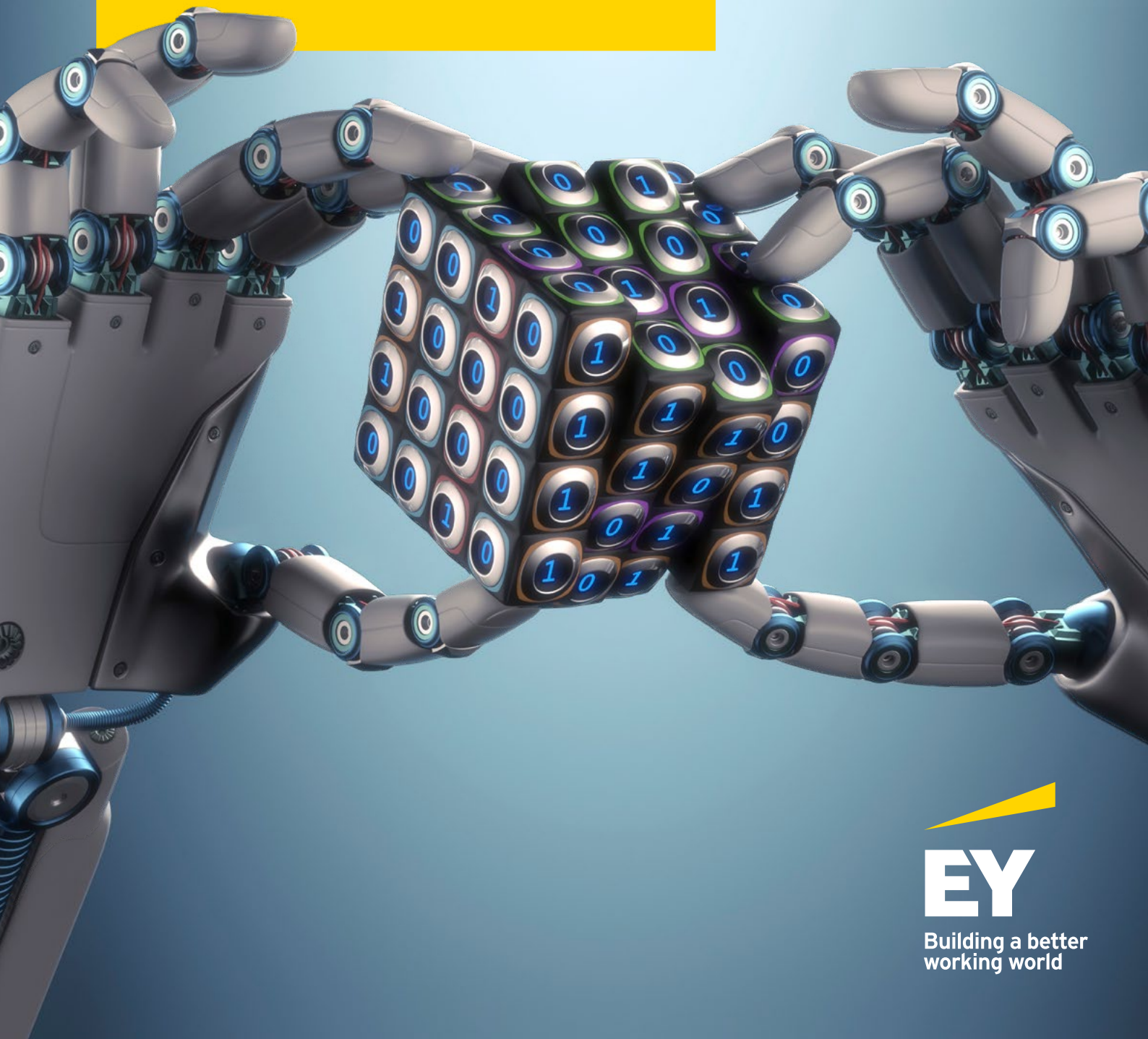
Propuesta de Reglamento europeo de inteligencia artificial

Mayo 2021



Building a better working world

Propuesta de Reglamento europeo de inteligencia artificial: Respuesta a cuestiones clave

La Comisión Europea ha avanzado en su estrategia para conseguir un entorno de IA confiable en la Unión Europea (EU), proponiendo una legislación, en forma de reglamento, que cubre el suministro y utilización de IA.

