceso de ajustes; y, lo que es más importante, (ii) si el responsable del tratamiento aplicó técnicas adecuadas y eficaces de conservación de la privacidad (por ejemplo, la privacidad diferencial).

Medidas relativas a los resultados del modelo

53. El último ámbito de evaluación se refiere a los métodos o medidas añadidos al propio modelo de IA que puedan no afectar al riesgo de extracción directa de datos personales para el modelo por parte de cualquier persona que acceda directamente a él, pero que pueda reducir la probabilidad de obtener datos personales relacionados con los datos de entrenamiento obtenidos de consultas.

3.2.2.2 Análisis del modelo de IA

54. Para que las autoridades de control evalúen la solidez del modelo de IA diseñado en relación con la anonimización, un primer paso es asegurarse de que el diseño se ha desarrollado según lo previsto y está sujeto a una gobernanza de ingeniería eficaz. Las autoridades deberán evaluar si los responsables del tratamiento han llevado a cabo auditorías (internas o externas) basadas en documentos que incluyan una evaluación de las medidas elegidas y de su impacto para limitar la probabilidad de identificación. Esto podría incluir el análisis de los informes de las revisiones de códigos, así como un análisis teórico que documente la idoneidad de las medidas elegidas para reducir la probabilidad de reidentificación del modelo en cuestión.

3.2.2.3 Pruebas del modelo de IA y resistencia a los ataques

55. Por último, las autoridades de control deberán tener en cuenta el alcance, la frecuencia, la cantidad y la calidad de las pruebas que el responsable del tratamiento haya realizado sobre el modelo. En particular, las autoridades deberán tener en cuenta que las pruebas que se hayan realizado correctamente y que abarquen ataques muy conocidos y de última generación, solo se pueden considerar como pruebas que demuestran la resistencia a dichos ataques. En la fecha del presente dictamen, esto podría incluir, entre otras cosas, pruebas estructuradas contra: (i) atributo e inferencia de los miembros; (ii) exfiltración; (iii) regurgitación de los datos de entrenamiento; (iv) inversión del modelo; o (v) ataques de reconstrucción.

3.2.2.4 Documentación

56. Los artículos 5, 24, 25 y 30 del RGPD y, en casos de probable alto riesgo para los derechos y libertades de los interesados, el artículo 35 del RGPD, exigen que los responsables del tratamiento documenten adecuadamente sus operaciones de tratamiento. Esto también se aplica a cualquier tratamiento que incluya el entrenamiento de un modelo de IA, incluso si el objetivo del tratamiento es la anonimización. Las autoridades de control deberán tener en cuenta dicha documentación y cualquier evaluación periódica de los riesgos consiguientes para el tratamiento realizado por los responsables del tratamiento, ya que son pasos fundamentales para demostrar que no se tratan datos personales.

57. **El CEPD considera que las autoridades de control deberán tener en cuenta la documentación siempre que sea necesario evaluar una alegación de anonimato en relación con un modelo de IA determinado. El CEPD señala que, si una autoridad de control no puede confirmar, tras evaluar la reclamación de anonimato, también a la luz de la documentación, que se adoptaron medidas eficaces para anonimizar el modelo de IA, la autoridad de control estaría en condiciones de**

considerar que el responsable del tratamiento no ha cumplido sus obligaciones de rendición de cuentas en virtud del artículo 5, apartado 2, del RGPD. Por lo tanto, también deberá tenerse en cuenta el cumplimiento de otras disposiciones del RGPD.

58. Lo ideal sería que las autoridades de control verificaran si la documentación del responsable del tratamiento incluye:

a. cualquier información relativa a las evaluaciones de impacto relativas a la protección de datos (EIPD), incluidas las evaluaciones y decisiones que hayan determinado que una EIPD no era necesaria;

b. cualquier consejo o comentario proporcionado por el delegado de protección de datos («**DPD**») (cuando se haya designado -o debiera haberse designado- un DPD);

c. información sobre las medidas técnicas y organizativas adoptadas durante el diseño del modelo de IA para reducir la probabilidad de identificación, incluido el modelo de amenaza y las evaluaciones de riesgos en las que se basan estas medidas. Esto deberá incluir las medidas específicas para cada fuente de conjuntos de datos de entrenamiento, incluidas las URL fuente pertinentes y las descripciones de las medidas adoptadas (o ya adoptadas por proveedores terceros de conjuntos de datos);

d. las medidas técnicas y organizativas adoptadas en todas las fases a lo largo del ciclo de vida del modelo que bien hayan contribuido a la ausencia de datos personales en el modelo bien hayan verificado dicha ausencia;

e. la documentación que demuestre la resistencia teórica del modelo de IA a las técnicas de reidentificación, así como los controles diseñados para limitar o evaluar el éxito y el impacto de los principales ataques (regurgitación, ataques de inferencia de afiliación, exfiltración, etc.). Esto podrá incluir, en particular: (i) la relación entre la cantidad de datos de entrenamiento y el número de parámetros del modelo, incluido el análisis de su impacto en el modelo[38]; (ii) las métricas sobre la probabilidad de reidentificación basadas en el estado actual de la técnica; (iii) los informes sobre cómo se ha probado el modelo (quién, cuándo, cómo y en qué medida) y (iv) los resultados de las pruebas;

f. la documentación facilitada al responsable o responsables del tratamiento que desplieguen el modelo o a los interesados, en particular la documentación relativa a las medidas adoptadas para reducir la probabilidad de identificación y en relación con los posibles riesgos residuales.

3.3 Sobre la adecuación del interés legítimo como base jurídica para el tratamiento de datos personales en el contexto del desarrollo y el despliegue de modelos de IA

59. Para responder a las preguntas 2 y 3 de la solicitud, el CEPD proporcionará en primer lugar observaciones generales sobre algunos aspectos importantes que las autoridades de control deberán tener en cuenta, independientemente de la base jurídica del tratamiento, al evaluar cómo pueden los

[38] Ricciato F., *A Cautionary Reflection on (Pseudo-)Synthetic Data from Deep learning on Personal Data*, Privacy in Statistical Databases Conference (PSD 2024), Antibes, Francia, septiembre de 2024, diapositivas disponibles en: https://cros.ec.europa.eu/system/files/2024-10/20240926_PSD2024_Ricciato_v6_1.pdf y Belkin M., Hsu D., Ma S., & Mandal S. (2019), *Reconciling modern machine-learning practice and the classical bias-variance trade-off*. Actas de la Academia Nacional de Ciencias, 24 de julio de 2019, 116(32) 15849-15854, disponible en: https://www.pnas.org/doi/10.1073/pnas.1903070116

responsables del tratamiento demostrar el cumplimiento del RGPD en el contexto de los modelos de IA. A continuación, sobre la base de las Directrices 1/2024 sobre el tratamiento de datos personales basado en el artículo 6, apartado 1, letra f) del RGPD[39], el CEPD examinará los tres pasos que requiere la evaluación del interés legítimo en el contexto del desarrollo y la implantación de modelos de IA.

3.3.1 Observaciones generales

60. El CEPD recuerda que el RGPD no establece ninguna jerarquía entre las diferentes bases jurídicas establecidas en el artículo 6, apartado 1, del RGPD[40].

61. El artículo 5 del RGPD establece los principios relativos al tratamiento de datos personales. El CEPD destaca aquellos que son significativos para el presente Dictamen y deberán al menos ser tenidos en cuenta por las autoridades de control a la hora de evaluar modelos de IA específicos, así como los requisitos más pertinentes de otras disposiciones del RGPD, teniendo en cuenta el ámbito de aplicación del presente Dictamen.

62. **Principio de responsabilidad proactiva** (artículo 5, apartado 2, del RGPD) - Este principio establece que el responsable del tratamiento será responsable del cumplimiento del RGPD y deberá ser capaz de demostrarlo. En este sentido, las funciones y responsabilidades de las partes que tratan datos personales en el contexto del desarrollo o despliegue de un modelo de IA deberán evaluarse antes de que tenga lugar el tratamiento, con el fin de definir las obligaciones de los responsables o corresponsables del tratamiento, y de los encargados del tratamiento (si los hubiera), desde el principio.

