

Una aproximación a la futura regulación de la inteligencia artificial en la Unión Europea*

An approach to future EU's artificial intelligence act

SARA GARCÍA GARCÍA

Universidad de Valladolid
sara.garciag@uva.es
ORCID: 0000-0001-7220-0368



Este artículo está sujeto a una [licencia “Creative Commons Reconocimiento-No Comercial” \(CC-BY-NC\)](https://creativecommons.org/licenses/by-nc/4.0/).

DOI: <https://doi.org/10.24197/ree.79.2022.304-323>

Resumen: La Inteligencia Artificial es una realidad presente y de futuro que participará en numerosísimos ámbitos del día a día de los Estados y sus ciudadanos. Los sistemas de IA son un arma de doble filo, tan ventajosos como peligrosos. Aprovechar sus beneficios y convertir a Europa en referencia económica, técnica y jurídica en la materia a nivel mundial, así como limitar sus efectos nocivos, es el objetivo que se ha propuesto la Unión Europea y para el que propone un marco normativo que pretende vertebrar a través de la que llama Ley de Inteligencia Artificial.

Palabras clave: inteligencia artificial; protección de datos; Mercado Único Digital; Reglamento.

Abstract: Artificial Intelligence is a present and a future reality that will be involved in many areas of the daily lives of States and their citizens. AI systems are a double-edged sword, they are as advantageous as dangerous. Harnessing its benefits making Europe an economic, technical and legal world-reference, as well as limiting its harmful effects, is the objective that the European Union has set itself this 2021. To reach that goal the EU has proposed a legal framework that intends to structure through the Artificial Intelligence Act.

Keywords: artificial intelligence; data protection; Digital Single Market; regulation.

* Este trabajo se ha realizado en el marco del III Congreso Internacional Jóvenes Investigadores sobre la Unión Europea, celebrado en el Instituto de Estudios Europeos los días 7 y 8 de octubre de 2021.

1. INTRODUCCIÓN

El futuro es sostenible y digital. Esa es una realidad a la que, nos guste o no, estamos abocados y conviene estar preparados para cuando llegue; especialmente desde el Derecho que, por un lado, tendrá que afrontar y atender necesidades nuevas y peculiares que cambian *a máxima velocidad*, pero también, por otro, se verá transformado en su actuación y práctica.

La Unión Europea es consciente de ello y adaptarse a ese futuro es uno de los grandes objetivos de la actual Europa, reflejados en las dos grandes y más recientes iniciativas legislativas en las que ésta se ha embarcado:¹ por un lado, la regulación de la neutralidad climática, un objetivo vinculante para el año 2050 que transformará nuestro entorno socio-económico tal y como lo conocemos hoy y cuyo alcance está siendo regulado con la tramitación de la conocida como *Ley Europea del Clima*,² y por otro, la regulación de la Inteligencia Artificial (en adelante IA), cuyos trabajos preparatorios inició la Comisión en el año 2018³ y ahora se ven reforzados y dirigidos a conseguir una regulación de la IA en el conjunto de la Unión de forma irremediable;⁴ una futura ordenación que complementará a otra anterior y relevante, próxima en la materia,

¹ De hecho, son dos materias comunicadas, pues la Unión Europea reconoce que *«las tecnologías digitales como la inteligencia artificial son motores clave para alcanzar los objetivos del Pacto Verde»*: Libro Blanco sobre la inteligencia artificial, un enfoque europeo orientado a la excelencia y la confianza COM (2020) 65 final, de 19 de febrero de 2020 (en adelante Libro Blanco).

² Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece el marco para lograr la neutralidad climática y se modifica el Reglamento (UE) 2018/1999 («Ley del Clima Europea»), de 4 de marzo de 2020: COM (2020) 80 final. Puede verse un comentario en García García, Sara (2021): "Construcción y aplicación de la llamada Ley Europea del Clima: el paso definitivo hacia la neutralidad climática y la energía verde en la Unión Europea". *La Ley. Unión Europea* (27), pp.

³ Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Inteligencia artificial para Europa, COM (2018) 237 final, de 25 de abril de 2018.

⁴ Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión: COM (2021) 206 final, de 21 de abril de 2021 (en adelante Propuesta).

como es la relativa a la protección de datos, consumidores o la ciberseguridad.⁵

En este comentario nos vamos a centrar en comprender y conocer las bases más esenciales, esta vez, de la Propuesta de regulación del segundo de los retos de futuro de la Unión Europea: la Ley de Inteligencia Artificial. Una Propuesta que desarrolla la Unión con base en el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), que trata de *la adopción de medidas para garantizar el establecimiento y el funcionamiento del mercado interior*, como parte de la Estrategia para el Mercado Único Digital de la Unión Europea.⁶

