REVISTA DE

PRIVACIDAD Y DERECHO DIGITAL

DIRECTOR • D. PABLO GARCÍA MEXÍA

NÚMERO MONOGRÁFICO
REGLAMENTO EUROPEO DE IA
UAM
Universidad Autónoma de Madrid

AÑO IX • MAYO-AGOSTO 2024 • NÚMERO 34

ISSN: 2444-5762

OBLIGACIONES DE LOS PROVEEDORES (*)

OBLIGATIONS OF THE PROVIDERS

RICARDO RIVERO ORTEGA
Universidad de Salamanca

(*) Este trabajo se recibió el 3 de junio de 2024 y fue aceptado el 1 de agosto.

REVISTA DE
PRIVACIDAD Y DERECHO DIGITAL

RESUMEN

La regulación europea de la Inteligencia Artificial establece una serie de obligaciones informativas y técnicas para posibilitar el control de los proveedores de sistemas. Ante una normativa tan prolija, se hace necesario definir correctamente su alcance, límites y garantías favorables a la iniciativa e innovación de las empresas, así como precisar su aplicabilidad a los poderes públicos.

PALABRAS CLAVE: *Regulación de la inteligencia artificial, obligaciones de los proveedores de IA, evaluación de conformidad.*

ABSTRACT

The european regulation of AI establish information obligations of providers and techniques to enable its control. Given so much complex regulations, a correct definition of its scope, limits and favorable guarantees for the initiative and innovation of companies is necessary, as well as specifying its applicability to public powers.

KEYWORDS: *AI Regulation; AI providers obligations; conformity assessment procedure.*

SUMARIO

I.- INTRODUCCIÓN

La Inteligencia Artificial ha pasado de ser una quimera de ciencia ficción a convertirse en un producto/servicio cotidiano, fabricado y ofrecido por empresas sujetas a una regulación similar en muchos aspectos a la que se proyecta sobre otros sectores de la industria. Al igual que ocurre con las demás tecnologías, antes de someterlas a leyes, deben ponderarse sus riesgos, posibles beneficios e incluso los efectos trascendentes sobre el futuro del ser humano, incorporando consideraciones éticas y de filosofía jurídica a su tratamiento por el Derecho. De esto se ocupan expertos cuyas obras conviene consultar, pues nos alertan de las implicaciones del enfoque que adoptemos sobre nuestro concepto de persona y el devenir de las sociedades contemporáneas[1].

Europa quiere destacar por su defensa del humanismo y los derechos de las gentes, contraponer su modelo al de China, por ejemplo, poco escrupuloso en su limitación de las herramientas más amenazadoras. Así, todos los documentos previos al reglamento aprobado han puesto énfasis en las garantías. En lo más práctico, la regulación europea de la inteligencia artificial incorpora un "nuevo enfoque" en su pionera legislación de estas tecnologías, en el ánimo de evitar retrocesos o inhibiciones de las empresas que desarrollan aplicaciones llamadas a cambiar nuestras vidas[2].

Entre estas dos líneas -filosofía de protección de los derechos y regulación técnica de nuevo enfoque, con instrumentos de control de riesgos y de calidad- se sitúa el tratamiento de las

1 LLANO ALONSO, Fernando Higinio, *Homo ex machina. Ética de la inteligencia artificial ante el horizonte de la singularidad tecnológica*, Tirant lo Blanch, Valencia, 2024.

2 ÁLVAREZ GARCÍA, Vicente, "La regulación de la inteligencia artificial en Europa a través de la técnica armonizadora del nuevo enfoque", *Revista General de Derecho administrativo*, 63, 2023. FERNÁNDEZ HERNÁNDEZ, Carlos, "El Reglamento de Inteligencia Artificial. Un nuevo marco regulador para una tecnología en continua evolución", *Derecho Digital e Innovación*, 19, 2024.

obligaciones de los proveedores, planteado desde los primeros documentos preparatorios con el fin de proteger a los usuarios y evitar los mayores riesgos de abuso en su utilización. Por ello se ha puesto particular énfasis en la transparencia de los sistemas, su fiabilidad y su explicabilidad, la protección de datos personales y la prevención de los riesgos[3].

Todas estas exigencias se proyectan sobre los sujetos y organizaciones que se lucran o logran sus objetivos creando, comercializando o poniendo a disposición de terceros sistemas de IA; empresas y también organismos públicos afectados por la nueva norma.

A los efectos del Reglamento, se entiende que es proveedor "una persona física o jurídica o autoridad, órgano u organismo de otra índole públicos que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA y lo introduzca en el mercado o pongan en servicio el sistema de IA con su propio nombre o marca comercial, previo pago o gratuitamente". La norma nos ofrece un concepto muy amplio que incluye sujetos públicos y privados, en distintos eslabones de una cadena compleja de creación y distribución de los productos/servicios de IA.

Por su amplitud y complejidad, esta definición de proveedor plantea los primeros problemas serios relacionados con el estatuto y las obligaciones, toda vez que al no diferenciar sujetos públicos y privados –particulares y autoridades- la incidencia de los controles, las exigencias de aportación de información o las posibles sanciones podrían, de no excepcionarse, no ser distintas. Algunos procedimientos no parecen fácilmente aplicables a determinados organismos públicos, que sin embargo en muchos casos entrarán en este concepto de los proveedores.

3 MARTÍNEZ ESPÍN, Pascual, "La propuesta de marco regulador de los sistemas de inteligencia artificial en el mercado de la UE", *Revista CESCO de Derecho del consumo*, 46, 2023.

Cuando no puedan ser considerados proveedores, las autoridades públicas serán "responsables del despliegue", definidos como "persona física o jurídica o autoridad, órgano u organismo de otra índole públicos que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional". Y estos sujetos serán afectados también por algunas de las obligaciones previstas en el reglamento, de modo que un círculo de organizaciones mucho más amplio estará sujeto a las previsiones que analizaremos a continuación.

Las siguientes páginas se dedican al análisis del estatuto del proveedor, a sus obligaciones concretas, predicables de sujetos públicos y privados. Comenzaré no obstante recordando algunas cuestiones básicas relativas a la posición jurídica de quien se sujeta a un marco regulatorio, la imposición de obligaciones mediante normas legales, el rango requerido y los límites a su establecimiento derivado de los principios del Estado de Derecho.

