ARI 143/2024
5 de noviembre de 2024

La Inteligencia Artificial en riesgo en la Unión Europea: no es la regulación, es la implementación

Judith Arnal | Investigadora principal, Real Instituto Elcano | @judith_arnal

Tema

Las dificultades en la aplicación de las normativas de la Unión Europea sobre protección de datos e inteligencia artificial frenan la innovación en un terreno clave y en evolución constante.

Resumen

La implementación del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) en la Unión Europea (UE) y no la propia normativa en sí está frenando la innovación tecnológica. La arquitectura de gobernanza de protección de datos de la UE es muy compleja, dando lugar a interpretaciones contradictorias en función del Estado miembro. Esta situación está llevando a empresas de todo tipo a detener el despliegue de proyectos transformadores en la UE. El caso de Meta es paradigmático: tanto el Reino Unido como la UE cuentan con la misma normativa (GDPR), pero el Reino Unido ha considerado con relativa rapidez que Meta puede entrenar su modelo de Inteligencia Artificial (IA) generativa empleando datos públicos de primera parte compartidos por los usuarios de Instagram y Facebook sobre la base jurídica de interés legítimo, mientras que la UE sigue sin llegar a una posición clara, lo que ha llevado a Meta a paralizar el avance de su proyecto en la UE. Estas barreras derivadas de la aplicación de la normativa pueden ser aún más dañinas para las *startups*, que cuentan con menos recursos para afrentar un marco regulatorio incierto. Para que la UE sea competitiva en la carrera global por el desarrollo de la IA, es necesario mejorar la coordinación entre las autoridades nacionales de protección de datos, que deberían adoptar con celeridad resoluciones pragmáticas de las que no deberían desviarse.

Análisis

1. Introducción

La reciente aprobación del pionero Reglamento de Inteligencia Artificial en la UE ha generado ríos de tinta. Muchas de las visiones se han centrado en torno a la inmensa capacidad de la UE de producir normativa y su consiguiente limitado impulso innovador. También se ha incidido en la progresiva pérdida de importancia del denominado “efecto Bruselas”, acuñado por la profesora de Columbia Anu Bradford, para referirse al poder unilateral de la UE de fijar marcos regulatorios de referencia.

Si bien muchas de las recientes innovaciones en IA se están produciendo fuera de la UE, es crítico que la UE no se quede al margen de su aplicación. La UE no necesita estar detrás de cada innovación tecnológica, pero sus empresas sí deberían aplicarlas

para poder permanecer competitivas. Lamentablemente, la puesta en funcionamiento en la UE del GDPR puede dejar a las empresas de la UE al margen de la aplicación de avances en el terreno de la IA. Como se explicará a continuación, no se trata tanto de la normativa en sí, la GDPR, sino de su interpretación e implementación por las autoridades de la UE. En efecto, el GDPR, acordado en 2016 y aplicado desde 2018, está vigente también en el Reino Unido en términos similares a los de la UE. Pero las autoridades del Reino Unido están interpretando la normativa de una manera muy diferente a la UE y mucho más proclive a los avances tecnológicos.

Puede resultar sorprendente que el GDPR y no únicamente el Reglamento de IA puedan tener un efecto en el desarrollo de esta tecnología en la UE. Ello es debido a que mientras que el Reglamento de IA se centra sobre todo en el desarrollo técnico seguro de la IA, el GDPR pone el foco en el otorgamiento de derechos a los individuos cuando se procesan sus datos. De este modo, el Reglamento de IA y el GDPR han de verse de manera conjunta, con el segundo completando los derechos individuales en los casos de sistemas de IA que tratan información personal.

Las dificultades en la aplicación de la normativa, unidas a la profusa actividad regulatoria de la UE, hacen que resulte muy complicado innovar tecnológicamente sobre un terreno que parece estarse moviendo continuamente.

En este análisis, se presentan dos secciones introductorias sobre la importancia del empleo de datos para entrenar los modelos de IA y la compleja gobernanza europea en materia de protección de datos, antes de pasar a explicar sobre la base de un caso paradigmático las dificultades que la UE está encontrando en la puesta en funcionamiento efectiva del GDPR y los efectos que esto puede tener para el futuro tecnológico de nuestra jurisdicción.

2. La importancia del uso de datos para entrenar los modelos de IA y las ventajas de los modelos de código abierto

La IA generativa es un tipo de IA que emplea modelos especializados de *machine learning* para generar distintos tipos de resultados, como texto, imágenes y audio. La IA generativa se apoya sobre los denominados modelos fundacionales, que constituyen modelos básicos sobre los que luego se elaboran modelos más especializados. Para preparar estos modelos más especializados, es necesario entrenamiento con bases de datos extensas y complejas, que pueden consistir en texto, audio, imágenes o vídeo. Los conocidos como *large language models* (LLM) son un tipo específico de modelo fundacional entrenado sobre miles de millones de palabras, que pueden generar respuestas de lenguaje natural.

