3.
Innovación pública y Administración digital

La supervisión del cumplimiento del Reglamento de inteligencia artificial por las autoridades de vigilancia del mercado

The supervision of compliance with the Artificial Intelligence Act by market surveillance authorities

Lorenzo Cotino Hueso[1]
Catedrático de Derecho Constitucional
Universidad de Valencia. Valgrai

RESUMEN: Este estudio examina la supervisión de los sistemas de inteligencia artificial (IA) en la Unión Europea bajo el Reglamento de IA (RIA), destacando el papel de las Autoridades de Vigilancia del Mercado (AVM). Se analiza la normativa general de la UE y particular de la IA aplicable, la designación de las AVM de IA por los Estados miembros y con los recursos necesarios para garantizar su efectividad. El artículo aborda las actividades proactivas y reactivas que deben acometer las AVM, incluidas la planificación estratégica, la evaluación del cumplimiento y la imposición de medidas correctivas ante infracciones. Se destacan los poderes de las AVM para acceder a documentación técnica y supervisar las pruebas de IA en condiciones reales. Además, se discuten las variedades de criterios que se están dando en la designación de las AVM de IA en distintos países, con las particularidades que se dan con la Agencia Española

[1] cotino@uv.es. OdiseIA. El presente estudio es resultado de investigación de los siguientes proyectos: MICINN Proyecto "Derechos y garantías públicas frente a las decisiones automatizadas y el sesgo y discriminación algorítmicas" 2023-2025 (PID2022-136439OB-I00) financiado por MCIN/AEI/10.13039/501100011033/; Proyecto "Algoritmic law" (Prometeo/2021/009, 2021-24 Generalitat Valenciana); "Algorithmic Decisions and the Law: Opening the Black Box" (TED2021-131472A-I00) y "Transición digital de las Administraciones públicas e inteligencia artificial" (TED2021-132191B-I00) del Plan de Recuperación, Transformación y Resiliencia. Estancia Generalitat Valenciana CIAEST/2022/1, Convenio de Derechos Digitales-SEDIA Ámbito 5 (2023/C046/00228673) y Ámbito 6. (2023/C046/00229475), proyecto "Derecho, Cambio Climático y Big Data", Grupo de Investigación en Derecho Público y TIC como investigador de la Universidad Católica de Colombia.

de Supervisión de la Inteligencia Artificial (AESIA) como AVM en España, y el papel a desarrollar por otras como la Agencia Española de Protección de Datos (AEPD).

Palabras clave: Inteligencia Artificial, Reglamento de inteligencia artificial, Unión Europea, autoridades de vigilancia del mercado, supervisión normativa

ABSTRACT: This study examines the supervision of artificial intelligence (AI) systems in the European Union under the AI Act, highlighting the role of Market Surveillance Authorities (MSAs). It discusses the general EU and AI-specific regulations applicable, the designation of AI MSAs by Member States and the resources needed to ensure their effectiveness. The article discusses the proactive and reactive activities to be undertaken by the AVMs, including strategic planning, compliance assessment and the imposition of corrective measures for infringements. It highlights the powers of AVMs to access technical documentation and monitor AI testing under real-life conditions. In addition, the varieties of criteria that are taking place in the designation of AI AVMs in different countries are discussed, with the particularities of the Spanish Agency for the Supervision of Artificial Intelligence (AESIA) as AVM in Spain, and the role to be developed by others such as the Spanish Data Protection Agency (AEPD).

Keywords: Artificial Intelligence, Artificial Intelligence Regulation, European Union, market surveillance authorities, regulatory oversight, regulatory oversight

1. INTRODUCCIÓN AL —BASTANTE DESCONOCIDO— "NUEVO MARCO REGULATORIO", AUTORIDADES DE VIGILANCIA DEL MERCADO Y SU REGULACIÓN GENERAL Y PARTICULAR

1.1. Algunas interrogantes que pretende responder este estudio

El presente estudio pretende dar una respuesta a cuestiones como las que siguen: ¿qué normativa regula la supervisión de los sistemas de inteligencia artificial en la Unión Europea y cómo se combina la normativa general de vigilancia del mercado y la particular del Reglamento de IA de la UE (RIA) [2]? Respecto de

[2] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que

las Autoridades de Vigilancia del Mercado (AVM) en razón de su regulación general y la particular del RIA, ¿quiénes las designa?, ¿qué autoridades de IA están designándose en la UE hasta el momento y bajo qué criterios?, ¿qué recursos deben tener? ¿qué poderes tienen? ¿cómo garantizan el cumplimiento de las normativas?, ¿qué tipos de actividades proactivas y reactivas deben desarrollar?, ¿cómo pueden conocer e investigar si un sistema de IA de alto riesgo cumple con los requisitos?, ¿cómo deben actuar cuando detectan un sistema que incumple el RIA o que presenta un riesgo? ¿qué medidas pueden imponer?, ¿qué papel juegan respecto de las pruebas de IA en condiciones reales?, ¿cómo contribuyen las AVM a la protección de los derechos fundamentales en relación con los sistemas de IA, y de qué manera cooperan con otras autoridades reguladoras para garantizar la protección de estos derechos? ¿qué papel puede tener la AESIA como AVM principal y su relación con otras como la Agencia Española de Protección de Datos?

Para dar respuesta a estas cuestiones, el presente estudio aborda la regulación de las AVM en la UE de cara a la supervisión del cumplimiento del nuevo RIA. [3] Para ello se integra la regulación general de la vigilancia del mercado y sus autoridades y la particular regulación que hay al respecto en el RIA. Aquí se apuntan los ámbitos de actuación posibles de la AESIA en el contexto de las diferentes AVM existentes en el ámbito de la IA según el RAI. En primer término se expone y concreta la necesidad de designación de las AVM de la IA, así como la AVM principal, así como la obligación de que las mismas cuenten con los recursos adecuados para cumplir eficazmente sus funciones. Igualmente se expone que se deben garantizar unos poderes mínimos y suficientes para supervisar el mercado, realizar inspecciones y, si es necesario, imponer medidas correctivas o sanciones a los operadores que no cumplan con la legislación.

El estudio se centra en las funciones que debe desarrollar una AVM, distinguiendo esencialmente unas actividades proactivas y las reactivas. Así, entre las "proactivas" que ayudan a prevenir incumplimientos, se incluyen el conocimiento exhaustivo del ecosistema de IA, la planificación estratégica de la vigilancia. Asimismo, la UE considera "esencial" la realización de campañas informativas, alertas y de concienciación dirigidas tanto a consumidores como a operadores

---

se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), DOUE núm. 1689, de 12 de julio de 2024, DOUE-L-2024-81079. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689

[3] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), DOUE núm. 1689, de 12 de julio de 2024, DOUE-L-2024-81079. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689

económicos. En este sentido, el RIA se centra en la orientación y asesoramiento a PYMES (art. 70.8 RIA). Las funciones que pueden calificarse como "reactivas" de las AVM suponen las de evaluación y comprobación de cumplimiento de los sistemas de IA en el mercado y estas atribuciones se concretan entre otras en las posibilidades de acceso a información sobre los sistemas IA, declaraciones de conformidad de los mismos o solicitud y acceso la documentación técnica de estos sistemas de alto riesgo, incluso la posibilidad de requerir el acceso al código fuente del sistema IA. Estas actividades también incluyen la capacidad de realizar inspecciones y, de ser necesario, requerir a los operadores de los sistemas IA que tomen medidas para asegurar que los sistemas de IA cumplan con la legislación relevante o imponer que lo hagan.

Se analizan de modo concreto las funciones específicas en razón del Reglamento de IA de supervisión, control y corrección. Así se exponen los casos donde los sistemas de IA sí que cumplen con el RIA, pero presentan riesgos y exigen actuación de la AVM. O el importante supuesto en el que los proveedores de sus sistemas IA, pese a que persiguen los fines de alto riesgo del Anexo III, no consideran que sean de alto riesgo, lo cual exige una actuación de tales proveedores ante la AVM de IA. Entre otras cuestiones especiales también se analizan las futuras funciones de las AVM de gestión de reclamaciones por usuarios o afectados. Asímismo, más allá de las actividades propias de la supervisión de las AVM, se analizan las funciones específicas que las AVM en razón del RIA en supuestos de exención de evaluación de la conformidad, para las pruebas en condiciones reales y las actividades en cooperación con la Comisión y la Oficina de IA respecto de los sistemas IA generales. También, la actividad que deben desarrollar las AVM de IA de apoyo en el caso de incidentes graves de los sistemas y en los supuestos en los que actúan autoridades de derechos fundamentales con relación a sistemas de IA.

Finalmente, se describe la actual situación de variada designación de AVM en la Unión Europea, siendo que en algunos países quizá se siga más la posición del CEPD (Comité Europeo de Protección de Datos), designando a autoridades de protección de datos como AVM. No obstante, al igual del caso de España en el que se da un marcado protagonismo a una nueva AVM, la AESIA, otros países como Alemania o Dinamarca se han desmarcado del CEPD con autoridades del ámbito de redes y digitales.

1.2. La inteligencia artificial se integra en el —bastante desconocido— "nuevo marco regulatorio" y la actuación de las autoridades de vigilancia del mercado

El RIA ya está en vigor, sin perjuicio de las distintas fases graduales de su aplicación, que en ocasiones llevan hasta el importante periodo de seis años para el caso de la IA de alto riesgo del sector publico. En todo caso, ya se están

generando los entornos institucionales para la aplicación de esta norma, el 24 de enero de 2024 se creó la Oficina Europea de la IA [4] y antes (la AESIA en España) [5]

Es importante destacar que el RIA ha encajado la regulación de la IA en el ámbito de la seguridad y garantía de los productos, las normas de armonización y el modelo del llamado «nuevo marco legislativo». Se trata del marco por el que se establecen unas bases comunes para la comercialización, evaluación y vigilancia de productos en la Unión Europea (Comisión Europea s.f. *a, b* y *c*). Todo sea dicho, es un modelo con el que los juristas en general no estamos muy familiarizados y son muy escasas las aportaciones doctrinales. Al respecto, destaca especialmente desde hace lustros en España Álvarez García (2020, 2024 y con Tahiri Moreno 2023) y, más recientemente, Palma Ortigosa (2024 *a* y *b*). Este nuevo marco legislativo supone la aplicación de las normas armonizadas y de las especificaciones comunes en el ámbito de la inteligencia artificial. Y este nuevo marco legislativo implicando un conjunto normativo complejo en el que destacan el Reglamento sobre la normalización europea de 2012[6], el Reglamento por el que se regula la acreditación[7], la Decisión ordenadora de los mecanismos de evaluación de la conformidad[8], asímismo, y de particular interés en el presente estudio, el Reglamento sobre la vigilancia del mercado[9].