La regulación detallada del reglamento nos muestra el cumplimiento parcial de algunas de estas condiciones de imposición de deberes u obligaciones, pero su ubicación en anexos o en códigos de conducta plantea dudas de rango normativo, efectividad y aplicabilidad práctica en algunos casos. Por otro lado, buena parte de las obligaciones de los proveedores se encuentran en otra normativa sectorial de considerable importancia, que es la orientada hacia la protección de datos de carácter personal, muy avanzada en Europa y objeto de reformas recientes que afectan por supuesto a los proveedores de IA.

II.- LA NATURALEZA JURÍDICA DE LAS OBLIGACIONES DERIVADAS DE UN MARCO REGULATORIO

Todas las empresas están sujetas a condicionantes normativos pensados para la protección de los consumidores y la prevención de riesgos. En esto consiste en gran medida el objeto del Derecho administrativo económico[4]. Aunque el principio general de partida en la regulación debe ser la libertad, el derecho a emprender iniciativas económicas se modula en atención a otros intereses generales. Tales limitaciones de la libertad no han captado suficiente atención en los análisis dogmáticos, quizás porque se da por supuesto que existan regulaciones limitadoras y controles[5].

La doctrina administrativista se ha referido a la "imposición de deberes de comportamiento", empleando el concepto "deber", para separar la connotación de reciprocidad u onerosidad propia de la obligación (de signo contractual), cuando es el poder público quien establece exigencias de hacer o no hacer. Aquí se diferencian los deberes impuestos por la Administración y los "deberes normativos fiscalizados por la Administración", cuyo principal problema sería "la extensión concreta de cómo el deber legal tiene que ser cumplido por el administrado"[6].

Es en el ámbito tributario donde más se han desarrollado y analizado estos deberes, traducidos además en exigencias de suministro de datos. Así, el deber de información ha ocupado a la doctrina fiscalista, cuyas aportaciones sobre la extensión y

4 RIVERO ORTEGA, Ricardo, *Derecho administrativo económico*, Marcial Pons, 2022.

5 Los estudiosos del Derecho administrativo en Estados Unidos, en cambio, se dividen entre quienes defienden la necesidad de la regulación (SUNSTEIN y BREYER, por ejemplo) y quienes consideran que esta ha fracasado y llegan a discutir la propia legitimidad de este tipo de intervenciones (COGLIANESE, HAMBURGER). Efectivamente, los excesos regulatorios pueden asfixiar la innovación y producir graves perjuicios económicos.

6 GARCÍA DE ENTERRÍA, Eduardo/FERNÁNDEZ RODRÍGUEZ, Tomás-Ramón, *Curso de Derecho administrativo*, Cívitas, Madrid, 2022.

límites del deber de información nos pueden ayudar al definir las obligaciones de los proveedores de servicios de IA, pues casi todas ellas tienen algún carácter informativo, de transparencia o aportación de datos relevantes. Hasta qué punto una empresa tiene que "desnudarse" delante de la Administración en sus prácticas o técnicas es una cuestión que se puede plantear tanto en el ámbito financiero como en la regulación de riesgos[7].

Por supuesto, un criterio relevante a la hora de ponderar la corrección de este alcance es el principio de proporcionalidad, muy útil como piedra de toque de cualquier intervención limitadora o condicionante de los derechos y libertades, en su triple test de necesidad, adecuación y menor restricción posible.

En todo caso, el establecimiento de obligaciones tiene una serie de implicaciones jurídicas y requiere el cumplimiento de presupuestos propios del Estado constitucional. La exigencia de una norma con rango de Ley o equivalente, que se satisface en este caso de los proveedores de sistemas de IA al incluirse las obligaciones un reglamento europeo. También la necesidad de precisar conforme a un principio de tipicidad la obligación, por razones de seguridad jurídica.

Esto es lo que veremos hacen los anexos del Reglamento europeo de inteligencia artificial y otras herramientas (códigos de conducta y especificaciones técnicas). La tipificación consiste en la descripción pormenorizada del contenido, sobre todo cuando se trata de obligaciones de colaboración o de carácter informativo. En muchos sectores regulados, el punto más difícil de resolver y también el que da lugar a un mayor número de controversias precisamente consiste en la determinación del alcance de los deberes de aportar datos, cuáles, cuándo y por qué motivos[8].

7 PEÑA AMORÓS, Mª del Mar, *El deber de información*, Dykinson, 2020.

8 RIVERO ORTEGA, Ricardo, *El Estado vigilante. Consideraciones jurídicas sobre la función inspectora de la Administración*, Tecnos, 1999.

El principal problema que nos vamos a encontrar en el tratamiento jurídico de las obligaciones impuestas a las empresas en contextos regulatorios es su falta de precisión, el recurso a cláusulas generales y conceptos indeterminados para trasladar deberes a los proveedores de servicios, sin concretar muchas veces en qué consista exactamente la obligación. Así sucede en parte al determinar el alcance de las obligaciones de comunicación y transparencia, asociadas también a la explicabilidad de la IA[9].

Especialmente, la "transparencia interna" para evaluadores y usuarios, nos interesa en este análisis porque forma parte del estatuto de los proveedores en su capítulo de obligaciones. Estas obligaciones afectan a derechos fundamentales, pero será necesario valorar hasta qué punto permiten atenuar los derechos de propiedad y libertad de empresa que también reconoce nuestro Ordenamiento[10]. Sobre la mayoría de los productos y servicios que consumimos no tenemos ni necesitamos información muy detallada, ni siquiera cuando se trata de alimentos que ingerimos o medicinas que se introducen en nuestro organismo, así que en la práctica más que reforzar las obligaciones informativas sobre los usuarios, parecen tener pleno sentido las obligaciones de aportación de datos precisos a los reguladores.

El despliegue del reglamento europeo de IA planteará estas cuestiones y otras, así por ejemplo la pretensión de concretar las obligaciones mediante códigos de buenas prácticas. Inmediatamente surge la pregunta de si pueden establecerse obligaciones jurídicas mediante códigos de buenas prácticas, porque el Reglamento contempla esta herramienta de autorregulación, aunque los códigos de buenas prácticas no pueden considerarse

9 COTINO, Lorenzo, "Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida", Revista Española de Transparencia, 16, 2023.

