REVISTA DE

PRIVACIDAD Y DERECHO DIGITAL

DIRECTOR • D. PABLO GARCÍA MEXÍA

AÑO IX • MAYO-AGOSTO 2024 • NÚMERO 34

ISSN: 2444-5762

USUARIOS DE LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL Y SUS OBLIGACIONES (*)

USERS OF ARTIFICIAL INTELLIGENCE SYSTEMS AND THEIR OBLIGATIONS

Por MERCEDES FUERTES

Catedrática de Derecho Administrativo.
Universidad de León

(*) Este trabajo se recibió el 28 de mayo de 2024 y fue aceptado en junio.

REVISTA DE
PRIVACIDAD Y DERECHO DIGITAL

RESUMEN

La autora analiza en este estudio las obligaciones específicas que han de cumplir los usuarios de los sistemas de inteligencia artificial teniendo en cuenta las diversas categorías de riesgos que presentan tales sistemas y las moratorias para la efectiva aplicación del Reglamento europeo previstas.

PALABRAS CLAVE: *Sistemas de Inteligencia Artificial. Usuarios de los sistemas de inteligencia artificial. Obligaciones de los usuarios. Responsables del despliegue de sistemas de inteligencia artificial. Obligaciones de los responsables del despliegue. Sistemas de inteligencia artificial de riesgo alto. Moratoria del Reglamento.*

ABSTRACT

In this study, the author analyses the specific obligations to be met by users of artificial intelligence systems, taking into account the various categories of risks posed by such systems and the expected moratoriums on the effective application of the European Regulation.

KEYWORDS: *Artificial Intelligence Systems. Users of artificial intelligence systems. Obligations of users. Deployers of artificial intelligence systems. Obligations of those responsible for deployment. High-risk artificial intelligence systems. Moratorium on the Regulation.*

SUMARIO

Agradezco a la dirección de esta Revista la invitación para realizar algunas consideraciones sobre las diversas obligaciones de los usuarios que precisa el Reglamento de inteligencia artificial. Conviene analizar y, sobre todo, debatir el contenido de este texto complejo -más complejo que extenso- por su relevancia. Pero también porque le seguirán otras disposiciones que tratarán de embridar la desaforada carrera tecnológica que estamos presenciando. Por ello, resulta oportuno, a raíz de un

debate constructivo, precisar los conceptos, atinar con un régimen jurídico ante los numerosos y dispares conflictos que suscitan los sistemas de inteligencia artificial, así como aclarar la redacción evitando la compleja lectura, las reiteraciones y otros defectos. Pues desde hace años se insiste en mejorar la "técnica legislativa" además de resultar imprescindible un correcto uso del español[1].

Sin perjuicio de la posible formulación de algunas críticas, la culminación de esta regulación ha de valorarse en términos generales de manera positiva. Los obstáculos durante su tramitación se hicieron evidentes: dificultades de atender a un ámbito tan innovador y de desarrollo tan acelerado, recordemos que avanzada la tramitación aparecieron los sistemas que generan contenidos y se introdujeron nuevas precisiones; tensiones entre las perspectivas diversas de los Gobiernos; posiciones distintas entre las grandes corporaciones empresariales, algunas voces solicitando incluso moratorias técnicas y normativas. Las negociaciones en el seno de las instituciones europeas consiguieron limar notables aristas, sortear significativos escollos y ofrecer un acuerdo final sobre el marco de regulación. No obstante, insisto en la concurrencia de dos circunstancias que generan dureza en la lectura: una, que todos los debates, audiencias y trabajos se desarrollaron en un inglés tecnológico, por lo que las expresiones jurídicas no son siempre afortunadas e, incluso, quizá la urgencia en facilitar versiones en todos los idiomas abuse de asociaciones con expresiones inapropiadas (me refiero a esas "traducciones" calificadas como "falsos amigos"); dos, y es un problema general de muchas normas europeas, la insistente adición de enmiendas genera una exposición con un hilo conductor no siempre coherente.

1 Santiago Muñoz Machado, como Director de la Real Academia de la Lengua Española, ha impulsado la Red Panhispánica del lenguaje claro que ha elaborado guías para un lenguaje claro y accesible, además de los libros de estilo, de ortografía y buen uso del español que se facilitan a través de la página de esa Real Academia. Vid. también su reciente libro *Fundamentos del lenguaje claro*, Ed. Espasa, 2024.

Partiendo de esta complejidad, adentrémonos en esta disposición con ánimo de analizar un aspecto concreto: qué obligaciones han de cumplir determinados usuarios con el fin de prevenir, reducir o corregir riesgos.

Porque su finalidad, la que motivó su impulso y ha persistido durante toda su tramitación, es atender a los riesgos, tratar de evitarlos o, al menos, minorarlos. Que los trepidantes avances, en la medida de lo posible, no se desparramen de manera desenfrenada pues hay que ser conscientes de los peligros que la frenética expansión de los sistemas de inteligencia artificial pueden traer.

Este Reglamento sigue la lógica de tantas previsiones normativas sobre la seguridad de los productos. Sin impedir la innovación, ni el desarrollo de estos sistemas, las instituciones europeas han fijado unas mínimas reglas con el fin de reducir el desconcierto, la preocupación ante las consecuencias desconocidas de un desenvolvimiento tan rápido y, con ello, asentar cierta confianza de los ciudadanos. Un marco jurídico que se irá completando y actualizando por la Comisión Europea pues son varias, e importantes, las delegaciones normativas establecidas.

No se establece, por tanto, un régimen jurídico integral de tales sistemas de inteligencia artificial. Ha quedado pospuesto, por ejemplo, entre otros aspectos trascendentes, el debate de la regulación del régimen de responsabilidad patrimonial[2]. Pero este marco jurídico sí acoge, como veremos, ciertas pautas éticas de comportamiento.

Centrado el objetivo en prevenir los riesgos, se abre la lente visual, un gran angular, para englobar el amplio ámbito de aplicación subjetivo que está afectado por esta disposición. Detengámonos en el mismo pues a quienes abarque ese foco serán los destinatarios de determinadas obligaciones.

2 Me refiero a la Propuesta de Directiva que adaptará las normas de responsabilidad civil extracontractual a la inteligencia artificial, COM (2022) 303, de 28 de septiembre de 2022.

I.- USUARIOS Y RESPONSABLES DEL DESPLIEGUE

Junto a los más directos partícipes en la creación y extensión de esta tecnología, quienes la diseñan, la desarrollan o comercializan, concurren circunstancias peculiares e intensas (la complejidad y sofisticación ínsita en su corazón, la ingente información de la que se nutre, cómo se interpreten sus resultados, entre otras), que reclaman la necesidad de contemplar cómo se maneja y cómo va funcionando. Por ello, interesa atender también a quienes utilizan los sistemas de inteligencia artificial, los usuarios.

En los documentos iniciales de trabajo, así como en la propuesta que finalmente presentó la Comisión Europea, hace ya tres años, se anunciaba que el Reglamento se aplicaría "a los usuarios del sistema de inteligencia artificial que se encuentren en la Unión"[3]. Vocablo este de usuarios que fue variando en los debates del Parlamento Europeo y del Consejo. En determinado momento, una enmienda precisó la condición de determinados usuarios, que se reflejó en algunos textos con el palabro "implementador" y en otros con la locución "responsable del despliegue". Es esta una mejor expresión dentro de la complejidad de delimitar las diferencias de *status* jurídicos de todos aquellos que utilizan un sistema informático.

Tales matices lingüísticos, de usuario a responsable del despliegue, no han afectado a la esencia de la definición legal inicial. Se ha mantenido con las mismas palabras desde la primera propuesta de la Comisión. Porque es ahora responsable del despliegue -como antes era el usuario- cualquier persona que haya incorporado y utilice para el ejercicio de funciones públicas, para su actividad profesional o comercial, un sistema de inteligencia artificial (art. 3.4).

3 Art. 29 de la Propuesta de la Comisión Europea de Reglamento de normas armonizadas en materia de inteligencia artificial COM (2021) 206, de 21 de abril.

Dos notas esenciales son las que delimitan el concepto. Una, que la utilización del sistema de inteligencia artificial esté bajo su responsabilidad, porque sea quien dirige la organización, o supervisa o vigila su funcionamiento. Dos, que el uso tenga por finalidad el ejercicio de sus competencias, que atienda al desenvolvimiento de su actividad profesional o mercantil. La utilización de estos sistemas en el ámbito exclusivamente particular y privado queda fuera de los focos de este Reglamento.

Esta definición legal acoge tanto a las personas físicas o como a las jurídicas. Alberga cualquier entidad, ya sea privada o de naturaleza pública porque se trata de una norma de carácter general, común a todos.

Cualquier profesional, empresario, compañía, que incorpore un sistema para el desarrollo de sus actividades, prestación de servicios, relaciones comerciales..., ha de atender a estas previsiones. Cualquier persona, aunque se trate de un único profesional o empresario; cualquier empresa, grande o pequeña. Hace años que se han difundido sistemas asequibles para ser utilizados sin tener especiales conocimientos de programación: sistemas creativos para el diseño particular de páginas web, de servicios permanentes de atención al cliente, de disponibilidad de repuestos y suministros, de reserva de citas previas, de precisar las mejores rutas de reparto, las distintas predicciones de ingresos y costes, y otras muchas utilidades que facilitan la llevanza del negocio a un profesional, empresario o a pequeñas empresas.

Y también cualquier "autoridad pública, órgano u organismo". La definición incluye a cualquier Administración u organismo público, lógicamente también a las instituciones europeas, a sus órganos y organismos (cosa que recuerda el considerando 23)[4].

4 Sobre las transformaciones que exige en el ámbito de las actuación administrativa la inteligencia artificial recomiendo desde este momento: Menéndez, E. *From bureaucracy to artificial intelligence: the tension between effectiveness and guarantees,* Wolters Kluwer, CEDAM. 2023; y el colectivo dirigido por Gamero, E. *Inteligencia artificial y sector público: retos, límites y medios,* Tirant lo Blanch, 2023.

No se aplicará a las autoridades de terceros países ni a organismos internacionales (art. 2.4)

Esa alusión a la "personalidad" no ha de interpretarse, a mi juicio, en el sentido de excluir a comunidades de bienes, a otros grupos o a colectivos sin personalidad jurídica, a fondos públicos carentes de personalidad, así como a otras formas pintorescas dentro del amplio vestuario de disfraces que ofrece el sector público. Asumirán personalmente sus miembros las específicas obligaciones atendiendo a la clasificación de riesgos del sistema, salvo que concretas previsiones en sus estatutos o acuerdos establezcan otras reglas de organización y funcionamiento que determinen la responsabilidad. Con relación a los fondos públicos sin personalidad jurídica u otros entes públicos, la responsabilidad será del organismo al que esté adscrito.

Quedan únicamente fuera de este régimen jurídico quienes utilicen esos sistemas de inteligencia artificial para determinados usos. Así, con fines militares, de defensa o de seguridad nacional, pues se mantiene dentro de la exclusiva competencia de los Estados miembros sin perjuicio de la política europea de seguridad y defensa (arts. 4.2 y 42 y ss del TUE).

Igualmente quedan fuera de este marco jurídico los sistemas que se usen en el ámbito privado, así como aquellos utilizados de manera exclusiva para la investigación y el desarrollo científico, (art. 2. apartados 6 y 10). Por tanto, en la Universidad, los profesores que utilicen estos sistemas dentro de sus actividades propias de estudio o investigación científica, quedarán fuera del ámbito de aplicación. Sí veremos que deberán -deberemos- atender a específicas obligaciones con relación al uso de algunos sistemas, como los que controlan los exámenes con el fin de evitar fraudes. Lo mismo que estará lógicamente obligada la Universidad como institución al utilizar estos sistemas de inteligencia artificial en el ejercicio de sus funciones, en la gestión de su actividad.