63. **Principios de licitud, lealtad y transparencia** (artículo 5, apartado 1, letra a) del RGPD) - Al evaluar la licitud del tratamiento en el contexto de los modelos de IA, a la luz del artículo 6, apartado 1 del RGPD, el CEPD considera útil distinguir las distintas fases del tratamiento de datos personales[41]. El principio de lealtad, que está estrechamente relacionado con el principio de transparencia, exige que los datos personales no sean tratados mediante métodos injustos o mediante engaño, o de una manera «*injustificablemente perjudicial, ilícitamente discriminatoria, inesperada o engañosa para el interesado*»[42]. Teniendo en cuenta la complejidad de las tecnologías implicadas, la información sobre el tratamiento de datos personales en el marco de los modelos de IA debe facilitarse, por tanto, de manera accesible, comprensible y fácil de usar[43]. La transparencia sobre el tratamiento de datos personales incluye, en particular, el cumplimiento de las obligaciones de información establecidas en los artículos 12 a 14 del RGPD[44], que también exigen, en caso de toma de decisiones automatizada, incluida la elaboración de perfiles, información significativa sobre la lógica implicada, así como la

[39] Véanse las Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024.
[40] Ibid., apartado 1.
[41] Informe del CEPD sobre el trabajo realizado por el Grupo de Trabajo de ChatGPT, adoptado el 23 de mayo de 2024, apartado 14.
[42] Informe del CEPD sobre el trabajo realizado por el Grupo de Trabajo de ChatGPT, adoptado el 23 de mayo de 2024, apartado 23; Directrices 4/2019 del CEPD sobre el artículo 25 Protección de datos por diseño y por defecto, versión 2.0, adoptadas el 20 de octubre de 2020, apartado 69; Directrices del Grupo de Trabajo del Artículo 29 sobre transparencia en virtud del Reglamento 2016/679, revisadas y adoptadas el 11 de abril de 2018, refrendadas por el CEPD el 25 de mayo de 2018, apartado 2.
[43] Directrices del Grupo de Trabajo del artículo 29 sobre transparencia en virtud del Reglamento (UE) 2016/679, revisadas y adoptadas el 11 de abril de 2018, refrendadas por el CEPD el 25 de mayo de 2018, apartado 5.
[44] Véase también el considerando 39 del RGPD que establece que «*Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados [...]*».

importancia y las consecuencias previstas del tratamiento para el interesado[45]. Teniendo en cuenta que las fases de desarrollo de los modelos de IA pueden implicar la recopilación de grandes cantidades de datos de fuentes de acceso público (por ejemplo, mediante técnicas de *web scraping*), el recurso a la excepción prevista en el artículo 14, apartado 5, letra b), del RGPD se limita estrictamente a los casos en que se cumplen plenamente los requisitos de esta disposición[46].

64. **Principios de limitación de la finalidad y de minimización de datos** (artículo 5, apartado 1, letras b) y c), del RGPD) - De conformidad con el principio de minimización de datos, el desarrollo y despliegue de modelos de IA requiere que los datos personales sean adecuados, pertinentes y necesarios en relación con la finalidad. Esto puede incluir el tratamiento de datos personales para evitar los riesgos de posibles sesgos y errores cuando esto se identifica de forma clara y específica dentro de la finalidad, y los datos personales son necesarios para dicha finalidad (por ejemplo, no puede alcanzarse eficazmente mediante el tratamiento de otros datos, incluidos datos sintéticos o anonimizados)[47]. El WP29 ya subrayó que «*la finalidad de la recogida debe identificarse de forma clara y específica* [...]»[48]. A la hora de evaluar si la finalidad perseguida es legítima, específica y explícita, y si el tratamiento cumple el principio de minimización de datos, hay que identificar en primer lugar la actividad de tratamiento en cuestión. En particular, las diferentes fases dentro de las fases de desarrollo o despliegue pueden constituir la misma actividad de tratamiento o actividades diferentes, y pueden implicar sucesivos responsables o corresponsables del tratamiento. En algunos casos, es posible determinar la finalidad que se perseguirá durante la implantación del modelo de IA en una fase temprana de desarrollo. Incluso en los casos en los que no sea así, debería estar claro el contexto de la implantación y, por lo tanto, habría que considerar de qué manera este contexto influye en la finalidad del desarrollo. Al revisar la finalidad del tratamiento en una determinada fase de desarrollo, las autoridades de control deben esperar cierto grado de detalle por parte del responsable o responsables del tratamiento y una explicación de cómo estos detalles dan forma a la finalidad del tratamiento. Esto puede incluir, por ejemplo, información sobre el tipo de modelo de IA desarrollado, sus funcionalidades previstas y cualquier otro contexto pertinente que ya se conozca en esa fase. El contexto del despliegue también podría incluir, por ejemplo, si se está desarrollando un modelo para su despliegue interno, si el responsable del tratamiento tiene la intención de vender o distribuir el modelo a terceros después de su desarrollo, o incluso si el modelo está destinado principalmente a ser desplegado con fines de investigación o comerciales.

65. **Derechos de los interesados** (Capítulo III del RGPD) - A pesar de la necesidad de que las autoridades de control garanticen el respeto de todos los derechos de los interesados cuando los responsables del tratamiento desarrollen e implanten modelos de IA, el CEPD recuerda que siempre que un responsable del tratamiento invoque el interés legítimo como base jurídica, el derecho de oposición previsto en el artículo 21 del RGPD se aplica y debe garantizarse[49].

[45] Artículo 13, apartado 2, letra f), del RGPD y artículo 14, apartado 2, letra g), del RGPD.
[46] Informe del CEPD sobre el trabajo realizado por el Grupo de Trabajo de ChatGPT, aprobado el 23 de mayo de 2024, apartado 27.
[47] Además, el artículo 10, apartado 5, de la Ley de IA establece normas específicas para el tratamiento de categorías especiales de datos personales en relación con los sistemas de IA de alto riesgo con el fin de garantizar la detección y corrección de sesgos.
[48] Grupo de Trabajo del Artículo 29: Dictamen 03/2013 sobre limitación de la finalidad (WP203), pp. 15-16.
[49] De conformidad con el artículo 21 del RGPD, si un interesado se opone, por motivos relacionados con su situación particular, al tratamiento de los datos personales que le conciernen, el responsable del tratamiento

3.3.2 Consideraciones sobre las tres etapas de la evaluación del interés legítimo en el contexto del desarrollo y la implantación de modelos de IA

66. A fin de determinar si un determinado tratamiento de datos personales puede basarse en el artículo 6, apartado 1, letra f), del RGPD, las autoridades de control deberán verificar que los responsables del tratamiento hayan evaluado y documentado cuidadosamente si se cumplen las tres condiciones acumulativas siguientes: (i) la persecución de un interés legítimo por parte del responsable del tratamiento o de un tercero; (ii) el tratamiento es necesario para perseguir el interés legítimo; y (iii) sobre el interés legítimo no prevalecen los intereses ni los derechos y libertades fundamentales de los interesados[50].

3.3.2.1 Primer paso - Persecución de un interés legítimo por parte del responsable del tratamiento o de un tercero

67. Un interés es el interés o beneficio más amplio que un responsable del tratamiento o un tercero puede tener al participar en una actividad de tratamiento específica[51]. Aunque el RGPD y el TJUE reconocen varios intereses como legítimos[52], la evaluación de la legitimidad de un interés determinado debe ser el resultado de un análisis caso por caso.

68. Como recuerda el CEPD en sus Directrices sobre el interés legítimo[53], un interés puede considerarse legítimo si se cumplen los tres criterios acumulativos siguientes:

a. El interés es lícito[54];

b. El interés se articula de forma clara y precisa; y

---

dejará de tratar esos datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado o para la formulación, el ejercicio o la defensa de reclamaciones. Por lo tanto, los dos aspectos que deberán tener en cuenta las autoridades de control son si el responsable del tratamiento puede demostrar tales razones legítimas imperiosas y si puede ejercerse el derecho de oposición.

[50] TJUE, sentencia de 4 de julio de 2023, asunto C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), apartado 106; TJUE, sentencia de 11 de diciembre de 2019, asunto C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), apartado 40. Véanse también las Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0 adoptada el 8 de octubre de 2024, apartado 12 y siguientes. Como se recuerda en dichas Directrices, esta *«evaluación debe realizarse al inicio del tratamiento, con la participación del delegado de protección de datos (si se ha designado), y debe ser documentada por el responsable del tratamiento de conformidad con el principio de rendición de cuentas establecido en el artículo 5, apartado 2, del RGPD*».

[51] Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 14.

[52] Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 16.

[53] Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 17.

[54] TJUE, sentencia de 4 de octubre de 2024, asunto C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), apartado 49, en la que el TJUE subrayó que un interés legítimo no puede ser contrario a la ley. A este respecto, el CEPD subraya que, en su caso, deben tenerse en cuenta los marcos legislativos a la hora de evaluar la licitud de un interés determinado. Véase, por ejemplo: el artículo 26, apartado 3, y el artículo 28 del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) («DSA») sobre publicidad prohibida dirigida a menores; el artículo 5, apartados 1 y 2, de la Ley de IA sobre prácticas de IA prohibidas (prácticas de manipulación y por debajo del umbral de conciencia); el tratamiento en violación de los derechos de propiedad intelectual y las disposiciones de la Directiva (UE) 2019/790 sobre los derechos de autor y derechos afines en el mercado único digital.

c. El interés es real y presente, no especulativo.