La supervisión del mercado busca asegurar que los productos cumplan con la normativa, en nuestro caso el RIA, que garantizan una alta protección en aspectos como los derechos fundamentales, la salud y la seguridad. Este propósito se lleva a cabo mientras se mantiene la libre circulación de productos sin restricciones excesivas, conforme a la legislación de armonización de la Unión Europea o cualquier otra normativa relevante de la Unión. La supervisión de mercado proporciona a los ciudadanos un nivel uniforme de protección en todo el mercado único, sin importar el origen del producto, y es muy relevante para los intereses de los operadores económicos, ya que contribuye a eliminar la com-

---

4 *Decisión de la Comisión de 24.1.2024 por la que se crea la Oficina Europea de Inteligencia Artificial*, Bruselas, 24.1.2024C(2024) 390 final, https://ec.europa.eu/newsroom/dae/redirection/document/101625

5 La creación y habilitación legal fue por la Ley 28/2022, de 21 de diciembre, en concreto, su D.A 7ª reguló la creación. Asimismo, según Ley 28/2022, la AESIA está adscrita orgánica al Ministerio de Asuntos Económicos y Transformación Digital, a través de su Secretaria-o SEDIA. Su regulación se da por Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto.

6 Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea.

7 Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación.

8 Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre un marco común para la comercialización de los productos y por la que se deroga la Decisión 93/465/CEE del Consejo.

9 Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) n.º 765/2008 y (UE) n.º 305/2011.

petencia desleal. Los Estados miembros deben organizar y realizar el seguimiento de los productos en sus mercados, tanto comercializados internamente como importados. El objetivo es asegurar que estos productos hayan sido diseñados y fabricados de acuerdo con los estándares y procedimientos regulados, incluyendo los requisitos de marcado y documentación.

Cuando se considera necesario, la autoridad de vigilancia del mercado AVM debe exigir a los operadores económicos que implementen medidas correctivas adecuadas y proporcionadas para cumplir con las normativas. Si los operadores no toman medidas correctivas, las AVM deben intervenir para asegurar que los productos sean retirados del mercado o se mantengan fuera de este, y que los operadores irresponsables o delincuentes sean penalizados. Asimismo, procede aplicar sanciones proporcionales y disuasorias (Comisión Europea, 2022:104, ap. 1.1.).

El objetivo general de las AVM es la vigilancia eficaz del mercado en su territorio de los productos comercializados en línea y fuera de línea con respecto a los productos que estén sujetos a la legislación de armonización de la Unión. Para ello han de hacer comprobaciones apropiadas documentales y, en su caso, físicas, a partir de una planificación en una estrategia nacional de vigilancia del mercado. Las AVM han de lograr que los operadores económicos adopten las medidas correctivas apropiadas y proporcionadas en relación con el cumplimiento de la legislación aplicable y si no lo hacen, imponerles tales medidas (art. 11 RVM).

1.3. El Reglamento (UE) 2019/1020 como norma general y el Reglamento de inteligencia artificial como norma especial. Algunas definiciones

Cabe tener en cuenta que el Reglamento (UE) 2019/1020 sobre vigilancia del Mercado (en adelante RVM) es la regulación general aplicable, que establece las bases. Ahora bien, el RIA es la norma especial, por lo que si contempla elementos más específicos que el RVM es la aplicable por ser ley especial. Así se hará referencia en este estudio. Sin embargo, en muchos casos, las normas especiales tienen carácter complementario y no invalidan la regulación del RVM (Comisión Europea, 2022:105).

Cabe también señalar que además, de la normativa general y especial reguladora, es posible que se adopten actos de ejecución por la Comisión con relación a aspectos concretos, como "las condiciones uniformes de las comprobaciones" de las autoridades (art. 11. 4º RVM), y parámetros de referencia y técnicas para las comprobaciones (art. 25. 8º RVM)[10], sobre el "sistema de información y comuni-

[10] "La Comisión, previa consulta a la Red, podrá adoptar actos de ejecución que establezcan parámetros de referencia y técnicas para las comprobaciones sobre la base de análisis de riesgos comunes a escala".

cación para recoger, tratar y almacenar información" (art. 34.8º RVM), relativos a la cooperación internacional, como sistemas específicos de control previo a la exportación (art. 35.10º RVM) y aprobaciones concedidas (art. 35.10º RVM).

Así las cosas, resulta preciso conocer el marco general de vigilancia del mercado conjuntamente con cualquier especialidad que introduzca al respecto del RAI como norma especial aplicable.

Resulta de interés recordar alguna definición normativa de especial incidencia, como "vigilancia del mercado", "autoridad de vigilancia del mercado", "medida correctiva", "medida voluntaria" o "autoridad nacional competente".

Así, el artículo 3 RVM define

> 3) "«vigilancia del mercado»: las actividades efectuadas y las medidas tomadas por las AVM para velar por que los productos cumplan los requisitos establecidos por la legislación de armonización de la Unión aplicable y garantizar la protección del interés público amparado por dicha legislación;"
>
> 4) «autoridad de vigilancia del mercado»: la autoridad designada por un Estado miembro, de conformidad con el artículo 10, responsable de efectuar la vigilancia del mercado en el territorio de ese Estado miembro;[11]
>
> 16) «medida correctiva»: toda medida adoptada por un operador económico para poner fin a un incumplimiento, cuando lo exija una AVM o por propia iniciativa del operador económico;
>
> 17) «medida voluntaria»: medida correctiva no exigida por una autoridad de vigilancia del mercado;

Por su parte, el art. 3 RIA, define "48) «autoridad nacional competente»: una autoridad notificante o una autoridad de vigilancia del mercado; en lo que respecta a sistemas de IA puestos en servicio o utilizados por instituciones, órganos y organismos de la Unión, las referencias hechas en el presente Reglamento a autoridades nacionales competentes o a AVM se interpretarán como referencias al Supervisor Europeo de Protección de Datos".

2. DESIGNACIÓN, PODERES Y RECURSOS QUE LOS ESTADOS DEBEN ASEGURAR A LAS AVM DE INTELIGENCIA ARTIFICIAL

Cada Estado designa a la o a las diferentes AVM. Así, en general, los Estados miembros deben designar una o varias AVM y una oficina de enlace única para tareas de coordinación. Ello es responsabilidad de las autoridades públicas nacionales (art. 10. 1º RVM). Asimismo, no existen requisitos a escala de la Unión sobre la asignación de responsabilidades entre las autoridades, ya sea sobre una

[11] El art. 3 RIA 26) define "«autoridad de vigilancia del mercado»: la autoridad nacional que lleva a cabo las actividades y adopta las medidas previstas en el Reglamento (UE) 2019/1020;".

base funcional o geográfica, siempre que la vigilancia sea eficaz y abarque todo el territorio. En esta línea, el RIA dispone que "Cada Estado miembro establecerá o designará al menos una autoridad notificante y al menos una AVM como autoridades nacionales competentes a los efectos del presente Reglamento" (art. 70, Sección 2, Autoridades nacionales competentes).

En el caso del RIA "Los Estados miembros comunicarán a la Comisión la identidad de las autoridades notificantes y de las AVM y las funciones de dichas autoridades, así como cualquier cambio posterior al respecto. […] Los Estados miembros designarán una AVM que actúe como punto de contacto único para el presente Reglamento y notificarán a la Comisión la identidad de dicho punto." (art. 70. 2º RIA).

En general, también se dispone que los Estados miembros han de proporcionar a las AVM las facultades, los recursos y la experticia necesarios para desempeñar efectivamente sus funciones (art. 14.1º RVM). En el caso del RIA, también se pretende asegurar que cuenten con "recursos técnicos, financieros y humanos adecuados, y de infraestructuras", así como personal con conocimientos específicos (art. 70. 3º RIA)[12]. Será obligatorio informar a la comisión al respecto en un año desde la entrada en vigor (art. 70.6º RIA)[13]

Además de recursos, de manera concreta el RIA señala que "Las autoridades nacionales competentes adoptarán las medidas adecuadas para garantizar un nivel adecuado de ciberseguridad" (art. 70. 4º RIA).

De igual modo, cada Estado debe reconocerles unas facultades mínimas y poderes. Es importante señalar que cada estado puede determinar que ciertas facultades sean implementadas a través de otras entidades gubernamentales o por medio de resoluciones judiciales (art. 14.3º RVM). Cada Estado "Al otorgar los poderes" pueden optar porque los ejerzan "directamente por las autoridades de vigilancia del mercado, bajo su propia autoridad", "recurriendo a otras

---

12 "3. Los Estados miembros garantizarán que sus autoridades nacionales competentes dispongan de recursos técnicos, financieros y humanos adecuados, y de infraestructuras para el desempeño de sus funciones de manera efectiva con arreglo al presente Reglamento. En concreto, las autoridades nacionales competentes dispondrán permanentemente de suficiente personal cuyas competencias y conocimientos técnicos incluirán un conocimiento profundo de las tecnologías de IA, datos y computación de datos; la protección de los datos personales, la ciberseguridad, los riesgos para los derechos fundamentales, la salud y la seguridad, y conocimientos acerca de las normas y requisitos legales vigentes. Los Estados miembros evaluarán y, en caso necesario, actualizarán anualmente los requisitos en materia de competencias y recursos a que se refiere el presente apartado."