El Reglamento aplicará a la IA utilizada o introducida en el mercado de la UE, con independencia de si los proveedores están establecidos dentro o fuera del territorio de la Unión.

Los sistemas de IA estarán sujetos a distintos niveles de obligaciones y prohibiciones dependiendo de los riesgos que planteen a la salud, la seguridad y los derechos fundamentales de las personas en la UE.

Se propone un régimen sancionador al estilo del RGDP o de la normativa de competencia, con multas de hasta 30 millones de euros o el 6% del volumen de negocio total anual mundial. Las obligaciones y requisitos se dirigen, no sólo a los proveedores de sistemas de IA, sino también a las entidades que utilizan esos sistemas o que son parte de la cadena de valor (fabricantes, importadores, distribuidores).

La gobernanza de datos cobra una nueva dimensión ya que ahora necesitará ser más completa y estará sujeta, no sólo a las obligaciones del RGPD, sino también a este nuevo reglamento de IA, dado el riesgo de mayores sanciones.

El 21 de abril de 2021 la Comisión Europea publicó su propuesta de Reglamento sobre Inteligencia Artificial (propuesta de Reglamento), junto con una Comunicación sobre el impulso de un enfoque europeo para la Inteligencia Artificial.

La presidenta de la Comisión, Ursula von der Leyen, dejó clara la intención de regular la IA desde el inicio de su mandato en 2019. Desde entonces, se han publicado distintos actos preparatorios, incluyendo un Libro Blanco sobre la cuestión y una serie de resoluciones del Parlamento Europeo emitidas en octubre de 2020 (sobre Ética, Responsabilidad y Derechos de Propiedad Intelectual). Todos estos actos preparatorios se basan en la Comunicación sobre IA de 2018 y las guías para una IA confiable del Grupo de Expertos de Alto Nivel en Inteligencia Artificial, que son aplicables en la actualidad y constituyen un marco para las organizaciones que forman parte del ecosistema de IA.

Junto con la propuesta de Reglamento, la Comisión también ha propuesto un nuevo marco regulatorio para las máquinas, actualizando las normas de seguridad para generar confianza en los nuevos productos y tecnologías digitales. Entre otros objetivos, la propuesta de nuevo Reglamento sobre Máquinas, que sustituirá a la Directiva 2006/42/CE, pretende abordar los riesgos que plantean las tecnologías digitales emergentes (como la robótica o el Internet de las Cosas, además de la IA) y será complementario del Reglamento de IA. El Reglamento cubrirá los riesgos de seguridad que traen consigo los sistemas de IA, mientras que el Reglamento sobre Máquinas aplicará en relación con la integración segura de los sistemas de IA en la maquinaria en general, para evitar poner en peligro la seguridad de la máquina en su conjunto.

1 ¿Qué IA entrará dentro del ámbito de aplicación de la propuesta de Reglamento?

Se propone una única definición de IA:

> *"El software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el Anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa."*

Es importante tener en cuenta que la propuesta de Reglamento aplica a la forma en que se utiliza la IA, no a la tecnología en sí. La definición pretende tener vocación de futuro y ser tecnológicamente neutra y el objetivo es que abarque lo máximo posible.

Existen algunos tipos de IA que quedan fuera del ámbito de aplicación de la propuesta de Reglamento. Uno es la IA legada, entendiendo por tal la IA introducida en el mercado o puesta en servicio antes de la fecha de aplicación. La Comisión ha indicado que desea acelerar el proceso legislativo para que entre el vigor el Reglamento, quizá a partir de 2022. Las organizaciones que esperan poner en funcionamiento sus herramientas de IA rápidamente para que queden excluidas del alcance del Reglamento deben tener en cuenta que, si la herramienta experimenta cambios significativos en el diseño o en la finalidad prevista después de la fecha de aplicación, entonces quedarán sujetas al Reglamento en todo caso.