10 PEÑA AMORÓS, Mª del Mar, "Derechos fundamentales y deber de información", Gaceta Fiscal, 2024.

auténticas normas[11]. Y, sin embargo, el Considerando 116 de la Directiva así lo apunta: "Los códigos de buenas prácticas deben abarcar las obligaciones de los proveedores de modelos de IA de uso general y de modelos de uso general que presenten riesgos sistémicos".

Los procesos de certificación y las evaluaciones de conformidad devienen también claves en el cumplimiento de estas obligaciones. De esta forma, el instrumental de seguimiento de las obligaciones es distinto al más convencional del Derecho administrativo clásico, aunque no sea tan innovador si nos fijamos en la regulación de la seguridad de los productos industriales o en otros ámbitos donde impera la regulación por sujetos privados y la autoregulación[12].

III.- LAS OBLIGACIONES CONCRETAS: ARTÍCULOS 16, 50, 53 Y 55 DEL REGLAMENTO EUROPEO

Ya he tratado el concepto de "proveedor", así como el de "responsable del despliegue" en la introducción de este trabajo. Ahora diferenciaré el régimen de las obligaciones tal y como lo hace el reglamento, en función de los niveles de riesgo asociados a los sistemas, comenzando por los de "alto riesgo", definidos en primer lugar, continuado con los de "riesgo sistémico" y terminando con los de "uso general". A mayor nivel de riesgo, más y más intensas obligaciones, pues al fin estas sirven para permitir un grado de control mayor sobre los proveedores o sujetos responsables de los sistemas de IA.

11 SADDY, André, "Códigos de buenas prácticas. Concepto, naturaleza y su configuración como fuente de Derecho administrativo", en *Regulación y competencia en servicios de interés económico genera*l, 2017.

12 DARCANULLETA GARDELLA, Mercé, Autoregulación y Derecho público: la autoregulación regulada, Marcial Pons, 2005.

Fuera de la regulación específica de cada tipo de proveedor, el reglamento contempla también obligaciones comunes y genéricas. Así, su artículo 4 les conmina a adoptar medidas de "alfabetización en materia de IA" orientadas a su personal. Así mismo, las "prácticas de inteligencia artificial prohibidas", señaladas en el artículo 5, comportan obligaciones negativas de los proveedores (no hacer). Estas prohibiciones no son triviales porque condicionan sobremanera el desarrollo técnico de los sistemas.

El primer artículo del Reglamento europeo dedicado a las obligaciones de los proveedores es el 16, dirigido a los proveedores y responsables del despliegue de sistemas de IA de alto riesgo. El Reglamento identifica los sistemas de "alto riesgo" en su artículo 6, en un modo sumamente esclarecedor si nos fijamos en la definición en negativo (lo que no son sistemas de alto riesgo), en aquellos casos que "…no plantea un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas…", así como en varios supuestos que este precepto detalla.

La primer obligación de la lista es velar por el cumplimiento de los requisitos de la sección 2 (sistema de gestión de riesgos; sometimiento a pruebas previas para determinar medidas de gestión de riesgos; prácticas de gobernanza y gestión de datos; detección y prevención de sesgos; elaboración y actualización de documentación técnica; conservación de registros; transparencia y comunicación de información a los responsables del despliegue; posibilidades de vigilancia humana mediante el desarrollo de interfaces; precisión, solidez y ciberseguridad).

Esta obligación es en realidad una "metaobligación", es decir, una obligación sobre el cumplimiento de obligaciones, refuerzo o recordatorio de los requisitos que deben cumplirse, varios de los cuales se reiteran en las siguientes obligaciones.

La siguiente obligación es indicar en el sistema o su embalaje que se trata de un sistema de alto riesgo, su nombre comercial

y dirección de contacto. Este tipo de advertencias sirven para dejar constancia del peligro propio del producto/servicio y favorecer la trazabilidad, una de las técnicas básicas de control de riesgos (con muchas aplicaciones ensayadas en el Derecho alimentario). La cuestión del etiquetado no está del todo resuelta en el Reglamento. Por eso se ha propuesto una etiqueta complementaria que advertiría de los riesgos y ofrecería más información a los usuarios[13].

La tercera obligación es cumplir con un sistema de gestión de calidad, cuyas características son detalladas por el artículo 17: estrategia de cumplimiento de la normativa (incluyendo evaluación de conformidad y gestión de las modificaciones); técnicas, procedimientos y actuaciones sistemáticas para el control y verificación del diseño; técnicas, procedimientos y actuaciones sistemáticas para el aseguramiento de la calidad; procedimientos de examen, prueba y validación antes, durante y después, con su frecuencia; especificaciones técnicas; sistemas y procedimientos de gestión de datos; sistema de gestión de riesgos; sistema de vigilancia poscomercialización; procedimientos de notificación de un incidente grave; gestión de la comunicación con las autoridades nacionales; procedimientos para llevar registro de toda la documentación; gestión de recursos y seguridad del suministro; marco de rendición de cuentas que defina las responsabilidades del personal directivo.

El deber de conservación de la documentación prevista en el artículo 18 incluye esta primera remisión y otras a los artículos 11 (sobre documentación técnica), y 17 (sistema de gestión de calidad). Además de estos documentos, deben conservarse los relativos a los cambios aprobados por los organismos, las decisiones de los organismos y la declaración UE de conformidad. Serán los Estados miembros los que establezcan los plazos de conservación de la documentación y sus condiciones.

13 STUURMAN, kees7LACHAUD, Eric, "Regulating IA. A Label to complete the proposed Act of Artificial Intelligence", *Computer Law and Security Review*, 2022.

Los proveedores también han de conservar los archivos de registros generados automáticamente por los sistemas. Esos registros dejan constancia de su operatividad y permiten trazar incidencias y comprobar si se están controlando los riesgos y cumpliendo las condiciones de seguridad, calidad y protección de datos. La regulación de esos registros se encuentra en el artículo 19 con fines de trazabilidad al fin.

La siguiente obligación prevista es la de someterse periódicamente a la evaluación de conformidad, un requisito que después analizaremos con más detalle en su régimen del artículo 43. Este tipo de certificación es una de las claves del modelo de regulación y control por el que ha optado la Unión Europea, en línea con otras modalidades de garantía de seguridad de otros muchos productos.