Tampoco se aplicarán estas disposiciones a la investigación, actividades de prueba y desarrollo de los modelos de inteligencia artificial antes de su puesta a disposición o comercialización (art. 2.8). Y, en algunos casos, los sistemas que se difundan con códigos abiertos o licencias libres, pues no podrán eludir las prohibiciones establecidas ni el régimen de los sistemas de alto riesgo y deberán garantizar su transparencia (art. 2.12).

Ese gran angular que se ha abierto para contemplar el horizonte subjetivo de aplicación es extraordinariamente amplio. Mira lógicamente a todos los Estados miembros. Por ello, todas aquellas personas que residen en la Unión, así como aquellas instituciones y compañías que tengan establecimiento en la Unión Europea estarán sujetas a estas disposiciones. Pero abarca más: aún localizándose en otros Estados, se exige el respeto a las disposiciones de este Reglamento cuando los resultados generados por el sistema de inteligencia artificial se utilicen dentro de la Unión Europea (art. 2 letras b y c).

Anótese la singularidad: incluso aunque el sistema de inteligencia artificial no se comercialice ni preste servicios en la Unión Europea. Y ello porque se es consciente de las múltiples relaciones que se traban con corporaciones extranjeras a raíz de las cuales se utilizan de manera lícita información y datos procedentes de la Unión. Si tales compañías extranjeras ofrecen los resultados del sistema, incluso sin comercializarlos, habrán de cumplir las previsiones de este Reglamento. El propósito de esta amplia extensión es evitar que se eludan las obligaciones por la mera circunstancia de estar localizada una empresa fuera de la Unión (considerando 22). El sistema de inteligencia artificial no solo es relevante por su diseño y estructura, es trascendente por el nutriente y, en consecuencia, si hay información y datos que proceden de Europa, han de respetarse las reglas de la Unión.

Dentro de la determinación del ámbito subjetivo de aplicación aparece otra locución diferente al "usuario" y al "responsable del despliegue". A saber, "persona afectada". Tiene tal consideración

cualquier ciudadano que, estando en el territorio de la Unión Europea, quede bajo el influjo de un sistema de inteligencia artificial (art. 1 *g)*). La existencia de afectados será un límite para el funcionamiento de algunos sistemas de inteligencia artificial, además de que se recuerdan los derechos que tienen ante los riesgos de estos sistemas.

Expuesto ese amplio ámbito de aplicación subjetivo, se estructura la regulación clasificando los sistemas de inteligencia artificial en sucesivas categorías por los riesgos que se intuyen. Se parte de aquellos que aparentemente presentan menos peligro -la inexistencia de riesgos no cabe en el ámbito informático-, porque se entiende que las tareas automatizadas se desenvuelven en un marco bastante controlado. En otro rango se alojan aquellos donde hay una interacción que genera particularidades, además de cierta incertidumbre. El siguiente nivel distingue aquellos sistemas que presentan riesgos notables y que, por ello, exigen mayores cautelas y, en último lugar, se señalan aquellos cuyo uso se considera inaceptable por la intromisión en la vida de los ciudadanos o porque, aunque se ignora qué riesgos pueden generar, se barrunta su notable peligro. De ahí que se prohíban.

Conozcamos esas obligaciones cuyo cumplimiento confiemos que minore los riesgos.

II.- HONESTE VIVERE, ALTERUM NON LAEDERE

El uso de una tecnología es desbordante, inunda todos los espacios vitales, se incorpora a las relaciones jurídicas, a los hábitos profesionales, son unos sistemas con infinitas posibilidades y, en consecuencia, tienen infinitos riesgos... Estas y otras consideraciones conducen a que se subrayen desde el primer

momento los básicos deberes y obligaciones para una prudente utilización.

En este sentido, procede un recordatorio básico. Vivimos tiempos en que parecen desvanecerse los perfiles de instituciones jurídicas, se agrietan las columnas que dan solidez al Estado de Derecho, hay ciudadanos que se desentienden de los deberes constitucionales, de esas responsabilidades elementales que se asumen por vivir en sociedades abiertas que se amparan en las garantías del Estado social y democrático. Parece olvidarse que los sistemas democráticos son frágiles y que resulta imprescindible un mínimo comportamiento respetuoso y tolerante con los conciudadanos para que esta sociedad abierta se mantenga. La fuerza de una Constitución reside en la firme determinación de los ciudadanos de defenderla, pues únicamente cuando cada persona se siente obligado en preservar ese marco, se pueden defender la libertad y los derechos fundamentales.

Apunto esta idea que, en principio, resulta elemental, porque parte de la crisis institucional y democrática que presenciamos tiene su causa en la débil educación cívica, en que no se insiste en el comportamiento responsable y en el cumplimiento de deberes con la misma convicción con la que se exigen y defienden los derechos.

Y parto de este recordatorio elemental porque ha de estar muy presente en el uso de las nuevas tecnologías que han explosionado ofreciendo un universo de posibilidades reales, efectivas, unas posibilidades que solo se habían soñado o imaginado por algunos escritores[5].

Ha de hacerse hincapié en que la utilización de estos sistemas que generan tantas ventajas, beneficios, un caudal voluminoso

5 En otras ocasiones he recordado los textos de Homero, Herón de Alejandría... y, partir de ahí podríamos recorrer tantas novelas que incluyen sistemas de automatización y extraños seres (las sucesivas obras basadas en la leyenda de Fausto, Frankestein, el hombre mecánico de Melville, los robots ajedrecistas del siglo XIX, las novelas de Julio Verne, etc.

de facilidades... tiene como presupuesto una actitud responsable, el respeto a unos deberes generales, el cumplimiento de unas obligaciones específicas. Todo derecho tiene su previo o simultáneo deber. Toda ventaja o beneficio procede de una previa responsabilidad. Porque, en caso contrario, habrá, como mínimo, un enriquecimiento injusto.

En estos sistemas de inteligencia artificial ha de exigirse con rigor esa responsabilidad, una exquisita diligencia en su uso. Son sistemas que se extienden, anegan y empapan muchas actuaciones sin que se adviertan la colosal información que ha deglutido, los vínculos que ha establecido, los pasos intermedios que ha realizado, las alternativas que ha descartado... hasta llevar en breve tiempo a un resultado. Un resultado que despertará la admiración al procesar ingente volumen de información en unos segundos. Admiración que la rutina atenuará. Pero la eventualidad de que en ese complejo sistema se hayan producido asociaciones de datos no buscadas, que se hayan desechado otras opciones, que arroje soluciones distintas a las esperadas, en fin, así como que hayan existido intromisiones mediante ciberataques, hace necesaria esa mayor atención y conciencia en su utilización[6].

Por ello, además de seguir las instrucciones específicas de uso, es imprescindible mantener una actitud cabal que se concreta en respetar unos deberes generales, al menos, como condensó Ulpiano en la expresión que he utilizado para este epígrafe: *honeste vivere, alterum non laedere* (Digesto 1.1.10.1).

Este clásico aforismo encuentra dos claras manifestaciones en el Reglamento de inteligencia artificial. Por un lado, una relación de usos prohibidos para evitar daños a otras personas; por otro, el respeto a unos códigos de conducta.

6 Resultan preocupantes las noticias que se suceden sobre ciberataques a estos sistemas que, por ejemplo, facilitan los controles de calidad del abastecimiento de agua a las poblaciones o el tráfico viario. Así, hace unos días se difundió el ataque a determinados sistemas de los vehículos lo que les condujo a ignorar las señales de tráfico.

Como tantos otros instrumentos y herramientas que utilizamos, los sistemas de inteligencia artificial resultan extraordinariamente versátiles y, por ello, lógicamente, no deberán utilizarse como medios de aquellas conductas reprochables, tipificadas como delitos o infracciones administrativas. En este sentido, el Reglamento prevé en su artículo 5 prohibiciones de uso por considerarlos inaceptables en una sociedad civilizada. Enuncia en apartados -sin una acertada sistemática- varios supuestos teniendo en cuenta que esta regulación, lógicamente, no desplaza otras previsiones de usos prohibidos y delimitación de infracciones ("*no afectará a las prohibiciones aplicables cuando una práctica de inteligencia artificial infrinja otra legislación de la Unión*").

En dos grandes grupos cabe clasificar estas prohibiciones. Uno, aquellas que se dirigen a proteger la identidad de cada persona, su privacidad e intimidad. Por ello, se veta la captación y tratamiento de imágenes para ampliar bases de datos de reconocimiento facial, ya provengan de circuitos cerrados de televisión o de un "raspado no selectivo" de otras que circulan por Internet. Igualmente se restringe el análisis de las expresiones con el fin de inferir emociones, creencias o identificar las intenciones de los actos personales (se admite alguna excepción por motivos de seguridad como los sistemas que alertan del cansancio del piloto de una aeronave). Tampoco catalogar a las personas por sus comportamientos y darles puntuaciones, previsión que repele el sistema de crédito social chino[7]; así como, fuera del estricto marco de requisitos en el ámbito judicial, realizar predicciones sobre el riesgo de comisión de delitos.

Un segundo grupo de prohibiciones se dirigen a garantizar la libertad personal, a evitar que los sistemas manipulen el comportamiento al distorsionar la verdad, adulterar o engañar... Esta injerencia de la tecnología en la esencia de la personalidad, que

7 Junto a documentales que se han difundido por los medios de comunicación, realiza una exposición detallada de este sistema Avaro, D. *El Sistema de Crédito Social chino. Vigilancia, paternalismo y autoritarismo,* Ed. Biblos, Buenos Aires, 2023.

podría tanto identificar los procesos mentales como alterarlos, es lo que ha de protegerse mediante un firme reconocimiento de los "neuroderechos" como desde hace tiempo están defendiendo varios científicos y, entre ellos, descato la labor de Valentín Fuster[8].

Procede insistir en las actitudes leales de *pro rei veritate*, de programar con autenticidad la información, que no haya estímulos subliminales. La manipulación es el abono de graves peligros, tanto en las relaciones sociales, por lo que corrompen la sociedad, como en las relaciones privadas o económicas.

El retorcimiento de los conceptos, la falsificación de las ideas llevaría a encerrarse en la "cueva" que denunció **Platón** en su obra *La República*[9]. La manipulación origina la percepción de una imágenes deformadas, inadecuadas, aquellas que en cada momento muestren quienes mueven los hilos del teatro de sombras chinescas en que se convertiría la sociedad. Los ciudadanos quedarían recluidos inconscientemente en un espacio turbio, sin la luz del sentido crítico, y con sus movimientos limitados ante el estrechamiento cada vez más angosto de las opciones que generan los filtros de los sistemas informáticos. Y, lo que no es menos grave, personas con una actitud sumisa, muy distinta a la enfurecida del Segismundo de **Calderón de la Barca**.

El riesgo es grave, tanto en las relaciones privadas (un ejemplo: las empresas de seguros ya han alertado de cómo se están trastocando con rapidez de manera muy sencilla las fotos tras un accidente de tráfico), como en el ámbito social ante las corrientes manipuladoras de la opinión pública. De ahí que la obligación

8 Resultan ilustrativas, y por ello recomendables, las conferencias de Valentín Fuster muchas de las cuales están disponibles a través de Internet. La Unión Europea suscribió en 2023 en León, una Declaración sobre la neurotecnología que debe centrarse en la persona y respetar los derechos humanos. Entre las últimas publicaciones jurídicas destaco la monografía de Beltrán de Heredia, I. *Inteligencia artificial y neuroderechos: la protección del yo inconsciente de la persona*, Ed. Aranzadi, 2023.

