OPINIÓN

JUEVES 12 DE SEPTIEMBRE DE 2024

Inteligencia Artificial – Europa “en la pole positon” de su regulación

Por LUIS H. VIZIOLI (*)
Vizioli & Triolo Abogados

El 12 de julio de 2024 se publicó en el **Diario Oficial de la Unión Europea el Reglamento Europeo de Inteligencia Artificial** (“Reglamento”), también conocido como la Ley de Inteligencia Artificial (AI Act, por sus siglas en inglés), el cual entró en vigencia el pasado 1 de agosto de 2024. Es una propuesta legislativa desarrollada por la Comisión Europea para regular el uso de la inteligencia artificial (IA) en la Unión Europea (UE).

Al hablar de IA, es inevitable recordar innumerables largometrajes y bibliografía de corte futurista en los cuales se nos presenta un mundo distópico gobernado por máquinas inteligentes que superan y subyugan a la humanidad. En contraposición con dichos temores populares reflejados en la pantalla grande y en novelas, la promulgación del Reglamento representa un enfoque realista y proactivo para evitar tal escenario. En vez de dejar librado a su suerte y sin control el desarrollo de IA, este Reglamento establece un marco regulatorio diseñado para supervisar y servir de guía a su desarrollo, asegurando que se respeten los derechos fundamentales del individuo y la sociedad. Al regular la IA de manera responsable, la UE procura fomentar la innovación en un entorno seguro y ético, evitando abusos en el desarrollo frenético de la IA, contrastando así con la idea de un futuro

donde ésta se convierte en una amenaza para la humanidad.

I. Objetivo.

Su objetivo es establecer un marco legal que garantice la seguridad, la transparencia, y el respeto a los derechos fundamentales en el desarrollo y uso de sistemas de IA.

Conforme el artículo 1 del Reglamento "El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales, en particular la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de inteligencia artificial («sistemas de IA») en la Unión, así como brindar apoyo a la innovación".

De la propia definición de su objetivo legislativo se desprenden un sinnúmero de elementos que explican, en su conjunto, el extenso y ambicioso alcance de la iniciativa y el cuidado que la misma profesa en favor del ser humano.

Su objetivo principal se centra en:

- Establecer un marco regulatorio que propicie la innovación en IA, y permita a empresas y desarrolladores europeos competir a nivel de la unión y en forma global, adhiriendo a altos parámetros éticos y de seguridad en un mismo plano de igualdad;
- Proteger a los ciudadanos europeos de forma tal que los sistemas de IA no vulneran la seguridad física y emocional o violen derechos fundamentales garantizados por la normativa de la UE o derechos locales, tales como la discriminación y/o privacidad; y
- Exigir que los sistemas de IA sean transparentes en cuanto a su funcionamiento y marco decisorio. Ello conlleva la obligación -en cabeza de los desarrolladores- de cumplir ciertas pautas estrictas en cuanto a su desarrollo, puesta en el mercado, utilización y post evaluación, así también como la posibilidad que los usuarios puedan cuestionar y denunciar resultados potencialmente negativos.

II. Ámbito de Aplicación.

Su ámbito de aplicación se circunscribe dentro de la UE a: los proveedores que introduzcan en el mercado sistemas de IA; los responsables del despliegue de sistemas de IA que estén establecidos o ubicados en la UE o en un tercer país, cuando la información generada por el sistema de IA se utilice en la UE; los fabricantes, importadores y distribuidores de sistemas de IA; los representantes autorizados de los proveedores que no estén establecidos en la

Unión; y las personas afectadas que estén ubicadas en la UE.

En contraposición, el Reglamento no es aplicable en aquellos ámbitos que quedan fuera de la aplicación del derecho de la UE. Asimismo, no afecta a las competencias de los Estados miembros en materia de seguridad nacional, y se entiende sin perjuicio de las normas establecidas por otros actos jurídicos de la UE relativos a la protección de los consumidores y a la seguridad de los productos, entre otros derechos fundamentales.

Cabe destacar que el Reglamento no aplica a los sistemas de IA desarrollados y puestos en servicio específicamente con la investigación y el desarrollo científicos como única finalidad. Tampoco aplica respecto de aquellos sistemas de IA que, se introduzcan en el mercado, se pongan en servicio o se utilicen, con o sin modificaciones, exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades.