También están obligados los proveedores a elaborar una declaración UE de conformidad, cuyas condiciones se regulan en el artículo 47. Más adelante nos detendremos en la naturaleza de esta declaración, su vínculo al control de la seguridad y la calidad de los productos industriales y a otros ámbitos como la sanidad. Básicamente se tratan de conjuntos de información no financiera que demuestran el cumplimiento de la normativa del sector de referencia, técnicas propias de la certificación y normalización[14].

Otra obligación es colocar el marcado CE de IA de alto riesgo en el sistema o, si no fuera posible, en su embalaje o la documentación. La insistencia en que se puedan identificar los sistemas de alto riesgo es comprensible, al igual que en otros productos se advierte de su peligrosidad a quienes accedan a su uso. Tales advertencias serán relevantes también en el momento de imputar responsabilidades si se producen daños por una utilización inadecuada de los sistemas de alto riesgo.

14 BRITO MARQUINA, Avelino, "Verificaciones, la última frontera de la certificación", *Calidad. Revista mensual de la Asociación Española para la Calidad*, 1, 2020.

También han de cumplir las obligaciones de registro previstas en el artículo 49.1 del Reglamento. Deben adoptar medidas correctoras necesarias y facilitar la información prevista en el artículo 20 (retirar del mercado o desactivar sistemas que no cumplan el Reglamento, investigar las causas de riesgos e informar a las autoridades de vigilancia del mercado y a los organismos notificados. Habrán de demostrar de forma motivada ante la autoridad nacional competente la conformidad del sistema de alto riesgo con sus requisitos y velarán por que el sistema cumpla todos los requisitos de accesibilidad.

El artículo 17 añade a todas estas obligaciones la de establecer un sistema de gestión de calidad, consignado de manera sistemática y ordenada en la documentación con todos los aspectos de cumplimiento de la normativa. Este sistema debe hacer referencia a las especificaciones técnicas que se cumplirán y los procedimientos de gestión de datos, los sistemas de vigilancia postcomercialización y los procedimientos de notificación de un incidente grave, entre otras garantías para el cumplimiento de las obligaciones, moduladas en función del tamaño del proveedor.

Mención aparte merece la letra m) del apartado 1 de este artículo 17, pues exige "un marco de rendición de cuentas que defina las responsabilidades del personal directivo y de otra índole en relación con todos los aspectos enumerados en este apartado". La identificación de las responsabilidades es una obligación trascendente por sus posibles consecuencias ulteriores, en línea con la tendencia actual de despliegue de sistemas de cumplimiento y asignación de funciones concretas a instancias determinadas en el organigrama de las empresas.

Otra obligación regulada en el artículo 18 es la conservación de la documentación durante un plazo de diez años desde la introducción en el mercado o la puesta en servicio del sistema de IA. Así mismo, deben conservar los archivos de registro generados automáticamente (artículo 19) y adoptar medidas correctoras sobre las que deben informar (artículo 20), cooperar

con las autoridades competentes, dando acceso a información y archivos (artículo 21) e informar a las autoridades sobre sus representantes autorizados (artículo 22).

Otros artículos que enuncian obligaciones de los proveedores se ubican en el Capítulo IV del Reglamento, sobre obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA. El artículo 50, primero de esta serie se refiere a los sistemas de IA destinados a interactuar directamente con personas físicas (obligación de informar de que están interactuando con un sistema de IA), a los sistemas que generen contenido sintético de audio, imagen, vídeo o texto (que sea posible detectar que ha sido generado o manipulado de manera artificial), a los sistemas de reconocimiento de emociones o categorizaciones biométricas (información a las personas expuestas y protección de datos). En fin, se establecen obligaciones de información para que las personas puedan identificar la IA y diferencien sus productos y servicios.

El siguiente precepto en este capítulo dedicado a obligaciones de los proveedores es el 53, que se proyecta sobre los modelos de IA de uso general. La elaboración y mantenimiento de la documentación técnica del modelo, su inteligibilidad para otros proveedores, el establecimiento de directrices para respetar los derechos de autor, puesta a disposición del contenido utilizado para el entrenamiento del modelo, y la cooperación con la Comisión y las autoridades nacionales competentes. El recurso a códigos de buenas prácticas para demostrar el cumplimiento de las obligaciones se prevé en el apartado cuarto de este precepto, demostrando la relevancia de estas pseudofuentes normativas en la regulación de la IA.

El artículo 55 del Reglamento regula las obligaciones de los proveedores de modelos de IA de uso general con riesgo sistémico, un concepto definido en el apartado 65 del artículo 3: "un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables

en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor".

Esta lista coincide en gran parte con la anterior. Evaluación de los modelos de conformidad para reducir riesgo sistémico, evaluación y reducción de los riesgos sistémicos: vigilancia y comunicación sin demora de los incidentes graves; comunicarán las medidas correctoras para resolver esos incidentes y velarán para que se establezca un nivel adecuado de protección de la ciberseguridad.

La prueba del cumplimiento de estas obligaciones puede realizarse mediante la adhesión a códigos de buenas prácticas previstos en el artículo 56, hasta que se publique una norma armonizada. De no optar por esta forma de demostración, tendrán que seguir otro medio adecuado aprobado por la Comisión. Todo parece indicar que los códigos de buenas prácticas funcionarán por tanto con un carácter pseudonormativo complementario. No son obligatorios, pero si no se cumplen será difícil demostrar que no se ha incurrido en incumplimiento de obligaciones porque el sistema de control funciona de tal forma que es el proveedor el que tiene que demostrar que cumple (inversión de la carga de la prueba) el cumplimiento de sus obligaciones, no la autoridad de control la que debe presentar pruebas del incumplimiento[15].

Es el artículo 51 del Reglamento el que nos ofrece las reglas de clasificación de los modelos de IA con riesgo sistémico, que han de cumplir alguno de estos requisitos: capacidades de

15 Recientemente he analizado la inversión de la carga de la prueba que se observa en la práctica del Derecho administrativo sancionador, en mi artículo publicado en la REDA de 2024, RIVERO ORTEGA, Ricardo, "¿Presuntos inocentes o presuntos culpables? La prueba de la responsabilidad subjetiva en el Derecho administrativo sancionador", *Revista Española de Derecho administrativo*, 2024.

gran impacto (alertadas por grupos de expertos científicos); cantidades acumuladas de cálculo medidas en FLOP superiores a 10^25.

