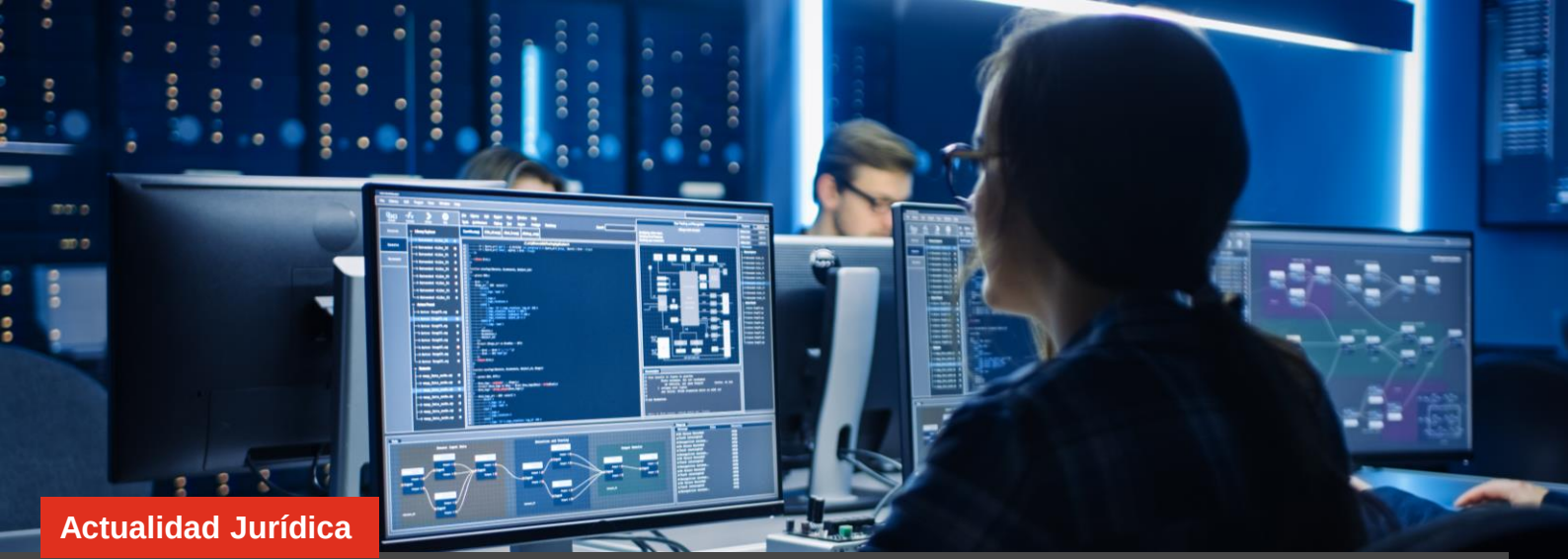


Actualidad Jurídica

Creación del *Sandbox* regulatorio de la Inteligencia Artificial

Noviembre 2023

Analizamos la puesta en marcha del primer entorno controlado de pruebas para ensayar la aplicación de ciertos requisitos previstos en la Propuesta de Reglamento de IA

Creación del *Sandbox* Regulatorio

El **Real Decreto 817/2023, de 8 de noviembre**, tiene como objeto la creación del primer entorno controlado de pruebas (*Sandbox*), en colaboración con la Comisión Europea, para ensayar la aplicación de ciertos requisitos previstos en la **Propuesta de Reglamento de Inteligencia Artificial** (en adelante, la "Propuesta IA") a los sistemas de inteligencia artificial de alto riesgo, con el objetivo de obtener, como resultado de este ensayo, unas guías basadas en la evidencia y la experimentación que ayuden a las empresas al cumplimiento de la Propuesta IA.

Esta iniciativa, tal y como describe el expositivo del Real Decreto, forma parte de la estrategia española de **transformación digital** (Agenda de España Digital 2026), a la vez que responde al compromiso establecido en la **Carta de Derechos Digitales** para "establecer un marco ético y normativo que refuerce la protección de los derechos individuales y colectivos".

De esta manera, España toma la delantera y es el **primero de los Estados Miembros en poner en funcionamiento un Sandbox en materia de Inteligencia Artificial** (IA), avanzándose así a lo establecido en el artículo 53 de la Propuesta, por el que se prevé la implementación de este tipo de entornos controlados para, entre otros:

- Fomentar la innovación y la competitividad
- Facilitar el acceso al mercado europeo para los sistemas de IA
- Mejorar la seguridad jurídica y contribuir al intercambio de buenas prácticas entre autoridades
- Contribuir al aprendizaje regulatorio basado en evidencias extraídas del campo de pruebas

El *Sandbox* utilizará como referencia, durante toda su vigencia, la Propuesta IA según la posición del Consejo de la Unión Europea de 25 de noviembre de 2022, por lo que las obligaciones que finalmente puedan resultar aplicables a los sistemas de IA estarán condicionadas por la aprobación del texto definitivo del Reglamento europeo de la IA, que actualmente se encuentra en fase de negociación mediante trílogos.