69. Sin perjuicio de las otras dos etapas exigidas por la evaluación del interés legítimo, los siguientes ejemplos pueden constituir un interés legítimo en el contexto de los modelos de IA: (i) desarrollar el servicio de un agente conversacional para ayudar a los usuarios; (ii) desarrollar un sistema de IA para detectar contenidos o comportamientos fraudulentos; y (iii) mejorar la detección de amenazas en un sistema de información.

3.3.2.2 Segundo paso - Análisis de la necesidad del tratamiento para perseguir el interés legítimo

70. El segundo paso de la evaluación consiste en determinar si el tratamiento de los datos personales es necesario para los fines del interés o intereses legítimos perseguidos[55] («prueba de necesidad»).

71. El considerando 39 del RGPD señala que «*Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios»*. De acuerdo con las orientaciones anteriores del TJUE y del CEPD, la condición relativa a la necesidad del tratamiento debe examinarse a la luz de los derechos y libertades fundamentales de los interesados, y en conjunción con el principio de minimización de datos consagrado en el artículo 5, apartado 1, letra c), del RGPD[56].

72. La metodología a la que se refiere el TJUE tiene en cuenta el contexto del tratamiento, así como los efectos sobre el responsable del tratamiento y sobre los interesados. Por lo tanto, la evaluación de la necesidad implica dos elementos: (i) si la actividad de tratamiento permitirá la persecución de la finalidad[57]; y (ii) si no existe una forma menos intrusiva de perseguir esta finalidad[58].

---

[55] Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartados 28 a 30.

[56] TJUE, sentencia de 4 de julio de 2023, asunto C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), apartados 108 y 109, en referencia también al TJUE, sentencia de 11 de diciembre de 2019, asunto C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), apartado 48; TJUE, sentencia de 9 de noviembre de 2010, asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke (ECLI:EU:C:2010:662), apartados 85 y 86; TJUE, sentencia de 22 de junio de 2021, asunto C-439/19, *Latvijas Republikas Saeima* (ECLI:EU:C:2021:504), apartados 98, 109, 110, 113. Véanse también, por ejemplo: Directrices 3/2019 del CEPD sobre el tratamiento de datos personales a través de dispositivos de vídeo, versión 2.0, adoptadas el 29 de enero de 2020, apartados 24-26 y 73; Directrices 2/2019 del CEPD sobre el tratamiento de datos personales con arreglo al artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados, versión 2.0, adoptadas el 8 de octubre de 2019, apartados 23-25; Dictamen 11/2024 del CEPD sobre el uso del reconocimiento facial para racionalizar el flujo de pasajeros en los aeropuertos, versión 1.1, adoptada el 23 de mayo de 2024, apartado 27.

[57] Véase TJUE, sentencia de 16 de diciembre de 2008, asunto C-524/06, *Heinz Huber/Bundesrepublik Deutschland* (ECLI:EU:C:2008:724), apartado 66. También en el mismo asunto, véanse las conclusiones del Abogado General Poiares Maduro en el asunto C-524/06, *Heinz Huber/Bundesrepublik Deutschland* (ECLI:EU:C:2008:194), apartado 16, en las que se afirma lo siguiente: «*el criterio que aquí debe seguirse es el de la eficacia, e incumbe al Tribunal nacional aplicarlo. La pregunta que éste debe hacerse es si existen otras formas de tratamiento de datos a través de las cuales las autoridades de inmigración podrían aplicar la normativa sobre régimen de residencia. En el supuesto de que dicho Tribunal responda afirmativamente a esa pregunta, deberá declararse que el almacenamiento y tratamiento de datos centralizado para ciudadanos de la Unión es ilegal. No es necesario que el sistema alternativo sea el más eficaz o adecuado; basta con que pueda cumplir sus objetivos adecuadamente. Dicho de otro modo, aunque el registro central sea más eficaz, apropiado o manejable que sus alternativas (como los registros descentralizados, locales), han de preferirse estos últimos si pueden ser utilizados para indicar el régimen de residencia de ciudadanos de la Unión»*.

[58] Véase TJUE, sentencia de 27 de septiembre de 2017, asunto C-73/16, *Peter Puškár* (ECLI:EU:C:2017:725), apartado 113: *Así pues, corresponde al tribunal remitente comprobar si la elaboración de la lista controvertida y la inclusión en ella de los interesados son adecuadas para cumplir los objetivos que persiguen y si no existen medios menos gravosos para alcanzarlos*»; véanse también, por ejemplo, las conclusiones del Abogado General

73. Por ejemplo, y según el caso, el volumen previsto de datos personales implicados en el modelo de IA deberá evaluarse a la luz de alternativas menos intrusivas que puedan estar razonablemente disponibles para lograr con la misma eficacia la finalidad del interés legítimo perseguido. Si la consecución de la finalidad también es posible a través de un modelo de IA que no implique el tratamiento de datos personales, deberá considerarse que el tratamiento de datos personales no es necesario. Esto es especialmente relevante para el desarrollo de modelos de IA. Al evaluar si se cumple la condición de necesidad, las autoridades de control deberán prestar especial atención a la cantidad de datos personales tratados y si es proporcionado perseguir el interés legítimo en juego, también a la luz del principio de minimización de datos.

74. La evaluación de la necesidad también debe tener en cuenta el contexto más amplio del tratamiento previsto de los datos personales. La existencia de medios menos intrusivos para los derechos y libertades fundamentales de los interesados puede variar en función de si el responsable del tratamiento tiene una relación directa con los interesados (datos propios) o no (datos de terceros). El TJUE proporcionó algunas consideraciones que deben tenerse en cuenta al analizar la necesidad del tratamiento de los datos propios a efectos del interés o los intereses legítimos perseguidos (aunque en el contexto de la divulgación de dichos datos a terceros)[59].

75. La aplicación de garantías técnicas para proteger los datos personales también puede contribuir a cumplir la prueba de necesidad. Esto podría incluir, por ejemplo, la aplicación de medidas como las identificadas en la sección 3.2.2 de tal manera que no se logre la anonimización, pero que siga reduciendo la facilidad con la que se puede identificar a los interesados. El CEPD observa que algunas de estas medidas, cuando no son necesarias para cumplir el RGPD, pueden constituir salvaguardias adicionales, como se analiza con más detalle en la subsección «medidas de mitigación» de la sección 3.3.2.3[60].

3.3.2.3 Tercer paso - Prueba de ponderación

76. El tercer paso de la evaluación del interés legítimo es el «**ejercicio de ponderación**» (también denominado en el presente documento «**prueba de ponderación**»)[61]. Este paso consiste en identificar y describir los diferentes derechos e intereses opuestos en juego[62], es decir, por un lado, los intereses, los derechos y libertades fundamentales de los interesados y, por otro, los intereses del responsable del tratamiento o de un tercero. A continuación, deberán considerarse las circunstancias específicas del caso para demostrar que el interés legítimo constituye una base jurídica adecuada para las actividades de tratamiento en cuestión[63].

Rantos en el asunto C-252/21, *Meta/Bundeskartellamt*, ECLI:EU:C:2022:704, apartado 61, en el que se afirma lo siguiente: *«[...] Por lo tanto, debe existir, una relación estrecha entre el tratamiento y el interés perseguido, a falta de alternativas más respetuosas con la protección de datos personales, puesto que no es suficiente que el tratamiento sea simplemente útil para el responsable del tratamiento*».

[59] TJUE, sentencia de 4 de octubre de 2024, asunto C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), apartados 51-53.

[60] Véanse las Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 57.

[61] Véanse las Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartados 31 a 60.

[62] Véanse las Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 32.

[63] Véanse las Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 32, en las que también se hace referencia a la sentencia del TJUE de 4 de julio de 2023, asunto C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), apartado 110.