13 "6. A más tardar el … [un año a partir de la fecha de entrada en vigor del presente Reglamento] y cada dos años a partir de entonces, los Estados miembros presentarán a la Comisión un informe acerca del estado de los recursos financieros y humanos de las autoridades nacionales competentes, que incluirá una evaluación de su idoneidad. La Comisión remitirá dicha información al Comité para que mantenga un debate sobre ella y, en su caso, formule recomendaciones."

autoridades públicas" o en su caso "solicitando a los órganos jurisdiccionales competentes" que aprueben el ejercicio del poder concreto del que se trate.[14] Es más, los Estados también pueden asignar facultades adicionales más allá de las mencionadas en el RVM, cuestión de especial interés de cara a la AESIA.

Para la realización de los objetivos y actividades, las AVM han de contar con unos poderes mínimos (art. 14.4º RVM). Así, cabe destacar la facilitación de documentos e información por los operadores económicos, realizar sin previo aviso inspecciones in situ y comprobaciones, obtener pruebas, acceder a establecimientos, iniciar investigaciones, exigir que adopten medidas o imponer medidas correctivas, sanciones, adquirir de forma encubierta muestras para detectar incumplimientos y obtener pruebas, suprimir contenidos de interfaces en línea, exigir a proveedores de servicios de la sociedad de la información que restrinjan el acceso.

Como se adelantó, el ejercicio de estos poderes bien puede ser a través de la propia autoridad, otra o una autoridad judicial. Cabe señalar que, sin perjuicio de la particular naturaleza de cada poder, en principio, cabe la subcontratación, siempre que sigan siendo responsables de sus decisiones o no haya conflictos de intereses (por ejemplo, si se atribuyen a un organismo que lleva a cabo actividades de evaluación de la conformidad y se garantice la imparcialidad).[15] Asimismo, de manera concreta el artículo 74.6º RIA[16] dispone que las autoridades "podrán ejercer a distancia los poderes", en concreto las "inspecciones in situ y comprobaciones" y de inspeccionar muestras de manera encubierta (poderes art. 14.4º d) y j)[17].

---

[14] RVM, artículo 14, Poderes de las autoridades de vigilancia del mercado: […] 3. Al otorgar los poderes conforme al apartado 1, los Estados miembros podrán disponer que sean ejercidos de una de las maneras siguientes, según proceda:
a) directamente por las autoridades de vigilancia del mercado, bajo su propia autoridad;
b) recurriendo a otras autoridades públicas, de conformidad con la división de poderes y la organización institucional y administrativa del Estado miembro de que se trate;
c) solicitando a los órganos jurisdiccionales competentes que adopten la resolución necesaria para aprobar el ejercicio del poder de que se trate, también, en su caso, mediante un recurso, si la solicitud para la adopción de la resolución necesaria no prospera."

[15] A este respecto se indica que "pueden subcontratar tareas técnicas (como ensayos o inspecciones) a otro organismo, siempre que sigan siendo responsables de sus decisiones. Si las tareas técnicas se subcontratan a un organismo que lleva a cabo actividades de evaluación de la conformidad para los operadores económicos, no debe haber conflicto de intereses entre dichas actividades de evaluación de la conformidad y la evaluación de la conformidad para la autoridad de vigilancia del mercado. A la hora de subcontratar, la autoridad de vigilancia del mercado debe actuar con suma prudencia para garantizar que la imparcialidad del asesoramiento que recibe es irreprochable. La responsabilidad de cualquier decisión adoptada sobre la base de dicho asesoramiento debe corresponder a la autoridad de vigilancia del mercado." (Comisión Europea, 2022:107).

[16] "6. las autoridades de vigilancia del mercado podrán ejercer a distancia los poderes a que se refiere el artículo 14, apartado 4, letras d) y j), de dicho Reglamento, según proceda."

[17] "d) el poder para realizar sin previo aviso inspecciones in situ y comprobaciones físicas de los

3. ACTIVIDADES Y FUNCIONES PROACTIVAS: CONOCIMIENTO DEL ECOSISTEMA DE INTELIGENCIA ARTIFICIAL, PLANIFICACIÓN, ALERTAS Y LA "ESENCIAL" INFORMACIÓN Y CONCIENCIACIÓN

Se ha englobado en general las acciones de las AVM en acciones proactivas y reactivas (Unión Europea, 2017, 10 ss.). La vigilancia del mercado proactiva supone esencialmente un buen conocimiento del mercado, la planificación de su actuación y la aplicación de las campañas de vigilancia. La vigilancia del mercado reactiva implica las labores de evaluación, muestreo y reacción ante riesgos e incumplimientos que se detecten (Unión Europea, 2017, 12 ss.).

Por cuanto a las acciones proactivas de la AVM, se trataría en nuestro caso esencialmente de determinar el objetivo a supervisar. Así, procede detectar si existen en el mercado sistemas prohibidos, conocer qué operadores de sistemas IA de alto riesgo están activos, según sectores; qué sistemas están disponibles y cómo se ofrecen en el mercado. Se recomienda a las AVM que colaboren estrechamente con los sectores comerciales para identificar las cadenas de suministro y participaciones de mercado a través de análisis de mercado integral, que incluiría también la consulta con los consumidores o usuarios, esto es con los implementadores de IA. Puede ser adecuado emplear servicios de terceros para recopilar información verificable.

Se debe obtener un conocimiento exhaustivo, un "cribado" (Unión Europea, 2017, 12 ss.) del panorama del mercado nacional de sistemas IA de alto riesgo: escala y variedad de productos disponibles, la identidad y participación de mercado de los proveedores, el tipo de operadores económicos involucrados y los canales de distribución predominantes. A partir de ahí, la AVM debe tener una visión del tamaño general del mercado nacional, en nuestro caso de IA de alto riesgo o que puedan generar riesgos, nombres y la cuota de mercado de los agentes económicos que suministran tales sistemas IA; el tipo de agente económico (como fabricantes, importadores, distribuidores) y principales canales de venta y debe decidir a qué agentes económicos y productos debe dirigirse para obtener el resultado más eficaz. A partir de lograr una información de calidad, la AVM de IA correspondiente, habrá de planificar y priorizar su enfoque hacia aquellos operadores económicos y productos que resulten más críticos o de mayor riesgo. El monitoreo proactivo ha de tener en cuenta factores como los antecedentes de incumplimientos y tamaño de participación de mercado, como en productos específicos (Unión Europea, 2017, 12 ss.).

---

productos; […] j) el poder para adquirir muestras de productos, también bajo una identidad encubierta, para inspeccionar esas muestras y para someterlas a ingeniería inversa a fin de detectar incumplimientos y obtener pruebas".

Las campañas, estrategias y planificación de la vigilancia del mercado deberían:

— Establecer objetivos para comprobar la conformidad con las normativas vigentes para proteger al consumidor y eliminar la competencia desleal.
— Definir el alcance y la metodología de la evaluación.
— Planificar la duración de la campaña y realizar estudios preliminares para asegurar la disponibilidad de recursos adecuados.
— Establecer procedimientos claros para la eficacia de la campaña, incluyendo el desarrollo de códigos de práctica que faciliten la generación de informes estandarizados.

Ya en la ejecución de los planes, habrá de evaluarse su implantación y realizar informes así como difundir al sector y consumidores y el ecosistema de otras AVM implicadas o autoridades, los resultados.

Es de interés recordar que la actuación de vigilancia del mercado debe estar bajo una planeación y estrategia nacional, que es de obligatoria realización cada cuatro años por cada Estado (art. 13 RVM, Comisión Europea, 2022:107). No obstante, no es sencillo comprobar si esto se cumple en España.[18] Esta estrategia implica un "planteamiento coherente, exhaustivo e integrado de la vigilancia" y ha de incluir como mínimo expresión de la "frecuencia de productos no conformes", "tendencias del mercado", "ámbitos considerados prioritarios", "actividades de ejecución planeadas para reducir la presencia de incumplimientos" y "niveles mínimos de control previstos para las categorías de productos", así como una "evaluación de la cooperación con las autoridades" (Comisión Europea, 2022:107,. 7.3.2).

Teniendo en cuenta que "el objetivo de la vigilancia del mercado es ofrecer un alto nivel de protección de determinados intereses públicos, informar al público es un elemento esencial de dicha vigilancia" (Comisión Europea, 2022:108, 7.3.3). Se ha recordado que "Teniendo en cuenta que el objetivo de la vigilancia del mercado es ofrecer un alto nivel de protección de determinados intereses públicos, informar al público es un elemento esencial de dicha vigilancia". En este sentido, los Estados miembros deben asegurarse de que la información relevante sea accesible al público y a las partes interesadas para salvaguardar los intereses de los consumidores dentro de la Unión (art. 17 RVM). Ello implica información y concienciación tanto para consumidores como para los agentes económicos. En línea con el principio de transparencia, se debe permitir el acceso general al público a la información que posean las autoridades de los Estados miembros o la Comisión, relacionada con los riesgos potenciales para la salud, seguridad y otros intereses públicos amparados por la normativa de armonización de la

[18] No es sencillo localizar una de estas estrategias, cabe seguir como muestra, Gobierno de España (s. f.).

UE. Sin perjuicio de lo anterior, obviamente la transparencia está sujeta a las limitaciones necesarias para proteger los derechos de propiedad intelectual, la confidencialidad de la información comercial, la privacidad de los datos personales y las operaciones de control, investigación.

Otra función de control e investigación importante son las alertas a la ciudadanía y consumidores. Con el fin de mitigar el riesgo de daños o lesiones, las AVM están obligadas a asegurar que los consumidores en sus jurisdicciones sean prontamente informados sobre cualquier peligro o riesgo identificado asociado a productos, especialmente cuando el operador económico responsable no efectúe dicha alerta (art. 16, 3º y 5º RVM).