Otras tecnologías exentas son los sistemas de IA que sean componentes de sistemas informáticos de gran magnitud establecidos en virtud de determinados actos legislativos de la UE en materia de libertad, seguridad y justicia (sistemas de información de Schengen y visados, antecedentes penales o seguridad) que se hayan introducido en el mercado o se hayan puesto en servicio antes de 12 meses después de la fecha de aplicación del Reglamento (salvo que la sustitución o modificación de dichos actos legislativos redunde en un cambio significativo en el diseño o la finalidad prevista del sistema o sistemas de IA de que se trate). Finalmente, los sistemas de IA con finalidades militares y utilizados por las autoridades públicas de terceros países o las organizaciones internacionales en el marco de acuerdos internacionales con fines de aplicación de la ley y cooperación judicial con la Unión o con uno o varios Estados miembros, también quedan fuera del ámbito de aplicación.

2 ¿A qué organizaciones aplica?

La propuesta de Reglamento establece obligaciones para las organizaciones a lo largo de toda la cadena de valor. Esto incluye, no sólo proveedores[1] que introduzcan herramientas de IA en el mercado o que implementen sistemas de IA en la UE, sino también fabricantes, distribuidores, importadores y usuarios de dichos sistemas de IA.

Cualquier organización presente en la cadena de valor será considerada como proveedor en cualquiera de las circunstancias siguientes:

i. si utilizan la herramienta de IA en el mercado con su propio nombre o marca comercial;

ii. si modifican la finalidad prevista del sistema de IA; o

iii. si realizan una modificación sustancial.

En aquellos casos en los que se den las circunstancias de los apartados (ii) y (iii), el proveedor inicial dejará de ser responsable.

Los usuarios se definirán como toda persona física o jurídica,

1 Significa toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que desarrolle un sistema de IA o para el que se haya desarrollado un sistema de IA con vistas a introducirlo en el mercado o ponerlo en servicio con su propio nombre o marca comercial, ya sea de manera remunerada o gratuita.

autoridad pública, agencia u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional. Por consiguiente, todos los usuarios profesionales que hagan uso de sistemas de IA estarán sujetos a las obligaciones aplicables conforme a lo previsto en la propuesta de Reglamento.

3 ¿Dónde aplica?

El Reglamento tiene alcance extraterritorial. Aplicará, no sólo dentro de la Unión Europea, sino también a los proveedores o usuarios que estén establecidos o ubicados fuera del territorio de la Unión siempre que:

i. introduzcan o pongan en servicio sistemas de IA en la UE; o

ii. la información de salida generada por el sistema se utilice en la UE.

4 Un sistema de obligaciones proporcional a los riesgos: diferentes obligaciones para las diferentes finalidades de la IA

El Reglamento clasifica la IA en cuatro grupos:

- Prohibida,
- De alto riesgo,
- De riesgo bajo y
- De riesgo mínimo.

La severidad del enfoque regulatorio depende de la clasificación de la IA en cuestión. La legislación propuesta establece una estructura regulatoria que prohíbe algunos usos de la IA, impone muchas obligaciones a los usos de alto riesgo y pocas a los sistemas de IA que presentan menos riesgos.

Las organizaciones deberían ser conscientes de que la Comisión pretende prohibir ciertos usos de la IA que se consideran inaceptables porque:

i. se sirven de técnicas subliminales o se aprovechan de las vulnerabilidades de grupos específicos de personas por su edad o discapacidad para alterar de forma sustancial su comportamiento, de manera que cause o sea probable que cause perjuicios físicos o psicológicos;

ii. conducen a que las autoridades públicas realicen una puntuación o clasificación social (*social scoring*); o

iii. llevan a cabo identificación biométrica a tiempo real en espacios de acceso público (con determinadas excepciones).

En el extremo opuesto, para los sistemas de IA de riesgo mínimo, el marco indica que es probable que no existan restricciones importantes o que no exista ninguna.