La identificación del riesgo sistémico se precisa en el Anexo VIII del Reglamento, que establece los criterios para la clasificación de los modelos de uso general con este nivel de riesgo en función del número de parámetros del modelo, la calidad o el tamaño del conjunto de datos, la cantidad de cálculo utilizada para entrenar el modelo, sus modalidades de entrada y salida, las capacidades del modelo, sus repercusiones sobre el mercado interior, el número de usuarios finales registrados, etc.

IV.- LA EVALUACIÓN DE CONFORMIDAD

La comercialización de productos y servicios en la Unión Europea está sujeta a unas normas comunes que incluyen un régimen de evaluación y declaración de conformidad, contenido en el Reglamento de 9 de julio de 2008 por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos. Este reglamento establece la organización y funcionamiento para la acreditación de los organismos de evaluación de conformidad[16].

En esta norma también encontramos la definición de conceptos y herramientas que utiliza el nuevo Reglamento europeo. Así, por ejemplo, "especificación técnica", "norma armonizada", "acreditación" o "autoridad de vigilancia del mercado", entre otros. También se enuncian los principios generales de la acreditación,

16 ÁLVAREZ GARCÍA, Vicente, *Industri*a, Iustel, 2010. Más recientemente, del mismo autor, "Los instrumentos normativos reguladores de las especificaciones técnicas en la Unión Europea: un breve ensayo de identificación de nuevas fuentes del Derecho", *Revista General de Derecho Administrativo*, 63, 2023.

su funcionamiento, la acreditación transfronteriza, los requisitos de los organismos nacionales de acreditación, las obligaciones de informar y las medidas de vigilancia del mercado.

El Reglamento de IA proyecta este sistema sobre los proveedores de sistemas IA, dedicando varios considerandos a su aplicación, especialmente para los de alto riesgo, que además pueden formar parte de otros productos. Ya el Derecho europeo contempla la exigencia de la evaluación de conformidad para los productos de riesgo medio y alto.

Entre las peculiaridades de los sistemas de IA a los efectos del procedimiento de evaluación de conformidad, el Considerando 78 señala la necesidad de aplicar los requisitos esenciales de ciberseguridad de los productos digitales ("productos críticos importantes con elementos digitales"). Para ello se señala la cooperación con ENISA (Agencia de la Unión Europea para la Ciberseguridad).

Esta obligación de realizar la evaluación de conformidad está también vinculada a la de establecer un sistema de gestión de calidad y cumplir con todos los controles. Al fin, el régimen que se está proyectando sobre los sistemas de IA es el propio de la seguridad de los productos, contenido en normas transversales pensadas para que el poder público, auxiliado por entidades privadas especializadas, pueda evitar los riesgos asociados a la puesta en el mercado de determinados servicios o productos que pueden dañar a las personas o los bienes.

En el Reglamento de IA es el artículo 43 el que se dedica a la evaluación de la conformidad, a la que se deben someter los proveedores cuando apliquen las normas armonizadas (artículo 40) o las especificaciones comunes (artículo 41). Se presentan como alternativos dos procedimientos de evaluación de conformidad, respectivamente desarrollados en los anexos VI y VII. El primer está basado en el control interno, mientras el segundo se basa en la evaluación del sistema de gestión de calidad y la

evaluación de la documentación técnica, con la participación de un organismo notificado que se menciona en el anexo VII.

La sujeción al procedimiento de evaluación de conformidad basado en el sistema de gestión de calidad es obligatoria en aquellos casos en los cuales no existan normas armonizadas ni especificaciones comunes, el proveedor no haya aplicado toda la norma armonizada, no se hayan aplicado las especificaciones comunes o las normas armonizadas se hubieran aplicado con una limitación. Los sistemas de alto riesgo de los puntos 2 a 8 del Anexo III se deben atener al procedimiento de evaluación de conformidad fundamentado en control interno, sin participación de un organismo notificado. También se contemplan particularidades para los sistemas de IA de alto riesgo regulados por actos legislativos de armonización de la Unión.

Una vez un sistema ha superado un procedimiento de evaluación de conformidad, sólo tiene que someterse a un nuevo procedimiento cuando sea objeto de una "modificación sustancial". Esta previsión del apartado 4 del artículo es complementada con la precisión sobre sistemas que evolucionan ("continúen aprendiendo") a lo largo del tiempo. Si este progreso del sistema ha sido predeterminado por el proveedor en el primer procedimiento de evaluación de conformidad, no es necesario que pasen por un nuevo procedimiento porque no se consideran modificaciones sustanciales.

Los procedimientos de evaluación de conformidad dan lugar a la emisión de certificados (artículo 44) que pueden tener una validez máxima de cinco años, aunque pueden suspenderse antes si un sistema deja de cumplir los requisitos por su evolución.

El artículo 46 contempla supuestos de exención del procedimiento de evaluación de conformidad, una decisión que ha de responder a una solicitud debidamente motivada de una autoridad de vigilancia del mercado, siempre que se den circunstancias excepcionales de seguridad pública, protección de la vida

y la salud de las personas o el medio ambiente. También cabe esta exención por razones excepcionales de seguridad pública ante una amenaza específica.

La Declaración UE de conformidad es regulada en el artículo 47 y establece otra obligación de los proveedores. Redactar en un formato legible por máquina y firmado una por cada sistema de alto riesgo, poniéndola a disposición de las autoridades nacionales competentes por un período de diez años. Su contenido será afirmar que se cumplen los requisitos establecidos. Al fin estamos ante una suerte de "declaración responsable", similar a la que se prevén en otros muchos sectores de intervención administrativa.

El Anexo IV del Reglamento, detalla el procedimiento de evaluación de conformidad fundamentado en un control interno. El Anexo V explica la información que debe contener la declaración UE de conformidad: nombre y tipo del sistema de IA, nombre y dirección del proveedor o su representante, afirmación de la responsabilidad exclusiva del proveedor, declaración de conformidad con la normativa, declaración de ajuste a la normativa de protección de datos. El Anexo VII establece la secuencia de la conformidad fundamentada en la evaluación de un sistema de gestión de calidad y la evaluación de la documentación técnica.