III. Clasificación de Sistema de IA – Diversidad de Riesgos.

A los fines del Reglamento, "sistema de IA" significa "un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, 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 información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales."

El Reglamento clasifica los sistemas de IA en cuatro niveles de riesgo.

En forma sumaria, los sistemas de IA de riesgos "inaceptables" están directamente prohibidos. El Reglamento se concentra en los sistemas de IA de "alto riesgo", los que están estrictamente regulados. Mucho más breve es la regulación sobre los sistemas de IA de "riesgo limitado", los que quedan sujetos a obligaciones de transparencia más leves. Finalmente, el llamado "riesgo mínimo" no está regulado.

3.1 Riesgo Inaceptable – Prácticas de IA Prohibidas.

Está prohibida la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que:

(A) Manipule el comportamiento humano con el objetivo de alterar comportamiento individual o grupal.

Dentro de esta área se encuentra sistemas de IA que generen:

(a) Técnicas de manipulación subliminal que trascienden la conciencia; y

(b) la explotación de alguna vulnerabilidad de una persona o un grupo específico derivada de su edad o discapacidad, o de una situación social o económica específica.

(B) Califique socialmente a una persona o grupo con el fin de:

(a) evaluar o clasificarla en base a su comportamiento o características personales, de forma tal que dicha calificación genere un trato perjudicial o desfavorable hacia la/s mismas y que no guarde relación con los contextos donde se generaron o recabaron los datos originalmente o sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de éste.

(b) evaluar o predecir su intención criminal sustentado en la elaboración de su perfil, rasgos y características de su personalidad (ciertas excepciones aplican). Me pregunto ¿qué opinaría Césare Lombroso (1835-1909)?

(C) Propicie el reconocimiento facial en espacios públicos en tiempo real con el propósito de:

(a) inferir emociones de una persona en su lugar de trabajo y/o estudio (excepto bajo ciertos motivos médicos o de seguridad);

(b) crear o ampliar bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión.

(c) clasificar a las personas y permitir "... deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual... ". Esta prohibición no alcanza al conjunto de datos biométricos adquiridos legalmente; o

(d) aplicar la ley en general, salvo que dicho uso sea estrictamente necesario para la identificación y búsqueda selectiva de víctimas de secuestro, desaparecidos, trata o explotación humana o de personas sujetas o potencialmente pasibles de proceso penal con penas de al menos cuatro años de prisión. Su utilización queda sujeta a las garantías de los derechos fundamentales del individuo conforme la legislación local y, en ocasiones, a la previa o posterior autorización judicial.

3.2 Riesgo Alto

La clasificación de un sistema de IA como “de alto riesgo” se limita a aquellos que tengan un efecto perjudicial importante en la salud, la seguridad y los derechos fundamentales de las personas de la UE.

El Reglamento se centra en estos sistemas de IA “de alto riesgo” regulándolos de forma tal que sean fiables, sólidos, precisos y con un grado de ciber seguridad que permita su funcionamiento de manera uniforme durante todo su ciclo de vida útil.

La magnitud del perjuicio que puede causar esta categoría de sistema es directamente proporcional a la afectación de derechos fundamentales promulgados en la Carta de los Derechos Fundamentales de la UE (“Carta”) , cuyo rango contempla el derecho y respeto a la dignidad humana y a la vida privada y familiar; la libertad de reunión, de asociación, de expresión e información; la protección al consumidor y al medio ambiente; derecho a la igualdad de género; derechos del trabajador y personas discapacitadas; derecho a la tutela e imparcialidad judicial, y al principio de inocencia; derecho a la salud y educación, así como también a los derechos del niño consagrados éstos en la Carta y en la Convención sobre los Derechos del Niño de las Naciones Unidas.

Esta categoría cubre las siguientes áreas:

(A) Infraestructuras críticas. Son sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de infraestructuras digitales tales en actividades relacionadas con el suministro de agua, gas, calefacción y electricidad y/o tránsito. Ello así, atento que su mal funcionamiento podría alterar materialmente el desarrollo de actividades sociales y económicas a la vez que poner en peligro la vida y salud de las personas en masa.