9 La República, Libro VII.

de informar con claras marcas o etiquetas cuando se generen o manipulen imágenes, sonidos, audios o vídeos... Se excluyen, lógicamente, los contextos creativos, artísticos, ya sea de sátira, ficción "análogos".

Resulta urgente adoptar medidas eficaces contra estos peligros. No obstante, se ha previsto una moratoria de seis meses de este artículo 5 desde la entrada en vigor del Reglamento y, desde ese momento, podrá denunciarse su uso. Recordemos que quienes informen de la existencia de tales sistemas prohibidos cuentan con la protección del régimen desplegado por la Directiva de protección de los denunciantes (arts. 87 del Reglamento)[10].

Ese plazo es más breve que los dos años que con carácter general se establece como moratoria para la aplicación del Reglamento. Aún así, me parece excesivo. Si se insiste en las actualizaciones periódicas de los sistemas informáticos ante los graves riesgos de ciberataques ¿por qué, entonces, no se pueden actualizar en menos de seis meses esos sistemas tan invasivos y perniciosos? ¿por qué no se puede impedir que no se distribuyan ya los nuevos sistemas que se están ultimando con rapidez para aprovecharse de esa moratoria?

Una escueta consideración, pues ya otro trabajo en esta Revista (firmado por Martín Razquin) profundiza en estos preceptos: la transgresión deberá tener una contundente contestación en el Ordenamiento jurídico.

El régimen sancionador ha de completarse por los Estados miembros pues la regulación en este Reglamento es limitada: señala las sanciones cuando quien incurre en esas reprochables conductas es un "operador" y tienen esa consideración a sus efectos: el "proveedor, fabricante de productos, implantador, representante autorizado, importador o distribuidor" (art. 3.8),

10 Directiva 2019/1937, de 23 de octubre que, como sabemos, se ha incorporado al Ordenamiento español mediante la Ley 2/2023, de 20 de febrero.

así como también a los responsables del despliegue que incumplen determinadas obligaciones (art. 99). Pero eso no impide que el Ordenamiento jurídico español precise tipos delictivos o infracciones administrativas graves por conculcar las prohibiciones si es que tales conductas no quedan ya incluidas en los tipos existentes como la suplantación de personalidad, las injurias y calumnias, los delitos contra el honor u otros.

El Reglamento de inteligencia artificial se ocupa de precisar las multas que podrá imponer el Supervisor europeo de protección de datos a las instituciones y organismos europeos (art. 100). Una regulación relevante porque puede abrir la puerta a extender la imposición de multas a Administraciones y organismos públicos ante graves incumplimientos. Algo que, como es conocido, está excluido en muchos sectores[11].

Junto a tales prohibiciones hay que insistir en otra idea.

La conciencia de los riesgos, el avance hacia lo desconocido, la convicción de mantener las bases de la civilización ha generado numerosas llamadas de atención recordando unos compromisos éticos básicos. Porque hay que honrar la dignidad humana, defender la libertad individual, proteger los derechos fundamentales y de las libertades públicas. Sólo así la musa de la confianza acompañará el uso de los sistemas de inteligencia artificial.

Entre otros muchos documentos propiciados por las instituciones europeas, el Grupo de expertos para asesorar la estrategia sobre inteligencia artificial presentó unas directrices éticas como base insustituible[12]. Concretaron principios generales con el fin de garantizar el diseño y el uso de estos sistemas. Entre otros:

11 Vid. art. 40 del Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información o art. 77 de la Ley orgánica de protección de datos. Precisiones oportunas sobre este singular régimen jurídico realiza Domínguez Álvarez, J.L., *Iusdata y Administración pública,* Civitas, 2023.

12 Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, Directrices éticas para una IA fiable, Oficina de Publicaciones, 2019, disponible en https://data.europa.eu/doi/10.2759/14078.

el respeto a la autonomía humana, a la equidad y no discriminación, su solidez técnica y seguridad, su transparencia, garantizar el bienestar social y ambiental, así como prevenir el daño.

Tales principios hay que enmarcarlos en su específico contexto ante la complejidad y sofisticación de algunos sistemas[13]. Así, la transparencia se reconduce a la posibilidad de seguir el trazado de los procesos y de contar con una explicación adecuada. Pero sabemos que hay sistemas con una especie de "caja negra" integrada por modelos de aprendizaje interconectados, por miles de millones de instrucciones que dan resultados sin ser posible advertir el por qué, el cómo llegaron a esa conclusión. Se ha difundido el siguiente ejemplo: el modelo de "chat Gpt4" incluye en su caja negra más de ciento setenta y cinco mil billones de parámetros. Quizá en cifras se aprecie mejor la profunda inmensidad de los ceros: 175.000.000.000.000.000.

Es probable -al menos deseable- que el propio desarrollo tecnológico permita ofrecer aclaraciones más asequibles y sencillas de algunos parámetros. No obstante, habrá de incrementarse el esfuerzo de los programadores con vistas a facilitar esa información, la trazabilidad de los procesos, el seguimiento de las huellas porque también resulta necesario evaluar y realizar auditorías periódicas.

El Parlamento europeo insistió igualmente en 2020 en esa conciencia ética en el diseño de los sistemas de inteligencia artificial: han de respetar la dignidad humana, la autonomía individual, la seguridad, los derechos fundamentales reconocidos en la Carta europea[14]. Del mismo modo que se insistió en la preocupación

13 Entre otros comentarios, me remito al trabajo de Oliver, N *Inteligencia artificial, naturalmente*, ONTSI 2020, en el que con gran claridad resume la distinción que ha generalizado Jenna Burrell, quien diferencia: a) una opacidad derivada de la propiedad intelectual, b) otra porque sólo los entendidos conocen el lenguaje y lo entiendan y c) el aprendizaje profundo de la máquina que sólo los muy versados pueden interpretarlo

14 Resolución del Parlamento Europeo de 20 de octubre de 2020, de recomendaciones a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL), (2021/C 404/04).

por el impacto ambiental de la tecnología. En muchos de sus apartados se insiste una y otra vez la necesidad de mitigar y remediar el impacto general sobre "los recursos naturales, el consumo de energía, la producción de residuos, la huella de carbono, la emergencia climática y la degradación del medio ambiente". Pues es ingente el consumo de energía de estos sistemas ante las exigencias de la supercomputación[15]. Además de sus altos costes económicos[16].

Pero la exigencia ética ha de ser atendida en primer lugar. Y así se reitera en distintos foros internacionales[17].

Un compromiso ético que no se circunscribe a la estructura del sistema de inteligencia artificial por la labor de quienes lo diseñan. Ha de presidir el comportamiento de los usuarios. Recordemos que algunos de estos sistemas, con su mera puesta en marcha, coleccionan datos del usuario y, sobre todo, intensifican su "entrenamiento", de tal modo que pueden generar nuevas vinculaciones y otros resultados. De ahí la necesidad de que el comportamiento del usuario haya de ser correcto con el fin de evitar distorsiones en ese entrenamiento.

15 Algunos medios de comunicación han difundido el resumen de un artículo publicado en febrero de 2024 en la revista Nature sobre los impactos ambientales de estos sistemas de inteligencia artificial, lo que ha generado la presentación de un proyecto de ley en el Senado norteamericano para investigar y medir tales impactos. También en España, se han divulgado informaciones sobre el coste energético y la huella de CO2. En resumen, el entrenamiento de más de 200 mil millones de parámetros en los sistemas de inteligencia artificial generan 752 toneladas de CO2. Y hay sistemas donde los parámetros se han multiplicado (Megatron-Turing tiene 530 mil millones, PaLM tiene 540 mil millones de parámetros, y el recientemente aparecido GPT-4 aumenta hasta 170 billones de parámetros). Para advertir la densidad de esta cifra sirva la referencia de que un vuelo de ida entre Madrid a Múnich que genera media tonelada de CO2. En consecuencia, el entrenamiento equivale a miles y miles de vuelos.

16 Aspecto que ha sido considerado por el Artificial Intelligence Index Report 2024 del Instituto de la Universidad de Stanford HAI Human-centered Artificial Intelligence.

17 Sirva el mero recordatorio el Acuerdo del G7 de código de conducta bautizado como "Proceso de inteligencia artificial de Hiroshima, de 29 de octubre de 2023); las conclusiones de la Cumbre internacional sobre inteligencia artificial celebrada en Londres en noviembre de 2023; o de la Resolución de la Asamblea General de las Naciones Unidas reclamando el compromiso de respeto a los derechos humanos en el uso de los sistemas de inteligencia artificial (Resolución 21 de marzo de 2024).

En consecuencia ha de avanzarse en una especie de alfabetización con relación a estos sistemas de inteligencia artificial. Alfabetización que incluye el glosario del Reglamento para referirse a unos conocimientos básicos que, por supuesto, no han de llegar a "leer y escribir el sistema", sino a "*tomar conciencia de las oportunidades y los riesgos que plantea la inteligencia artificial, así como de los perjuicios que puede causar*" (art. 3 apartado 56).

Y, de ahí la importancia de la concreción y difusión de "códigos de conducta". Se confía en la difusión de pautas que vayan incorporándose como hábitos voluntarios (considerando 165).

Los proveedores de los sistemas son quienes están en mejor posición para su redacción, pero también podrán elaborarse por los responsables del despliegue que advierten cómo funcionan los sistemas en el seno de una organización y las incidencias que suscita su uso. Del mismo modo que pueden impulsarse tales pautas por investigadores o asociaciones civiles. En los considerandos se citan a las organizaciones de consumidores o a los sindicatos, pero no hay que ignorar que existen institutos científicos especializados, entre otros, el *Future of Life Institute* del MIT[18], el *Future of Humanity Institute* de Oxford[19], y, de manera más intensa, el *Alan Turing Institute*[20] que han difundido relevantes estudios sobre cómo deben los sistemas de inteligencia artificial atender a los valores y principios aceptados como éticos en las sociedades civilizadas.

Junto a tales iniciativas privadas, el Reglamento destaca el papel que pueden desempeñar la Oficina europea de inteligencia artificial, así como de las autoridades de los Estados miembros con el fin de difundir las mejores prácticas y soluciones técnicas (art. 95). Es más, se prevé que esa Oficina europea precise tales códigos de

18 https://futureoflife.org/

19 https://www.fhi.ox.ac.uk/

20 https://www.turing.ac.uk/

buenas prácticas en el plazo máximo de nueve meses a partir de la entrada en vigor del Reglamento, el 2 de mayo de 2025 (art. 56.9).

Pautas éticas y códigos de conducta resultan imprescindibles en el uso de los sistemas de inteligencia artificial "que generan contenidos", esto es, aquellos que no se han diseñado para una finalidad específica, sino como asistentes "sabelotodo". Estos sistemas son objeto de una atención especial en los artículos 51 y siguientes del Reglamento. Requieren mayor supervisión por los proveedores y, como veremos, obligaciones de los responsables en las instituciones y empresas que los utilizan. Pero también de los usuarios porque con ellos se interactúa. Quien utilice estos sistemas no debe incorporar noticias falsas ni erróneas ni realizar otro tipo de "usos indebidos", cosa que el Reglamento incluso considera "razonablemente previsible".