Entre ambos extremos, se encontrarían los sistemas de IA en los que se centran las obligaciones de la propuesta de Reglamento: por un lado, la IA de alto riesgo, que se permite sujeta al cumplimiento de determinados requisitos; y, por otro, determinados sistemas de riesgo bajo (i.e. suplantación, *bots*) que se someten a meras obligaciones de información y transparencia. Esto podría incluir la obligación de informar claramente a los humanos de que están interactuando con un sistema de IA o que se aplica el reconocimiento de emociones o la categorización biométrica, así como la obligación de etiquetar las llamadas ultrafalsificaciones o "deep fakes" (con algunas excepciones).

Dado este enfoque basado en los riesgos, la mayoría de las obligaciones y requisitos descritos en la propuesta de Reglamento se refieren a la IA de alto riesgo. La clasificación de un sistema de IA como de alto riesgo se basa en la finalidad prevista del mismo (en línea con la normativa en materia de seguridad de los productos). No sólo depende de las funciones que lleve a cabo, sino también de la finalidad específica y de las modalidades para las que se utilice el sistema.

Existen dos grandes grupos de IA que se consideran de alto riesgo:

i. Aquéllos destinados a ser utilizados como componentes de seguridad de productos[2], o que son en sí mismos productos que entran en el ámbito de aplicación de la legislación de armonización de la UE (tal y como se lista en el Anexo II) y que estén sujetos a una evaluación de la conformidad realizada por un tercero.

ii. Sistemas independientes en ocho áreas:

   a. Identificación biométrica y categorización de personas físicas.

   b. Gestión y funcionamiento de infraestructuras críticas.

   c. Empleo, gestión de los trabajadores y acceso al autoempleo.

   d. Acceso y disfrute de determinados servicios y ayudas esenciales de carácter público y privado.

   e. Educación y formación profesional.

   f. Aplicación de la ley y gestión de la migración, el asilo y el control fronterizo.

   g. Administración de justicia y procesos democráticos.

Las áreas están recogidas en el Anexo III, que es una lista fija y que será actualizada, de acuerdo con los criterios establecidos en el Reglamento, por la Comisión, pero con cierta intervención de los Estados miembros.

La IA de alto riesgo está sujeta al cumplimiento de determinadas obligaciones:

i. Gestión de riesgos

ii. Gobernanza de datos

iii. Documentación técnica

iv. Registro de documentación (trazabilidad)

v. Transparencia y suministro de información a usuarios

vi. Vigilancia humana

vii. Precisión

viii. Solidez y ciberseguridad

2 Componente de seguridad: componente físico o digital de una máquina, incluido el software, que sirva para desempeñar una función de seguridad y que se introduzca en el mercado por separado, cuyo fallo o funcionamiento defectuoso ponga en peligro la seguridad de las personas, pero que no sea necesario para que la máquina funcione o que pueda ser reemplazado por componentes normales para que la máquina funcione (Propuesta de Reglamento sobre Máquinas).

No es objeto del presente trabajo analizar en detalle cada uno de estos requisitos. Sin embargo, se recogen algunas ideas sobre tres de ellos a continuación:

Es necesario establecer, implementar, documentar y mantener sistemas de gestión de riesgos. Se trata de un proceso continuo, iterativo que debe estar en marcha a lo largo de todo el ciclo de vida del producto, que requiere de actualizaciones periódicas y sistemáticas. La finalidad prevista del sistema de IA y el sistema de gestión de riesgos en sí mismo deben tenerse en cuenta a la hora de evaluar el cumplimiento con los requisitos establecidos en la propuesta de Reglamento.