Ya en particular, el artículo 70. 8º RIA señala que las AVM competentes ofrecerán "orientaciones y el asesoramiento" sobre la aplicación del Reglamento, especialmente a PYME y startups, considerando las directrices del Comité y la Comisión cuando sea pertinente. Si debe orientar sobre sistemas de IA en áreas reguladas por otras normativas de la Unión, se realizarán consultas con las respectivas autoridades competentes.[19]

Además de lo anterior, cabe tener en cuenta la información anual a la Comisión. Así, el artículo 34 RVM establece un sistema de información y comunicación mantenido por la Comisión Europea. Este sistema recopila, procesa y almacena datos sobre la aplicación de la legislación de armonización de la Unión para mejorar el intercambio de información entre los Estados miembros y ofrecer una visión general de la vigilancia del mercado y sus tendencias. Este sistema es accesible para la Comisión, las AVM, las oficinas de enlace y las autoridades designadas. En virtud del mismo, se ha de desarrollar una interfaz pública para que los usuarios finales puedan consultar información relevante sobre la vigilancia del mercado.

Las oficinas de enlace de cada Estado, como sería la AESIA en España, son responsables de introducir datos en el sistema sobre las AVM, sus competencias y estrategias nacionales. Las autoridades de vigilancia ingresarán información detallada sobre los productos, las medidas tomadas, los resultados de los ensayos, las correcciones realizadas por los operadores económicos, y cualquier incumplimiento relevante. Las autoridades aduaneras, para el caso de que actúen respecto de sistemas IA, también aportarán datos sobre los productos que entran en la Unión Europea para garantizar el cumplimiento de la legislación. Se crearán interfaces electrónicas para facilitar el intercambio de datos entre los

---

[19] Art. 70.8º: "Las autoridades nacionales competentes podrán proporcionar orientaciones y asesoramiento sobre la aplicación del presente Reglamento, en particular a las pymes —incluidas las empresas emergentes—, teniendo en cuenta las orientaciones y el asesoramiento del Comité y de la Comisión, según proceda. Siempre que una autoridad nacional competente tenga la intención de proporcionar orientaciones y asesoramiento en relación con un sistema de IA en ámbitos regulados por otros actos del Derecho de la Unión, se consultará a las autoridades nacionales competentes con arreglo a lo dispuesto en dichos actos, según proceda."

sistemas nacionales y este sistema de información y comunicación. La Comisión establecerá los detalles sobre cómo se manejarán y compartirán estos datos a través de actos de ejecución.

Ya de forma más concreta para inteligencia artificial, el artículo 74.2º RIA impone la obligación de informar anualmente a la Comisión de "cualquier información" de "interés potencial" para "la aplicación" "de normas de competencia" y "el recurso a prácticas prohibidas" "y sobre las medidas adoptadas."[20]

4. ACTIVIDADES REACTIVAS: EVALUACIÓN, COMPROBACIONES, CORRECCIONES Y SANCIONES

4.1. Vigilancia, comprobaciones y acceso a información y documentación

Como se ha adelantado, las AVM deben identificar los productos o actores del mercado objetivo para maximizar su impacto. Luego, deben implementar esta estrategia *in situ* y proceder a la evaluación y en su caso análisis según sea necesario. Posteriormente, es fundamental evaluar el cumplimiento normativo y en su caso otros riesgos de los sistemas, lo que podría implicar la solicitud de información adicional a los agentes económicos, como el acceso a documentos técnicos. Procede tener en cuenta los presupuestos para realizar comprobaciones y evaluaciones, según indicios y elementos de riesgo; la realización de comprobaciones y evaluaciones y los requerimientos de información, declaraciones de conformidad o documentación técnica a las autoridades e incluso el acceso al código fuente.

Respecto de los presupuestos para realizar comprobaciones y evaluaciones, según indicios y elementos de riesgo. Si el objetivo general de las AVM es la vigilancia eficaz del mercado en su territorio, las actividades sustanciales son lla posibilidad de realizar inspecciones, comprobaciones y lograr que los operadores económicos adopten las medidas correctivas y si no lo hacen, imponerles tales medidas (art. 11 RVM).

Por cuanto a los controles (Comisión Europea, 2022:109, 7.4), deben efectuar las comprobaciones apropiadas, en una escala adecuada, de los productos comercializados ya sean productos en línea o no (art. 11. 1 a) y 3º RVM). La

---

[20] "2. Como parte de sus obligaciones de presentación de información en virtud del artículo 34, apartado 4, del Reglamento (UE) 2019/1020, las autoridades de vigilancia del mercado informarán anualmente a la Comisión y a las autoridades nacionales de competencia pertinentes de cualquier información recabada en el transcurso de las actividades de vigilancia del mercado que pueda ser de interés potencial para la aplicación del Derecho de la Unión en materia de normas de competencia. Asimismo, informarán anualmente a la Comisión sobre el recurso a prácticas prohibidas que se hayan producido durante ese año y sobre las medidas adoptadas."

adecuación de los controles va en consonancia con el riesgo y la necesidad de concentrar recursos (art. 11. 3º RVM) a partir de criterios como el nivel de posibles peligros, incumplimientos y riesgos asociados; frecuencia de ese producto en el mercado, actividades y operaciones, historial de incumplimientos de esos operadores económicos, información recibida de otros agentes (como otras autoridades, reclamaciones de los consumidores y los medios de comunicación), así como otras fuentes que puedan indicar incumplimientos, como incidentes y accidentes.[21]

En particular para los sistemas IA, se regulan los controles y evaluaciones en el artículo 79 RIA. Como punto de partida, los sistemas de IA que presentan un riesgo (definidos en general en artículo 3.19 RVM) se entenderán como «productos que presentan un riesgo» "para la salud, la seguridad o los derechos fundamentales de las personas" (art. 79. 1º RIA). Si hay motivos suficientes, la AVM ha de evaluar el sistema para verificar el cumplimiento del RIA. Se subraya en este precepto que "Debe prestarse una especial atención a los sistemas de IA que presenten un riesgo para los colectivos vulnerables". En el caso de riesgos a los derechos fundamentales, la AVM ha de informar a las autoridades de derechos fundamentales que en su caso sean competentes (por ejemplo, autoridades de protección de datos o de no discriminación) y "cooperará plenamente con ellos". Por su parte, los responsables de los sistemas han de cooperar con la AVM y las autoridades que intervengan.[22]

---

21 Art. 11. 3º RVM: "A la hora de decidir qué comprobaciones realizar, de qué tipos de productos y a qué escala, las autoridades de vigilancia del mercado seguirán un enfoque basado en el riesgo, teniendo en cuenta los siguientes factores:
a) los posibles riesgos e incumplimientos relacionados con el producto y, cuando esté disponible, su frecuencia en el mercado;
b) las actividades y las operaciones bajo el control del operador económico;
c) el historial de incumplimientos del operador económico;
d) cuando sea pertinente, los perfiles de riesgo realizados por las autoridades designadas con arreglo al artículo 25, apartado 1;
e) las reclamaciones de los consumidores y otra información recibida de otras autoridades, operadores económicos, medios de comunicación y otras fuentes que puedan indicar incumplimiento."

22 Art. 79: "1. Los sistemas de IA que presentan un riesgo se entenderán como «productos que presentan un riesgo» tal como se definen en el artículo 3, punto 19, del Reglamento (UE) 2019/1020, en la medida en que presenten riegos que afecten a la salud, la seguridad o los derechos fundamentales de las personas.
2. Cuando la autoridad de vigilancia del mercado de un Estado miembro tenga motivos suficientes para considerar que un sistema de IA presenta un riesgo mencionado en el apartado 1 del presente artículo, efectuará una evaluación del sistema de IA de que se trate para verificar su cumplimiento de todos los requisitos y obligaciones establecidos en el presente Reglamento. Debe prestarse una especial atención a los sistemas de IA que presenten un rigo para los colectivos vulnerables. Cuando se detecten riesgos para los derechos fundamentales, la autoridad de vigilancia del mercado informará también a las autoridades u organismos públicos nacionales pertinentes a que se refiere el artículo 77, apartado 1, y cooperará plenamente con ellos. Los operadores pertinentes cooperarán en lo necesario con la autoridad de vigilancia

Ya por cuanto a *la realización de comprobaciones y evaluaciones*, Las comprobaciones pueden ser a través de inspecciones en línea, visitas a instalaciones comerciales, industriales y de almacenamiento, a lugares de trabajo y otras instalaciones donde los productos son puestos en servicio, como en el caso de la inteligencia artificial, de los implantadores, solicitar la información necesaria, acceder a servicios IA incluso de forma encubierta, practicar ingeniería inversa respecto de los mismos o someterlos a exámenes y ensayos.

Puede haber actuaciones de un primer nivel centradas en elementos documentales y visuales (marcado CE y su colocación, la disponibilidad de la declaración UE de conformidad, la información adjunta al producto y la elección correcta de procedimientos de evaluación de la conformidad, comprobaciones de la información disponible en el sitio web, solicitud de la documentación de conformidad o la adquisición del producto para su posterior inspección). No obstante, en razón de los indicios y pruebas del riesgo, caben comprobaciones más profundas que exigen evaluaciones y seguimiento de los requisitos específicos del RIA. En este caso, se centrarían en la correcta aplicación del procedimiento de evaluación de la conformidad, el contenido de la declaración de conformidad. Obviamente, se han de tener en cuenta los informes de ensayo o certificados de evaluación de la conformidad del organismo notificado (art. 11. 5º RVM). Y aunque a menor nivel, también las certificaciones voluntarias del producto o la aplicación de un sistema de gestión de la calidad. En ningún caso hay que excluir de vigilancia aquellos sistemas por el hecho de que cuenten con sistemas voluntarios (Comisión Europea, 2022:110), [23].