Intereses, derechos y libertades fundamentales de los interesados

77. El artículo 6, apartado 1, letra f), del RGPD establece que, al evaluar los diferentes componentes en el contexto de la prueba de ponderación, el responsable del tratamiento deberá tener en cuenta los intereses y los derechos y libertades fundamentales de los interesados. Los intereses de los interesados son aquellos que pueden verse afectados por el tratamiento en cuestión. En el contexto de la fase de desarrollo de un modelo de IA, estos pueden incluir, entre otros, el interés en la autodeterminación y el mantenimiento del control sobre los propios datos personales (por ejemplo, los datos recogidos para desarrollar el modelo). En el contexto del despliegue de un modelo de IA, los intereses de los interesados pueden incluir, entre otros, los intereses en mantener el control sobre los propios datos personales (por ejemplo, los datos tratados una vez desplegado el modelo), los intereses financieros (por ejemplo, cuando el interesado utiliza un modelo de IA para generar ingresos, o una persona lo utiliza en el contexto de su actividad profesional), los beneficios personales (por ejemplo, cuando se utiliza un modelo de IA para mejorar la accesibilidad a determinados servicios) o los intereses socioeconómicos (por ejemplo, cuando un modelo de IA permite disfrutar de una mejor asistencia sanitaria, o facilita el ejercicio de un derecho fundamental como la educación)[64].

78. Cuanto más preciso se defina un interés a la luz de la finalidad prevista del tratamiento, mejor permitirá comprender claramente la realidad de los beneficios y riesgos que deben tenerse en cuenta en la prueba de ponderación.

79. En relación con los derechos y libertades fundamentales de los interesados, el desarrollo y el despliegue de modelos de IA pueden plantear graves riesgos para los derechos protegidos por la Carta de los Derechos Fundamentales de la UE (en lo sucesivo, la **Carta de la UE**), incluidos, entre otros, el derecho a la vida privada y familiar (artículo 7 de la Carta de la UE) y el derecho a la protección de los datos personales (artículo 8 de la Carta de la UE). Estos riesgos pueden producirse durante la fase de desarrollo, por ejemplo, cuando se extraen datos personales en contra de la voluntad de los interesados o sin su conocimiento. Estos riesgos también pueden producirse en la fase de despliegue, por ejemplo, cuando los datos personales son tratados por el modelo (o como parte del mismo) de una manera que contraviene los derechos de los interesados, o cuando es posible inferir, accidentalmente o mediante ataques (por ejemplo, inferencia de la afiliación, extracción o inversión del modelo), qué datos personales están contenidos en la base de datos de aprendizaje. Estas situaciones presentan un riesgo para la privacidad de los interesados cuyos datos podrían aparecer en la fase de despliegue del sistema de IA (por ejemplo, riesgo de reputación, robo o fraude de identidad, riesgo de seguridad en función de la naturaleza de los datos).

80. Dependiendo del caso de que se trate, también pueden existir riesgos para otros derechos fundamentales. Por ejemplo, la recopilación de datos a gran escala e indiscriminada por parte de modelos de IA en fase de desarrollo puede crear una sensación de vigilancia para los interesados, especialmente si se tienen en cuenta las dificultades para evitar que se obtengan datos públicos mediante «scraping». Esto puede llevar a las personas a la autocensura y presentar riesgos de socavar su libertad de expresión (artículo 11 de la Carta de la UE). En la fase de despliegue, también existen riesgos para la libertad de expresión cuando se utilizan modelos de IA para bloquear la publicación de contenidos de los interesados. Además, un modelo de IA que recomiende contenidos inadecuados a personas vulnerables puede presentar riesgos para su salud mental (artículo 3, apartado 1, de la Carta de la UE). En otros casos, la implantación de modelos de IA también puede tener consecuencias adversas para el derecho de la persona a participar en el mercado de trabajo (artículo 15 de la Carta de la UE), por ejemplo, cuando las solicitudes de empleo son preseleccionadas utilizando un modelo

[64] Véanse las Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 38.

de IA. Del mismo modo, un modelo de IA podría presentar riesgos para el derecho a la no discriminación (artículo 21 de la Carta de la UE), si discrimina a las personas sobre la base de determinadas características personales (como la nacionalidad o el género). Además, la implantación de modelos de IA también puede presentar riesgos para la protección y la seguridad de la persona (por ejemplo, cuando el modelo de IA se utiliza con fines maliciosos), así como riesgos para su integridad física y mental[65].

81. El despliegue de modelos de IA también puede afectar positivamente a determinados derechos fundamentales, por ejemplo, el modelo puede apoyar el derecho a la integridad mental de la persona (artículo 3 de la Carta), por ejemplo, cuando se utiliza un modelo de IA para identificar contenidos nocivos en línea, o el modelo puede facilitar el acceso a determinados servicios esenciales o facilitar el ejercicio de derechos fundamentales, como el acceso a la información (artículo 11 de la Carta de la UE) o el acceso a la educación (artículo 14 de la Carta de la UE).

Impacto del tratamiento sobre los interesados

82. El tratamiento de datos personales que tiene lugar durante el desarrollo y la implantación de modelos de IA puede afectar a los interesados de diferentes maneras, lo que puede ser positivo o negativo[66]. Por ejemplo, si una actividad de tratamiento conlleva beneficios para el interesado, estos pueden tenerse en cuenta en la prueba de ponderación. Aunque la existencia de tales beneficios puede llevar a la conclusión, por parte de una autoridad de control, de que los intereses, los derechos y libertades fundamentales de los interesados no prevalecen sobre los intereses del responsable del tratamiento o de un tercero, dicha conclusión solo puede ser el resultado de un análisis caso por caso que tenga en cuenta todos los factores adecuados.

83. El impacto del tratamiento sobre los interesados puede verse influido por (i) la naturaleza de los datos tratados por los modelos; (ii) el contexto del tratamiento; y (iii) las consecuencias ulteriores que el tratamiento pueda tener[67].

84. En relación con la **naturaleza de los datos tratados**, cabe recordar que, aparte de las categorías especiales de datos personales y datos relativos a infracciones y condenas penales que gozan respectivamente de protección adicional en virtud de los artículos 9 y 10 del RGPD, el tratamiento de algunas otras categorías de datos personales puede acarrear consecuencias significativas para los interesados. En este contexto, debe considerarse que el tratamiento de determinados tipos de datos personales que revelan información muy privada (por ejemplo, datos financieros o datos de localización) para el desarrollo y la implantación de un modelo de IA puede afectar seriamente a los interesados. En la fase de despliegue, las consecuencias de dicho tratamiento para los interesados pueden ser, por ejemplo, económicas (por ejemplo, discriminación en el contexto del empleo) o reputacionales (por ejemplo, difamación).

85. En relación con el **contexto del tratamiento**, es necesario identificar en primer lugar los elementos que podrían crear riesgos para los interesados (por ejemplo, la forma en que se ha desarrollado el modelo, la forma en que puede desplegarse el modelo o si las medidas de seguridad utilizadas para proteger los datos personales son adecuadas). La naturaleza del modelo y los usos operativos previstos desempeñan un papel clave en la identificación de esas posibles causas.

[65] Directrices 1/2024 sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 46.
[66] Véanse las Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 39.
[67] Véanse las Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 32.

86. También es necesario evaluar la gravedad de estos riesgos para los interesados. Puede considerarse, entre otras cosas, cómo se tratan los datos personales (por ejemplo, si se combinan con otros conjuntos de datos), cuál es la escala del tratamiento y la cantidad de datos personales tratados[68] (por ejemplo, el volumen total de datos, el volumen de datos por interesado, el número de interesados afectados)[69], la situación del interesado (por ejemplo, niños u otros interesados vulnerables) y su relación con el responsable del tratamiento (por ejemplo, si el interesado es un cliente). Por ejemplo, en ausencia de salvaguardias suficientes el uso del «web scraping» en la fase de desarrollo puede afectar significativamente a las personas, debido al gran volumen de datos recogidos, al gran número de interesados y a la recogida indiscriminada de datos personales.

87. Las **consecuencias adicionales** que pueda tener el tratamiento también deberán tenerse en cuenta a la hora de evaluar cómo afecta el impacto a los interesados. Las autoridades de control deben evaluar dichas consecuencias caso por caso, teniendo en cuenta los hechos específicos de que se trate.

88. Dichas consecuencias pueden incluir (pero no se limitan a) riesgos de violación de los derechos fundamentales de los interesados, como se describe en la subsección anterior[70]. Los riesgos pueden variar en probabilidad y gravedad, y pueden derivarse de un tratamiento de datos personales que pueda provocar daños físicos, materiales o inmateriales, en particular cuando el tratamiento pueda dar lugar a discriminación[71].

89. Cuando el despliegue de un modelo de IA implique el tratamiento de datos personales tanto de i) los interesados cuyos datos personales se incluyan en el conjunto de datos utilizado en la fase de desarrollo, como de ii) los interesados cuyos datos personales se traten en la fase de despliegue, las autoridades de control deberán distinguir y considerar los riesgos que afectan a los intereses, derechos y libertades de cada una de estas categorías de interesados al verificar la prueba de ponderación realizada por un responsable del tratamiento.