(B) Educación y formación profesional. Son sistemas de IA utilizados en el ámbito educativo y de formación profesional que mediante la evaluación del aprendizaje determinan la admisión a determinados claustros y/o trabajos. Estos sistemas podrían afectar el derecho a la educación y formación profesional, así como discriminar al individuo en razón de su edad, discapacidad, creencias, origen racial, religión u orientación sexual.

(C) Empleo y gestión de los trabajadores. Son aquellos sistemas de IA que se emplean en la contratación y selección de personal, así como en la posterior asignación de labores, la evaluación de su rendimiento y su continuidad laboral. Puede afectar derechos fundamentales tales como el derecho al trabajo, a una subsistencia digna, a la protección de los datos personales y a la intimidad.

(D) Servicios y prestaciones esenciales. Son sistemas de IA que permiten a las autoridades

conceder, reducir, ampliar o revocar el acceso a servicios y prestaciones esenciales, de carácter público y privado. Entre ellas encontramos las referidas a la salud, seguridad social, a la protección de la maternidad, enfermedades laborales, ayuda de vivienda, pensiones y jubilaciones en las cuales generalmente el individuo se encuentra con un alto grado de vulnerabilidad respecto de las propias autoridades.

Estos sistemas podrían tener un impacto material en los medios de subsistencia de las personas, a la vez que afectar derechos fundamentales, como el derecho a la protección social, a la no discriminación, y a la dignidad humana.

También son considerados dentro de esta categoría los sistemas empleados para evaluar la calificación crediticia o solvencia de las personas, atento a que tendrán un impacto directo en la inclusión financiera de la misma y en toda área en la cual la propia economía del individuo tenga incidencia.

Los sistemas de IA usados con estos fines pueden discriminar a determinadas personas o grupos y perpetuar patrones históricos de discriminación, como por motivos de origen racial o étnico, género, discapacidad, edad u orientación sexual, o generar nuevas formas de discriminación.

Finalmente, se incluyen en esta área los sistemas que administran y clasifican llamadas de emergencia y deciden el envío de asistencia en situaciones de emergencia, situaciones que importan decisiones críticas para la vida y la salud de las personas y sus propiedades.

3.3 Riesgo Limitado

Los sistemas de IA con riesgo limitado son aquellos que presentan un riesgo moderado para los usuarios y la sociedad. Estos sistemas no requieren una regulación tan estricta como los de alto riesgo, pero están sujetos a obligaciones específicas para garantizar la transparencia y la seguridad. Esto se traduce en la necesidad que el usuario, en la primera interacción, deba ser informado que está interactuando con un sistema de IA y/o que su contenido, imágenes o texto han sido generados de manera artificial. El clásico ejemplo es al servicio de chat box cuyo usuario debe ser consciente de que no está interactuando con un humano.

A tal efecto, la autoridad de aplicación facilitará la elaboración de códigos de buenas prácticas a nivel de la UE para la advertencia al usuario del origen artificial del contenido pertinente.

Estos sistemas no requieren una evaluación de conformidad previa a su puesta en el

mercado, pero se espera que los desarrolladores y operadores adopten medidas para mitigar cualquier riesgo residual y garantizar un uso seguro y responsable.

3.4 Riesgo Mínimo

Los sistemas de IA que presentan un riesgo bajo, como la mayoría de las aplicaciones de IA en videojuegos, no requieren una intervención regulatoria específica. Estas aplicaciones de riesgo mínimo, incluidas muchas de las que están disponibles en el mercado único de la UE, como los videojuegos con IA y los filtros de spam, no están sujetas a regulación directa.

Aunque no se menciona específicamente como una categoría en un artículo específico, se infiere de la estructura regulatoria que los sistemas que no caen bajo las otras categorías son considerados de riesgo mínimo. Sin embargo, el hecho de que el Reglamento no imponga obligaciones específicas para las aplicaciones de IA que no se encuentran dentro de las categorías de mayor riesgo, no exime de la necesidad de gestionar y abordar los riesgos legales asociados. Estos pueden incluir cuestiones relacionadas con la propiedad intelectual, la protección de datos, la confidencialidad, los secretos comerciales, la ciber seguridad, la defensa de los consumidores, y el derecho laboral, civil y penal, entre otros.