Asimismo, cabe tener en cuenta el *requerimiento de información, declaraciones de conformidad o documentación técnica a las autoridades e incluso el acceso al código fuente*. Así, la actuación de las AVM pasa en buena medida por el acceso a información, declaraciones o documentación técnica (Comisión Europea, 2022:110). Se garantiza el poder de las AVM de exigir la puesta a disposición de

---

del mercado y con las demás autoridades u organismos públicos nacionales a que se refiere el artículo 77, apartado 1."

[23] En caso de que los operadores económicos presenten informes de ensayo o certificados de evaluación de la conformidad expedidos por un organismo de evaluación de la conformidad acreditado, las autoridades de vigilancia del mercado deben tener debidamente en cuenta dichos informes o certificados [artículo 11, apartado 5, del Reglamento (UE) 2019/1020]. Las iniciativas voluntarias, como la certificación del producto o la aplicación de un sistema de gestión de la calidad, no pueden situarse en el mismo nivel que las actividades de vigilancia del mercado ejercidas por una autoridad. Aun así, pueden contribuir a eliminar riesgos e incumplimientos. No obstante, las autoridades de vigilancia del mercado deben ser imparciales con respecto a todas las marcas, etiquetas y disposiciones voluntarias: estas solo pueden tenerse en cuenta, de manera transparente y no discriminatoria, para la evaluación del riesgo y del cumplimiento. Por consiguiente, los productos no deben ser excluidos de las operaciones de vigilancia del mercado aunque hayan sido objeto de una certificación voluntaria o de otras iniciativas voluntarias.

la declaración UE de conformidad,[24] que acompañará al producto según la legislación de armonización, específica, en nuestro caso el RIA. Y si hay dudas sobre la conformidad del producto se puede solicitar información más detallada. Así, la documentación técnica debe ponerse a disposición en un plazo razonable cuando se dé una solicitud motivada[25]. Se deben evitar cargas desproporcionadas y, por ello, no debe solicitarse de manera sistemática sin indicios o motivos de preocupación. También pueden solicitarse certificados y decisiones del organismo notificado[26], si bien sólo cuando resulte claramente necesario y no, por ejemplo, cuando solo se deba comprobar un detalle (Comisión Europea, 2022:110). No facilitar la información o documentación adecuada y proporcionalidad supondrá un incumplimiento suficiente para poner en duda la conformidad del producto (*ídem*).

Por cuanto a la documentación técnica (Ramón, 2024), se recuerda que en general no es necesario conservarla dentro de la Unión, ni que deba guardarla el propio operador económico o proveedor de sistema IA. Lo que se requiere es que sea capaz de presentarla a petición de la autoridad nacional. Todo el acceso a la información está bajo regulación y garantías de confidencialidad. El proveedor facilitará la documentación relacionada con el incumplimiento alegado. En principio, sólo traducirá esa parte concreta y la AVM debe en su caso especificar claramente la parte de la documentación que debe ser traducida y conceder un plazo razonable para que se realice la traducción (Comisión Europea, 2022: 111). No se puede imponer un traductor acreditado o reconocido por las autoridades públicas para los documentos que se aportan.

Todo ello se replica o específica para el ámbito concreto de la inteligencia artificial por el RIA. Así, se subraya que los proveedores deben dar "pleno acceso a la documentación, así como a los conjuntos de datos de entrenamiento, validación y prueba utilizados para el desarrollo de los sistemas de IA de alto riesgo, también, cuando proceda y con sujeción a garantías de seguridad, a través de interfaces de programación de aplicaciones (API) o de otras herramientas y medios técnicos pertinentes que permitan el acceso a distancia." (art. 74.12º RIA)[27].

---

[24] Artículo 14.4º a) RVM las autoridades de vigilancia del mercado deben tener «el poder para exigir a los operadores económicos que faciliten los documentos, las especificaciones técnicas, los datos o la información pertinentes en relación con la conformidad y los aspectos técnicos del producto, lo que incluye el acceso al software incorporado, en la medida en que dicho acceso sea necesario para evaluar la conformidad del producto con la legislación de armonización de la Unión aplicable, en cualquier forma o formato y con independencia del soporte de almacenamiento o del lugar en que dichos documentos, especificaciones técnicas, datos o información estén almacenados, y para hacer u obtener copias de ellos".

[25] Artículo R2, apartado 9, del anexo I de la Decisión n.o 768/2008/CE

[26] *Ídem*.

[27] Artículo 74.12: "Sin perjuicio de los poderes previstos en el Reglamento (UE) 2019/1020, y cuando proceda y se limite a lo necesario para el desempeño de sus funciones, los proveedores concederán a las autoridades de vigilancia del mercado pleno acceso a la documentación, así como a los conjuntos de datos de entrenamiento, validación y prueba utilizados para el desa-

Por cuanto al más conflictivo acceso al código fuente, el artículo 74.13º requiere una "previa solicitud motivada y solo si se cumplen las dos siguientes condiciones", que sea "necesario para evaluar la conformidad" de un sistema de alto riesgo y que, además, "se han agotado todos los procedimientos de prueba o auditoría y todas las comprobaciones basadas en los datos y la documentación facilitados por el proveedor, o han resultado insuficientes".[28] La confidencialidad está especialmente subrayada por el artículo 74.14º y, en general, por el artículo 78 RIA (Vestri, 2024:65).

4.2. Adopción o imposición por el operador de medidas correctivas de vigilancia

Tras una evaluación, si la autoridad de vigilancia de mercado determina que un producto no cumple con la normativa de armonización —el RIA— o, aun siendo conforme, constituye un riesgo para la salud, seguridad o derechos fundamentales, debe aplicar una serie de procedimientos que aseguren la adopción de acciones oportunas y proporcionadas siguiendo los artículos 16, 18, 19 y 20 RVM y en su caso detallados en la particular armonización de la UE, en nuestro caso el RIA. Estas acciones correctivas se han de alinear con los procedimientos de salvaguardia de los artículos R31 y R32 del anexo I de la Decisión n.º 768/2008/CE (Comisión Europea, 2022:111 y Unión Europea, 2017, 23 ss.).

En cuanto al procedimiento a seguir, inicialmente las autoridades deben comunicarse con el operador económico implicado para notificarle sobre los hallazgos y permitirle exponer su postura dentro de un mínimo de diez días laborables, excepto en situaciones de urgencia. Posteriormente, se requerirá que implemente las medidas correctivas necesarias para remediar el incumplimiento o mitigar el riesgo, informando también al organismo notificado correspondiente, si procede según la legislación de armonización concreta. En su caso, habrá que revisar si el RIA añade prescripciones procedimentales especiales.

Respecto de las medidas que deben adoptar los operadores, por cuanto a la normativa general, cabe seguir especialmente el artículo 16 RVM y las medidas de su apartado 3º. Las medidas van desde correcciones menores hasta la retirada o el recobro de productos, y habrán de ajustarse proporcionalmente al nivel de riesgo o incumplimiento y no deben obstaculizar excesivamente la libre

---

rrollo de los sistemas de IA de alto riesgo, también, cuando proceda y con sujeción a garantías de seguridad, a través de interfaces de programación de aplicaciones (API) o de otras herramientas y medios técnicos pertinentes que permitan el acceso a distancia."

28 "Se concederá a las autoridades de vigilancia del mercado acceso al código fuente del sistema de IA de alto riesgo, previa solicitud motivada y solo si se cumplen las dos siguientes condiciones:
a) el acceso al código fuente es necesario para evaluar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en el capítulo III, sección 2, y
b) se han agotado todos los procedimientos de prueba o auditoría y todas las comprobaciones basadas en los datos y la documentación facilitados por el proveedor, o han resultado insuficientes."

circulación de los productos. En situaciones de riesgo significativo, se requiere una intervención más inmediata, como lo detallan los artículos 19 y 20 RVM, ssegún el peligro y la probabilidad de que ocurra. Si se estima que el riesgo es alto, se pueden implementar acciones rápidas y restrictivas sin aguardar las correcciones que adopte voluntariamente del operador económico. En cualquier caso, se le debe permitir al operador (el proveedor u otro sujeto del RIA) expresar su perspectiva a la brevedad posible después de cualquier acción tomada por las autoridades, la cual será prontamente revisada (art. 18.3º RVM).

En particular, en el caso del RIA se dispone que "cuando proceda", como en el transcurso de la evaluación o control del sistema, si se constata "que el sistema de IA no cumple los requisitos y obligaciones" del RIA, "exigirá sin demora indebida" al operador que "que adopte todas las medidas correctoras oportunas", bien para que cumpla, bien retirarlo del mercado. Se le marcará un plazo, bien el que se regule de forma específica en la normativa (por ejemplo, sistemas IA alto riesgo de Anexo I) o un máximo de quince días hábiles. El operador habrá de adoptar tales medidas (art. 79. 3º y 4º RIA).[29]

Si el operador del sistema IA no adopta las medidas la AVM prohibirá o restringirá la comercialización o su puesta en servicio, retirará el sistema y lo notificará a la Comisión y los otros Estados (art. 79. 5º RIA)[30] y velará por que se cumplan (art. 79. 9º RIA)[31]. En estas decisiones la AVM detallará claramente el sistema IA y los problemas, así como los motivos de la actuación (79. 6º RIA)

---

29 "3. Cuando, en el transcurso de tal evaluación, la autoridad de vigilancia del mercado o, cuando proceda, la autoridad de vigilancia del mercado en cooperación con la autoridad nacional pública a que se refiere el artículo 77, apartado 1, constate que el sistema de IA no cumple los requisitos y obligaciones establecidos en el presente Reglamento, exigirá sin demora indebida al operador pertinente que adopte todas las medidas correctoras oportunas para adaptar el sistema de IA a los citados requisitos y obligaciones, retirarlo del mercado o recuperarlo, dentro de un plazo que dicha autoridad podrá determinar y, en cualquier caso, en un plazo de quince días hábiles a más tardar o en el plazo que prevean los actos legislativos de armonización de la Unión pertinentes según corresponda.
La autoridad de vigilancia del mercado informará al organismo notificado correspondiente en consecuencia. El artículo 18 del Reglamento (UE) 2019/1020 será de aplicación a las medidas mencionadas en el párrafo segundo del presente apartado.
4. El operador se asegurará de que se adopten todas las medidas correctoras adecuadas en relación con todos los sistemas de IA afectados que haya comercializado en la Unión."