90. **Por último, el análisis de las posibles consecuencias ulteriores del tratamiento también deberá considerar la probabilidad de que estas consecuencias ulteriores se materialicen**. La evaluación de dicha probabilidad deberá hacerse teniendo en cuenta las medidas técnicas y organizativas existentes y las circunstancias específicas del caso. Por ejemplo, las autoridades de control pueden considerar si se han aplicado medidas para evitar un posible uso indebido del modelo de IA. En el caso de los modelos de IA que pueden desplegarse para diversos fines, como la IA generativa, esto puede incluir controles que limiten en la medida de lo posible su uso para prácticas perjudiciales, por ejemplo: la creación de productos ultrafalsos (*deepfakes*); los agentes conversacionales (*chatbots*) que se utilizan para la desinformación, el *phishing* y otros tipos de fraude; y la IA/los agentes de IA manipuladores (en particular, cuando son antropomórficos o proporcionan información engañosa).

Expectativas razonables de los interesados

91. Basándose en el considerando 47 del RGPD, *«En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento*

[68] Véanse las Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 43.
[69] TJUE, sentencia de 4 de julio de 2023, asunto C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), apartado 116.
[70] Véase el subapartado «Intereses, derechos y libertades fundamentales de los interesados» anterior.
[71] Véase la sección 2.3 de las Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024. Para más ejemplos, véase también el considerando 75 del RGPD.

con tal fin». En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior»[72].

92. Las expectativas razonables desempeñan un papel clave en la prueba de ponderación, entre otras cosas debido a la complejidad de la tecnología utilizada en los modelos de IA y al hecho de que puede resultar difícil para los interesados comprender la variedad de usos potenciales de un modelo de IA y el tratamiento de datos que implica[73]. A tal fin, la información facilitada a los interesados podrá tenerse en cuenta para evaluar si estos pueden esperar razonablemente que se traten sus datos personales. Sin embargo, aunque la omisión de información puede contribuir a que los interesados no esperen un determinado tratamiento, el mero cumplimiento de los requisitos de transparencia establecidos en el RGPD no es suficiente por sí mismo para considerar que los interesados pueden esperar razonablemente un determinado tratamiento[74]. Además, el mero hecho de que la información relativa a la fase de desarrollo de un modelo de IA se incluya en la política de privacidad del responsable del tratamiento no significa necesariamente que los interesados puedan razonablemente esperar que así sea; más bien, esto debe ser analizado por las autoridades de control en función de las circunstancias específicas del caso y teniendo en cuenta todos los factores pertinentes.

93. Al evaluar las expectativas razonables de los interesados en relación con el tratamiento que tiene lugar en la fase de desarrollo, es importante hacer referencia a los elementos mencionados en las Directrices del CEPD sobre el interés legítimo[75]. Además, dentro del objeto del presente Dictamen, es importante tener en cuenta el contexto más amplio del tratamiento. Esto puede incluir, entre otras cosas, si los datos personales estaban o no a disposición del público, la naturaleza de la relación entre el interesado y el responsable del tratamiento (y si existe un vínculo entre ambos), la naturaleza del servicio, el contexto en el que se recogieron los datos personales, la fuente a partir de la cual se recogieron los datos (por ejemplo, el sitio web o el servicio en el que se recogieron los datos personales y la configuración de privacidad que ofrecen), los posibles usos adicionales del modelo y si los interesados son realmente conscientes de que sus datos personales están en línea.

94. En la fase de desarrollo del modelo, las expectativas razonables de los interesados pueden variar en función de si los interesados hacen públicos o no los datos tratados para desarrollar el modelo. Además, las expectativas razonables también pueden diferir en función de si proporcionaron directamente los datos al responsable del tratamiento (por ejemplo, en el contexto de su uso del servicio), o si el responsable del tratamiento los obtuvo de otra fuente (por ejemplo, a través de un tercero, o mediante la técnica de raspado o *scraping*). En ambos casos, las medidas adoptadas para

[72] Véase también TJUE, sentencia de 4 de julio de 2023, asunto C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), apartado 112; TJUE, sentencia de 11 de diciembre de 2019, asunto C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA* (ECLI:EU:C:2019:1064), apartado 58; TJUE, sentencia de 4 de octubre de 2024, asunto C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), apartado 55.

[73] Por ejemplo, en la sentencia de 4 de julio de 2023, asunto C-252/21, *Meta/Bundeskartellamt* (ECLI:EU:C:2023:537), apartado 123, si bien el TJUE consideró que, en principio, la «mejora del producto» no puede excluirse como un interés legítimo, también consideró que «*parece dudoso [...] teniendo en cuenta el alcance de dicho tratamiento y su gran impacto en el usuario, así como el hecho de que este último no puede esperar razonablemente que esos datos sean tratados [...] que el objetivo de mejorar el producto pueda prevalecer sobre los intereses y los derechos fundamentales de dicho usuario, más aún en el supuesto de que este sea un niño*».

[74] Directrices 1/2024 sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 53.

[75] Directrices 1/2024 sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartados 50 a 54.

informar a los interesados de las actividades de tratamiento deben tenerse en cuenta a la hora de evaluar las expectativas razonables.

95. En la fase de despliegue del modelo de IA, es igualmente importante tener en cuenta las expectativas razonables de los interesados en el contexto de las capacidades específicas del modelo. Por ejemplo, en el caso de los modelos de IA que pueden adaptarse en función de las entradas proporcionadas, puede ser pertinente considerar si los interesados eran conscientes de que habían proporcionado datos personales para que el modelo de IA pudiera ajustar sus respuestas a sus necesidades y para que pudieran obtener servicios a medida. Además, también puede ser pertinente considerar si esta actividad de tratamiento solo afectaría al servicio prestado a los interesados (por ejemplo, la personalización de contenidos para un usuario específico) o si se utilizaría para modificar el servicio prestado a todos los clientes (por ejemplo, para mejorar el modelo de manera general). Al igual que en la fase de desarrollo, también puede ser especialmente pertinente considerar si existe un vínculo directo entre los interesados y el responsable del tratamiento. Este vínculo directo puede, por ejemplo, permitir al responsable del tratamiento facilitar fácilmente información a los interesados sobre la actividad de tratamiento y el modelo, lo que podría influir en las expectativas razonables de dichos interesados.

Medidas de mitigación

96. Cuando los intereses, derechos y libertades de los interesados parezcan prevalecer sobre el interés o intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, el responsable del tratamiento podrá considerar la introducción de medidas de mitigación para limitar el impacto del tratamiento sobre dichos interesados. Las medidas atenuantes son salvaguardias que deben adaptarse a las circunstancias del caso y depender de diferentes factores, en particular del uso previsto del modelo de IA. Estas medidas atenuantes tendrían por objeto garantizar que no se anulen los intereses del responsable del tratamiento o del tercero, de modo que el responsable del tratamiento pueda basarse en esta base jurídica.

97. Como se recuerda en las Directrices del CEPD sobre el interés legítimo, las medidas de mitigación no deben confundirse con las medidas que el responsable del tratamiento está legalmente obligado a adoptar en cualquier caso para garantizar el cumplimiento del RGPD, independientemente de si el tratamiento se basa o no en el artículo 6, apartado 1, letra f), del RGPD[76]. Esto es especialmente importante para las medidas que, por ejemplo, requieren cumplir con los principios del RGPD, como el principio de minimización de datos.

98. La lista de medidas que figura a continuación no es exhaustiva ni prescriptiva y la implantación de las medidas debe considerarse caso por caso. Aunque, dependiendo de las circunstancias, algunas de las medidas que se indican a continuación pueden ser necesarias para cumplir obligaciones específicas del RGPD, cuando no sea el caso pueden tenerse en cuenta como salvaguardias adicionales. Además, algunas de las medidas mencionadas a continuación se refieren a ámbitos que están sujetos a una rápida evolución y a nuevos avances, y las autoridades de control deberán tenerlas en cuenta a la hora de tratar un caso específico.

99. **En relación con la fase de desarrollo de los modelos de IA**, pueden adoptarse varias medidas para mitigar los riesgos que plantea el tratamiento de datos tanto propios como de terceros (incluso para mitigar los riesgos relacionados con las prácticas de raspado o *scraping* de sitios web). Sobre la base de lo anterior, el CEPD ofrece algunos ejemplos de medidas que pueden aplicarse para mitigar los

[76] Directrices 1/2024 sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 57.

riesgos detectados en la prueba de ponderación. Las autoridades de control deberían tener en cuenta estas medidas al evaluar los modelos de IA específicos caso por caso.