Recordemos que estos sistemas devoran toda la información y la relacionan siguiendo una lógica interna de predicción, considerando todas las circunstancias, valorando todas las alternativas y de ahí que la introducción de yerros puede dar lugar a sofismas necios, artificios temerarios, dislates mayúsculos... lo que llevará a perder fiabilidad y seguridad. Y, en este caso, el usuario será corresponsable. Un comportamiento honesto, siguiendo las instrucciones dadas por el proveedor, es el que debe presidir el uso de esos sistemas de capacidad espectacular, mientras se incorporan en su diseño pautas de corrección de tales disparates a través de los mecanismos de gestión de riesgos (art. 9) o se corrigen y evitan por la supervisión humana (art. 14).

III.- OBLIGACIONES DE LOS RESPONSABLES DEL DESPLIEGUE

Hemos de detenernos ya en las obligaciones específicas impuestas a quienes sean responsable del despliegue de un sistema de inteligencia artificial en una institución, profesión o negocio.

III.1.- ADVERTIR DEL ARTIFICIO

La primera precaución ante la extensión de estos sistemas es que los ciudadanos sean conscientes de que están relacionándose con un asistente artificial o que están bajo su radio de acción. El artículo 50 impone varias obligaciones, no solo a los proveedores para que en el diseño existan marcas o etiquetas específicas, sino también a los responsables del despliegue, quienes nos interesan en estos momentos[21].

Así, los sistemas que facilitan una relación recíproca, una directa interactuación con el fin de denunciar delitos u otras infracciones, han de dar noticia previa, salvo, dispone el Reglamento, que resulte "evidente" que se trata de un mecanismo elaborado, artificioso. Tal "evidencia" queda delimitada por el comportamiento de una persona "atenta y perspicaz", "razonablemente informada", consideraciones estas que pueden resultar indubitadas en ocasiones, pues se muestran dibujos animados especialmente significativos pero que, en otras ocasiones, aquellas que se han diseñado para facilitar la confianza de los usuarios, pueden generar una falsa percepción de que ciertamente el asistente es una persona con alguna responsabilidad o autoridad.

Quienes utilicen sistemas para generar textos, imágenes o vídeos han de avisar de tal circunstancia para evitar que los ciudadanos incurran en el error de considerarlos reales y auténticos. Si esa composición artificial tiene una finalidad artística, creativa, será suficiente en estos casos con hacer pública la existencia de elementos producidos por tales sistemas al inicio de la obra.

21 Entre otros, resultan ilustrativos los estudios de Miranzo Díaz, J. *Inteligencia artificial y Derecho Administrativo*, ICA-Tecnos, 2023; Boix A. y Soriano A., "Transparencia y control de uso de la inteligencia artificial por las Administraciones públicas", en la obra coordinada por Balaguer Callejón F. y Cotino Hueso, L. *Derecho público de la inteligencia artificial*, Fundación Giménez Abad, Zaragoza, 2023; Cotino, L, "Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público" y Martín Delgado, I., "La aplicación del principio de transparencia a la actividad administrativa algorítmica", ambos en obra colectiva Gamero, E., *Inteligencia artificial …*, cit. págs. 260 y ss., y págs. 132 y ss., respectivamente, sobre la transparencia y la corrección de discriminaciones y sesgos por las Administraciones públicas, a los que me remito.

Del mismo modo, cuando se utilicen sistemas de inteligencia artificial para generar textos e informar de asuntos de "interés público" ha de difundirse tal circunstancia. Quedan fuera de esta obligación aquellos casos en que ha existido una supervisión humana, un control editorial o esté prevista ya la responsabilidad por la publicación de ese contenido. Como, con carácter general, quedan excluidas de esta obligación de información el uso de sistemas que hayan sido autorizados legalmente para "detectar, prevenir, investigar o enjuiciar delitos".

Ha de advertirse en aquellas situaciones en que se admite alguna identificación biométrica. Por ejemplo, caso de ciertos controles de entrada como el sistema de acceso al espacio Schengen: un programa que comprueba los datos de identificación de los pasaportes, con otros faciales o huellas dactilares. Igualmente en consultas médicas donde ese análisis biométrico puede resultar determinante para una adecuada exploración. Como también si el tratamiento médico atiende al reconocimiento de emociones. En estos casos, ha de comunicarse del funcionamiento del sistema a las personas afectadas además, lógicamente, ha de garantizarse el escrupuloso respeto a la normativa de protección de datos personales pues estamos en ámbito de materia sensible.

Se exige, además, que se dé de manera clara y nítida en el primer momento, en la "primera interacción o exposición".

La Oficina europea deberá precisar buenas prácticas de "etiquetado y detección" que garanticen la rápida percepción por el usuario, que se adviertan con claridad que ha intervenido un sistema de inteligencia artificial. Es imprescindible que los ciudadanos se percaten desde el primer momento, por ello se ha habilitado a la Comisión Europea para que apruebe códigos de buenas prácticas como Derecho derivado, remisiones normativas denominadas "actos de ejecución" en la terminología del Tratado y que están sujetos a un control del Parlamento y el Consejo que pueden, en cualquier momento, requerir información,

así como la previa consulta a los "comités" integrados por representantes de los Estados miembros[22].

III.2.- CONJURAR LOS PELIGROS

Algunos sistemas de inteligencia artificial inciden en ámbitos sensibles de tal modo que, a pesar de las significativas ventajas de su uso, persiste la preocupación ante los riesgos que genera. Procede prestar mayor atención en su utilización pues el sistema opera, podríamos decir, "por su cuenta", pero no "por su cuenta y riesgo", en el sentido de asumir su responsabilidad. Esta recae en la institución que utiliza el sistema cuyos efectos, en algunos casos, pueden ser imprevisibles. De ahí que el Reglamento imponga obligaciones específicas que minoren los riesgos y, con ello, la responsabilidad.

Las obligaciones se concretan en actuaciones de prevención y supervisión, nuevas "cargas" como reconoció la Comisión Europea en la propuesta normativa donde apuntó, incluso, una aproximación de los posibles costes.

Es cierto que desde hace años la legislación europea y española están insistiendo en aligerar las cargas administrativas, especialmente de los empresarios, de tal modo que "*las Administraciones Públicas que en el ejercicio de sus respectivas competencias creen nuevas cargas administrativas para las empresas eliminarán al menos una carga existente de coste equivalente*" y que las memorias de impacto normativo han de valorar las nuevas cargas impuestas[23].

22 Vid. Reglamento 182/2011, de 16 de febrero, que establece las normas y los principios generales relativos al control por parte de los Estados miembros del ejercicio de competencias de ejecución de la Comisión Europea.

23 Art. 37 de la Ley 14/2013, de 27 de septiembre, de apoyo a los emprendedores y su internacionalización y art. 2 del Decreto 931/2017, de 27 de octubre, sobre la memoria de impacto normativo.

Sin embargo, en este ámbito donde se requiere un especial cuidado, estas obligaciones se consideran razonables y proporcionadas. La Comisión Europea señaló que no se han encontrado otras medidas que incidan menos en el comportamiento de estos responsables.

Para paliar en alguna medida su coste, el Reglamento anuncia el apoyo, especialmente a las pequeñas y medianas empresas por parte de la Unión Europea y de los Estados miembros. Se dotarán cuantiosos fondos europeos con este fin, además de la asistencia que llevarán a cabo la nueva Oficina europea de inteligencia artificial y las autoridades nacionales [24].

Presupuesto indispensable para el cumplimiento de estas obligaciones es que los sistemas estén diseñados para que sean "interpretados" por estos responsables y que se les traslade suficiente información sobre su funcionamiento con el fin de advertir los usos previstos, aquellos que están excluidos, las ventajas y limitaciones, las pautas o cambios predeterminados... Tales aspectos se relacionan a lo largo del artículo 13 del Reglamento, donde se establece que dicha información ha de ser "concisa, completa, correcta y clara, que sea pertinente, accesible y comprensible". Los proveedores deberán hacer un esfuerzo significativo para conseguir esa accesible comprensión. Una cauta previsión es que se ilustre con ejemplos. Ha de evitarse que las expresiones técnicas sean un obstáculo para la adecuada interpretación.

Estas obligaciones más específicas se exigirán en todos aquellos usos de los sistemas calificados de "alto riesgo". ¿Cuáles tienen tal calificación? Por un lado, aquellos que afecten a "la salud, la seguridad y los derechos fundamentales", como reiteran varios

24 En España, tanto el organismo RED.ES como INCIBE tienen una atención especial para las pequeñas y medianas empresas. Además, se acaba de aprobar una Estrategia de inteligencia artificial en la que se anuncian nuevas ayudas para las empresas (se cifran en 700 millones de euros), además de otras dirigidas al centro de supercomputación MareNostrum, el mayor centro de supercomputación de España, alojado en Barcelona.

preceptos. Así, aquellos sistemas que se integren dentro de los elementos de seguridad de determinados productos y estén sometido a una evaluación para ser comercializados o prestados de conformidad con la normativa europea mencionada en el Anexo I, que relaciona un largo listado que atiende a juguetes infantiles, ascensores, vehículos, diversa maquinaria...

Por otro lado, aquellos que se utilizan en ámbitos específicos a los que alude el Anexo III pero con una importante salvedad: quedan excluidos de manera explícita aquellos sistemas que se utilicen para actividades auxiliares o preparatorias, que no influyan en las decisiones del sistemas o que se utilicen con posterioridad a las actividades humanas con el fin de comprobar sus resultados y mejorarlas. Porque no es lo mismo, por ejemplo, utilizar sistemas para localizar bibliografía o jurisprudencia que para redactar resoluciones judiciales.

¿Cuáles son esos ámbitos a los que alude el citado Anexo III? Algunos sistemas que utilizan datos biométricos ya que es necesario prevenir los riesgos de que se difundan tales datos. Por ello, se distinguen aquellas situaciones en que su captación y uso están radicalmente prohibidos, caso de pretender clasificar por categorías a las personas, facilitar la identificación remota, analizar emociones... de aquellas otras permitidas como la identificación de un sospechoso o en el control interno de acceso a determinadas instalaciones.

Son también de alto riesgo los sistemas de inteligencia artificial que incorporan medidas de seguridad para la protección de infraestructuras críticas, esto es, elementos indispensables para el adecuado funcionamiento de servicios esenciales como el abastecimiento de agua, el suministro eléctrico u otros a los que atiende la Directiva 2022/2557, de 16 de diciembre[25].

25 Esta Directiva de protección de las entidades críticas ha dado un gran impulso a la armonización de normas mínimas de ciberseguridad en ámbitos esenciales y estratégicos. Explico las razones que motivaron su adopción, modificando la anterior perspectiva de la Unión en mi monografía *Metamorfosis del Estado. Maremoto digital y ciberseguridad*, Marcial Pons, 2021, págs.

También se consideran de alto riesgo los que se utilizan en el sistema educativo y de formación con el fin de valorar las solicitudes de admisión, la calificación de las pruebas y exámenes realizados, también la vigilancia para evitar comportamientos prohibidos por parte de los estudiantes. En el ámbito de las relaciones laborales, aquellos que analizan las solicitudes de empleo, los que distribuyen tareas teniendo en cuenta los comportamientos individuales, los que evalúan el rendimiento en el trabajo... Igualmente, los sistemas dirigidos a analizar las solicitudes de servicios sociales, así como aquellos otros que supervisan las prestaciones con el fin de revisarlas o suprimirlas; los que valoran las solvencia financiera o una calificación crediticia; los utilizados para precisar las condiciones de los seguros sanitarios o de vida; aquellos que ordenan la preferencia de las llamadas de emergencia o el triaje de pacientes para su atención sanitaria; en fin, aquellos utilizados para valorar el riesgo de comisión de un delito, así como para verificar la veracidad de las declaraciones...