IV. Obligaciones de los Proveedores de Sistemas de IA “de alto riesgo”.

El Reglamento desarrolla en forma estricta las obligaciones de los proveedores de sistemas de IA “de alto riesgo” centrándose en la gestión de riesgos, calidad de los datos, documentación técnica, transparencia y monitoreo continuo.

(A) Sistema de gestión de riesgos. Los proveedores deben implementar un sistema de gestión de riesgo de carácter continuo durante el ciclo de vida del sistema. El mismo requerirá revisiones y actualizaciones periódicas y sistemáticas, al igual que pruebas de calidad y funcionalidad. Deberá determinar los riesgos conocidos y previsibles (para la salud, la seguridad o los derechos fundamentales) tanto cuando se utilice conforme su finalidad como cuando se le dé un uso indebido “razonablemente previsible”, previo o post comercialización. También deberá prever las medidas para paliar dichos riesgos.

(B) Datos y gobernanza de datos. Se requiere el uso de datos de alta calidad y pertinentes para entrenar, validar y probar los sistemas de IA, asegurando su integridad y precisión. Se deben preservar y poner a disposición todo lo concerniente a las decisiones relativas al diseño; al origen, recolección, depuración, catálogo y finalidad de los datos; formulación de supuestos; el examen de potenciales “sesgos” discriminatorios y las medidas para mitigar o eliminar los mismos; detección de lagunas informativas.

(C) Documentación técnica. Los proveedores deben mantener documentación técnica detallada de sus sistemas de IA para garantizar la transparencia y trazabilidad. La misma debe brindarse en forma clara y completa de forma tal que la autoridad de contralor puede determinar el cumplimiento de las normas previstas para este tipo de sistema. Si se tratara de empresas "pyme" estas pueden simplificar el proceso completando ciertos formularios preestablecidos.

(D) Registro de actividades. Es obligatorio mantener registros automáticos de las actividades del sistema de IA para supervisar su funcionamiento y detectar posibles irregularidades. En forma particular, dichos registros deben visar por la detección de situaciones de riesgo, el seguimiento luego de su comercialización, y la vigilancia del funcionamiento del sistema.

(E) Transparencia y suministro de información. Los proveedores deben asegurarse de que los usuarios (incluyendo quienes los comercialicen) comprendan el funcionamiento del sistema de IA y sus limitaciones, facilitando información clara y accesible en forma de instrucciones de uso.

(F) Vigilancia Humana. Los sistemas de IA de alto riesgo se deben diseñar y desarrollar de forma que estén sujetos a supervisión por personas físicas durante el período que estén en uso. A tal efecto, el proveedor debe equiparlos con herramientas de interfaz humano-máquina adecuadas. Por su parte, las personas que estén a cargo de dicha supervisión deberán entender las capacidades y limitaciones y poder vigilar su funcionamiento, por ejemplo, con el objetivo de detectar, contener y resolver potenciales comportamientos anómalos.

V. Obligaciones de los Proveedores de Modelos de IA de Uso General

El Reglamento también centra su atención en los “modelos de IA”.

Básicamente, un modelo de IA es un componente específico que realiza el procesamiento de datos y genera resultados, como predicciones, recomendaciones, o decisiones. Es un algoritmo entrenado con datos para realizar ciertas tareas, pero por sí solo no constituye un sistema completo. Es el "motor" que impulsa el funcionamiento de un sistema de IA.

Es decir, el **modelo de IA** es un componente algorítmico que realiza tareas de procesamiento de datos, mientras que un **sistema de IA** es la aplicación completa que utiliza uno o más modelos de IA para interactuar con usuarios o entornos, y que está sujeto a regulación según su riesgo.

Los proveedores de modelos de IA de Uso General, deberán cumplir con ciertos procedimientos, tales como:

- Preparar la documentación técnica del modelo (incluyendo lo relacionado con el proceso de formación y ensayo y los resultados de la evaluación) y su actualización, y la pondrán a disposición de otros proveedores de IA que puedan llegar a integrarla con otros sistemas.
- Establecer protocolos para cumplir con la legislación de la UE en materia de propiedad intelectual.
- Poner a disposición del público un resumen para el entrenamiento del modelo de IA de uso general.