¿Hablamos?

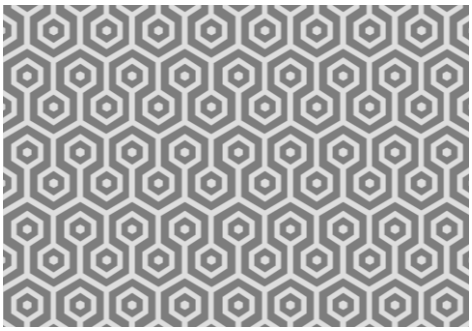
Assumpta Zorraquino
Socia responsable de Regulación Digital en el departamento de New Law de PwC Tax & Legal
assumpta.zorraquino@pwc.com

Roger Vilanova Jou
Abogada del área de Regulación Digital en el departamento de New Law en PwC Tax & Legal
roger.vilanova.jou@pwc.com

Lucía Etxe Rivas
Abogada del área de Regulación Digital en el departamento de New Law en PwC Tax & Legal
lucia.etxe.rivas@pwc.com

pwc

(...) tendrá una vigencia de treinta y seis (36) meses o, en su caso, hasta que resulte de aplicación el Reglamento europeo de IA".



Duración

El presente Real Decreto, que entró en vigor el 10 de noviembre de 2023**, tendrá una vigencia de treinta y seis (36) meses** o, en su caso, hasta que resulte de aplicación el Reglamento europeo de IA. Esta circunstancia evidencia que, una vez aprobada la versión final del Reglamento, **deberá valorarse la eficacia de las lecciones aprendidas en el marco del *Sandbox*.**

De esta forma, el *Sandbox* proporciona, por un espacio de tiempo determinado, un **contexto estructurado para el desarrollo de las actuaciones necesarias para que los proveedores de sistemas de IA,** puedan probar la implementación de ciertos requisitos definidos en el Real Decreto bajo la supervisión del órgano competente, que en este caso es la Secretaría de Estado de Digitalización e Inteligencia Artificial.

Aspectos esenciales de la norma

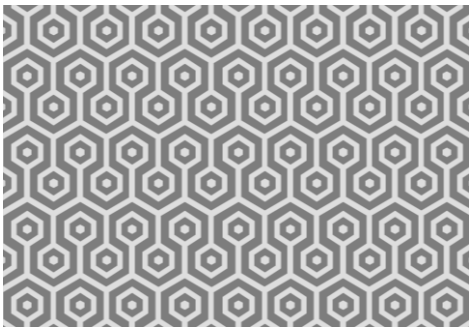
a) Objeto

El Real Decreto tiene por objeto establecer un entorno controlado de pruebas para ensayar el cumplimiento de ciertos requisitos por parte de algunos sistemas de inteligencia artificial que puedan suponer **riesgos para la seguridad, la salud y los derechos fundamentales de las personas**

b) Requisitos de elegibilidad

- A aquellos **proveedores** de IA y **usuarios** (personas jurídicas o administraciones y entidades del **sector público**) **residentes en España** o que tengan establecimiento permanente en España, o bien sean parte de una agrupación de entidades;
- En calidad de **usuario participante**, las personas jurídicas privadas o publicas que hagan uso de un sistema de inteligencia artificial de **alto riesgo, de propósito general o modelos fundacionales**, siempre que acceda conjuntamente con el proveedor IA;
- Se permite que se presente la solicitud de participación de **uno o varios sistemas de IA** considerados como de **alto riesgo** – enumerados en el Anexo II del Real Decreto-, de **propósito general o modelos fundacionales** (*foundational models*);
- Estos sistemas pueden ser de **nuevo desarrollo o sistemas ya establecidos**, con el requisito de que el nivel de desarrollo sea suficientemente avanzado como para que pueda comercializarse o ponerse en servicio dentro del espacio temporal del *Sandbox* o a su finalización;
- Las personas jurídicas privadas o administraciones públicas y entidades del sector público españolas que sean usuarias de alguno de los sistemas de IA objeto de la convocatoria, podrán acordar con el proveedor IA de dicho sistema la **participación conjunta** en este entorno.

El Real Decreto, **excluye del entorno de pruebas los sistemas de IA que tengan una finalidad militar o de seguridad nacional** cuando se sirvan de técnicas **subliminales** que trasciendan la consciencia de una persona para alterar su comportamiento cuando se sirvan de alguna de las **vulnerabilidades** de un grupo específico evalúen o **clasifiquen** a personas atendiendo a su conducta social, características personales o de su personalidad derivando



en un trato perjudicial o desfavorable o bien identifiquen biométrica y **remotamente** *en tiempo real* para su uso en espacios de acceso público con fines de aplicación de la ley, salvo para determinados supuestos específicos de investigación de **delitos o prevención de amenazas.**

c) ¿Cómo funcionarán las convocatorias para participar?