El requisito de gobernanza de datos es clave, no sólo porque sin datos no puede haber IA, sino también porque los datos utilizados para entrenamiento, validación y prueba definirán la legalidad (y ética) del sistema de IA. Más importante aún, quizá, infringir el requisito de gobernanza de datos trae consigo la sanción más alta de las establecidas en la propuesta de Reglamento (ver comentarios en el apartado 7 para más detalles sobre las sanciones). La propuesta de Reglamento establece varias características de la gobernanza de datos, ordenando que incluya ciertos criterios de calidad (que inciden en la elección del diseño, la recopilación de los datos, la formulación de supuestos, la evaluación previa, el examen atendiendo a posibles sesgos y la detección de lagunas o deficiencias en los datos), así como limitaciones técnicas. Por otra parte, en la medida en que sea estrictamente necesario a los efectos de garantizar la supervisión, detección y corrección de sesgos en relación con los sistemas de IA de alto riesgo, los proveedores de estos sistemas podrán tratar categorías especiales de datos personales, siempre que ofrezcan las salvaguardas apropiadas para los derechos y libertades fundamentales de las personas físicas, incluyendo limitaciones técnicas a la reutilización y la utilización de las medidas de seguridad y protección de la privacidad más recientes, como la seudonimización o el cifrado, cuando la anonimización pueda afectar de forma significativa la finalidad perseguida (i.e. cumplimiento del RGPD).

Por lo que se refiere al criterio de solidez y ciberseguridad, es importante destacar la presunción de cumplimiento de los sistemas de alto riesgo cuando hayan sido certificados o cuando se haya emitido una declaración de conformidad con arreglo a un esquema de ciberseguridad en virtud de la Ley de Ciberseguridad de la UE. En términos más generales, para disminuir la carga de cumplimiento, existen instrumentos para conseguir la presunción de conformidad con los requisitos, incluyendo la adhesión a estándares, especificaciones comunes, esquemas de ciberseguridad, evaluaciones de conformidad, certificados y declaraciones europeas de conformidad.

5 ¿Cómo deberían cumplir las organizaciones cuando desarrollen sistemas de IA?

Existen diferentes hitos a lo largo del ciclo de vida de un sistema de IA, con distintas acciones para alcanzar el cumplimiento en cada uno de ellos.

Antes de introducir un sistema de IA en el mercado o de su puesta en servicio, por ejemplo, el proveedor deberá asegurarse de que se han tenido en cuenta tanto la finalidad prevista como los sistemas de gestión de riesgos. Desde el comienzo del desarrollo del producto, el proveedor deberá establecer un modelo de gobernanza de datos adecuado (entrenamiento, validación y prueba de los conjuntos de datos), así como preparar la documentación técnica y la información o instrucciones para los usuarios. Asimismo, el proveedor deberá realizar una evaluación de la conformidad ex ante o equivalente, colocar el correspondiente marcado CE de conformidad y registrar el sistema en la base de datos de la UE.

Una vez la IA se encuentre operativa, será necesario adoptar medidas de supervisión, establecer un sistema de gestión y notificación de incidentes y llevar a cabo nuevas evaluaciones de conformidad cuando se produzca cualquier cambio en la finalidad o funciones de la IA. Deberán conservarse los archivos de registro (logs) durante el tiempo necesario conforme a su finalidad y a las normas jurídicas nacionales o del Derecho de la Unión, y deberá conservarse la documentación por un periodo de 10 años después de la introducción del sistema de IA en el mercado, a efectos de trazabilidad y rendición de cuentas.

6 ¿Qué sucede con los sistemas de IA que continúan "aprendiendo"?

En el texto de la propuesta de Reglamento se recogen diversas referencias específicas a los sistemas que continúan aprendiendo tras su introducción en el mercado o puesta en servicio. Éstos deben ser desarrollados de manera que se garantice que los posibles sesgos en la información de salida se subsanen debidamente con medidas de mitigación apropiadas.

La propuesta de Reglamento aclara que, para las IAs de autoaprendizaje, los cambios derivados del autoaprendizaje no se considerarán una modificación sustancial y, por tanto, no conllevarán la necesidad de realizar una nueva evaluación de la conformidad, siempre que los cambios en el sistema de IA de alto riesgo y su funcionamiento hayan sido predeterminados por el proveedor en el momento de la evaluación inicial de la conformidad y estén incluidos en la información recogida en la documentación técnica.

7 ¿Qué sucede si no se cumple?