Cuando el modelo de IA conlleva un "riesgo sistémico" (mayor trascendencia en cuanto a su incidencia colectiva a partir de parámetros específicos) los proveedores de modelos de IA de Uso General con riesgo sistémico también deberán: realizar evaluaciones y pruebas de modelos para identificar y mitigar los posibles riesgos sistémico, incluido su origen, y documentar los incidentes graves y las posibles medidas paliativas, notificando las mismas a la autoridad de aplicación. Por último, deberán garantizar un nivel adecuado de protección de la ciber seguridad.

VI. Gobernanza

El Reglamento designa varias autoridades responsables de la ejecución y supervisión de sus disposiciones Estas autoridades trabajan en conjunto para garantizar que los sistemas de IA se desarrollen y utilicen de manera segura y conforme a la normativa europea. Estas incluyen:

La Oficina Europea de Inteligencia Artificial, una entidad creada para apoyar la implementación, interpretación y supervisión del Reglamento a nivel de la UE. Esta entidad tiene por objeto la supervisión centralizada y coordinada del Reglamento, garantizando que las normas se apliquen de manera uniforme y efectiva en toda la UE.

Entre sus funciones se destacan la coordinación de las actividades con las respectivas autoridades nacionales competentes; el asesoramiento y orientación técnica y legal a las autoridades nacionales, empresas, y otras partes interesadas; la recopilación de información tendiente a mejorar el Reglamento y sus mecanismos; la cooperación entre Estados miembros; y la supervisión de los sistemas de IA comercializados en la UE.

Por su parte, cada Estado miembro de la UE debe designar una o más autoridades nacionales para supervisar la aplicación del Reglamento en su territorio. Son los "organismos notificados" entidades acreditadas por las autoridades nacionales competentes para realizar evaluaciones de conformidad de los sistemas de IA de alto

riesgo.

También se crea el Comité Europeo de Inteligencia Artificial, organismo que asegurar la coherencia en la aplicación del Reglamento en toda la UE. Este comité está compuesto por representantes de las autoridades nacionales y la Comisión Europea, y se encarga de coordinar y apoyar la implementación del Reglamento, así como de emitir directrices y recomendaciones.

Por su parte, la Comisión Europea supervisa en forma general la aplicación del Reglamento, y hasta tiene la facultad de intervenir en casos transfronterizos.

Finalmente, se establece el mecanismo para instrumentar un "foro consultivo" para brindar conocimientos técnicos y asesorar al Comité y a la Comisión, y un "grupo de expertos científicos independientes" destinado a apoyar las actividades relativas al cumplimiento previstas en el Reglamento.

VII. Sanciones

El Reglamento dispone un régimen sancionador con multas. Cada Estado miembro debe velar por la ejecución de las mismas y garantizar el debido proceso. Hay circunstancias atenuantes y agravantes, al igual que cierta protección a las empresas Pyme en virtud de su condición de tal.

Las multas procuran un efecto de disuasión y contemplan distintos rangos, a saber:

- Hasta 35 millones de Euro o 7% del volumen anual de negocio para empresas, lo que resulte mayor, por incumplir las prohibiciones del Reglamento (sistemas de IA de riesgo inaceptable).
- Hasta 15 millones de Euros o 3% del volumen anual de negocio, lo que resulte mayor, por incumplir las obligaciones del Reglamento (distintas de las prohibiciones) a proveedores, importadores, distribuidores, usuarios.
- Hasta 7.5 millones de Euros, o 1% del volumen anual de negocio, lo que resulte mayor, por suministrar información incorrecta a las autoridades nacionales competentes.

Asimismo, la imposición de estas multas conlleva la posibilidad que se prohíba el uso del sistema de IA de la empresa incumplidora, se revoquen certificaciones y licencias, y las personas físicas responsables por tales incumplimientos sean pasibles de acciones civiles o penales por daños.

VIII. Plazos

El Reglamento establece un extenso marco de hitos temporales para su entrada en vigor y aplicación (https://artificialintelligenceact.eu/es/implementation-timeline/), con el fin que todos los sujetos tengan posibilidad de acomodar su accionar al mismo. Ello también es aplicable a cada uno de los Estados miembros que tienen la obligación de asignar recursos, legislar y coordinar su actividad entre sí.