Y reitero: quedan fuera los sistemas que contribuyen a realizar actividades meramente auxiliares o preparatorias, los que no influyen en las decisiones del sistemas o que se utilicen con posterioridad a las intervenciones humanas con el fin de comprobar sus resultados y mejorarlas, caso, por ejemplo, de la comprobación de las medidas adoptadas para proteger una infraestructura crítica.

La necesidad de mantener al día este marco jurídico ante la imparable aceleración del desarrollo de estos sistemas, así como también, en términos generales, de las técnicas que pueden incorporar medidas de seguridad, ha generado que se habilite de manera explícita a la Comisión Europea para actualizar este Anexo III (arts. 7 y 97 del Reglamento).

Lógicamente se precisan los presupuestos que ha de tener en cuenta la Comisión, tanto para retirar esa alta precaución de riesgo de algún sistema, como para incluir otro del que se advierten sus peligros. La incorporación de ajustes en el diseño puede conducir a que se desvanezcan los temores considerables para

la inicial calificación siempre que satisfagan las reglas generales de seguridad del Derecho europeo. Y, a la inversa, la difusión de nuevos sistemas de inteligencia artificial, que puedan utilizarse en esos ámbitos sensibles y que presenten riesgos similares o más altos que los sistemas ya clasificados, originará su incorporación en esa categoría de alto riesgo. Para ello se exige que la Comisión realice una valoración detallada de diversos elementos como la finalidad del sistema, datos de los que se nutre y las probabilidades de generar tanto beneficios como perjuicios desproporcionados (art. 7).

Hay que ser conscientes de la rápida extensión y generalización de estos sistemas ante las ventajas de su utilización por todo tipo de organismos públicos, así como por las empresas, incluso pequeñas. ¿No conviene que los colegios, institutos y universidades utilicen sistemas para garantizar el comportamiento honesto en los exámenes? ¿han de descartarse las ventajas de las exploraciones médicas a distancia o la completa información que ofrecen programas sanitarios a la hora de graduar las urgencias? Los sistemas que ayudan a valorar las solicitudes de empleo, el análisis de los curricula, el rendimiento en el trabajo, la productividad de los funcionarios públicos, serán cada vez más frecuentes. Como aquellos que facilitan la supervisión del correcto uso de las ayudas y subvenciones o de los servicios sociales.

Señalados estos presupuestos, detengámonos ya en las concretas obligaciones que deberán cumplir todas aquellas instituciones o responsables del despliegue que incorporen sistemas de alto riesgo.

III.2. A.- De manera previa a su instalación

- Análisis de su incidencia en los derechos fundamentales.- El Reglamento exige evaluar el posible impacto sobre los derechos fundamentales de quienes se vean afectados por el sistema (art. 27). Esta obligación no se impone con

carácter general. Solo se dirige a determinadas instituciones. En concreto: todos los organismos públicos, las empresas privadas que prestan servicios públicos (estupendo recordatorio de una categoría clásica), así como quienes, ya tengan naturaleza pública o privada, evalúen las circunstancias personales en dos ámbitos muy sensibles, a saber, la prestación de servicios esenciales de asistencia pública, incluida la sanitaria, y la solvencia patrimonial o calificación crediticia, con la excepción de que se persiga el fraude financiero.

No será exigible tal análisis cuando la autoridad de vigilancia competente haya acordado, ante situaciones excepcionales, dispensar al proveedor del sistema de tal evaluación (art. 46.1).

Quedan igualmente excluidos todos aquellos organismos y empresas que gestionan un servicio estratégico y cuentan con infraestructuras críticas. Recordemos que, tras la nueva regulación de protección de entidades críticas, la Unión Europea ha ampliado los sectores considerados estratégicos precisando una evaluación rigurosa y detallada, un concienzudo análisis de riesgos... y, de ahí, su preferencia, que desplaza la atención a este precepto[26].

Junto a esta lógica exclusión, sin embargo no me parece tan razonable que no se exija la realización de una evaluación previa sobre el impacto en los derechos fundamentales al resto de "responsables del despliegue", esto es, a otras personas o empresarias ya que nos encontramos con sistemas que se han calificado de alto riesgo. Si ello se ha debido a no querer incrementar las cargas de los empresarios con otra obligación, me parece poco acertada la decisión.

26 Me refiero a la Directiva 2022/2557, de 14 de diciembre. Sobre su extensión, así como la divergente aplicación del régimen europeo previo que ha motivado la reforma, me remito a las consideración que realizo en Metamorfosis del Estado..., cit.

Los derechos fundamentales deben ser respetados por todos los ciudadanos y empresarios, y asumir la utilización de un sistema de inteligencia artificial que eventualmente puede lesionar algún derecho fundamental es causa suficiente para una actitud más cuidadosa. Además, hay que tener en cuenta que esta carga tiene un peso, podríamos decir, "liviano". Por un lado, la obligación solo se exige en el "primer uso del sistema". Pero, si con anterioridad ya se han realizado por otros organismos o, lo que es más probable, ha realizado minuciosas evaluaciones de impacto el proveedor, así como si ya se han realizado evaluaciones de impacto en el ámbito de la protección de datos, se entiende que queda satisfecha esta obligación. Por otro lado, la Oficina europea de inteligencia artificial tiene el encargo de elaborar un modelo de cuestionario que sea sencillo rellenar "mediante una herramienta automatizada", lo que facilitará tal evaluación.

El Reglamento precisa el contenido mínimo al que deben atender tales evaluaciones: a) procedimientos en los que se utilizarán; b) durante cuanto tiempo y frecuencia; c) qué personas pueden verse afectadas por su utilización, ya sean personas individuales o grupos de personas; d) qué tipo de riesgos les pueden perjudicar; e) qué medidas de supervisión humana se aplican; y f) qué medidas se adoptarán en caso de producirse perjuicios, incluidos los medios de reclamación. Aspectos que pueden describirse en asequibles formularios de ayuda.

- Información previa a los representantes de los trabajadores.- Previsión general en la legislación laboral es la información que ha de darse a los representantes de los trabajadores de manera previa[27]. El Reglamento obliga a

27 Sirva el recordatorio de la Directiva 2002/14, de 11 de marzo, que establece el marco general de información y consulta a los trabajadores, así como al artículo 64 del Estatuto de los trabajadores.

los proveedores a facilitar información con el fin de que se entienda el funcionamiento del sistema, un diseño que permita cierto conocimiento, unas mínimas exigencias de transparencia (art. 13). Por tanto, deberá ponerse a disposición de los representantes de los trabajadores tales explicaciones, así como responderse a sus dudas y, por su trascendencia, debido a los altos riesgos del sistema, debería generar el rápido traslado de esta información a todos los trabajadores.

Del mismo modo que debería facilitarse la información inversa como empieza a preocupar a las empresas. Esto es, qué sistemas de inteligencia artificial están empezando a utilizar los trabajadores por su cuenta y riesgo, pues conocen por su uso diario y doméstico algunas de sus ventajas.

- Registro previo.- Otra obligación a la que se sujeta solo a determinados "responsables del despliegue" es el registro en la base de datos que ha configurado la Unión Europea (arts. 26.8 y 49 del Reglamento). Afecta a las autoridades y organismos públicos. Quedan fuera las compañías privadas u otros profesionales que utilicen estos sistemas.

  La Comisión Europea, con la colaboración de los Estados miembros, creará la base de datos con el fin de ofrecer información accesible a cualquier ciudadano sobre los sistemas de alto riesgo que se utilicen en toda la Unión Europea: un resumen sencillo sobre su finalidad, los datos que colecciona y su funcionamiento. Servirá para el adecuado ejercicio de las funciones encomendadas a la Comisión y otras autoridades con competencias en este ámbito porque incorporará datos del proveedor y del sistema (art. 71 del Reglamento). De tal modo que, cuando estos concretos responsables, estas instituciones públicas, comprueban que el sistema no está debidamente registrado, se le impide su utilización (art. 26.8). Y aquí se abre un interrogante:

¿por qué no se impide igualmente la utilización a empresarios y profesionales?

Sabemos que los proveedores de los sistemas de alto riesgo han de registrarse en esa base de datos europea antes de ponerlo a disposición o comercializarlo (art. 6.4). En consecuencia, ¿por qué pueden utilizarlo empresarios y profesionales? o, incluso, el sector público empresarial cuando se impide a los organismos públicos. Dualidad que, a mi entender, no está justificada y generará problemas.

La información que ha de facilitarse para tal inscripción por los responsables del despliegue se recoge en el Anexo VIII sección C del Reglamento.

Quedan fuera de esta base de datos europea los sistemas de inteligencia artificial que se utilicen para proteger infraestructuras críticas. Las instituciones europeas carecen de información sobre qué entidades estratégicas tienen infraestructuras críticas, pues son datos que afectan a la seguridad de cada Estado miembro. De ahí que, desde la primera regulación europea del régimen jurídico para su protección especial, se excluyó informar a la Comisión sobre tales elementos cruciales. Recordemos que, a pesar de las políticas europeas de seguridad, del principio de solidaridad y ayuda mutua, también el Tratado admite que "*ningún Estado miembro estará obligado a facilitar información cuya divulgación considere contraria a los intereses esenciales de su seguridad*" (art. 346 TFUE). Por ello, en estos casos, el registro es nacional. En España, ejercen estas competencias el Comité de protección de las infraestructuras críticas.

III.2.B.- Adopción de medidas técnicas y organizativas

Incorporado un sistema de inteligencia artificial ha de garantizarse que se siguen las instrucciones de uso. Cada institución,

empresa o profesional, atendiendo a su propia estructura y a la complejidad del sistema, establecerá las medidas organizativas y técnicas que considere. El Reglamento alude a la propia "libertad", a la particular consideración de cada institución para "organizar sus propios recursos y actividades" porque tales medidas dependen de elementos internos y particulares (art. 26.3). Criterio éste distinto al que se ha seguido en otras disposiciones europeas, por ejemplo, en la normativa sobre seguridad de las redes y los sistemas de información, donde se exige la designación de un responsable de ciberseguridad que supervise las medidas adoptadas o notifique los incidentes. Este Reglamento de inteligencia artificial reconoce la autonomía para la organización de las atribuciones y responsabilidades.

Algunas organizaciones o empresas están creando ya un nuevo departamento, una unidad administrativa, un comité e, incluso, un director que asume la responsabilidad de la supervisión de estos sistemas. Junto a los acrónimos ingleses que salpican desde hace años los organigramas empresariales para hacer referencia al consejero o director ejecutivo (CEO), al responsable de la oficina de supervisión de cumplimiento normativo (CCO), al director de ciberseguridad (CISO), aparece ahora también el director de inteligencia artificial (CIAO, *chief intelligente artificial officer*).

Del mismo modo, se podrá establecer una lista de actividades previas antes del uso, como otros hábitos simultáneos a su utilización y medidas de control posterior con el fin de que todos aquellos funcionarios o todos aquellos trabajadores de la empresa que utilicen dispositivos con estos sistemas tengan un conocimiento suficiente de las mismas.