30 "Si el operador de un sistema de IA no adopta las medidas correctoras adecuadas en el plazo a que hace referencia el apartado 2, la autoridad de vigilancia del mercado adoptará todas las medidas provisionales adecuadas para prohibir o restringir la comercialización del sistema de IA en su mercado nacional o su puesta en servicio, para retirar el producto o el sistema de IA independiente de dicho mercado o recuperarlo. Dicha autoridad notificará estas medidas sin demora indebida a la Comisión y a los demás Estados miembros."

31 "9. Las autoridades de vigilancia del mercado velarán por que se adopten sin demora indebida las medidas restrictivas adecuadas respecto del producto o del sistema de IA de que se trate, tales como la retirada del producto o del sistema de IA de su mercado."

4.3. Medidas a adoptar por incumplimientos formales y, en su caso, actuaciones por autoridades fronterizas

En los casos de incumplimientos formales la actuación habrá que adecuarse a la proporcionalidad (Comisión Europea, 2022: 113). A este respecto, el artículo 83 RIA sobre "Incumplimiento formal", la AVM requerirá "que subsane el incumplimiento de que se trate, dentro de un plazo". Así sucede respecto de errores o ausencia del marcado CE, no declaración UE de conformidad correctamente, falta de registro en la base de datos, no designar a un representante, no contar con documentación técnica.[32] No obstante, si persiste, cabrá "restringir o prohibir la comercialización" (art. 83. 2º RIA).[33]

Para el caso de que actúen autoridades fronterizas, más extraño que se dé para el caso de sistemas IA, si consideran que el sistema no es conforme o que presenta un riesgo grave, deben suspender y facilitar información a la AVM (Comisión Europea, 2022:114). En estos supuestos, se precisa una decisión final sobre el producto y mientras tanto quedarán bajo vigilancia aduanera (art. 27 RVM), como "Producto peligroso" o "Producto no conforme". Es incluso posible una orden de destrucción por la autoridad fronteriza o a petición de las autoridades de vigilancia del mercado (Comisión Europea, 2022:115).

5. ACTIVIDADES ESPECÍFICAS DE SUPERVISIÓN DE IA, AUTORIZACIONES Y OTRAS PARTICULARES ACTIVIDADES DE LAS AVM DE IA

5.1. Actividades específicas de supervisión de las AVM en virtud del RIA y sanciones

Además de las funciones generales de vigilancia que se han expuesto, cabe señalar algunas más propias y específicas del RIA. Así, es importante significar

---

[32] Artículo 83 Incumplimiento formal: "1. Cuando la autoridad de vigilancia del mercado de un Estado miembro constate una de las situaciones indicadas a continuación, exigirá al proveedor correspondiente que subsane el incumplimiento de que se trate, dentro de un plazo que dicha autoridad podrá determinar:
a) se ha colocado el marcado CE contraviniendo el artículo 48;
b) no se ha colocado el marcado CE;
c) no se ha elaborado la declaración UE de conformidad con el artículo 47;
d) no se ha elaborado correctamente la declaración UE de conformidad con el artículo 47;
e) no se ha efectuado el registro en la base de datos de la UE de conformidad con el artículo 47;
f) cuando proceda, no se ha designado a un representante autorizado;
g) no se dispone de documentación técnica."

[33] "2. Si el incumplimiento a que se refiere el apartado 1 persiste, la autoridad de vigilancia del mercado del Estado miembro de que se trate adoptará medidas adecuadas y proporcionadas para restringir o prohibir la comercialización del sistema de IA de alto riesgo o para asegurarse de que se recupera o retira del mercado sin demora."

que puede darse el supuesto de que la AVM concluya que el sistema IA de alto riesgo "a pesar de cumplir con el presente Reglamento, presenta sin embargo un riesgo". En estos supuestos (art. 82 RIA), la AVM exigirá al operador que adopte las medidas oportunas para asegurar su cumplimiento. Desde el inicio se informará a la Comisión y los Estados y la Comisión, tras consultas, decidirá qué hacer.

También cabe tener en cuenta la actuación de la AVM en supuestos en los que el proveedor considera que su sistema no es de alto riesgo del Anexo III (art. 80). Así, si un sistema IA queda bajo uno de los 25 supuestos y finalidades del Anexo III, se presume que es de alto riesgo y el proveedor habrá de justificar que no lo es (art. 6.3º RIA). (Cotino, 2024 a). Para estos supuestos el artículo 80 establece un protocolo de actuación para las AVM. Así, si la autoridad sospecha que sí que podría ser un sistema de alto riesgo, debe evaluarlo. Si la evaluación revela que el sistema de IA es efectivamente de alto riesgo, la autoridad demandará al proveedor que tome medidas necesarias para cumplir con el RIA y corrija el problema en un plazo fijado por la autoridad. Si el uso del sistema de IA va más allá del ámbito nacional, la autoridad de vigilancia debe informar a la Comisión Europea y a los otros Estados miembros sobre la evaluación y las medidas requeridas al proveedor.

Por su parte, el proveedor debe asegurar que este sistema cumple con el RIA. De no hacerlo, se le aplicarán sanciones económicas según el artículo 99. El proveedor debe aplicar medidas correctoras y, si no lo hace, se aplicarán las disposiciones del artículo 79. Si se determina que hubo una clasificación errónea intencionada para eludir los requisitos reglamentarios, se impondrán multas al proveedor conforme al artículo 99. Para estas acciones, las AVM pueden realizar controles pertinentes, incluyendo el uso de datos almacenados en la base de datos de la UE.

Otro supuesto específico del RIA es la actuación de AVM en gestión de reclamaciones por usuarios o afectado. En general, las AVM deben garantizar que los consumidores y otros interesados puedan interponer reclamaciones, las cuales deben ser debidamente gestionadas y contar con un seguimiento en conformidad con el artículo 11. 7. a) RVM. Cabe recordar que el RIA se dirige a proveedores e implantadores de productos de IA y ciertamente ignora a los afectados por un sistema de IA, que ni siquiera se mencionan. [34] No obstante, desde las enmiendas 628 y 629 de junio de 2023 se propuso la inclusión de algunos derechos, y finalmente, se regula el derecho a presentar una reclamación ante una AVM (art. 85 RIA).[35] No obstan-

---

[34] Hasta junio de 2023 no se incluyó entre las definiciones la de "persona afectada", junto con diversos derechos en las enmiendas del Parlamento (Enmienda 174, art. 3. 1º, 8 bis). Las "personas afectadas" finalmente no se definen pero sí que forman parte del "alcance" del artículo 2.1.g) RIA. "personas afectadas que estén establecidas en la Unión."

[35] "Artículo 85. Derecho a presentar una reclamación ante una autoridad de vigilancia del mercado. Sin perjuicio de otras vías administrativas o judiciales de recurso, toda persona física o jurídica que tenga motivos para considerar que se ha infringido lo dispuesto en el presente Reglamento podrá presentar reclamaciones ante la autoridad de vigilancia del mercado pertinente.

te, el texto finalmente aprobado diluye la propuesta del Parlamento. Como señala López-Tarruella (2024) queda más bien en el ámbito de las buenas intenciones. Así, a diferencia del derecho reconocido en el artículo 77 del RGPD, el RIA regula un derecho a presentar una petición ante la AVM y, simplemente, "tales reclamaciones se tendrán en cuenta a la hora de llevar a cabo actividades" (art. 85 RIA). Además, cabe pensar que estas peticiones se verán obstaculizadas por la compleja distribución de competencias entre las AVM que se deriva del artículo 74 del RIA. Cabe llamar la atención del posible interés de una regulación específica de "procedimientos para el seguimiento de las reclamaciones" (art. 11.7º a) RVM)[36]

Las AVM deben tener el poder para imponer sanciones (art. 14.4º i) RVM) y los Estados miembros deben regular dichas sanciones (art. 41 RVM, Comisión Europea, 2022: 108, 7.3.4). Así debe tenerse en cuenta tanto el RVM como las disposiciones específicas del RIA, todo ello de forma acorde a la regulación y exigencias constitucionales de cada Estado. Sin duda alguna que el legislador español ha de actuar a este respecto dado que el RIA ha dejado enormes espacios a la definición legislativa. En su caso, se puede regular que las AVM reclamen al operador económico pertinente los costes de las actividades de vigilancia del mercado emprendidas en relación con un producto considerado no conforme (art. 15. 1º RVM, Comisión Europea, 2022: 108).

5.2. Autorizaciones de las AVM de IA respecto de pruebas en condiciones reales y en supuestos de exención de evaluación de conformidad

El RIA regula otras actuaciones particulares de las AVM de IA, como es el caso de las autorizaciones y actividades respecto de pruebas en condiciones reales (arts. 76 y 60) y las autorizaciones en supuestos de exención de evaluación de conformidad (art. 46 RIA). Por cuanto a las primeras, el RIA otorga a las AVM un papel activo y responsabilidades en la supervisión de pruebas de sistemas de IA (Cotino, 2024 b). Las pruebas de sistemas de IA de alto riesgo en condiciones reales precisan toda una serie de requisitos (art. 60 RIA) en los que están involucradas las AVM. Asimismo, el artículo 76 regula las facultades de las AVM en estos casos para la supervisión, verificación de cumplimiento de normativas, autorizar excepciones, adopción de medidas en caso de incidencias y la comunicación con otras autoridades.