100. **Medidas técnicas**

a. Medidas mencionadas en la sección 3.2.2 que sean adecuadas para mitigar los riesgos en juego, cuando dichas medidas no den lugar a la anonimización del modelo y no sean necesarias para cumplir otras obligaciones del RGPD o en virtud de la prueba de necesidad (segundo paso de la evaluación del interés legítimo).

101. Además de estas, otras medidas pertinentes podrían incluir:

b. Medidas de seudonimización: como, por ejemplo, medidas para evitar cualquier combinación de datos basados en identificadores individuales. Estas medidas pueden no ser adecuadas cuando la autoridad de control considere que el responsable del tratamiento demostró la necesidad razonable de recoger datos diferentes sobre una persona concreta para el desarrollo del sistema o modelo de IA en cuestión.

c. Medidas para enmascarar datos personales o sustituirlos por datos personales falsos en el conjunto de entrenamiento (por ejemplo, la sustitución de nombres y direcciones de correo electrónico por nombres y direcciones de correo electrónico falsos). Esta medida puede ser especialmente apropiada cuando el contenido sustantivo real de los datos no sea pertinente para el tratamiento global (por ejemplo, en el entrenamiento de LLM).

102. **Medidas que facilitan el ejercicio de los derechos individuales**

a. Observar un período de tiempo razonable entre la recogida de un conjunto de datos de entrenamiento y su uso. Esta salvaguardia adicional puede permitir a los interesados ejercer sus derechos durante este período, evaluándose el plazo razonable en función de las circunstancias de cada caso.

b. Proponer una exclusión voluntaria u «opt-out» incondicional desde el principio, por ejemplo, proporcionando un derecho discrecional de oposición a los interesados antes de que tenga lugar el tratamiento, con el fin de reforzar el control de las personas sobre sus datos, lo que va más allá de las condiciones del artículo 21 del RGPD[77].

c. Permitir a los interesados ejercer su derecho de supresión incluso cuando no se apliquen los motivos específicos enumerados en el artículo 17, apartado 1, del RGPD[78].

d. Permitir que los interesados presenten reclamaciones de regurgitación o memorización de datos personales y las circunstancias y medios por los que pueden reproducirse las reclamaciones, permitiendo a los responsables del tratamiento reproducir y evaluar las técnicas de desaprendizaje pertinentes para abordar las reclamaciones.

103. **Medidas de transparencia:** en algunos casos, las medidas paliativas podrían incluir medidas que proporcionen una mayor transparencia con respecto al desarrollo del modelo de IA. Algunas medidas, además del cumplimiento de las obligaciones del RGPD, pueden ayudar a superar la asimetría de la información y permitir a los interesados comprender mejor el tratamiento que implica la fase de desarrollo:

[77] Ibíd.
[78] Ibíd.

a. Publicación de comunicaciones públicas y fácilmente accesibles que vayan más allá de la información requerida en virtud de los artículos 13 o 14 del RGPD, por ejemplo, proporcionando detalles adicionales sobre los criterios de recopilación y todos los conjuntos de datos utilizados, teniendo en cuenta la protección especial de los niños y las personas vulnerables.

b. Formas alternativas de informar a los interesados, por ejemplo: campañas en diferentes medios de comunicación para informar a los interesados, campaña de información por correo electrónico, uso de visualización gráfica, preguntas más frecuentes, etiquetas de transparencia y fichas de modelos cuya sistematización podría estructurar la presentación de información sobre modelos de IA, e informes anuales de transparencia con carácter voluntario.

104. **Medidas de mitigación específicas en el contexto de la extracción de información de sitios web (web scraping):** Teniendo en cuenta que, como ya se ha mencionado, este tipo de extracción de información plantea riesgos específicos[79], podrían identificarse medidas paliativas específicas en este contexto. Cuando proceda, estos riesgos podrán ser tenidos en cuenta por las autoridades de control, además de las medidas de mitigación mencionadas anteriormente, al investigar a las personas responsables de extraer la información de sitios web.

105. Las medidas específicas, cuando no sean necesarias en el marco de la segunda fase de la evaluación del interés legítimo, pueden resultar útiles para mitigar el riesgo en el contexto de la extracción de información de sitios web. Estas medidas podrán incluir **medidas técnicas**, tales como:

a. Excluir del contenido de los datos de las publicaciones que puedan incluir datos personales que entrañen riesgos para determinadas personas o grupos de personas (por ejemplo, personas que podrían ser objeto de abusos, prejuicios o incluso daños físicos si la información se divulgara públicamente).

b. Garantizar que determinadas categorías de datos no se recojan o que determinadas fuentes queden excluidas de la recogida de datos; esto podría incluir, por ejemplo, determinados sitios web que son especialmente intrusivos debido a la sensibilidad de su objeto.

c. Excluir la recogida de sitios web (o secciones de sitios web) que se oponen claramente a esta técnica de extracción y a la reutilización de su contenido con el fin de crear bases de datos de entrenamiento de IA (por ejemplo, respetando los archivos robots.txt o ai.txt o cualquier otro mecanismo reconocido para expresar la exclusión del rastreo automatizado o el «raspado»).

d. Imponer otros límites pertinentes a la recogida, posiblemente incluyendo criterios basados en períodos de tiempo.

106. En el contexto de la extracción de información de sitios web, algunos ejemplos de medidas específicas **que facilitan el ejercicio de los derechos de las personas y la transparencia** pueden ser: la creación de una lista de exclusión voluntaria, gestionada por el responsable del tratamiento y que permita a los interesados oponerse a la recogida de sus datos en determinados sitios web o plataformas en línea

[79] Estas prácticas también pueden plantear cuestiones adicionales que no se abordan en el presente Dictamen; véase, por ejemplo, Pagallo U., Ciani Sciolla J., *Anatomy of web data scraping: ethics, standards, and the troubles of the law.* European Journal of Privacy Law & Technologies, (2023) 2 pp. 1-19; disponible en: https://doi.org/10.57230/EJPLT232PS.

proporcionando información que los identifique en dichos sitios web, incluso antes de que se produzca la recogida de datos[80].

107. **<u>Consideraciones específicas relativas a las medidas de mitigación en la fase de despliegue</u>:** Aunque algunas de las medidas mencionadas anteriormente también pueden ser pertinentes para la fase de despliegue, en función de las circunstancias, el CEPD proporciona a continuación una lista no exhaustiva de medidas de apoyo adicionales que pueden aplicarse y que deberán ser evaluadas por las autoridades de control caso por caso.

    a. Pueden tomarse, por ejemplo, **medidas técnicas** para evitar el almacenamiento, la regurgitación o la generación de datos personales, especialmente en el contexto de los modelos de IA generativa (como los filtros de salida), y/o para mitigar el riesgo de reutilización ilícita por parte de modelos de IA de propósito general (por ejemplo, marca de agua digital de los resultados generados por IA).

    b. **Medidas que faciliten o aceleren el ejercicio de los derechos de las personas** en la fase de despliegue, más allá de lo exigido por la ley, en particular, y no exclusivamente, en relación con el ejercicio del derecho a la supresión de datos personales de los datos de salida del modelo o a la deduplicación, y las técnicas posteriores al entrenamiento que intenten eliminar o suprimir datos personales.

108. Al investigar la implantación de un modelo de IA específico, las autoridades de control deberán considerar si el responsable del tratamiento ha publicado la prueba de ponderación que haya realizado, ya que esto puede aumentar la transparencia y la equidad. Como se menciona en las Directrices del CEPD sobre el interés legítimo, pueden considerarse otras medidas para proporcionar a los interesados información de la prueba de ponderación antes de cualquier recogida de datos personales[81]. El CEPD también reitera[82] que un elemento que debe tenerse en cuenta es si el responsable del tratamiento ha implicado al RPD, en su caso.

3.4 Sobre la posible repercusión que un tratamiento ilícito durante el desarrollo de un modelo de IA puede tener sobre la licitud del posterior tratamiento o explotación del modelo de IA.

109. Esta sección del dictamen aborda la pregunta 4 de la solicitud. Esta pregunta solicita aclaraciones sobre el posible impacto que un tratamiento ilícito durante la fase de desarrollo puede tener en el tratamiento posterior (por ejemplo, en la fase de despliegue del modelo de IA) o en el funcionamiento del modelo. La pregunta tiene por objeto abordar tanto la situación en la que dicho modelo de IA trata datos personales que se conservan en el modelo [pregunta 4, letra i), de la solicitud], como la situación en la que ya no interviene el tratamiento de datos personales en el despliegue del modelo de IA (es decir, el modelo es anónimo) [pregunta 4, inciso ii), de la solicitud].