La taxonomía de datos para entrenar los modelos de IA es amplia, pero a efectos de este artículo, distinguiremos tres categorías: (a) datos personales y no personales, (b) datos públicos y privados y (c) datos de primera parte y de terceros.

Los datos personales son aquellos que se refieren a una persona física identificada o identificable. Esto incluye cualquier información que pueda relacionarse con una persona específica, ya sea directa o indirectamente. Ejemplos de ello incluyen el

nombre, dirección, número de teléfono, correo electrónico, información financiera o dirección IP, entre otros. Por su parte, los datos no personales son aquellos que no pueden ser utilizados para identificar a una persona específica. Pueden ser datos agregados, anonimizados o que simplemente no contienen información que permita rastrear a un individuo. Algunos ejemplos son datos meteorológicos, estadísticas de tráfico, web anónimas o cantidad de usuarios en un servicio sin detalles personales.

Los datos públicos son accesibles para cualquier persona sin restricciones, ya que están publicados en fuentes oficiales o están simplemente abiertos al público en general. Ejemplos pueden ser los censos nacionales, la información financiera de empresas cotizadas o la información colgada por usuarios en redes sociales. Los datos privados son aquellos a los que sólo tienen acceso ciertas personas u organizaciones autorizadas. Estos datos están protegidos, ya sea por razones de privacidad, propiedad intelectual o porque su divulgación podría generar riesgos. Ejemplos de ello pueden ser el historial médico de un paciente, las bases de datos internas de una empresa o las conversaciones privadas por correo electrónico.

Los datos de primera parte son recopilados directamente por una empresa o entidad a partir de sus propios usuarios y clientes. Estos datos son generados a través de interacciones directas con los usuarios, ya sea en el sitio web, en aplicaciones, encuestas, registros de compras y servicios. Los datos de terceros son datos recopilados por una entidad externa, no directamente de los usuarios y clientes con los que una organización interactúa. Estos datos se obtienen de proveedores o agregadores de datos que los venden o los comparten a otras empresas.

Los modelos de IA pueden ser de código abierto o cerrado. En los modelos de código abierto, cualquier persona puede acceder al código fuente y los componentes del modelo, estudiarlo, modificarlo, mejorarlo o utilizarlo con fines específicos sin restricciones, siempre que se cumplan los términos de la licencia correspondiente. Los modelos de código abierto son especialmente útiles para empresas que necesitan desarrollar y personalizar soluciones de IA, sobre todo cuando trabajan con datos privados, como en centros de investigación médica, ya que permiten mayor flexibilidad y control sobre el desarrollo. Algunos ejemplos de modelos de código abierto son LLaMA de Meta, BERT de Google y DeepSpeech de Mozilla. En los modelos de código cerrado, el código fuente no está disponible al público y está controlado por la organización o empresa que lo desarrolló. Los modelos de código cerrado no permiten el tratamiento de datos privados, salvo que el modelo sea desarrollado por la propia empresa. Algunos ejemplos de modelos de código cerrado son GPT-4 de OpenAI, DeepMind's AlphaFold de Google y Amazon Rekognition de Amazon Web Services.

3. El GDPR y la complicada gobernanza de la protección de datos en la UE

Como se ha indicado anteriormente, el GDPR es el Reglamento General de Protección de Datos de la UE. Entre sus disposiciones, incluye las condiciones para la utilización de datos personales. En concreto, sólo se permite el procesamiento de datos personales en alguna de las siguientes cuatro situaciones: (a) cuando concurre consentimiento del individuo cuyos datos se están procesando; (b) cuando el procesamiento de datos es necesario para un contrato, una obligación personal legal o para salvar la vida de

alguien; (c) cuando el procesamiento de datos sirve el interés público o una función oficial; y (d) cuando hay interés legítimo. A efectos del procesamiento de datos personales para modelos de IA, las dos causas relevantes con el consentimiento y el interés legítimo.

La *Information Commissioner's Office* (ICO), es decir, la Autoridad de Protección de Datos del Reino Unido, establece que emplear el interés legítimo como base jurídica para el procesamiento de datos hace recaer la carga sobre la empresa procesadora de los datos, ya que si las autoridades públicas lo solicitan, tendrá que mostrar su evaluación de interés legítimo (LIA, por sus siglas en inglés), donde deberá haber sopesado la necesidad de procesar los datos personales frente a los intereses, derechos y libertades del individuo, teniendo en cuenta las circunstancias particulares. En los casos en que opera el interés legítimo, el procesador de datos puede tener que llegar a un acuerdo con las autoridades públicas, poniendo en marcha medidas para equilibrar los intereses de la empresa con los derechos del individuo. Sin embargo, bajo el consentimiento, la carga recae en el usuario, que tiene que decidir si acepta el procesamiento de sus datos personales o no y no suele haber medidas adicionales de equilibrio. La empresa procesadora de los datos sí tendrá que asegurarse de que el consentimiento sea transparente y voluntario, así como de que los usuarios puedan tener la posibilidad de retirarlo fácilmente en cualquier momento. Por tanto, el interés legítimo parece una base jurídica más sofisticada con los usuarios, que de lo contrario tendrían que otorgar su consentimiento sin ser verdaderamente conocedores de la normativa de protección de datos y las consecuencias de otorgar o denegar su consentimiento.