Además, al ser tan amplio el universo de aplicaciones que ofrece la multitud de sistemas de inteligencia artificial, será cada institución la que determine quién haya de manejarlos. Así, en un quirófano únicamente determinados especialistas, con una cualificación relevante, serán quienes puedan ser asistidos por sistemas quirúrgicos o los que atiendan a la modificación de las

dosis químicas; mientras que, por ejemplo, en los procedimientos de supervisión de las ayudas públicas u otros programas que ahorran la realización de un sin número de tareas repetitivas, todos aquellos funcionarios previamente aleccionados lo utilizarán y pronto lo incorporarán con soltura a sus hábitos.

Tales usuarios deberán seguir de manera rigurosa las instrucciones recibidas y para ello se exige que cuenten con unos conocimientos adecuados, una formación y competencia suficiente. Obligación en la que insiste el artículo 4 del Reglamento al señalar que "en la medida de lo posible" todas aquellas personas que se encarguen del funcionamiento y de la utilización de sistemas de inteligencia artificial tengan suficiente formación, conocimientos técnicos y experiencia.

Dentro de la institución se podrán adoptar pautas de utilización, códigos de conducta, además de reiterar aquellos difundidos por los proveedores de los sistemas (art. 95.3 del Reglamento). Con relación a estos códigos que inciden en sistemas de alto riesgo, la Comisión Europea ha de evaluarlos de manera periódica (cada cuatro años) con el propósito de considerar su extensión a otros sistemas que no sean de alto riesgo (art. 112.7).

Impone el Reglamento con carácter general, como medida técnica específica, la conservación de aquellos archivos que el propio sistema de inteligencia artificial genera de manera automática, aquellos en los que quedan registradas las sucesivas operaciones y que permitirán interpretar, en su caso, la nítida huella temporal de la actividad realizada. Porque estos sistemas de alto riesgo han de permitir su seguimiento a lo "largo de todo el ciclo de vida", además de otras capacidades tan relevantes como: detectar modificaciones en sus instrucciones internas o facilitar la vigilancia durante su funcionamiento (artículo 12 del Reglamento).

En principio, salvo otra previsión específica, tal conservación ha de preservarse durante seis meses (apartado seis del art. 26 del Reglamento).

Como singularidad, se reitera la conservación de tales archivos por las entidades financieras. No obstante, sabemos que existe abundante normativa sectorial que exige la conservación de documentación: en el ámbito tributario, en el ámbito contable, los registros de órdenes de operaciones bursátiles, también para prevenir el blanqueo de capitales o facilitar la lucha contra el terrorismo, determinados archivos policiales, etc.

En resumen, junto a la *lex specialis* que despliega importantes obligaciones que inciden en la organización y en las actuaciones técnicas, este Reglamento insiste en la adopción de medidas específicas para garantizar el correcto funcionamiento de los sistemas. Unas medidas que se completan con el deber de vigilancia en el que hemos de detenernos.

III.2.C.- Vigilancia y supervisión humana

El Reglamento insiste en mantener una constante vigilancia con el fin de que los sistemas se utilicen de manera adecuada, que se sigan de manera rigurosa las instrucciones, que se introduzcan datos correctos... Datos que, se señala de manera explícita, han de ser "pertinentes" y "representativos" (art. 26.4).

Los sistemas tragan con voracidad la información, la retienen, trituran, desmenuzan, consideran el amplio abanico de variables para, gracias a la potencia de la computación, ofrecer en poco tiempo resultados. El incremento de la capacidad de "supercomputación" es una de las causas del desarrollo de estos sistemas de inteligencia artificial. Pero que los frutos sean útiles dependerá, no sólo de cómo se ha configurado el sistema, también de los elementos introducidos. Informaciones erróneas, anotaciones falsas, apuntes inexactos...generarán otro desenlace distinto. En algunos ámbitos, la existencia de una insignificante variación en los datos iniciales incide de tal manera que origina propuestas drásticamente diferentes, imprevistas. Es lo que se estudia por los matemáticos y físicos bajo el nombre de

"teoría del caos", que ha de entenderse en su sentido científico y no en su acepción de desorden mayúsculo.

De ahí otra trascendental obligación: que los datos que se incorporen, siempre que se "ejerza control" sobre los mismos sean, por un lado, pertinentes y, por otro, "suficientemente representativos" (art. 26.4 del Reglamento). La obligación surge cuando existe algún control sobre los datos. Cuando estos provienen de hechos indubitados, de solicitudes presentadas, de otras circunstancias o informaciones externas sobre las que no se puede incidir la obligación queda matizada. En tales casos, habrá que actuar siguiendo meramente las instrucciones y persiguiendo la finalidad buscada.

Cuando exista alguna actividad de expurgo previo, los datos han de ser pertinentes y representativos. Pertinentes, porque han de ser ciertos y contener la información que conviene analizar para el adecuado cumplimiento de las funciones; representativos, porque se exige que sean significativos y adecuados, descartando aquellos atípicos, extraños, irregulares que pueden distorsionar la perspectiva del resultado, así como el sucesivo aprendizaje del sistema.

Como en tantas otras ocasiones, dependerá de las concretas funciones de la organización, de la complejidad del sistema y su finalidad determinar el alcance de esta obligación. En ocasiones, funcionarios o trabajadores incorporan datos fijos, únicos, que no generan especiales problemas. Sin embargo, en otros ámbitos, desde la construcción de grandes obras de ingeniería al análisis minucioso de reacciones a sustancias químicas, habrá de ponderarse cuáles son los datos más pertinentes y representativos.

Con relación a los sistemas de inteligencia artificial "generales", aquellos que no tienen un propósito específico, conviene insistir en la incorporación de datos representativos para evitar que el sistema se emborrache y revele, como explican los técnicos, "alucinaciones", errores derivados de los múltiples procesos de

análisis de probabilidades y predicciones con tal cúmulo de intoxicación por la desinformación.

Del funcionamiento del sistema ha de darse cuenta al proveedor. La justificación es comprensible. Resulta conveniente conocer si responde a las expectativas generadas y, sobre todo, cómo evoluciona. Tal información facilitará al proveedor cumplir con sus obligaciones de seguimiento dentro de la planificación cuyos contenidos básicos detallará la Comisión europea (art. 72 del Reglamento).

Si se advirtiera la presentación efectiva de un riesgo, deberá suspenderse la utilización y comunicar de inmediato al proveedor tal incidencia ("sin demora indebida" es la imprecisa expresión del Reglamento en la versión española). Esa misma información ha de remitirse a la autoridad competente con el fin de analizar los riesgos (art. 79). Autoridad con la que se exige una leal cooperación (art. 26.12).

Lógicamente cualquier incidente grave ha de comunicarse, también al distribuidor y al importador. A los efectos de la aplicación de este Reglamento se define el "incidente grave" como aquel que produce unas consecuencias de trascendental entidad: fallecimiento, daños que comprometen la salud, incumplimientos de obligaciones que protegen los derechos fundamentales, alteración crucial del funcionamiento de una infraestructura crítica y otras específicas mencionadas en el apartado 49 del artículo 3.

Como en otros preceptos, se singulariza un recordatorio en el ámbito de las entidades financieras cuya regulación más detallada impone unas especiales reglas de vigilancia pues se entiende satisfecha esta obligación de vigilancia y comunicación si se han cumplido las normas específicas ya establecidas.

También en otros muchos sectores existen precisiones detalladas tanto sobre la vigilancia del funcionamiento del negocio, como de los sistemas de comunicaciones electrónicas. Esa *lex specialis*, ley propia del sector, puede satisfacer plenamente es-

tas obligaciones que ahora recoge el Reglamento de inteligencia artificial y, en consecuencia, debería aplicarse la misma razón: su correcto seguimiento servirá para acreditar también que se satisfacen estas obligaciones. Así, por ejemplo, en todos los servicios esenciales y estratégicos que han de cumplir unas reglas de seguridad específicas y han de notificar incidentes, muchos más que los considerados en este Reglamento[28].

Sin duda se desarrollarán e incorporarán sistemas informáticos que auditen, verifiquen y supervisen otros sistemas. No obstante, la precaución ante lo imprevisto, en ámbitos donde se han considerado riesgos altos, hace que se obligue también a una supervisión humana (art. 26.2). Lo que requiere un presupuesto básico: que el proveedor del sistema lo diseñe de tal modo que permita tal supervisión (art. 14).

A los efectos que ahora nos interesan, esto es, qué obligaciones tiene el responsable del despliegue han de destacarse algunas consideraciones.

En primer lugar, se concreta el ámbito mínimo de la supervisión en estos sistemas de alto riesgo, a saber, la preocupación por cómo afectan a la "salud, seguridad y derechos o fundamentales". Dentro de la institución el responsable puede decidir lógicamente extender la verificación del funcionamiento a otros extremos pero, en estos ámbitos tan sensibles se imponen controles específicos con el propósito de reducir al mínimo tales riesgos teniendo que considerar, además, que alguien haga un "uso indebido" del sistema[29]. Ayudará, sin duda, que el proveedor especifique medidas para tal supervisión en las instrucciones.

28 Me refiero a la Directiva 2022/2555, de seguridad de las redes, conocida como NIS 2. Sobre la evolución de ese régimen jurídico y sus carencias me remito a las consideraciones que realicé en Metamorfosis..., cit.; y Heredero, C., "Nueva Directiva Europea NIS2: un avance en la regulación de la ciberseguridad para las actuales sociedades digitalizadas," *Derecho Digital e Innovación,* núm. 16, 2023, realiza un análisis de esta Directiva.

29 Vid. Gallone, G., *Riserva di umanitá e funzioni amministrative,* Wolters Kluwer, CEDAM, 2023.

En segundo lugar, resulta indispensable para garantizar la eficacia de esta obligación que quienes supervisen cuenten con la "competencia, formación y autoridad necesarias". Se establecen algunos aspectos que permiten delimitar el conocimiento de los supervisores. En concreto: han de entender de manera adecuada el sistema, su capacidad y limitaciones de tal modo que detecte y resuelva "anomalías, problemas y comportamientos inesperados"; se exige que no incurra en el "sesgo de automatización", que no confíe en exceso en el funcionamiento automático; ha de interpretar correctamente los resultados y, además, ha de contar con facultades específicas para intervenir en el funcionamiento o decidir sobre los resultados. Ámbitos sobre los que se realizan relevantes precisiones.

Porque se exige que el supervisor pueda "decidir, en cualquier situación concreta, no utilizar el sistema", así como "descartar, invalidar o revertir los resultados de salida" que se hayan generado e, incluso, "interrumpir el sistema" bien pulsando un botón de parada u otro procedimiento que permita que se detenga de manera segura (letras d y e del art. 14.4). Ello supone unos conocimientos técnicos especiales para, como hemos visto, detectar y resolver anomalías, problemas y comportamientos inesperados.

Tales previsiones han de superar un obstáculo: en la actualidad existe una notable carencia de profesionales con conocimientos informáticos suficientes para ocupar la demanda de puestos de trabajo tanto en las Administraciones públicas como en las empresas[30].

Sin perjuicio de que en los próximos años se incremente de manera muy significativa la formación de especialistas, anoto dos observaciones. Es la primera que, como en tantas ocasiones a lo largo de la lectura del Reglamento, dependerá de la comple-

30 Entre los muchos documentos e informes que resaltan esta carencia, me remito al publicado por la Asociación DigitalEs, que agrupa a las principales empresas españolas de telecomunicaciones, tecnología e innovación digital: "Anatomía de la brecha de talento tecnológico" publicado en mayo de 2024.

jidad interna del sistema de inteligencia artificial la exigencia de la concreta capacitación del supervisor. Algunos sistemas calificados de alto riesgo siguen unas pautas absolutamente uniformes, como sujetos a raíles ferroviarios, siempre las mismas, sin capacidad de modular otras circunstancias, de tal modo que puede resultar más asequible esa actividad de supervisión del funcionamiento. Otros, sin embargo, incorporan tal sofisticación, tantísima información, tal cúmulo de posibilidades, de valoración de alternativas, que resulta complejo desentrañar hasta qué punto, en un proceso, el sistema se ha "salido del libro", esto es, ha creado, ha inventado otra pauta que es la que ha llevado al resultado.