- Tras el proceso de **pre-registro** para mostrar interés finalizado el pasado 31 de octubre, las convocatorias para la participación en el *Sandbox* se aprobarán mediante **resolución de la Secretaría de Estado de Digitalización e IA** que se publicarán en el portal web de la Secretaría Desde el día siguiente de publicación de la convocatoria, el **plazo máximo para la presentación de las solicitudes será de 20 días hábiles**.

- En la convocatoria se especificará, entre otros aspectos, el **número de sistemas** de inteligencia artificial seleccionados, la **duración** del entorno controlado de pruebas, las **condiciones** para la participación conforme a los requisitos del Real Decreto, los **criterios** que se tendrán en cuenta para la evaluación de solicitudes, así como el peso de los mismos y los canales de comunicación;

- La solicitud deberá ir acompañada de una **memoria técnica** y una **declaración responsable** sobre el cumplimiento del principio de responsabilidad proactiva en materia de protección de datos.

El Real Decreto relaciona una **serie de documentación que deberán aportar** los participantes en el *Sandbox* para acreditar el cumplimiento de la normativa de protección de datos. Por ello, es especialmente relevante que las entidades participantes puedan asegurar el cumplimiento de requisitos como la llevanza actualizada de un **Registro de Actividades del Tratamiento (RAT),** con la realización de **análisis de riesgos para los derechos y libertades de las personas físicas,** y cuando sea necesario, la realización de una **Evaluación de Impacto relativa a la Protección de Datos (EIPD),** así como otros elementos listados en el Anexo V del Real Decreto, entre los que se incluye **un informe del Delegado de Protección de Datos (DPD)** en relación con el cumplimiento de la normativa de protección de datos en el sistema de IA.

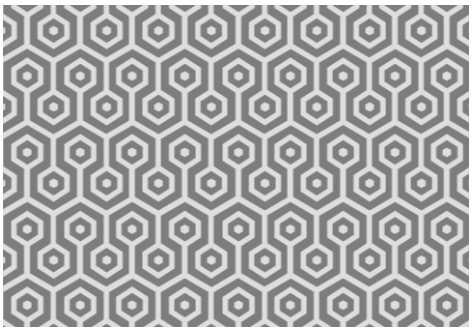
- La **Subdirección General de Inteligencia Artificial y Tecnologías Habilitadoras Digitales**, será la encargada de **valorar las solicitudes** según los criterios previstos en el Real Decreto, incluyendo el **grado de innovación del producto, el grado de impacto social y el grado de madurez del sistema;**

- La Secretaría deberá dictar **resolución** motivada en el que se anuncien los participantes del proyecto en un **plazo máximo de 60 días hábiles** desde la fecha de publicación de la convocatoria.

d) ¿Cómo se desarrollará el Sandbox?

La participación en el entorno controlado de pruebas tendrá como **objetivo cumplir con la implementación de los siguientes requisitos en los sistemas de IA**, con base a las especificaciones facilitadas por la Secretaría, que podrá ofrecer guías técnicas de ayuda y soporte:

- Establecimiento, implementación documentación y mantenimiento de un **sistema de gestión de riesgo del sistema de IA**;



- La **garantía** sobre los conjuntos de **datos** empleados para el entrenamiento del sistema;
- La **documentación técnica** del sistema de IA;
- El **registro automático de eventos (*logs*)** a lo largo del ciclo de vida del sistema;
- La seguridad sobre la **transparencia** para los usuarios del sistema, **evitando los posibles sesgos discriminatorios** que se puedan dar;
- Las **instrucciones de uso** en formato electrónico para que sea comprensible para los usuarios;
- Un diseño del sistema para que pueda ser **supervisado** por **personas físicas**;
- El desarrollo de la finalidad prevista con un nivel **adecuado de precisión, solidez y ciberseguridad**.

i. Declaración de cumplimiento (autoevaluación)

A la finalización de la etapa de desarrollo, el proveedor participante deberá realizar una **declaración de cumplimiento de los requisitos acordados.**

Esta declaración se iniciará con un **proceso de autoevaluación por parte del proveedor de IA**, y en su caso, el usuario participante, donde se valorarán y verificarán el cumplimiento según las recomendaciones que la Secretaría les facilite.

ii. Examen por la Secretaría

Una vez finalizada la autoevaluación, el participante presentará en la sede electrónica de la Secretaría competente la **documentación** indicada, que será examinada principalmente en lo relativo al **sistema de gestión de la calidad, la documentación técnica o el plan de seguimiento posterior a la comercialización.**

Esta evaluación determinará si dicha documentación es **favorable o no**. En el caso de ser favorable, el participante deberá **exponer la pertinencia de la autoevaluación de cumplimiento**. Por otro lado, en el caso de considerarse no favorable, el órgano competente le otorgará un plazo de 3 meses para permitirle cumplir con los requisitos.

iii. Implementación de un plan de seguimiento posterior a la comercialización

Tras esta fase, los proveedores y/o usuarios de IA deberán implementar un **sistema de seguimiento posterior a la comercialización**, para lo cual los participantes deberán documentar un sistema que sea **proporcional a los riesgos y uso previsto del sistema de IA**.