El incumplimiento de las obligaciones expone a una organización a sanciones económicas de hasta un máximo de 30 millones de euros o hasta el 6% del volumen de negocio total anual mundial del ejercicio financiero anterior, si este importe fuera superior. En la escala inferior, las sanciones podrán ser de hasta 10 millones de euros o hasta el 2% del volumen de negocio total anual mundial, con una cuantía intermedia de 20 millones de euros o de hasta el 4% del volumen de negocio total anual mundial.

Las infracciones que conllevan la máxima sanción se reservan a aquéllas que suponen la inobservancia de la categoría de prácticas o sistemas de IA prohibidos o el incumplimiento de los requisitos de gobernanza de datos. El segundo nivel de sanciones se impondrá en caso de incumplir con cualesquiera otros requisitos u obligaciones de la propuesta de Reglamento. Finalmente, las sanciones menos graves, aunque sustanciales, se impondrán por la presentación de información inexacta, incompleta o engañosa a organismos notificados y a las autoridades nacionales competentes en respuesta a una solicitud.

Para decidir la cuantía de la multa, se tendrán en cuenta todas las circunstancias relevantes, teniendo debidamente en cuenta:

i. la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias;

ii. si otras autoridades ya han impuesto multas administrativas al mismo operador por la misma infracción; y

iii. el tamaño y la cuota de mercado del operador que comete la infracción.

8 Supervisión del cumplimiento, nuevas autoridades y base de datos de la UE para sistemas de IA de alto riesgo independientes

Se designarán y establecerán nuevas autoridades especializadas para hacer cumplir la propuesta de Reglamento. A nivel nacional se designará una autoridad nacional de supervisión, una autoridad notificante y una autoridad de vigilancia del mercado. Las autoridades nacionales serán competentes para coordinar y representar al Estado miembro en el Comité Europeo de Inteligencia Artificial, para designar y supervisar a los organismos notificados (organismos de evaluación de la conformidad), para supervisar el cumplimiento de los operadores (con verificación previa de los organismos notificados cuando la evaluación de la conformidad sea preceptiva) y para sancionar en casos de incumplimiento. Cuando resulte necesario realizar una evaluación de la conformidad por un tercero, dichas evaluaciones no serán realizadas por las autoridades, sino por organismos notificados, designados a tal efecto, de acuerdo con la propuesta de Reglamento y cualquier otra normativa de armonización de la UE que resulte aplicable. A nivel de la UE, la Comisión juega un papel clave a la hora de modificar la propuesta de Reglamento por medio de actos delegados y de establecer estándares mediante actos de ejecución. Además, se constituirá un nuevo Comité Europeo de Inteligencia Artificial (formado por representantes de la Comisión, un miembro de cada una de las 27 autoridades nacionales competentes y el Supervisor Europeo de Protección de Datos). La Agencia de la Unión Europea para la Ciberseguridad (ENISA) podrá intervenir en relación con cuestiones relacionadas con la ciberseguridad. Finalmente, la Comisión, en colaboración con los Estados miembros, creará una base de datos europea para la IA de alto riesgo independiente. Esta base de datos contendrá cierta información, que será accesible al público, relativa a los sistemas de IA de alto riesgo, que deberán registrarse antes de su introducción en el mercado.

Si bien quedarán sujetos a obligaciones de confidencialidad como cualquier otra autoridad regulatoria, cabe destacar que las autoridades supervisoras (y organismos notificados) podrán tener acceso a los datos, documentación, propiedad intelectual, información confidencial y secretos comerciales (incluyendo el código fuente).

9 ¿Pretende la propuesta de Reglamento ser omnicomprensiva y abordar todas las cuestiones relacionadas con la IA?

El Reglamento es horizontal, con un enfoque intersectorial, pero las regulaciones sectoriales específicas podrán incluir particularidades para las industrias verticales. Algunos de los retos que plantea la IA fueron objeto de las resoluciones emitidas por el Parlamento Europeo en octubre de 2020. La propuesta no aborda la responsabilidad, los derechos de propiedad intelectual y ciertos temas éticos esenciales, pese a que los considerandos de la propuesta de Reglamento recalcan ampliamente las cuestiones éticas.