El Reglamento se publicó en el Diario Oficial de la UE el pasado 12 de julio de 2024 y entró en vigencia el 1 de agosto.

A partir de su entrada en vigencia, se establecen distintos plazos en particular para la aplicación gradual de las distintas disposiciones. En forma sumaria, los más relevantes son:

- a los seis meses (2/2/25), entran en vigencia las prohibiciones sobre distintos sistemas de IA (capítulo 1 y 2 del Reglamento).
- a los doce meses (2/8/24), entran en vigencia los capítulos relacionados con organismos competentes, modelos de uso general, gobernanza, confidencialidad y sanciones.
- a los veinticuatro meses (2/8/26), comienza a aplicarse el Reglamento en general, salvo por ciertas disposiciones de sistemas de IA de alto riesgo, las cuales entrarán en vigencia a los treinta y seis meses (2/8/27).
- a los veinticuatro meses (2/8/26), los Estados miembros deberán haber establecido regulación de IA a nivel nacional y garantizado un adecuado mecanismo de cooperación entre las distintas autoridades.

IX. Conclusiones

El Reglamento representa un avance crucial en la creación de un marco legal coherente, homogéneo y seguro para el desarrollo y aplicación de la IA en la UE. Al centrarse en un enfoque basado en el riesgo, asegura que las aplicaciones más críticas en cuanto a su impacto en la sociedad sean sometidas a una adecuada supervisión, al mismo tiempo que promueve la innovación en áreas con menor riesgo. La implementación de esta normativa es esencial para equilibrar el progreso tecnológico con la protección de los derechos fundamentales de los ciudadanos.

La propia existencia del Reglamento tiene ya un impacto significativo en la práctica de los abogados europeos que asesoran a empresas, especialmente en áreas relacionadas con la tecnología, la regulación, y la protección de derechos. Por carácter transitivo, es de esperar que ocurra lo mismo con la profesión a nivel nacional

Será clave la capacitación para poder asesorar a los clientes en:

- la interpretación de las obligaciones del Reglamento (en nuestro caso, en la legislación local

correspondiente), especialmente en lo que respecta a la clasificación y gestión del riesgo de los sistemas de IA.
- la revisión y actualización de contratos relacionados con el desarrollo, la compra y el uso de sistemas de IA.
- el asesoramiento respecto de la recolección, almacenamiento, y procesamiento de datos para garantizar que cumplan con las regulaciones sobre protección de datos, seguridad, y privacidad.
- el análisis de posibles responsabilidades y contingencias legales, y sus correspondientes estrategias para minimizar conflictos derivados del uso indebido o fallas de sistemas de IA.
- las estrategias para alentar un proceso de innovación y competitividad dentro del marco legal.
- el entendimiento de las nuevas obligaciones y mejores prácticas bajo la normativa aplicable, asegurando que todas las partes involucradas comprendan sus responsabilidades y el impacto del uso de IA.

En resumen, la promulgación del Reglamento (y a futuro la legislación local aplicable) exige, pero también presenta una oportunidad, para que los abogados ampliemos nuestro entendimiento respecto de los aspectos técnicos y normativos específicos de la IA, y consolidemos lazos con el cliente como asesores clave en la gestión del riesgo, el cumplimiento normativo de la IA, y la estructuración de negocios relacionados a ella.

(Link al Reglamento):

https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf

https://artificialintelligenceact.eu/es/

Citas

(*) Luis Hernán Vizioli es abogado, matriculado en el Estado de Nueva York (1997), y el Colegio Público de Abogados de la Capital Federal (1992). Se desempeñó en estudios jurídicos de Buenos Aires, San Pablo y Nueva York. Es egresado de la Facultad de Derecho y Ciencias Sociales de la Universidad de Buenos Aires (1991). Obtuvo un LLM de la Universidad de Illinois, Urbana - Champaigne, EE.UU. (1994) y un posgrado en Derecho de las Telecomunicaciones, Radiodifusión y Medios en la UBA (2002). Visiting Researcher en la Florida International University, Miami, EE.UU. (2016). Socio - Vizioli & Triolo Abogados – LHV@viziolitriolo.com.ar / www.viziolitriolo.com.ar.