110. Antes de abordar determinados escenarios específicos, el CEPD presenta las siguientes consideraciones generales.

[80] Salvo que el responsable del tratamiento acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.
[81] Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 68.
[82] Directrices 1/2024 del CEPD sobre el tratamiento de datos personales sobre la base del artículo 6, apartado 1, letra f), del RGPD, versión 1.0, adoptadas el 8 de octubre de 2024, apartado 12.

111. En primer lugar, las aclaraciones facilitadas en esta sección se centrarán en el tratamiento de datos personales en la fase de desarrollo realizada sin respetar el principio de licitud establecido en el artículo 5, apartado 1, letra a), del RGPD y en el artículo 6 del RGPD específicamente (en lo sucesivo, «la **ilicitud**»)[83]. En la misma línea, las consideraciones del CEPD se centrarán en el impacto que la ilicitud del tratamiento durante la fase de desarrollo tiene sobre la licitud [es decir, el cumplimiento del artículo 5, apartado 1, letra a), del RGPD y del artículo 6 del RGPD] del tratamiento o la operación posteriores del modelo. No obstante, el CEPD señala que el tratamiento realizado en la fase de desarrollo también puede dar lugar a infracciones de otras disposiciones del RGPD, como la falta de transparencia hacia los interesados, o la protección de datos desde el diseño o por defecto, que no se analizan en el presente Dictamen.

112. En segundo lugar, a la hora de abordar esta cuestión, el principio de rendición de cuentas, que exige que los responsables del tratamiento sean responsables y demuestren el cumplimiento de, entre otras cosas, el artículo 5, apartado 1, del RGPD y el artículo 6 del RGPD[84], desempeña un papel fundamental. Esto también es cierto en el caso de la necesidad de evaluar qué organización es responsable de la actividad de tratamiento en cuestión y si surgen situaciones de corresponsabilidad del tratamiento (ya que pueden estar inextricablemente vinculadas) [85]. Teniendo en cuenta la importancia de las circunstancias fácticas de cada caso, incluso en lo que se refiere al papel desempeñado por cada parte implicada en el tratamiento, las consideraciones del CEPD deben entenderse como observaciones generales que deben ser evaluadas caso por caso por las autoridades de control.

113. En tercer lugar, el CEPD destaca que, de conformidad con el artículo 51, apartado 1, del RGPD, las autoridades de control se encargarán de «*supervisar la aplicación del [RGPD], con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión»*. Por lo tanto, es competencia de las autoridades de control evaluar la licitud del tratamiento y ejercer las facultades que les confiere el RGPD en consonancia con su marco nacional[86]. En tales casos, las autoridades de control gozan de facultades discrecionales para evaluar las posibles infracciones y elegir medidas adecuadas, necesarias y proporcionadas, de entre las mencionadas en el artículo 58 del RGPD, teniendo en cuenta las circunstancias de cada caso concreto [87].

114. **Cuando se detecte una infracción, las autoridades de control podrán imponer medidas correctivas, como ordenar a los responsables del tratamiento, teniendo en cuenta las circunstancias de cada caso, que adopten medidas para subsanar la ilicitud del tratamiento inicial.** Estas medidas pueden incluir, por ejemplo, la imposición de una multa, la imposición de una limitación temporal al tratamiento, la supresión de parte del conjunto de datos que se haya tratado ilícitamente o, cuando

[83] TJUE, sentencia de 4 de mayo de 2023, asunto C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), apartados 55-57.
[84] TJUE, sentencia de 4 de mayo de 2023, asunto C-60/22, *Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), apartado 53.
[85] Directrices 07/2020 del CEPD sobre los conceptos de responsable del tratamiento y encargado del tratamiento en el RGPD, versión 2.1, adoptadas el 7 de julio de 2021, apartado 55.
[86] Es posible que haya que tener en cuenta normas nacionales específicas. Véase, por ejemplo, el artículo 2-decies del Código italiano de protección de datos (Decreto legislativo 196/2003), que establece que los datos tratados en violación de las normas de protección de datos no pueden utilizarse. Esto se entiende sin perjuicio de otros marcos jurídicos nacionales, como las leyes penales.
[87] Véase a este respecto el considerando 129 del RGPD, así como la sentencia del TJUE de 26 de septiembre de 2024, asunto C-768-21, T*R/Land Hessen* (ECLI:EU:C:2024:785), apartado 37; la sentencia del TJUE de 7 de diciembre de 2023, en los asuntos acumulados C-26/22 y C-64/22, SCHUFA Holding (Libération de reliquat de dette) (ECLI:EU:C:2023:958), apartado 57; y TJUE, sentencia de 14 de marzo de 2024, asunto C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), apartado 34.

esto no sea posible, dependiendo de los hechos en cuestión, teniendo en cuenta la proporcionalidad de la medida, la orden de supresión de todo el conjunto de datos utilizado para desarrollar el modelo de IA o el propio modelo de IA. Al evaluar la proporcionalidad de la medida prevista, las autoridades de control pueden tener en cuenta las medidas que puede aplicar el responsable del tratamiento para subsanar la ilicitud del tratamiento inicial (por ejemplo, una repetición del segundo entrenamiento).

115. El CEPD también destaca que, cuando los datos personales se tratan ilícitamente, los interesados pueden solicitar la supresión de sus datos personales, con sujeción a las condiciones establecidas en el artículo 17 del RGPD, y que las autoridades de control pueden ordenar la supresión de los datos personales de oficio[88].

116. Al evaluar si una medida es adecuada, necesaria y proporcionada, las autoridades de control podrán tener en cuenta, entre otros elementos, los riesgos planteados para los interesados, la gravedad de la infracción, la viabilidad técnica y financiera de la medida, así como el volumen de datos personales implicados.

117. Por último, el CEPD recuerda que las medidas adoptadas por las autoridades de control en virtud del RGPD se entienden sin perjuicio de las adoptadas por las autoridades competentes en virtud de la Ley de IA o de otros marcos jurídicos aplicables (por ejemplo, la legislación sobre responsabilidad civil).

118. En las secciones siguientes, el CEPD abordará tres supuestos contemplados en la pregunta 4 de la solicitud, en los que las diferencias radican en si los datos personales tratados para desarrollar el modelo se conservan en el modelo, o si el tratamiento posterior lo realiza el mismo responsable del tratamiento u otro responsable.

3.4.1 Supuesto 1. Un responsable del tratamiento trata ilícitamente datos personales para desarrollar el modelo, los datos personales se conservan en el modelo y posteriormente son tratados por el mismo responsable del tratamiento (por ejemplo, en el contexto del despliegue del modelo).

119. Este escenario se refiere a la pregunta 4, letra i), de la solicitud, en la situación en la que un responsable del tratamiento trata ilícitamente datos personales (es decir, incumpliendo el artículo 5, apartado 1, letra a), y el artículo 6 del RGPD) para desarrollar un modelo de IA, el modelo de IA conserva información relativa a una persona física identificada o identificable y, por lo tanto, no es anónimo. A continuación, los datos personales son tratados posteriormente por el mismo responsable del tratamiento (por ejemplo, en el contexto de la implantación del modelo). En relación con este escenario, el CEPD aporta las siguientes consideraciones.

120. La facultad de la autoridad de control de imponer medidas correctoras al tratamiento inicial (como se explica en los anteriores apartados 113, 114 y 115) afectaría, en principio, al tratamiento posterior (por ejemplo, si la autoridad de control ordena al responsable que suprima los datos personales tratados ilícitamente, tales medidas correctoras no permitirían a este último tratar posteriormente los datos personales objeto de las medidas).

121. Por lo que se refiere específicamente al impacto del tratamiento ilícito en la fase de desarrollo sobre el tratamiento posterior (por ejemplo, en la fase de despliegue), el CEPD recuerda que corresponde a

[88] A este respecto, el Dictamen 39/2021 del CEPD sobre si el artículo 58, apartado 2, letra g) del RGPD podría servir de base jurídica para que una autoridad de control ordene de oficio la supresión de datos personales en una situación en la que dicha solicitud no haya sido presentada por el interesado, apartado 28. Véase también, a este respecto, la sentencia del TJUE de 14 de marzo de 2024, asunto C-46/23, *Újpesti Polgármesteri Hivatal* (ECLI:EU:C:2024:239), apartado 42.

las autoridades de control llevar a cabo un análisis caso por caso que tenga en cuenta las circunstancias específicas de cada caso.