La propuesta de Reglamento no afecta a la aplicación de las normas de responsabilidad de los prestadores de servicios de intermediación de la futura Ley de Servicios Digitales, que sustituirá a la Directiva de Comercio Electrónico. Esta norma introducirá obligaciones relacionadas con la transparencia y auditoría de los sistemas algorítmicos para las organizaciones que conecten a los consumidores con productos, servicios y contenido multimedia. Por este motivo, la propuesta de Reglamento no se refiere a los algoritmos utilizados en plataformas online y en el ecosistema de la sociedad de la información. Es posible que ciertos algoritmos utilizados en la publicidad programática se prohíban por tratarse de prácticas de manipulación o explotación. Pero, como se indicaba anteriormente, esto requeriría una modificación de la lista de sistemas de IA prohibidos, ya que actualmente no están incluidos.

Por su parte, las normativas de protección de datos, de competencia y de consumidores complementarán la propuesta de Reglamento, junto con los marcos legales sectoriales específicos.

10 Similitudes entre el Reglamento y el RGPD

Como se mencionaba más arriba, la nueva regulación sobre IA será complementaria del Reglamento General de Protección de Datos (RGPD) y no afectará a su aplicación. Además, existen muchas similitudes entre ambos Reglamentos, lo que da a entender que la Comisión pretende conseguir un objetivo similar con este nuevo instrumento legal: establecer un estándar o referente global que incorpore el respeto por los derechos fundamentales.

Otros ejemplos de paralelismos entre la propuesta de Reglamento y el RGPD incluyen:

i. El ámbito extraterritorial: los requisitos y obligaciones aplican a los proveedores y usuarios de sistemas de IA en la UE, con independencia de si los sistemas están ubicados dentro o fuera del territorio de la Unión;

ii. El esquema de sanciones para las infracciones también es similar, aunque el Reglamento propone un incremento en comparación con el RGPD;

iii. La metodología incluye autoevaluaciones ex ante (evaluaciones por terceros cuando los sistemas de IA están destinados a ser utilizados para la identificación biométrica remota de personas) para verificar la conformidad con los requisitos, así como la supervisión continua a lo largo del ciclo de vida del sistema de IA;

iv. Las obligaciones de rendición de cuentas exigen que los operadores lleven registros y conserven documentación que pruebe el cumplimiento durante un periodo de conservación establecido;

v. Los proveedores ubicados fuera de la UE pero que comercialicen la IA dentro de la Unión deben designar un representante legal que se encuentre en la UE y que podrá responder por los incumplimientos del Reglamento;

vi. Los requisitos deben implementarse desde el diseño, ex ante, en el caso de IA de alto riesgo y la responsabilidad comienza desde el principio del proceso;

vii. Una vez el Reglamento entre en vigor, habrá una moratoria de 24 meses para adaptarse;

viii. El marco pivota en torno a la piedra angular de la finalidad del sistema de IA: esta finalidad determinará el cumplimiento en relación con la transparencia sobre el objetivo de la IA;

ix. Un enfoque basado en los riesgos para las medidas técnicas y organizativas;

x. Las organizaciones disponen de flexibilidad para determinar la ruta o las soluciones técnicas para lograr el cumplimiento. La forma de cumplir con los requisitos es abierta, teniendo en cuenta el estado de la técnica.

11 Fechas importantes que tener en cuenta

El proceso legislativo podría durar más de un año hasta que se apruebe el Reglamento, aunque a las instituciones europeas les gustaría agilizar el proceso lo máximo posible, siendo conscientes de que, de otra manera, se perdería su propósito.

Una vez esté aprobado, entrará en vigor 20 días después de su publicación y habrá una moratoria de dos años antes de que sea plenamente aplicable. En la práctica esto supone que las organizaciones contarán con 24 meses para adaptarse a las obligaciones de la IA durante los cuales no estarán sujetas a sanciones, aunque deberán garantizar el cumplimiento.

12 ¿Qué deberían hacer las organizaciones antes de que se apruebe el Reglamento?