En muchos casos, las disposiciones del GDPR son vagas y hasta cierto punto ambiguas, lo que conlleva la necesidad de interpretación. Y es aquí donde entra en juego la compleja gobernanza de la UE en materia de protección de datos. En particular, cada Estado miembro de la UE cuenta con su propia autoridad de protección de datos, esto supone ya 27 interpretaciones potencialmente diferentes. A esto hay que sumar las 16 autoridades de protección de datos que hay por cada *land* alemán. Esto asciende ya a 43 opiniones que pueden ser diferentes. Y para finalizar, la normativa de protección de datos se aplica más allá de la UE, teniendo en cuenta también a Liechtenstein, Noruega e Islandia, es decir, el Espacio Económico Europeo (EEE). Esto nos lleva a 46 visiones potencialmente distintas. A pesar de que existen mecanismos de coordinación bajo el *European Data Protection Board* (EDPB), estos no funcionan en muchas ocasiones. De hecho, de acuerdo con el segundo informe de la Comisión Europea sobre la aplicación del GDPR, los participantes en el mercado indican que: (a) autoridades de protección de datos en tres Estados miembros tienen una visión diferente sobre la base legal adecuada para el procesamiento de datos personales al realizar un ensayo clínico; (b) con frecuencia existen opiniones divergentes sobre si una entidad es responsable o encargada del tratamiento; (c) en algunos casos, las autoridades de protección de datos no siguen a nivel nacional las directrices del EDPB; y (d) estos problemas se agravan cuando múltiples autoridades de protección de datos dentro de un mismo Estado miembro adoptan interpretaciones contradictorias.

Esta falta de coherencia no impide a las autoridades nacionales de protección de datos adoptar prohibiciones o sanciones. Algunas de las más conocidas son la prohibición (ya

levantada) de la autoridad italiana con respecto al ChatGPT de OpenAI, la multa a Deliveroo también por la autoridad italiana en relación con su sistema automático de *rating* de rendimiento de sus repartidores o la multa de la autoridad francesa a Cleaview AI por su plataforma de reconocimiento facial. Y sin lugar a dudas, destacan las actuaciones de la autoridad irlandesa de protección de datos, que de acuerdo con su informe anual de 2023, fue responsable del 87% de las multas del GDPR en toda la UE, la mayoría de las cuales estaban dirigidas a Meta, con sede en Dublín, por infracciones de privacidad. Y es precisamente una decisión de la autoridad irlandesa en relación con Meta la que ha vuelto a generar polémica, como se explica en la siguiente sección.

4. El caso paradigmático de Meta: el entrenamiento de modelos de IA con datos públicos de primera parte

En mayo de 2024, Meta informó a sus usuarios de un cambio en su política de privacidad, por el que la compañía podría emplear sus *posts* en Facebook e Instagram desde 2007 para entrenar su modelo de IA (LLaMa). En lugar de utilizar la base jurídica del consentimiento (*opt-in*), Meta argumentó que se apoyaría sobre el interés legítimo, informando a los usuarios y proporcionándoles el derecho a negarse al empleo de sus datos (*opt-out*). Los *chats* entre particulares quedarían excluidos de este uso.

El 6 de junio de 2024, el grupo NOYB (*None of your business*) dirigido por el austriaco Max Schrems, que dio lugar a las dos conocidas sentencias del Tribunal de Justicia de la UE sobre el flujo de datos personales entre la UE y Estados Unidos (EEUU), presentó una queja ante 11 autoridades nacionales de protección de datos de la UE, pidiendo a las autoridades que pongan en marcha un procedimiento de urgencia para detener este cambio inmediatamente, antes de su entrada en vigor el 26 de junio de 2024. NOYB argumenta que el empleo de datos para tecnologías IA es extremadamente amplio, que Meta carece de interés legítimo y que se está colocando la carga sobre el usuario.

Tras la petición de la autoridad de protección de datos irlandesa, que constituye la autoridad líder para Meta, el 14 de junio de 2024, la compañía anunció su decisión de pausar sus planes de entrenar su modelo LLaMa con contenido público compartido por adultos en Facebook e Instagram en todo el EEE. A efectos de la taxonomía presentada en el apartado dos, se trataría de datos personales, públicos y de primera parte, ya que Facebook e Instagram son redes sociales que pertenecen a Meta. La autoridad irlandesa dio la bienvenida a esta decisión de Meta e indicó que seguiría trabajando con la empresa, en coordinación con el resto de las autoridades europeas, en este tema.