Situaciones singulares como la perplejidad de matemáticos al intentar comprender todos los pasos que ha dado un sistema de inteligencia artificial para explicar proposiciones irresolubles durante siglos o por qué se ganaron y por qué se perdieron algunas partidas del juego del go en el mítico enfrentamiento entre AlphaGo y Sedol han sido bien narradas[31]. Pueden considerarse acontecimientos especiales, anecdóticos, pero no hay que descartar que la extraordinaria celeridad en cómo se incrementa la complejidad de los sistemas reduzca la posibilidad de explicar sus pasos.

En fin, deberá intensificarse la formación de especialistas para garantizar esa supervisión cuya falta, en caso de originarse daños, generará la correspondiente exigencia de responsabilidad[32].

31 Vid. Satoy, M., *Programados para crear. Cómo está aprendiendo a escribir, pintar y pensar la inteligencia artificial,* Acantilado, 2020; y Labatut, B., *Maniac,* Anagrama, 2023.

32 Coincido por ello con Ponce Solé, J. que hace años ya advirtió de estas exigencias de supervisión y responsabilidad, "Reserva de humanidad y supervisión humana de la inteligencia artificial", *El Cronista,* núm. 100, págs. 58 y ss.; y "Seres humanos e inteligencia artificial: discrecionalidad artificial, reserva de humanidad y supervisión humana" dentro de la obra colectiva *Inteligencia artificial*..., cit. págs. 196 y ss.

III.2.D.- Información a los afectados

Ha de informarse a los ciudadanos del uso de sistemas de alto riesgo cuando les afecten los resultados de los procesos. Noticia que ha de darse, incluso, cuando se ha utilizado el sistema como mera ayuda a lo largo del procedimiento para adoptar la decisión (art. 26.11).

Esta previsión requiere, sin embargo, varias puntualizaciones.

Hace años que el Reglamento de protección de datos ha reconocido, con carácter general, el derecho a los ciudadanos de no ser objeto de una decisión que les afecte basada de manera exclusiva en un proceso automatizado (art. 22 RGPD). Derecho que el mismo precepto matizaba al admitir decisiones automatizadas en varias situaciones, entre otras, cuando existe un consentimiento previo, así como cuando esté autorizado tal proceso por el Derecho de la Unión Europea (apartado segundo)[33].

Por tanto, los sistemas de alto riesgo que incidan en datos personales encontrarán su amparo en este Reglamento si satisfacen tales exigencias del consentimiento previo o una habilitación europea.

Además, hay actuaciones y procesos en los que se utilizan tales sistemas de alto riesgo y que no inciden en esos datos personales, de tal modo que podrán ser utilizados y, en ese caso, ha de informarse. Como en aquellas otras ocasiones en que el procedimiento ha sido impulsado o ha contado con la participación voluntaria de las personas: análisis de pruebas físicas, resolución de solicitudes de ayudas, convocatorias de oposiciones, asesoramiento financiero...

Sin embargo, no surge tal deber de información en el ámbito de la protección de las entidades e infraestructuras críticas, ni

33 Vid. Ballesteros, L.A., *Las fronteras de la privacidad. El conflicto entre la seguridad jurídica y los datos personales en una sociedad amenazada y tecnológica*, Comares, 2020; así como Gamero E., "Sistemas automatizados en la toma de decisiones en el Derecho administrativo español", *RGDA*, núm. 63, 2023.

tampoco cuando el Derecho de la Unión haya previsto excepciones o restricciones específicas, como establece el artículo 86 del propio Reglamento de inteligencia artificial. Tal es el caso de las previsiones establecidas en el ámbito de las investigaciones policiales y la justicia penal (Directiva 2016/680, de 26 de abril).

Interesa subrayar que la obligación de informar no queda circunscrita únicamente a señalar que se ha utilizado un sistema de alto riesgo. Deberá indicarse la finalidad, el ámbito de la ayuda o decisión, así como, en determinados casos, una explicación "clara y significativa" (art. 86 del Reglamento).

Es cierto que este precepto tiene carácter supletorio, pues "se aplicará únicamente" si no existe otra regulación comunitaria y, sobre todo, puede quedar desplazado ante excepciones y restricciones previstas en el Derecho de la Unión (86.2).

En conclusión, cuando no exista otra *lex specialis,* habrá de informarse y aclararse a los afectados por qué se confía en ese sistema, en ese avance en los procesos de análisis o decisión: qué ventajas aporta frente al anterior modo de actuar más tradicional, qué experiencia se ha conseguido... comentarios que pueden realizarse de manera previa o posterior a su utilización y que resultarán insuficientes si no se completan con "explicaciones claras y significativas" sobre el resultado. Porque explicar implica esclarecer qué denota el resultado obtenido, algo que lógicamente ha de realizarse *ex post.*

IV.- LARGAS MORATORIAS Y DERECHO TRANSITORIO

La *vacatio legis* se extendió, como es frecuente en el Derecho de la Unión, durante veinte días tras la publicación en el Diario Oficial. Sin embargo, se ha decidido posponer la aplicación de este nuevo régimen jurídico. Se ha establecido una larga moratoria,

con matices, precisiones y excepciones que retrasarán el despliegue efectivo del Reglamento.

Así, con carácter general, será exigible a los dos años de su entrada en vigor, el dos de agosto de 2026.

Sin embargo, y aquí está la primera precisión, la aplicación de los dos primeros capítulos que aluden a las disposiciones generales, así como a las prácticas prohibidas, será efectiva a los seis meses de la entrada en vigor, el 2 de febrero de 2025. Pero, una excepción importante, se excluye el régimen de calificación de los sistemas de alto riesgo para los que se ha fijado un plazo de tres años. Plazo también con varios matices.

Existen especialidades con relación a otros capítulos pues se aplicará el Reglamento al año de su entrada en vigor, según establece el artículo 113, con relación a: la nueva organización en la Unión Europea, esto es, la creación de la Oficina de inteligencia artificial, la constitución del Consejo europeo de inteligencia artificial y del Grupo científico de expertos, así como de un Foro consultivo (capítulo VII); la obligación de que los Estados miembros designen autoridades de supervisión (sección IV del capítulo III); la obligación de confidencialidad (art 78); el régimen de los sistemas generativos o de "propósito general" (capítulo V); el régimen sancionador con excepción del régimen del artículo 101 que se refiere a los sistemas generales o de propósito general (capítulo XII). En esos casos, el régimen jurídico será exigible a partir del 2 de agosto de 2025 (art. 113).

Interesa igualmente saber que el Reglamento tiene una eficacia retroactiva media. Esto es, con relación a los sistemas de inteligencia artificial existentes, así como los que aparezcan durante esos meses hasta la efectiva aplicación, quedan sujetos al régimen de transitoriedad establecido en el artículo 111. La finalidad: facilitar una adaptación progresiva a las nuevas obligaciones, buscar cierto equilibrio, cierta proporcionalidad entre el esfuerzo y coste que implica construir algunos sistemas,

su extensa comercialización y difusión, y la seguridad jurídica que ofrece el eficaz cumplimiento de este régimen jurídico.

Así, todos los "operadores", también por tanto quienes ahora nos interesan, los responsables del despliegue, deberán garantizar este marco jurídico europeo con relación a los sistemas calificados de alto riesgo cuando, después de la moratoria, una actualización del sistema implique "cambios significativos de diseño", esto es, modificaciones substanciales que trastoquen su finalidad, incidan en elementos no previstos inicialmente en su diseño y, en consecuencia, afecten al cumplimiento de los requisitos esenciales exigidos por el Reglamento en los artículos 9 y ss.

Los responsables del despliegue deberán atender, en principio, al contenido de las actualizaciones de los sistemas de alto riesgo para advertir, en caso de que no lo indique de manera explícita el proveedor, cómo afectan los cambios al sistema, si son sustanciales.

Este régimen transitorio apunta otras precisiones relevantes mediante una cadena de excepciones, particularidades y puntualizaciones.

Porque se establece el objetivo de que las autoridades públicas deberán satisfacer las exigencias del Reglamento relativas a todos los sistemas de alto riesgo que utilicen a más tardar a los seis años de la entrada en vigor (2 de agosto de 2030). Esto afectará a aquellos que se hayan introducido durante estos meses de moratoria y no sufran modificaciones sustanciales. Sin embargo, y empiezan las reglas especiales, con relación a los sistemas de alto riesgo que se utilicen en las actividades de seguridad a las que alude el anexo X, esto es, sistemas de información Schengen, de información de visados, sistemas de interoperabilidad para la cooperación judicial y policial y otros semejantes. En concreto, se ha fijado la fecha del 31 de diciembre de 2030 para su total adaptación al Reglamento con relación a aquellos sistemas que se comercialicen o pongan a disposición durante

el plazo de tres años desde la entrada en vigor del Reglamento. Esto es, la moratoria inicial de dos años se prorroga un año más, hasta mediados de 2027. Aunque, nuevo matiz, cuando se actualice la regulación de esa normativa de seguridad citada en el anexo X, tales sistemas serán objeto de evaluación.

A mi juicio, resultan plazos muy largos: seis años. De ahí que la Comisión Europea haya impulsado un "Pacto" con el fin de planificar la aplicación del Reglamento, en la medida de lo posible, con antelación. Con este fin ha convocado a los interesados para difundir las prácticas que se están analizando e incorporando, así como fomentar compromisos y códigos de conducta[34].

Es cierto que la celeridad con la que se producen los avances tecnológicos generará, por un lado, que a los nuevos sistemas que aparezcan dentro de dos años se les aplicará íntegramente el Reglamento. Por otro lado, que también las actualizaciones de los sistemas se suceden con notable rapidez y, en caso de que afecten a elementos sustanciales, en caso de modificaciones esenciales, implicará su sujeción al Reglamento.

En este sentido, y como mero elemento de comparación, recuerdo las fechas de evolución de uno de los sistemas generativos conocidos, el ChatGPT. Según las noticias que se han publicado sobre su proceso de desarrollo relativas a los parámetros básicos de las sucesivas versiones, el diseño inicial se concretó en 2018. Al año siguiente, ya se había configurado una segunda versión que también se actualizó tras otro año de entrenamiento y que se presentó públicamente en noviembre de 2022. A partir de ahí, hay una aceleración en los cambios, pues en unos meses, en marzo del 23, hay una nueva versión, y tras otros meses de entrenamiento, en diciembre se bautiza otra.

En resumen, el desarrollo y los cambios son constantes y, por ello, tras la moratoria los sistemas de inteligencia artificial deberán someterse a este régimen jurídico. Pero ello no ha de minorar

34 Vid. https://digital-strategy.ec.europa.eu/es/policies/ai-pact

la preocupación por el desparrame durante esta larga moratoria porque además de ser continuos los cambios, lo trascendente es que se producen con extraordinaria celeridad. Nuestros tiempos, nuestra percepción del tiempo se volatiliza al advertir las referencias de la supercomputación.