En el caso de que se produzcan **cambios sustanciales** en el sistema de IA de alguno de los proveedores participantes o en su titularidad, se deberá comunicar previamente a la Secretaría de Estado de Digitalización e Inteligencia Artificial quien decidirá si el proveedor IA participante continúa o no en el entorno y en qué condiciones.

iv. Finalización del entorno de pruebas

Con carácter previo a la finalización del entorno de pruebas, los proveedores y usuarios deberán entregar un **informe** a la **Subdirección General de Inteligencia Artificial y Tecnologías Habilitadoras Digitales**. El contenido de este informe se indicará en las **guías** que ofrezca el órgano competente.

Tras completar las fases del entorno controlado de pruebas, las empresas participantes recibirán un **documento acreditativo** de su participación junto a un informe en el que se valoren los resultados obtenidos.

En resumen

El ***Sandbox* Regulatorio de la Inteligencia Artificial,** pretende ser un espacio ideado para **conectar a las autoridades competentes con los desarrolladores** y entidades usuarias de sistemas de IA.

Esta propuesta española tiene como objetivo generar directrices de **buenas prácticas** y comprobar el desarrollo de estos sistemas en el ordenamiento jurídico.

El Real Decreto mediante el que se establece el entorno controlado de pruebas, establece quienes pueden participar en dicho entorno y el **procedimiento de participación** a seguir. También se establecen las **garantías** que regirán dicho procedimiento, junto al **régimen de responsabilidades** de los sujetos participantes.

Este proceso servirá asimismo para poner a prueba el funcionamiento de la **nueva Agencia Española de Supervisión de la Inteligencia Artificial.**

e) ¿Qué garantías exige el Real Decreto para los participantes?

- **Protección de datos**

La aceptación a la participación del entorno controlado implica el compromiso y reconocimiento de cumplimiento de la normativa en materia de propiedad intelectual.

- **Confidencialidad**

Se aplicará la garantía de confidencialidad respecto la información que aporten tanto los proveedores como los usuarios participantes sobre procedimientos propios de las empresas u otras entidades, planes comerciales, derechos de propiedad intelectual e industrial o secretos empresariales, así como sobre los datos e información facilitados durante el proceso de autoevaluación.

- **Utilización posterior de la información anonimizada**

La información recabada por el órgano competente podrá ser utilizada cuando se garantice su completa anonimización, para la elaboración de guías de buenas prácticas.

f) ¿Cuál es el régimen de responsabilidad de los participantes?

En materia de responsabilidad, tanto el proveedor IA participante como, en su caso, el usuario participante será **responsable de los daños sufridos por cualquier persona como consecuencia de la aplicación del sistema** de inteligencia artificial en el contexto del entorno controlado.

Conclusiones

El propósito de este *Sandbox* español es **implementar de manera práctica y poner en funcionamiento los requisitos incluidos en la Propuesta de Reglamento de la IA**, de forma que tanto las entidades participantes como las autoridades competentes puedan **evaluar** su **aplicabilidad** y **cumplimiento**. Tendrá como resultado la **elaboración de un informe,** que se publicará en el portal web de la Secretaria de Estado de Digitalización e IA, que tendrá como objetivo destacar **las buenas prácticas y lecciones aprendidas,** así como unas Guías técnicas de ejecución y supervisión basadas en la evidencia y la experimentación.

Los resultados podrán ser empleados en el futuro por la Comisión Europea para la **elaboración de Directrices de la Unión Europea** y, como contribución al proceso de normalización, para **facilitar el cumplimiento del Reglamento sobre IA por parte de las empresas** y, en particular, las PYMES.

Esta iniciativa, ya prevista en el artículo 53 de la Propuesta de Reglamento de la IA, forma parte de la estrategia de transformación digital, denominada Agenda **España Digital 2026**, por la que España está tomando el **liderazgo de la implementación anticipada** de la normativa europea en materia Inteligencia Artificial.

Las lecciones aprendidas del presente *Sandbox* deberán ser **analizadas y comparadas** una vez se haya aprobado el **texto definitivo del Reglamento de la IA**, actualmente en fase de negociación mediante trílogos. Desde el departamento de Regulación Digital de PwC Tax & Legal seguiremos de cerca su evolución.