Todos estos procedimientos son pues diseñados en su secuencia y cuentan con la experiencia de su aplicación en otros sectores de ingreso en el mercado de productos y servicios, así que sólo queda decir que representan una considerable oportunidad de negocio para las entidades especializadas en garantizar que se cumplen las especificaciones técnicas y el resto de las normas que componen un nuevo sistema de fuentes del Derecho, tal y como lo ha descrito Vicente Álvarez García[17].

17 ÁLVAREZ GARCÍA, Vicente, "Los instrumentos normativos reguladores de las especificaciones técnicas en la unión Europea…", *Revista General de Derecho administrativo*, cit.

La sujeción de los proveedores a mecanismos de evaluación de conformidad, en el caso de los de mayor riesgo, es una buena alternativa a la intensificación de controles públicos que podrían ser más gravosos. Ahora bien, esos controles van a tener lugar, y en un sector de tan rápido avance tecnológico pueden colisionar con las necesidades de las empresas y su capacidad de responder a las demandas de información y datos de las autoridades de vigilancia del mercado, así que puede haber conflictos y litigiosidad derivada de esta regulación.

V.- LA ACTUALIZACIÓN PROGRESIVA DE LAS OBLIGACIONES DE LOS PROVEEDORES Y OTRAS POSIBLES FUENTES DE LITIGIOSIDAD

Así, la seguridad jurídica suele asociarse a un conjunto de normas dado, previsible, cierto en su aplicación, presupuestos que no concurren en este régimen porque las especificaciones técnico, los códigos de conducta, los anexos del reglamento e incluso la interpretación de sus contenidos puede variar a lo largo del tiempo. Las evoluciones de las tecnologías y la comprensión de sus efectos sobre los derechos cambian efectivamente y esto puede suponer que lo que un día se considera suficiente desde el punto de vista del control y la aportación de datos deje de serlo tiempo después, con sobresalientes consecuencias.

Hay que destacar que el apartado 3 del artículo 44, sobre certificados, permite que se suspenda o retire el certificado de un sistema por incumplimiento sobrevenido de los requisitos de su concesión. Aunque todas las decisiones sobre certificados se puedan recurrir y deban tomarse respetando el principio de proporcionalidad, lo cierto es que esta posibilidad genera una cierta inseguridad en los proveedores.

Revista de Privacidad y Derecho Digital
ISSN digital 2444-5762, NÚM. 34, Madrid, Mayo-Agosto (2024), págs. 90-120

Sin duda, el concepto "estado de la técnica" es relevante en las regulaciones dirigidas al control del riesgo[18]. Las normas en estos sectores recurren a expresiones como "la mejor tecnología disponible", concepto jurídico indeterminado útil para establecer una "cláusula de progreso", proyectada en este caso sobre operadores privados (o públicos) que realizan actividades marcadas por la progresiva innovación. Los requerimientos de actualización al avance tecnológico se pueden canalizar a través de los actos delegados a la Comisión en el artículo 97, que puede actualizar los anexos VI y VII del Reglamento "a la luz del progreso técnico".

La normativa europea también contempla el proceso continuo de verificación y las técnicas concretas para garantizar la rendición de cuentas de los proveedores de servicios de IA[19]. La imputación de responsabilidades en marcos regulatorios de prevención del riesgo comporta esta constante actualización, de tal modo que la imputabilidad de daños, los deberes de diligencia y la culpabilidad en las infracciones administrativas dependerán de una ponderación que evoluciona según avanzan los conocimientos técnicos, las percepciones sociales y la experiencia[20].

Además de esta cuestión del cambio progresivo de los requisitos a los proveedores, otro punto de posible conflicto se deriva de las numerosas exigencias de aportación de datos e información, que pueden situar a las empresas ante el riesgo de perder sus ventajas competitivas. En la normativa europea se contemplan garantías compensatorias o "contradeberes", destacadamente los deberes de confidencialidad y reserva de los evaluadores, para garantizar la protección del secreto industrial. También se

18 ESTEVE PARDO, José, "La regulación de riesgos: gestionar la incertidumbre", *El Cronista del Estado Social y Democrático de Derecho*, 2021.

19 Desai, Deven R/Kroll, Joshua, "Trust but Verify: A Guide to Algoithms and the Law", *Harvard Journal of Law and Tecnology*, 1, 2017.

20 HOFMANN, Herwig, "The Duty of Care in EU Public Law – A Principle Between Discretion and Proportionality", *Review of European Administrative Law*, 13, 2020.

contemplan mínimas previsiones frente a los abusos en la exigencia de información.

Así, el artículo 20.3 del reglamento establece que: "Toda información obtenida por una autoridad nacional competente con arreglo al presente artículo se tratará de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78". El artículo 78 desarrolla ese deber de confidencialidad de la Comisión, las autoridades de vigilancia del mercado, los organismos notificados y cualquier persona física o jurídica que participe en la aplicación del reglamento, obligadas a proteger los derechos de propiedad intelectual e industrial, o los secretos comerciales.

En esta línea también se manifiesta el apartado 7 del artículo 53, sobre obligaciones de proveedores de modelos de uso general: "Toda información o documentación obtenida en virtud del presente artículo, incluidos los secretos comerciales, se tratarán de conformidad con las obligaciones de confidencialidad establecidas en el artículo 78".

Ya hemos citado el apartado 3 del artículo 78, conforme al cual sólo se puede solicitar la información estrictamente necesaria para proteger la seguridad y la confidencialidad de la información, y una vez recopilados los datos, se suprimirán todos aquellos que no sean necesarios para los fines legítimos de prevención del riesgo (apartado 2 del artículo 78).

Finalmente, una posible fuente de litigiosidad y cierta rebaja de garantías puede derivarse de la inversión de la carga de la prueba a la hora de determinar la culpabilidad por el incumplimiento de obligaciones de precaución de daños. El reglamento traslada a los proveedores la obligación de demostrar, a través de la evaluación de conformidad o con sus sistemas internos de calidad, que han cumplido todos los requisitos, pero incluso si así se realiza, cuando se produzcan incidentes imprevistos o daños concretos no siempre será fácil determinar si obedecerán a errores

del proveedor o al cumplimiento de especificaciones técnicas o códigos de conducta insuficientes.

VI.- ¿SERÁ LA UNIÓN EUROPEA UN ÁMBITO MENOS PROPICIO A LA INNOVACIÓN DEBIDO A ESTE MARCO REGULADOR?