¿Por qué facilitar que durante dos años funcionen sin restricciones sistemas de alto riesgo? ¿Por qué permitir que durante seis meses se usen sistemas que se considerarán prohibidos? ¿Se es consciente de los billones de cálculos que en un solo día realiza una computadora?[35]

Sin dejar de lado estas inquietudes, hay que realizar unas últimas consideraciones porque no he concluido con las obligaciones de los responsables del despliegue de los sistemas de inteligencia artificial. Hemos de detenernos en otro aspecto.

V.- CONTRIBUCIÓN AL DESARROLLO DE LOS SISTEMAS

Las instituciones que incorporan sistemas de inteligencia artificial en el ejercicio de sus funciones o en su negocio pueden quedar sujetas a otras obligaciones, además de las que acabamos de repasar. En concreto, a las obligaciones, lógicamente más rigurosas, establecidas para los proveedores (art. 25 del Reglamento). Y ello porque se entiende que en sus comportamientos están "desarrollando" ciertamente el sistema, están acrecentando sus aplicaciones y ese incremento de capacidad del sistema impone una responsabilidad mayor.

35 Excede al propósito de este trabajo incidir en qué ámbitos resulta más peligrosa la moratoria de algunos sistemas de alto riesgo. Pero ha de tenerse mínima noción de lo que suponen los procesos de supercomputación. Las unidades de esas anotaciones se llaman "comas flotantes" a los que alude el glosario del Reglamento de inteligencia artificial (art. 3.67) y la básica, "peta-FLOTS-día" implica mil billones de cálculos por segundo. Un ejemplo expresivo que facilita Jordi Torres (2023) para comparar la celeridad es que un ordenador personal necesitaría, al menos, un año para alcanzar ese peta-FLOTS-día.

¿En qué situaciones, quien ha adquirido un sistema y lo utiliza, se sujeta a las obligaciones de los proveedores? En aquellos casos que, tras comprobar su funcionamiento, advertir las ventajas de su uso, los efectos prácticos, repara en otras posibilidades del sistema, en la facultad de nuevas utilidades, en la viabilidad de otros fines... y ello le lleva a incorporar nuevas instrucciones de tal manera que lo modifica de manera sustancial.

Como ya he señalado en otras ocasiones anteriores a lo largo de este texto, son tan dispares los sistemas de inteligencia artificial que, a efectos de esta regulación, lo primero que hay que advertir es que algunos sistemas generan internamente constantes cambios y alteraciones, a raíz del mayor cúmulo de datos introducidos o de una combinación de los mismos, pues tienen tales instrucciones previas para ese aprendizaje. En este sentido, importa subrayar que aquellos parámetros predeterminados por el proveedor en la evaluación inicial y que originarán cambios a lo largo de su funcionamiento no son considerados "modificaciones sustanciales" a los efectos de incrementar las obligaciones de los responsables del despliegue (art. 43.4 del Reglamento).

En el glosario de conceptos que recoge el artículo 3, aparecen delimitadas las "modificaciones sustanciales" como los cambios que no estén previstos o planificados en la evaluación inicial y por los cuales, bien se altera la finalidad original o bien afectan a "la conformidad del sistema" con los requisitos establecidos para estos sistemas de alto riesgo tales como los presupuestos de ciberseguridad, solidez, gestión de riesgos, transparencia y otros que se exigen en los artículos 8 y siguientes del Reglamento (apartado 23).

Para que ciertamente opere una mayor responsabilidad de las Administraciones, empresas o profesionales resulta necesario que haya una decisión de añadir nuevas instrucciones al sistema. Las nuevas cargas y responsabilidades han de derivar de una previa voluntad consciente de modificación. Del mismo modo que se somete a esas obligaciones a la institución que

añade su nombre o marca al sistema. Esa confesada muestra de que entiende que está contribuyendo a su desarrollo, probablemente por cómo está nutriendo de datos al sistema, genera la mayor responsabilidad.

Junto a esta conciencia, hay otro dato objetivo clave que determina ese salto hacia una mayor responsabilidad: el propio sistema de inteligencia artificial advierte de ese cambio sustancial. Y es que, entre los requisitos del diseño, el Reglamento exige que estos sistemas cuenten con la capacidad de indicar tal cambio (art. 12).

En todo caso, hay que insistir en que los cambios e instrucciones en el sistema han de incidir en elementos sustanciales del sistema para que puedan originar nuevas obligaciones. Añadidos que pudieran calificarse de formales, auxiliares, accesorios, no pueden conducir a imponer obligaciones como si estas instituciones fueran ciertamente diseñadoras, proveedoras de los sistemas. Un requisito que ha de interpretarse en sentido riguroso por la consecuencia de incrementar la responsabilidad. Manifestaciones de esta contribución serán las que resulten de realizar pruebas y ensayos en espacios controlados.

Las nuevas obligaciones se extienden a ofrecer mayor información, realizar evaluaciones, entre otras que son objeto de análisis específico en otro trabajo de esta misma revista firmado por Ricardo Rivero. Me remito al mismo.

Concluyo con una precisión: el uso de los sistemas de inteligencia artificial se ha extendido notablemente, ciertamente estamos como sumergidos en ese entramado de procesos automáticos. Como si al navegar por Internet los sistemas de inteligencia artificial nos han empujado a bucear y, a partir de ahí, estamos ya rodeados de agua. Esperemos que no nos introduzcan en un saco amniótico.

Por ello termino con una advertencia: para la realización de este estudio no he utilizado sistemas de inteligencia artificial. No he

consultado a ningún asistente informático, a ningún sistema de generación de contenido. Pero sé que, una vez que este texto se digitalice, habrá sistemas que lo incorporen. Les deseo una buena digestión si ello contribuye a promover el debate entre juristas sobre la necesaria regulación de la inteligencia artificial. Porque somos los juristas, junto con otros técnicos y profesionales, quienes tenemos que precisar el régimen jurídico de los sistemas para poder confiar en su uso.

VI.- CONCLUSIONES

La publicación de trabajos en esta Revista de privacidad y Derecho digital exige terminar con unas sucintas conclusiones enumeradas. De manera escueta recuerdo algunas de mis consideraciones:

1º Todos los usuarios de sistemas de inteligencia artificial hemos de respetar unas mínimas normas éticas, así como seguir los códigos de conducta e instrucciones que se difundan de tales sistemas.

2º Las Administraciones, empresas y profesionales que incorporen sistemas en el ejercicio de sus funciones, negocios o actividades han de garantizar unas pautas de transparencia para que los ciudadanos estén advertidos de su uso.

3º Además, cuando tales sistemas sean calificados de alto riesgo, deberán adoptar específicas medidas organizativas, de carácter técnico, ser objeto de supervisión humana e informar a quienes afecten tales procesos de su utilización.

4º El Reglamento de inteligencia artificial prevé una moratoria extensa para exigir su efectiva aplicación. Cosa que, a mi juicio, puede poner en riesgo el esfuerzo conseguido de sistematizar este régimen jurídico.

5º He reflexionado y he escrito este trabajo sin ninguna asistencia de sistema inteligencia artificial pero soy consciente de que la digitalización del mismo será alimento para alguno de esos sistemas. Espero que tal digestión sea nutritiva con el fin de generar un debate entre juristas sobre la regulación de la inteligencia artificial.

VII.- BIBLIOGRAFÍA

Son numerosos los libros y artículos que analizan el régimen jurídico de los sistemas de inteligencia artificial. A continuación únicamente completo los datos de las referencias mencionadas a lo largo del texto y me remito, pues su lectura ilustrará, a los números monográficos de las Revistas El Cronista del Estado social y democrático de Derecho, núm. 100/2022; a la Revista Jurídica de Asturias, núm. 45/2022; al libro colectivo dirigido por Eduardo Gamero y coordinado por Francisco Pérez Guerrero, *Inteligencia artificial y sector público: retos, límites y medios,* Tirant lo Blanch 2023; así como a las ponencias y comunicaciones presentadas en el Congreso de la Asociación Española de Profesores de Derecho Administrativo celebrado en Vigo en 2024.

ALONSO GARCÍA, C., "Sistema Viogén: fallos y algunas propuestas de mejora", Congreso de la Asociación Española de Profesores de Derecho Administrativo, Vigo, 2024

AVARO, D., El Sistema de Crédito Social chino. Vigilancia, paternalismo y autoritarismo, Ed. Biblos, Buenos Aires, 2023.

BALLESTEROS MOFFA, L.A., *Las fronteras de la privacidad. El conflicto entre la seguridad jurídica y los datos personales en una sociedad amenazada y tecnológica*, Comares, 2020.

BELTRÁN DE HEREDIA, I., *Inteligencia artificial y neuroderechos: la protección del yo inconsciente de la persona*, Ed. Aranzadi, 2023.

BOIX PALOP, A. Y SORIANO ARNANZ, A., "Transparencia y control de uso de la inteligencia artificial por las Administraciones públicas", en la obra coordinada por F. Balaguer Callejón y L. Cotino Hueso *Derecho público de la inteligencia artificial*, Fundación Giménez Abad, Zaragoza, 2023.

COTINO, L., "Discriminación, sesgos e igualdad de la inteligencia artificial en el sector público" en la obra colectiva dirigida por Eduardo Gamero, *Inteligencia artificial y sector público: retos, límites y medios,* Tirant lo Blanch, págs. 260 y ss., 2023.

DOMÍNGUEZ ÁLVAREZ, J.L., *Iusdata y Administración pública,* Civitas, 2023.

FUERTES, M., *Metamorfosis del Estado. Maremoto digital y ciberseguridad,* Marcial Pons, 2022.

GALLONE G., *Riserva di umanitá e funzioni amministrative,* Wolters Kluwer, CEDAM, 2023.

GAMERO E., "Sistemas automatizados en la toma de decisiones en el Derecho administrativo español", *RGDA*, núm. 63, 2023.

GARCÍA MEXÍA, P., "Inteligencia artificial: una mirada desde el Derecho", *Anales de la Academia Matritense del Notariado*, tomo 60, pág. 117, 2020.

HEREDERO, C., "Nueva Directiva Europea NIS2: un avance en la regulación de la ciberseguridad para las actuales sociedades digitalizadas", *Derecho Digital e Innovación,* núm. 16, 2023.

LABATUT, B., *Maniac,* Anagrama, 2023.

MARTÍN DELGADO, I., "La aplicación del principio de transparencia a la actividad administrativa algorítmica", en la obra colectiva Eduardo Gamero, *Inteligencia artificial y sector público: retos, límites y medios,* Tirant lo Blanch, págs. 132 y ss., 2023.

MENÉNDEZ, E., *From bureaucracy to artificial intelligence: the tension between effectiveness and guarantees,* Wolters Kluwer, CEDAM, 2023.

MIRANZO DÍAZ, J. *Inteligencia artificial y Derecho Administrativo*, ICA-Tecnos, 2023

OLIVER, N., *Inteligencia artificial, naturalmente*, ONTSI 2020

PONCE, J., "Reserva de humanidad y supervisión humana de la inteligencia artificial", *El Cronista,* núm. 100, págs. 58 y ss. 2022;

"Seres humanos e inteligencia artificial: discrecionalidad artificial, reserva de humanidad y supervisión humana" dentro de la obra colectiva *Inteligencia artificial y sector público*, coord. por E. Gamero y F.L. Guerrero, Tirant lo Blanch, págs. 196 y ss., 2023.

SATOY, M., *Programados para crear. Cómo está aprendiendo a escribir, pintar y pensar la inteligencia artificial,* Acantilado, 2020.

TORRES, J., *La inteligencia artificial explicada a los humanos,* Plataforma editorial, 2023.

Síganos en Linked

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

www.rdu.es

2444-5762