Abordando conceptos erróneos de la Inteligencia Artificial

La autoridad británica de protección de datos (ICO) ha llevado a cabo una consulta pública sobre los usos que hace el sector de áreas específicas de IA generativa. A partir de los resultados, ha publicado unas aclaraciones para que los desarrolladores cum

La inteligencia artificial generativa es un método de desarrollo de aplicaciones y servicios basado en un uso intensivo de los datos. Como explica el considerando 7 del RGPD en relación a dichos avances, se requiere “un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza”.

Desde la Agencia Española de Protección de Datos (AEPD) se publicó conjuntamente con el Supervisor Europeo de Protección de Datos los 10 Malentendidos sobre el Machine Learning (Aprendizaje Automático) en 2022, donde ya se aclararon una serie de interpretaciones equívocas acerca del machine learning. En este artículo nos hacemos eco de la reciente publicación de la Information Commissioner's Office (ICO) del Reino Unido, sobre malentendidos o conceptos erróneos destacados respecto a la inteligencia artificial (IA) y su relación con la protección de datos (Tackling misconceptions | ICO), cuyos resultados es interesante trasladar al castellano. Este trabajo es parte de la respuesta más amplia a una consulta sobre IA generativa llevada a cabo por el ICO (Information Commissioner’s Office response to the consultation series on generative AI | ICO).

A continuación, se describen los malentendidos que identifica el ICO:

1. El tratamiento "incidental" o "agnóstico" de datos personales sigue constituyendo un tratamiento de datos personales, por tanto, se aplica la protección de datos.

Esta afirmación subraya que el tratamiento de datos personales en el ámbito de la IA sigue estando sujeto a la normativa de protección de datos, incluso cuando se considera incidental o no intencionado. En la consulta pública realizada por el ICO, muchos desarrolladores de IA generativa afirmaron que no tenían la intención de tratar datos personales y que el procesamiento de este tipo de datos fue puramente incidental. En este sentido, los desarrolladores de IA generativa deben evaluar, con precisión y de forma previa, si sus modelos manejan datos personales y, en su caso, garantizar el cumplimiento de la normativa aplicable.

2. La práctica común no equivale a satisfacer las expectativas razonables de las personas.

Las organizaciones no deben asumir que una determinada forma de tratamiento estará dentro de las expectativas razonables de las personas, simplemente porque se considera una "práctica común"; es decir, el hecho de que una práctica sea común no implica necesariamente que pueda llevarse a cabo de forma lícita porque los interesados la consideren razonable.

Esto es particularmente relevante cuando se trata del uso novedoso de datos personales para entrenar una IA generativa de manera invisible (p.ej., recabando los datos mediante web scraping y sin informar a los interesados) o años después de que alguien los proporcionara para un propósito diferente (cuando sus expectativas eran, por defecto, diferentes). El principio de transparencia exige que los responsables del tratamiento informen de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo sobre el uso de los datos personales, y en este caso, tal principio deberá aplicar al entrenamiento de los modelos y la reutilización de datos personales con fines distintos a los originalmente previstos.

3. Diferencia entre "información de identificación personal" y "datos personales".

Muchas organizaciones centran sus esfuerzos de cumplimiento de la IA generativa en torno al concepto de "información de identificación personal" (PII, por sus siglas en inglés). Sin embargo, para garantizar el cumplimiento normativo en protección de datos deberían considerar el tratamiento de cualquier "dato personal". Este último es un concepto más amplio y legalmente definido en el RGPD, que incluye cualquier información relativa a una persona física identificada o identificable, lo que abarca un espectro más amplio que la PII. Este matiz es clave para evitar interpretaciones erróneas en la aplicación de las obligaciones normativas.

4. Las organizaciones no deben considerar directamente aplicable la jurisprudencia sobre el cumplimiento de la protección de datos en los motores de búsqueda al ámbito de la IA generativa.

Algunos encuestados trataron de aplicar las decisiones históricas de los tribunales sobre los motores de búsqueda al contexto de la IA generativa.

Sin embargo, existen diferencias clave que hacen que la lógica de estas decisiones judiciales pueda no ser aplicable. Por ejemplo, mientras que un motor de búsqueda tiene la intención de indexar, clasificar y priorizar la información y ponerla a disposición del público, la IA generativa va más allá al sintetizar la información y producir nuevos contenidos en sus salidas. Los operadores de motores de búsqueda tradicionales también permiten a las personas ejercer sus derechos, en particular el derecho de supresión, lo que no es una práctica habitual en los desarrolladores de IA generativa. En la UE, esto refuerza la necede un análisis específico del cumplimiento del RGPD y de los nuevos riesgos para los derechos y libertades asociados a la generación de contenido a partir de datos personales.

En resumen, la jurisprudencia relacionada con los motores de búsqueda no puede extrapolarse automáticamente a la IA generativa.

5. Los modelos de IA generativa pueden incorporar datos personales.

El ICO también señala que algunos desarrolladores argumentaron que sus modelos no "almacenan" datos personales. Sin embargo, la realidad es que los modelos de IA generativa pueden retener información con la que han sido entrenados y, en algunos casos, esta puede ser recuperable o divulgable. Desde la perspectiva del RGPD, esto tiene implicaciones significativas, especialmente en lo que respecta al principio de minimización de datos y al derecho de supresión.

6. El alcance de la protección de datos y su relación con otros marcos normativos.

Algunos encuestados por el ICO manifestaron que el principio de licitud implicaba que la autoridad de supervisión de protección de datos podía proporcionar opiniones u orientación sobre la legalidad en regímenes distintos de la protección de datos. Sin embargo, la protección de datos no puede ser utilizada como una herramienta para interpretar la legalidad en otros ámbitos normativos. Si bien el incumplimiento de otras normativas puede conllevar también una infracción del RGPD (p. ej., en el caso de un tratamiento ilícito de datos personales), las autoridades de protección de datos no son competentes para determinar la legalidad en otras materias.

7. No existe una "excepción para la IA" en la normativa de protección de datos.

Algunos desarrolladores argumentan que la IA generativa debería beneficiarse de un trato diferenciado respecto a la normativa de protección de datos.

Las organizaciones deben ser conscientes de que no hay excepciones generales ni exenciones para la IA generativa. Si una organización está tratando datos personales, en cualquier contexto, se aplicará toda la normativa de protección de datos. Además, es fundamental que las organizaciones adopten un enfoque de "protección de datos desde el diseño y por defecto" para garantizar el respeto a los derechos de los interesados.

En definitiva, la publicación del ICO ofrece una serie de aclaraciones relevantes sobre la aplicación de la normativa de protección de datos a la IA generativa, que desde la AEPD consideramos útiles transmitir a los responsables de tratamientos de datos personales que desarrollan o emplean IA generativa.

Fuente: https://www.aepd.es/

LINK DE LA NOTICIA