Los primeros pasos de una nueva tecnología siempre suscitan incertidumbres, incluidas las regulatorias. En torno a la regulación, su necesidad, ventajas y posibles efectos adversos existe una controversia más aguda en los Estados unidos que en Europa. Los juristas americanos se dividen entre partidarios y detractores de las intervenciones regulatorias, con opiniones muy críticas. En la Unión Europea, en cambio, parece haber consenso sobre la conveniencia y necesidad de la regulación.

Entre las distintas opciones regulatorias posibles sobre la inteligencia artificial, la Unión Europea ha aprobado una que establece intensas exigencias y multiplica los controles sobre los proveedores. Además, lo ha hecho adelantándose a otros reguladores nacionales y supranacionales, de tal modo que convierte su experiencia en un modelo sujeto a la prueba de la reacción de los operadores. Ciertamente, parece que con el reglamento se prevendrán los riesgos, pero también se va a convertir la Unión Europea en una suerte de campo de pruebas regulatoria, pudiendo avanzar en el diseño de técnicas y mecanismos de control por delante de otros países. La experiencia puede ser un éxito o generar problemas (quizás ambas cosas).

Para alcanzar el éxito deseado de la estrategia, el Capítulo VI, sobre medidas de apoyo a la innovación, es desde mi punto de vista una muestra del afán de la Unión europea por evitar que su regulación y controles asusten a las empresas. Así, se prevén espacios controlados de pruebas para la IA (artículos 57 y 58), se

regula el tratamiento de datos personales para el desarrollo de sistemas de IA (artículo 59), se prevén pruebas de sistemas de IA de alto riesgo en condiciones reales fuera de espacios controlados de pruebas para la IA (artículo 60), se regula el consentimiento informado para participar en pruebas en condiciones reales fuera de los espacios controlados de pruebas para la IA (artículo 61), se favorecen las empresas emergentes (artículo 62) y se contemplan excepciones para proveedores específicos (artículo 63).

VII.- LA APLICACIÓN A LOS PODERES PÚBLICOS PROVEEDORES O RESPONSABLES DEL DESPLIEGUE

Hasta ahora hemos analizado el régimen de obligaciones de los proveedores en el Reglamento. El concepto de proveedor no diferencia entre empresas privadas y autoridades públicas, lo cual tiene su lógica si de lo que se trata es de prevenir los riesgos y daños derivados del uso de la inteligencia artificial. Ahora bien, el modelo regulatorio por el que se opta responde a los parámetros clásicos de una relación jurídica entre un organismo de supervisión público y sujetos particulares, no tan sencillo de proyectar cuando también se trata de controlar organismos del Estado.

Debe tenerse presente, además, que los usos públicos de la inteligencia artificial suelen estar vinculados al ejercicio de potestades administrativas, algunas de las cuales sirven a la seguridad pública o la persecución de los delitos, tareas ambas de difícil compatibilidad con los principios de transparencia o explicabilidad llevados a su extremo. Así pues, algunos de estos usos no pueden reconducirse a mi juicio a los mismos controles que los aplicables a las herramientas desplegadas por las empresas privadas. Por ello se contemplan excepciones, aunque no del todo afianzadas en la literalidad de la norma.

Un ejemplo de la peculiaridad del uso de los sistemas de IA con fines públicos lo encontramos en la previsión del artículo 27 del Reglamento, que exige a los responsables del despliegue de sistemas de alto riesgo una evaluación de impacto a los derechos fundamentales. Este precepto se orienta hacia los responsables del despliegue que sean organismos de Derecho público o entidades privadas que presten servicios públicos.

El artículo 43 del Reglamento, al regular la evaluación de conformidad, contiene al final de su primer apartado un inciso que reza lo siguiente: "...cuando se prevea la puesta en servicio del sistema de IA de alto riesgo por parte de las autoridades encargadas de la aplicación de la ley, las autoridades de inmigración o las autoridades de asilo, o por las instituciones, órganos u organismos de la Unión, la autoridad de vigilancia del mercado mencionada en el artículo 74, apartado 8 o 9, según proceda, actuará como organismo notificado". Esto significa que el control de este procedimiento corresponde directamente a la autoridad pública, lo cual parece lógico. Un control privado sobre autoridades u organismos públicos no parece muy adecuado.

Las exenciones del procedimiento de evaluación de conformidad, previstas en el artículo 46, pueden aplicárseles también a los organismos públicos, toda vez que muchas de sus aplicaciones pueden tener implicaciones sobre la seguridad, la salud o la protección del medio ambiente.

La evaluación de conformidad y la sujeción a una normativa diseñada para empresas, proyectada sobre organismos públicos prestadores de servicios públicos, puede dar lugar a complejidades varias que no podemos tratar en esta breve contribución. El ámbito de aplicación y las excepciones del Reglamento no han sido demasiado precisos en su definición diferenciada de proveedores privados y públicos. Ahora sólo apuntamos que esta falta de separación puede ser fuente de dificultades interpretativas y aplicativas.

VIII.- CONCLUSIONES

PRIMERA: La regulación europea de la inteligencia artificial aspira a orientar en clave humanista y de respeto de los derechos mediante un sistema de controles y un nuevo enfoque. Si se logra un equilibrio entre las garantías, los controles y los márgenes necesarios para la innovación empresarial, esta nueva normativa será exitosa.

SEGUNDA: Es muy importante precisar la naturaleza y alcance de las obligaciones de los proveedores, así como reconocer la importancia de nuevas herramientas jurídicas para constatar su cumplimiento (códigos de buenas prácticas, especificaciones técnicas y evaluaciones de conformidad). Una adecuada comprensión de sus efectos sobre el estatuto de los proveedores será presupuesto de la seguridad jurídica en el sector de la IA europea.

TERCERA: Los proveedores de sistemas de alto riesgo están sujetos a más obligaciones que todos los demás, por razones bien comprensibles. Estas obligaciones tienen un carácter informativo e incluyen el despliegue de sistemas de calidad, prevención y trazabilidad de riesgos y evaluación de conformidad.