De conformidad con el Reglamento (UE) 2019/1020, tales reclamaciones se tendrán en cuenta a la hora de llevar a cabo actividades de vigilancia del mercado y se tramitarán de conformidad con los procedimientos específicos establecidos con este fin por las autoridades de vigilancia del mercado."

[36] "7. Las autoridades de vigilancia del mercado establecerán los siguientes procedimientos en relación con los productos sujetos a la legislación de armonización de la Unión: a) procedimientos para el seguimiento de las reclamaciones o los informes sobre cuestiones relativas a los riesgos o los incumplimientos."

Así, con carácter general las AVM han de tener competencias y poderes necesarios para garantizar tales requisitos (art. 76.1º RIA) y que las pruebas en condiciones reales se ajusten a lo dispuesto en el presente Reglamento. También lo harán si tales pruebas en condiciones reales lo son en un espacio controlado de pruebas (art. 76. 2º RIA). La AVM habrá de haber "aprobado" las pruebas así como el "plan de la prueba" que debe presentar el proveedor-es. Cabe señalar que se consideran aprobados si no hay respuesta en 30 días, incluso aunque el Derecho nacional no regule una aprobación tácita (art. 60. 4º a) y b) RIA). La AVM recibirá asimismo notificaciones que expliquen la prórroga de la duración de seis meses, por hasta seis meses más, si bien no se requiere actividad por la AVM.

Las AVM deben contar con poderes para exigir a estos proveedores de las pruebas en condiciones reales "información, realizar sin previo aviso inspecciones a distancia o in situ y controlar la realización de las pruebas en condiciones reales y los sistemas de IA de alto riesgo relacionados. Las AVM harán uso de dichos poderes para garantizar que las pruebas en condiciones reales se desarrollen de manera segura." (art. 60. 6º RIA).

Las AVM serán informadas de "cualquier incidente grave detectado (art. 60. 7º RIA). En estos casos, o si considera que algo no se cumple, podrá decidir suspender o acabar las pruebas (art. 76.3º a) RIA) o exigir que modifiquen las pruebas (art. 76.3º b) RIA), siempre de manera motivada indicando cómo impugnar sus decisiones, también lo comunicará a las AVM de otros Estados en que se haya probado el sistema (art. 76. 4º y 5º RIA). A las AVM se les "notificará" "la suspensión o la terminación de las pruebas en condiciones reales y los resultados finales." (art. 60. 8º RIA).

Por otra parte, el artículo 46 regula cuándo los sistemas de IA de alto riesgo pueden ser eximidos temporalmente de los procedimientos estándar de evaluación de conformidad, se persiguen así motivos de seguridad pública o con el fin de proteger la vida y la salud de las personas, el medio ambiente o activos fundamentales de la industria y de las infraestructuras. Y las AVM tienen un papel significativo. Así, la AVM puede permitir excepcionalmente la utilización de sistemas de IA de alto riesgo por razones de seguridad o para proteger la vida, la salud, el medio ambiente, o activos clave. Esto deberá realizarse por un tiempo limitado hasta que se complete la evaluación de conformidad oficial. Cualquier autorización dada debe ser comunicada a la Comisión Europea y otros Estados miembros, si bien cabrá excluir datos más confidenciales sistemas IA de aplicación de la ley. La Comisión o los Estados pueden formular objeciones a la autorización. En ese caso la Comisión consultará al Estado miembro correspondiente y tomará una decisión sobre si la autorización está justificada o no, en su caso podrá retirar la autorización. En el caso de sistemas IA de alto riesgo asociados con productos ya regulados, solo se aplicarán las exenciones ya establecidas en esos actos de armonización.

5.3. Actividades de las AVM con relación a incidentes y autoridades de derechos fundamentales y cooperación con la Comisión y la Oficina IA respecto de la IA de uso general

El RIA establece algunas atribuciones concretas a las AVM de IA para colaborar o asistir a las autoridades de protección de derechos fundamentales. Estas autoridades de derechos fundamentales y en el ámbito de sus funciones, respecto de sistemas del Anexo III, pueden solicitar cualquier documentación para ejercer sus funciones y competencias (art. 77. 1º RIA). En estos casos han de comunicarlo a la AVM de IA (la AESIA). Asimismo, de no ser suficiente esta información o documentación, pueden solicitar a la AVM la organización de pruebas del sistema de IA de alto riesgo a través de medios técnicos para determinar si ha habido un incumplimiento de la normativa de derechos fundamentales. De considerarse razonable por la AVM, ésta "organizará las pruebas con la estrecha colaboración de la autoridad u organismo público solicitante en un plazo razonable" (art. 77.3 º RIA).

Asimismo y por otra parte, a la AVM cuando le notifican un incidente grave sobre "el incumplimiento de obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales" (art. 3. 49 c) RIA), habrá de informar a las autoridades de protección de derechos fundamentales correspondientes (art. 73. 7º sobre Notificación de incidentes graves, RIA).

Por cuanto a la cooperación con Comisión y la Oficina IA con relación a la IA de uso general, como es sabido, en materia de IA de uso general (Capítulo V, Castillo 2024), el protagonismo lo tiene la Comisión, cuyas actividades al respecto ejecuta a través de la Oficina de IA de la UE tanto en la definición de criterios y normas, como para la vigilancia y supervisión (entre otros, art. 75. 1º RIA, (Hernández Peña, 2024:87). En general, las AVM pueden solicitar a la Comisión que ejerza sus facultades "para ayudar" a llevar a cabo sus actividades (art. 78 RIA).[37]

No obstante, existen supuestos más concretos de actuación en cooperación o peticiones específicas por las AVM. Así, si los "sistemas de IA de uso general que pueden ser utilizados directamente por los responsables del despliegue al menos para una de las finalidades clasificadas como de alto riesgo" "cooperarán con la Oficina de IA para llevar a cabo evaluaciones del cumplimiento" (art. 75. 2º RIA).

---

[37] Artículo 88: "Cumplimiento de las obligaciones de los proveedores de modelos de IA de uso general. 1. La Comisión tendrá competencias exclusivas para supervisar y hacer cumplir el capítulo V, teniendo en cuenta las garantías procedimentales previstas en el artículo 94. La Comisión debe confiar la ejecución de estas tareas a la Oficina de IA, sin perjuicio de las competencias de organización de la Comisión y del reparto de competencias entre los Estados miembros y la Unión en virtud de los Tratados.
2. Sin perjuicio de lo dispuesto en el artículo 75, apartado 3, las autoridades de vigilancia del mercado podrán solicitar a la Comisión que ejerza las facultades previstas en la presente sección, cuando resulte necesario y proporcionado para ayudar a que se lleven a cabo las actividades de su competencia en virtud del presente Reglamento."

En esos casos se informa al Comité y otras AVM. También, en las investigaciones que son propias a las AVM sobre sistemas de alto riesgo, si después de intentarlo no pueden acceder a determinada información de un modelo de IA general, presentan solicitud a Oficina de IA, que le presentará antes de 30 días toda la que considere pertinente", se garantizará la confidencialidad (art. 75. 3º RIA).

6. PARA ACABAR, LA DESIGNACIÓN DE LAS AVM DE INTELIGENCIA ARTIFICIAL HASTA EL MOMENTO Y LAS AUTORIDADES DE PROTECCIÓN DE DATOS

Cabe subrayar que el RIA en diversas ocasiones orienta la designación de unas determinadas AVM, si bien deja en última instancia a cada Estado su designación. No obstante, de ir en contra de estas orientaciones del RIA se requiere una justificación. Así sucede en casos relativos a los productos del Anexo II. Listado A, la AVM de estos productos será aquella que viene siendo AVM para esos productos. Cabe la opción de que los Estados Miembros designen a otra AVM, en estos casos esa AVM pueda coordinarse con el resto de AVM que supervisan esos productos. Así, respecto de los sistemas de IA del Anexo II sólo excepcionalmente la AESIA podría asumir la vigilancia del mercado, por lo que en principio la AESIA no debería ser la AVM sin perjuicio de ser la autoridad principal y de referencia en España.

Respecto de los sistemas de IA utilizados por entidades financieras (art. 74. 6º RIA), la AVM para estos supuestos debería la autoridad nacional de supervisión de esas entidades financieras, como el Banco de España. No obstante, y de modo excepcional los Estados miembros pueden nombrar a otra AVM. No parece la opción más adecuada en un sector tan especializado y con trayectoria.

Asimismo, para los sistemas de IA para fines de aplicación de la ley, asilo, administración de justicia, procesos electorales o sistemas de IA de identificación biometría el RIA apunta a las autoridades —auténticamente— independientes específicas, como resulta especialmente las autoridades independientes de protección de datos (art. 74.6º RIA).[38]

Aunque la AESIA no fuera la AVM en tales supuestos y que lo fuera en muchos casos la AEPD, en todo caso la AESIA podría ejercer un papel fundamental

---

[38] "8. En el caso de los sistemas de IA de alto riesgo enumerados en el anexo III del presente Reglamento, punto 1, en la medida en que los sistemas se utilicen a los efectos de la garantía del cumplimiento del Derecho, la gestión de fronteras y la justicia y la democracia, y en el caso de los sistemas de IA de alto riesgo enumerados en el anexo III, puntos 6, 7 y 8, del presente Reglamento, los Estados miembros designarán como autoridades de vigilancia del mercado a efectos del presente Reglamento *bien a las autoridades de control encargadas de la protección de datos competentes con arreglo al Reglamento (UE) 2016/679 o a la Directiva (UE) 2016/680,* bien a cualquier otra autoridad designada con arreglo a las mismas condiciones establecidas en los artículos 41 a 44 de la Directiva (UE) 2016/680".

de liderazgo regulatorio, planificador y organizativo, de especial importancia para todos los sistemas IA de anexo I, además de ser punto coordinador con la UE. A lo anterior cabe añadir que la AESIA podría asumir en virtud de la regulación nacional competencias de control y vigilancia de sistemas de IA no regulados por el RIA, como pueda ser, especialmente, el uso de IA que no sea de alto riesgo por el sector público no jurisdiccional.