Aunque el Reino Unido también pausó inicialmente los planes de Meta, el pasado 13 de septiembre, Meta anunció que ya podía proceder, confirmando la base legal del interés legítimo y la combinación de información y sistema de *opt-out*. Y la base jurídica era exactamente la misma: el GDPR. Pero claramente, la implementación de la normativa, derivada de una gobernanza muy diferente, es otra.

.

Conclusiones

En una reciente sentencia de 4 de octubre de 2024, el Tribunal de Justicia de la UE aclara que el interés legítimo no se limita a lo regulado por ley, sino que abarca cualquier interés lícito, como el comercial, siempre que sea legal. El responsable del tratamiento de datos debe informar a los interesados sobre los fines y la base legal del tratamiento, y demostrar que los datos se recogen de manera lícita y transparente.

Lo cierto es que una vez que los datos son públicos, como ocurre con los *posts* de redes sociales, la diferencia entre datos de primera parte y datos de terceros parece irrelevante, ya que los datos de terceros de un responsable del tratamiento son, por definición, siempre los datos de primera parte de otro responsable del tratamiento. Lo que sí tiene total relevancia es si los datos son públicos o privados. Y en este caso, está claro que son datos públicos, de modo que lo que realmente importa, toda vez que existe interés lícito, incluso de naturaleza comercial, es la manera en que se informa a los usuarios del tratamiento a que se someterán sus datos, preparando una evaluación adecuada de la existencia de interés legítimo y proporcionando un mecanismo fácil y creíble de *opt-out*. Si se establece un mecanismo que combina adecuadamente información y posibilidad de *opt-out*, no existe realmente ninguna razón para impedir el uso de datos públicos recopilados en las redes sociales, ya sean de primera o de tercera parte.

Pero incluso si las autoridades europeas de protección de datos consideraran que no concurre interés legítimo por parte de Meta y que, por tanto, la empresa debería optar por el consentimiento o el *opt-in*, harían bien en comunicar de manera rápida esta interpretación.

Más allá de este caso concreto, que ha sido analizado en detalle por su carácter paradigmático, lo que parece evidente es que la UE no puede permitirse operar bajo esta fuerte incertidumbre en la aplicación de su normativa. No se trata de la normativa en sí, ya que como se ha explicado, el Reino Unido cuenta con el mismo GDPR, sino de la compleja gobernanza y la aplicación dispar de la normativa según el Estado miembro. Y en este caso, además, estamos ante un Reglamento, de aplicación directa, y no una Directiva, que requiere de la transposición a nivel nacional por parte de los Estados miembros. Este es sólo un ejemplo más, un síntoma de una enfermedad burocrática que afecta a la UE y que puede dejarla convaleciente durante mucho tiempo.

En este sentido, se considera fundamental aumentar la dotación de recursos del EDPB, que debería resolver las dudas jurídicas que se vayan planteando a la mayor brevedad posible. Una vez resueltas, las autoridades nacionales de protección de datos deberían poner en funcionamiento sin ningún tipo de matiz las directrices del EDPB, evitando así cualquier tipo de fragmentación.

Si bien la decisión de empresas como Meta de parar el desarrollo de sus avances en la UE puede ser pernicioso para nuestro futuro tecnológico (LLaMA es un modelo de IA de código abierto, que puede ser empleado por otras empresas para crear su propio modelo de IA adaptado a sus necesidades), el efecto que esto puede llegar a tener en *startups* es aún mayor. Es evidente que las *bigtechs* cuentan con todos los recursos necesarios para interpretar la normativa de protección de datos e incluso litigar con

nuestras autoridades. Pero este no es el caso de las *startups*, que deberían contar con el marco regulatorio más claro posible para poder desarrollar sus ideas e incorporar la privacidad dentro de sus estructuras técnicas y administrativas de servicio.

Una valoración similar ha sido recogida en una carta firmada por empresarios como el presidente y CEO de Eriksson (Börje Ekholm), el vicepresidente de Pirelli (Marco Tronchetti Provera), el fundador y CEO de Spotify (Daniel Ek), el CEO de Thyssenkrupp AG (Miguel López) y académicos de Harvard (Stefano Iacus)**.** Las mismas ideas se defienden en una carta conjunta de Mark Zuckerberg y Daniel Ek, animando a la UE a eliminar la incertidumbre regulatoria para así abrazar la IA de código abierto.

Y es que, efectivamente, una aplicación fragmentada de la normativa pone a la UE en riesgo de perderse la revolución de la IA.