122. **La cuestión de si las fases de desarrollo y despliegue implican fines separados (que constituyen, por tanto, actividades de tratamiento separadas) y la medida en que la falta de base jurídica para la actividad de tratamiento inicial afecta a la licitud del tratamiento posterior, debe evaluarse caso por caso, en función del contexto del caso.**

123. Por ejemplo, en lo que respecta específicamente a la base jurídica del artículo 6, apartado 1, letra f), del RGPD, cuando el tratamiento posterior se basa en un interés legítimo, el hecho de que el tratamiento inicial fuera ilícito debe tenerse en cuenta en la evaluación del interés legítimo (por ejemplo, en relación con los riesgos para los interesados o el hecho de que los interesados no puedan esperar dicho tratamiento ulterior). En estos casos, la ilicitud del tratamiento en la fase de desarrollo puede afectar a la licitud del tratamiento ulterior.

3.4.2 Supuesto 2. Un responsable del tratamiento trata datos personales ilícitamente para desarrollar el modelo, los datos personales se conservan en el modelo y son tratados por otro responsable del tratamiento en el contexto de la implantación de dicho modelo

124. Este escenario se refiere a la pregunta 4, letra i), de la solicitud. Difiere del supuesto 1 (en la sección 3.4.1 del presente dictamen), ya que los datos personales son tratados posteriormente por otro responsable del tratamiento en el contexto de la implantación del modelo de IA.

125. El CEPD recuerda que la determinación de las funciones asignadas a estos diferentes agentes en el marco de la protección de datos es un paso esencial para determinar qué obligaciones se aplican en virtud del RGPD y quién es responsable de dichas obligaciones, y que las situaciones de control conjunto también deben tenerse en cuenta al evaluar las responsabilidades de cada una de las partes en virtud del RGPD. Por lo tanto, las observaciones que figuran a continuación deben considerarse elementos generales que las autoridades de control deben tener en cuenta cuando proceda. Por lo que se refiere a este supuesto 2, el CEPD formula las siguientes consideraciones.

126. En primer lugar, cabe recordar que, de conformidad con el artículo 5, apartado 1, letra a), del RGPD, interpretado a la luz del artículo 5, apartado 2, de dicho Reglamento, cada responsable del tratamiento debe garantizar la licitud del tratamiento que lleva a cabo y ser capaz de demostrarlo. Por consiguiente, las autoridades de control deberán evaluar la licitud del tratamiento llevado a cabo por i) el responsable del tratamiento que desarrolló originalmente el modelo de IA, y ii) el responsable del tratamiento que adquirió el modelo de IA y trata los datos personales por sí mismo.

127. En segundo lugar, la consideración efectuada en los apartados 113, 114 y 115 del presente dictamen es pertinente en el caso que nos ocupa, por lo que respecta a la facultad de las autoridades de control de intervenir en relación con el tratamiento inicial. El artículo 17, apartado 1, letra d), del RGPD (supresión de datos tratados ilícitamente) y el artículo 19 del RGPD (obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento) también pueden, dependiendo de las circunstancias del caso, ser pertinentes en este contexto, por ejemplo en relación con la notificación que el responsable del tratamiento que desarrolle el modelo debe llevar a cabo frente al responsable del tratamiento que despliegue el modelo.

128. En tercer lugar, en relación con el posible impacto de la ilicitud del tratamiento inicial en el tratamiento posterior realizado por otro responsable del tratamiento, las autoridades de control deberán llevar a cabo dicha evaluación caso por caso.

129. **Con el fin de asegurarse de que el modelo de IA no se desarrolló mediante el tratamiento ilícito de datos personales, las autoridades de control deberán tener en cuenta si el responsable del tratamiento que despliega el modelo llevó a cabo una evaluación adecuada, como parte de sus obligaciones de rendición de cuentas[89] para demostrar el cumplimiento del artículo 5, apartado 1, letra a), y del artículo 6 del RGPD.** Dicha evaluación por parte de las autoridades de control deberá tener en cuenta si el responsable del tratamiento ha evaluado algunos criterios no exhaustivos, como la fuente de los datos y si el modelo de IA es el resultado de una infracción del RGPD, en particular si dicha infracción fue determinada por una autoridad de control o un órgano jurisdiccional, de modo que el responsable del tratamiento que despliega el modelo no podía ignorar que el tratamiento inicial era ilícito.

130. El responsable del tratamiento deberá considerar, por ejemplo, si los datos proceden de una violación de la seguridad de datos personales o si el tratamiento ha sido objeto de la constatación de una infracción por parte de una autoridad de control o un órgano jurisdiccional. **El grado de evaluación del responsable del tratamiento y el nivel de detalle esperado por las autoridades de control pueden variar en función de diversos factores, incluido el tipo y el grado de los riesgos que plantea el tratamiento en el modelo de IA durante su despliegue en relación con los interesados cuyos datos se utilizaron para desarrollar el modelo.**

131. El CEPD observa que la Ley de IA exige a los proveedores de sistemas de IA de alto riesgo que elaboren una declaración de conformidad de la UE[90], y que dicha declaración contiene una declaración de que el sistema de IA pertinente cumple la legislación de la UE en materia de protección de datos[91]. El CEPD observa que tal autodeclaración puede no constituir una conclusión concluyente de conformidad con el RGPD. No obstante, las autoridades de control podrán tenerlo en cuenta a la hora de investigar un modelo de IA específico.

132. Las mismas consideraciones formuladas en el apartado 123 de este dictamen también son pertinentes en el presente asunto. Cuando las autoridades de control verifiquen si el responsable del tratamiento evaluó la idoneidad del interés legítimo como base jurídica para el tratamiento que lleva a cabo, y cómo lo hizo, la ilicitud del tratamiento inicial debe tenerse en cuenta como parte de la evaluación del interés legítimo, por ejemplo, evaluando los riesgos potenciales que pueden surgir para los interesados cuyos datos personales fueron tratados ilícitamente para desarrollar el modelo. En la prueba de ponderación deben tenerse debidamente en cuenta aspectos diferentes, ya sea de carácter técnico (por ejemplo, la existencia de filtros o limitaciones de acceso impuestas durante el desarrollo del modelo, que el responsable del tratamiento posterior no puede eludir o en los que no puede influir, y que podrían impedir el acceso a los datos personales o su divulgación) o de naturaleza jurídica (por ejemplo, la naturaleza y la gravedad de la ilicitud del tratamiento inicial).

3.4.3 Supuesto 3. Un responsable del tratamiento trata ilícitamente datos personales para desarrollar el modelo y, a continuación, garantiza que el modelo sea anónimo, antes de que el mismo responsable o cualquier otro inicie otro tratamiento de datos personales en el contexto de la implantación.

133. Este supuesto se refiere a la pregunta 4, inciso ii), de la solicitud y se refiere a un caso en el que un responsable del tratamiento trata ilícitamente datos personales para desarrollar el modelo de IA, pero lo hace de manera que se garantice que los datos personales sean anonimizados, antes de que el

[89] Artículo 5, apartado 2, del RGPD y artículo 24 del RGPD.
[90] Artículo 16, letra g), y artículo 47 de la Ley de IA.
[91] Anexo V, punto 5, de la Ley de IA.

mismo responsable o cualquier otro responsable del tratamiento inicie otro tratamiento de datos personales en el contexto de la implantación. En primer lugar, el CEPD recuerda que las autoridades de control son competentes y tienen la facultad de intervenir en relación con el tratamiento relacionado con la anonimización del modelo, así como con el tratamiento realizado durante la fase de desarrollo. Así pues, las autoridades de control pueden, en función de las circunstancias específicas del caso, imponer medidas correctivas a este tratamiento inicial (como se explica en los apartados 113, 114 y 115 anteriores).

134. Si puede demostrarse que el funcionamiento posterior del modelo de IA no implica el tratamiento de datos personales, el CEPD considera que el RGPD no se aplicaría[92]. Por lo tanto, la ilicitud del tratamiento inicial no debería afectar al funcionamiento posterior del modelo. Sin embargo, el CEPD subraya que la mera afirmación del anonimato del modelo no basta para eximirlo de la aplicación del RGPD, y señala que las autoridades de control deberán evaluarlo teniendo en cuenta, caso por caso, las consideraciones aportadas por el CEPD para responder a la pregunta 1 de la solicitud.

135. **Cuando los responsables del tratamiento traten posteriormente los datos personales recogidos durante la fase de despliegue, una vez que el modelo se haya anonimizado, se aplicará el RGPD en relación con estas actividades de tratamiento. En estos casos, por lo que se refiere al RGPD, la licitud del tratamiento llevado a cabo en la fase de despliegue no debería verse afectada por la ilicitud del tratamiento inicial.**

4 Observaciones finales

136. Este Dictamen se dirige a todas las autoridades de control y se publicará de conformidad con lo dispuesto en el artículo 64, apartado 5, letra b), del RGPD.

Por el Comité Europeo de Protección de Datos

La Presidenta

Anu Talus

[92] Considerando 26 del RGPD.