Todo hay que decir, que no es extraño que las CCAA creen una autoridad que ejerza las funciones de AVM respecto de su sector público, como es posible también en materia de protección de datos.

Pese a que al momento de cerrar estas páginas el RIA ya está en vigor, su aplicación es muy gradual y respecto de la vigilancia del mercado ha de pasar por diversas etapas. Han de tomarse decisiones de designarse las AVM y en su caso crearlas o adaptarlas para sus nuevas funciones. Es un momento muy preliminar tanto en España como en otros países del que se cuenta con muy poca información conocida del estado de deliberaciones y decisiones en cada Estado miembro.

El Comité Europeo de Protección de Datos (CEPD, 2024) en su declaración del 16 de julio de 2024 en una natural visión corporativa se ha postulado a favor, como regla general, de la designación como AVM principal y coordinadora de inteligencia artificial a las autoridades de protección de datos. Se viene a afirmar que el RGPD viene a ser un complemento del RIA, siendo que además el RGPD se aplica completamente al tratamiento de datos personales en el ciclo de vida de los sistemas de IA, especialmente en aquellos considerados de alto riesgo del Anexo III. De ahí que se apueste y recomiende que sean las autoridades de protección de datos para la supervisión de los sistemas de IA. Y ello no sólo en los ámbitos en los que el RIA se inclina por estas autoridades, como esencialmente en el ámbito de IA con datos biométricos y usos policiales y criminales.

En diversos países es muy posible que la autoridad de protección de datos será designada como AVM, al menos de los ámbitos que el propio RIA inclina a hacerlo. Pero no respecto de otros ámbitos ni como AVM principal y coordinadora de cara a la Comisión Europea.

Así, parece que será en el caso de Bélgica (*Autorité de la protection des données*). También es posible que en el caso de República Checa (*Office for Personal Data Protection*), pero se barajan también otras como el Ministerio de Industria y la Autoridad Nacional de Seguridad Cibernética. También todo indica que en Estonia la autoridad de datos (*Data Protection Inspectorate*) será AVM, pero no necesariamente la única, algo similar parece en Grecia, Portugal o Irlanda, entre otras. No obstante, al momento de cerrar estas páginas no hay decisiones conocidas o definitivas al respecto.

También en algunos países parece que se designarán autoridades ya existentes, como las especializadas en materia digital. Así será en Dinamarca con la

Agencia Digital Danesa (*Digitaliseringsstyrelsen*), también podría ser en el caso de República Checa respecto del Ministerio de Industria y la Autoridad Nacional de Seguridad Cibernética). En el caso de Alemania ya se ha designado a la Agencia Federal de Redes (*Bundesnetzagentur*) y Agencia Federal para la Seguridad de la Información (*BSI*).

En nuestro país sin duda que la AESIA ha nacido para ser la AVM principal de IA y parece que tendrá una fuerza centrípeta muy relevante como AVM. Sin embargo, no resultaría muy sencillo justificar que la AESIA asuma también funciones de supervisión en materias más propias de las autoridades de protección de datos según el propio RIA, como es el caso del ámbito biométrico y usos policiales y penales, dada la trayectoria de la AEPD. Tampoco parece muy natural que la AESIA asuma la supervisión en el ámbito bancario frente al Banco de España. Y en todo caso en el ámbito jurisdiccional debe ser el CGPJ como he sostenido (Cotino,2024c) y se ha confirmado recientemente (CGPJ, 2024).

De igual modo, baste indicar la endeblez y falta de legalidad de la regulación de la AESIA, del todo insuficiente para asumir toda una serie de funciones que aquí se han descrito como propias de la supervisión como AVM de IA. De igual modo, su falta de independencia es patente, especialmente si ha de asumir funciones de AVM propias de la AEPD o del ámbito bancario, en las que la independencia ha de ser plena (Cotino, 2024d). Lo mismo sucede respecto del ámbito de sistemas de IA con impacto electoral, terreno en el que su falta de independencia necesaria es también palmario. Pero estas ya son cuestiones que bien merecen otro estudio.

BIBLIOGRAFÍA

Álvarez García, Vicente:

— (2020): *Las normas técnicas armonizadas (Una peculiar fuente del Derecho europeo)*, Madrid: Iustel.

— (2024): *La aplicación de las normas armonizadas y de las especificaciones comunes en el ámbito de la inteligencia artificial (artículos 40 y 41 Reglamento)*.

Álvarez García, Vicente y Tahiri Moreno, Javier (2023): «La regulación de la inteligencia artificial en Europa a través de la técnica armonizadora del nuevo enfoque», *Revista General de Derecho Administrativo*, 63.

Castillo, José Antonio (2024): «Inteligencia artificial de uso general, modelos fundacionales (y "Chat GPT") en el Reglamento de inteligencia artificial», en Cotino Hueso, L. y Simón Castellanos, P. (coords.): *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Cízur Menor: Aranzadi La Ley.

CEPD (2024): *Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework*, de 16 de julio, https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_en [Consulta: 12/10/2024.]

Comisión Europea:

— (s.f. *a*): *The implementation of market surveillance in Europe* [en línea], https://single-market-economy.ec.europa.eu/single-market/goods/building-blocks/market-surveillance/organisation_en?prefLang=es. [Consulta: 12/10/2024.]

— (s.f. *b*): *Market surveillance for products* [en línea], https://single-market-economy.ec.europa.eu/single-market/goods/building-blocks/market-surveillance_en?prefLang=es. [Consulta: 12/10/2024.]

— (s.f. *c*): *Single Market Compliance Space, European Market and Product Surveillance Information Exchange System for Official Bodies, Consumers and Businesses (ICSMS)* [en línea], https://webgate.ec.europa.eu/single-market-compliance-space/market-surveillance. [Consulta: 12/10/2024.]

— (2022): *Guía azul sobre la aplicación de la normativa europea relativa a los productos*, Bruselas: Comisión Europea, 104.

Consejo General del Poder Judicial (CGPJ) (2024): *Informe sobre el impacto del Real Decreto-Ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del plan de recuperación, transformación y resiliencia en materia de servicio público de la justicia, función pública, régimen local y mecenazgo, en relación con el punto neutro judicial, el control de las herramientas de inteligencia artificial en la administración de justicia y la emisión de actos de juicios "en abierto"*, CGPJ, junio.

Comité Europeo de Protección de Datos (CEPD) (2024): *Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework* [en línea], https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_en. [Consulta: 16/07/2024.]

Cotino Hueso, Lorenzo:

— (2024a): «Alcance y delimitación de los sistemas de alto riesgo en el Reglamento de inteligencia artificial", Cotino Hueso, L. y Simón Castellanos, P. (coords.): (2024): *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Cízur Menor: Aranzadi La Ley.

— (2024b): «Sandbox, espacios controlados y pruebas en condiciones reales de sistemas de inteligencia artificial en el Reglamento. Medidas para PYMES, startups y microempresas», en Cotino Hueso, L. y Simón Castellanos, P. (coords.): *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Cízur Menor: Aranzadi La Ley.

— (2024c): «El uso jurisdiccional de la inteligencia artificial: habilitación legal, garantías necesarias y la supervisión por el CGPJ», *Actualidad Jurídica Iberoamericana*, 21, monográfico. https://revista-aji.com/.

— (2024d): «Cómo abordar jurídicamente el impacto de la inteligencia artificial en los derechos fundamentales», en *Derecho y Tecnologías*, Fundación Ramón Areces, Madrid.

Gobierno de España (s. f.), *Marco Estratégico Nacional General para la Vigilancia del Mercado de Productos no alimentarios, (MENVIME)* Versión 1.0, España 2022–2025, https://www.consumo.gob.es/es/servicios/publicaciones-programa-editorial/programa-editorial/marco-estrategico-nacional-general-vigilancia-mercado-producto-no-alimenticios [Consulta: 12/06/2024.]

Hernández Peña, Juan Carlos (2024): «La gobernanza y vigilancia del Reglamento de inteligencia artificial: autoridades de vigilancia del mercado, Comisión y las diversas entidades», en Cotino Hueso, L. y Simón Castellanos, P. (coords.): *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Cízur Menor: Aranzadi La Ley.

López-Tarruella Martínez, A. (2024): «Vías de recurso para los particulares en el reglamento de inteligencia artificial", en Cotino Hueso, L. y Simón Castellanos, P. (coords.): *Tratado sobre el Reglamento … cit*.

Palma Ortigosa, Adrián:

— (2024a): «La evaluación de la conformidad en el diseño y producción de sistemas basados en IA en el contexto del "Nuevo Marco Legislativo"», en Cotino Hueso, L. y Simón Castellanos, P. (coords.): *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Cízur Menor: Aranzadi La Ley.

— (2024b): «¿Quién es quién en el Reglamento Europeo de Inteligencia Artificial? Las autoridades notificantes y los organismos notificados», *Actualidad Jurídica Iberoamericana*, 21, 598-617. https://revista-aji.com/. [Consulta: 12/06/2024.]

Ramón Fernández, Francisca (2024): "Sistemas de gestión de calidad, documentación técnica y conservación en el Reglamento", Cotino Hueso, L. y Simó Castellanos, P. (coords.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi La Ley, Cízur Menor.

Vestri, Gabriele (2024): «Acceso a documentación y confidencialidad en el Reglamento de inteligencia artificial», en Cotino Hueso, L. y Simón Castellanos, P. (coords.): *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Cízur Menor: Aranzadi La Ley.

Unión Europea (2017): *Buenas prácticas de vigilancia del mercado,* enero de 2017, ADCO, Ref. Ares(2017)2337704 – 06/05/2017, https://www.aragon.es/documents/20127/31455048/Gu%C3%ADa+de+buenas+pr%C3%A1cticas+de+vigilancia+del+mercado+UE.pdf/6de2d204-b386-e3e7-539d-322741d667c4?t=1579769712429 [Consulta: 12/06/2024.]