CUARTA: Los proveedores de IA de riesgo sistémico también están sujetos a previsiones especiales de control y suministro de información. No se enfrentan a prohibiciones tan estrictas como los de alto riesgo, pero sus deberes de cooperación con las autoridades de vigilancia son intensos. Así mismo, algunas de las garantías propias de los sistemas de alto riesgo se extienden a los de riesgo sistémico.

QUINTA: Los proveedores de IA de uso general están sujetos a las obligaciones propias de muchos fabricantes o suministradores de bienes y servicios regulados por el Derecho europeo. En este caso, el menor nivel de riesgo comporta

menos obligaciones de realización de procedimientos como la evaluación de conformidad y otros controles.

SEXTA: La actualización progresiva de las prevenciones y garantías de trazabilidad e inteligibilidad de los sistemas de IA, mediante la adaptación a la mejor tecnología disponible, suponen obligaciones adicionales y sostenidas en tiempo real. El ritmo acelerado de evolución de estas técnicas permite anticipar algunas dificultades en el cumplimiento de esa obligación, así como posibles controversias en su exigencia.

SÉPTIMA: La proyección de las normas de control, transparencia y suministro de información aplicables a los proveedores de sistemas de IA de alto riesgo a los poderes públicos puede dar lugar a complejidades interpretativas y aplicativas. Las excepciones previstas en el Reglamento no parecen suficientemente explícitas.

OCTAVA: Una regulación más avanzada de la IA en Europa que en otros mercados podría producir sobre la inversión, la investigación y la innovación. Si los requisitos de transparencia, trazabilidad y control son percibidos por los proveedores como desproporcionados, o retrasan sus desarrollos, esto perjudicará la imagen y el funcionamiento del mercado interior europea. En cambio, si los controles se muestran eficientes y adecuados, el modelo regulatorio será copiado por otros países.

NOVENA: El reconocimiento de derechos de secreto industrial y el blindaje de los deberes de confidencialidad son garantías de las empresas frente al riesgo de que el cumplimiento de sus obligaciones produzca filtraciones de su *know how* dañinas para la competencia y los incentivos de innovación. Los reguladores han de ser muy cuidadosos en sus exigencias informativas, adaptándolas a lo verdaderamente indispensable para cumplir sus cometidos.

DÉCIMA: Una cuestión de gran importancia en el régimen de las obligaciones es la relativa a las responsabilidades derivadas de su incumplimiento, especialmente cuando se produzcan daños que puedan ser sancionables e indemnizables. La carga de la prueba del cumplimiento de la obligación se traslada mediante el régimen del Reglamento en gran medida a los proveedores, en una rebaja de garantías que es común a otros sectores. En un ámbito de tecnologías tan complejas, las cuestiones probatorias sobre cumplimiento e incumplimiento de obligaciones pueden dar lugar a serios problemas.

IX.- BIBLIOGRAFÍA

ÁLVAREZ GARCÍA, Vicente, *Industria*, Iustel, 2010.

ÁLVAREZ GARCÍA, Vicente, "La regulación de la inteligencia artificial en Europa a través de la técnica armonizadora del nuevo enfoque", *Revista General de Derecho administrativo*, 63, 2023.

ÁLVARÉZ GARCÍA, Vicente, "Los instrumentos normativos reguladores de las especificaciones técnicas en la Unión Europea: un breve ensayo de identificación de nuevas fuentes del Derecho", *Revista General de Derecho Administrativo*, 63, 2023.

BRITO MARQJINA, Avelino, "Verificaciones, la última frontera de la certificación", *Calidad. Revista mensual de la Asociación Española para la Calidad*, 1, 2020.

COBBE, Jeniffer/SINGH, Jatinder, "Artificial Intelligence as a Service: Legal Responsabilities, Liabilites and Policy Challenges", *Computer Law & Security Review*, 42

COTINO, Lorenzo, "Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida", *Revista Española de Transparencia*, 2023.

DARCANULLETA GARDELLA, Mercé, Autoregulación y Derecho público: la autoregulación regulada, Marcial Pons, 2005.

DESAI, Deven R./KROLL, Joshua, "Trust but Verify: A Guide to Algorihtms and the Law", *Harvard Journal of Law and Technology*, 31, 2017.

ESTEVE PARDO, José, "La regulación de riesgos: gestionar la incertidumbre", *El Cronista del Estado Social y Democrático de Derecho*, 2021.

FERNÁNDEZ HERNÁNDEZ, Carlos, "El Reglamento de Inteligencia Artificial. Un nuevo marco regulador para una tecnología en continua evolución", *Derecho Digital e Innovación*, 19, 2024.

GARCÍA DE ENTERRÍA, Eduardo/FERNÁNDEZ RODRIGUEZ, Tomás-Ramón, *Curso de Derecho administrativo*, Cívitas,

HOFFMANN, Herwig, "The Duty of Care in EU Public Law – A Principle Between Discretion and Proportionality", *Review of European Administrative Law*, 13, 2020.

MARTÍNEZ ESPÍN, Pascual, "La propuesta de marco regulador de los sistemas de inteligencia artificial en el mercado de la UE", *Revista CESCO de Derecho del consumo*, 46, 2023.

PEÑA AMORÓS, Mª del Mar, *El deber de información*, Dykinson, 2020.

PEÑA AMORÓS, Mª del Mar, "Derechos fundamentales y deber de información", *Gaceta Fiscal*, 450, 2024.

RIVERO ORTEGA, Ricardo, *El Estado vigilante*, Tecnos, 1999.

RIVERO ORTEGA, Ricardo, *Derecho administrativo económico*, Marcial Pons, 2022.

RIVERO ORTEGA, Ricardo, *Derecho e inteligencia artificial: cuatro estudios*, Okejnik, 2023.

RIVERO ORTEGA, Ricardo, "¿Presuntos inocentes o presuntos culpables? La prueba de la responsabilidad subjetiva en el Derecho administrativo sancionador", Revista Española de Derecho administrativo, 2024.

SADDY, André, "Códigos de buenas prácticas. Concepto, naturaleza y su configuración como fuente de Derecho administrativo", en *Regulación y competencia en servicios de interés económico genera*l, 2017.

STUUMAN, kees/Lachaud, Eric, "Regulating iA. A Label to complete the proposed Act of Artificial Intelligence", *Computer Law and Security Review*, 2022.

Síganos en Linked

Visite nuestra web e infórmese de las novedades y actividades formativas que realizamos

www.rdu.es

2444-5762