Un reglamento es un instrumento legislativo que en el sistema de la UE no requiere de transposición al Derecho nacional ni de desarrollos adicionales para ser vinculante. El Reglamento de IA comenzará a ser imperativo una vez entre en vigor, tras su publicación, durante el periodo de moratoria (ver comentarios en apartado 11). Esto significa que las autoridades de supervisión podrán solicitar pruebas de cumplimiento (i.e. documentación, archivos de registro) desde el primer día de aplicación.

Hasta que finalice el proceso legislativo y se apruebe el Reglamento, el texto actual de la propuesta está sujeto a cambios. Pero, a pesar de las modificaciones finales, el mensaje clave seguirá siendo el mismo: se prohibirán ciertos usos de la IA, mientras que otros se considerarán de alto riesgo y estarán sujetos a estrictos requisitos regulatorios. Por tanto, considerando que la IA se utiliza cada vez más por organizaciones en distintas áreas de actividad (e.g. RRHH, big data, bots o seguridad), lo primero que hay que hacer es asegurarse de que las organizaciones son conscientes del futuro marco aplicable a la IA. En segundo lugar, después de evaluar la clasificación del sistema de IA (determinando la aplicación de la propuesta de Reglamento), crear un inventario y mapeo de la IA que se utiliza actualmente (tanto directamente, como a través de herramientas de terceros) es crucial para planificar la estrategia de IA y datos y evitar urgencias a última hora o exponerse a riesgos de incumplimiento. Una parte del ejercicio de mapeo consistirá en entender mejor la posición de la organización en la cadena de valor, ya que es fundamental para blindar la responsabilidad y asumir únicamente las consecuencias de modificaciones deliberadas de la finalidad o de la propia IA. Un conocimiento adecuado de la IA que esté implementada o que se pretenda implementar será la base para elaborar un modelo de gobernanza de IA y datos a medida. Una vez se hayan determinado de forma apropiada los usos y finalidades de los sistemas, se podrá iniciar un análisis de deficiencias seguido de un análisis de riesgos, aunque es probable que dicho análisis deba actualizarse una vez se haya publicado el texto definitivo.

Incluso sin la propuesta de Reglamento, las organizaciones tienen que pensar sobre su estrategia de digitalización, incluyendo los casos en los que las herramientas de IA sustentan servicios, productos y actividades clave. Este ejercicio sentará las bases de las políticas de IA y gobernanza de datos (incluyendo los ángulos ético, técnico y legal), así como la implementación de la gestión de riesgos específica para la IA, a efectos de fomentar un enfoque de *"cumplimiento desde el diseño"*.

13 Conclusión: actuar lo antes posible

Es importante entender el Reglamento y el impacto que tendrá sobre las organizaciones, especialmente si actualmente no cuentan con un registro o inventario de todas las herramientas y procesos de IA.

Los equipos de EY que prestan asesoramiento en materia legal, técnica, de políticas públicas y gobernanza están trabajando juntos para ofrecer una solución integral para los clientes, que promueva las mejores prácticas. Las organizaciones que no comiencen con la clasificación de la IA que estén utilizando, produciendo o contratando a terceros corren el riesgo de no tener tiempo suficiente para cumplir.

Dr. Peter Katko

Responsable de Derecho Digital de EY Global & EMEIA

Socio, Ernst & Young Law GmbH

+49 89 14331 25951

peter.katko@de.ey.com

Blanca Escribano Cañas

Socia, Responsable de Derecho Digital - España

Ernst & Young Abogados, S.L.P.

+34 699 637 620

Blanca.Escribano.Canas@es.ey.com

EY | Building a better working world

En EY trabajamos para construir un mundo que funcione mejor, ayudando a crear valor a largo plazo para los clientes, las personas, la sociedad y generar confianza en los mercados de capital.

Gracias al conocimiento y la tecnología, los equipos de EY, en más de 150 países, generan confianza y ayudan a las compañías a crecer, transformarse y operar.

EY es líder mundial en servicios de auditoría, fiscalidad, estrategia, asesoramiento en transacciones y servicios de consultoría. Nuestros profesionales hacen las mejores preguntas para encontrar nuevas respuestas a los desafíos a los que nos enfrentamos en el entorno actual.

ey.com/es_es