Por la transversalidad de la cuestión, la Unión afronta esta tarea en el contexto de su competencia en diversos sectores en los que se utilizan o previsiblemente se utilizarán sistemas de IA tales como industria, investigación, empleo, educación y, sobre todo, mercado interior.⁷ Y lo hace consciente de su necesidad y urgencia por ser ahora, cuando otras potencias mundiales como Estados Unidos, China, Japón o Canadá están haciendo lo propio, el momento de afrontar este reto y posicionar a la Unión Europea a la vanguardia técnica y jurídica de la cuestión, evitando además «*una fuga de cerebros que la convierta en consumidora de soluciones desarrolladas en otros lugares*».⁸

1. QUÉ ES LA INTELIGENCIA ARTIFICIAL

1.1. Descripción general de la IA

El objetivo de este breve análisis es comprender el contenido y alcance jurídico de la Propuesta realizada por la Unión Europea a finales de abril de 2021 de regular la llamada *Inteligencia Artificial*. Pues bien,

⁵ Vid. el Reglamento (UE) *general de protección de datos* 2016/679, de 27 de abril de 2016; la Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores; o el Reglamento (UE) *sobre la Ciberseguridad* 2019/881, de 17 de abril de 2019.

⁶ Vid. apartado 2 de la Propuesta, p. 6.

⁷ Vid. COM (2018) 237 final, op. cit. p. 2.

⁸ *Ibidem*, p. 7.

para ello el primer paso necesario es determinar qué se entiende –o, mejor, qué entiende la Unión Europea– por Inteligencia Artificial.

El apartado 1 del artículo 3 de la Propuesta de Reglamento para armonizar la IA define un *sistema de inteligencia artificial* como el *software que se desarrolla siguiendo una o varias técnicas o enfoques específicos*⁹ «y que puede, para un conjunto determinado de objetivos definidos por el ser humano, generar resultados tales como contenidos, predicciones, recomendaciones o decisiones que influyen en entornos con los que se interactúa». ¹⁰ Este sistema, este software puede estar o no integrado en dispositivos de *hardware* (ejemplos típicos en este caso serían los coches autónomos o los drones)¹¹ y adquiere de su entorno *datos* que interpreta de forma estructurada y no estructurada «razonando, según el conocimiento que el sistema tenga, o procesando la información derivada de los datos adquiridos» cuál es la mejor actividad que pueda ser desarrollada con el propósito de alcanzar el objetivo establecido.¹²

Esta es la descripción del objeto específico de la Propuesta de Reglamento, pero no es una definición general de IA. No existe ni a nivel técnico ni, por supuesto, jurídico una definición establecida y

⁹ Todos esas técnicas o enfoques están enumerados en el Anexo I de la Propuesta; concretamente habla de: «Estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo. Estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico). Estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización».

¹⁰ Apartado 1 del art. 3 de la Propuesta: «Sistema de inteligencia artificial (sistema de IA): el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa».

¹¹ Cfr. AI HLEG (2019): *A definition of ai: main capabilities and disciplines*. Brussels: European Commission. Dicho lo anterior, baste con recordar que cuando hablamos de *software* lo hacemos del «conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora», siendo *hardware* el «conjunto de aparatos de una computadora»: DRAE.

¹² AI HLEG (2019) op. cit. Vid. Fanni, Simona. (2020): “La inteligencia artificial y el cuerpo humano digital: a la búsqueda del *habeas data*” en *Ius et Scientia* (Vol. 6, nº 2), pp. 200 a 224.

unánimemente aceptada de la IA. NAVAS NAVARRO reconoce que cada autor afronta esta tarea de forma diferente, por lo que ofrecer un concepto común es, por el momento, algo complicado.¹³ Con carácter básico y general podríamos definir la IA como «*la capacidad de las máquinas para usar algoritmos, aprender de los datos y utilizar lo aprendido en la toma de decisiones tal y como lo haría un ser humano*».¹⁴

1.2. La IA como parte o complemento de otras materias

Así definida, la IA se identifica como «*una de las partes más importantes de la economía de los datos*», del llamado *mercado único digital*;¹⁵ es más, «*sin datos, no hay inteligencia artificial*»,¹⁶ dice la

¹³ Esta autora expone como una definición común aquella que define la IA como «*campo de la ciencia y la ingeniería que se ocupa de la comprensión, desde el punto de vista informático, de lo que se denomina comúnmente comportamiento inteligente. También se ocupa de la creación de artefactos que exhiben este comportamiento*»: Navas Navarro, Susana et ali. (2017): *Inteligencia artificial. Tecnología y derecho*. Valencia: Tirant lo Blanch, pp. 23 y 24.

¹⁴ Vid. Rouhiainen, Lasse (2018): *Inteligencia artificial. 101 cosas que debes saber hoy sobre nuestro futuro*. Barcelona: Alienta Editorial, p. 17. La IA es un concepto global que comprende muchas sub-áreas; el CESE enumera como sub-áreas a las que afecta la IA «*la informática cognitiva (cognitive computing: algoritmos capaces de razonamiento y comprensión de nivel superior —humano—), el aprendizaje automático (machine learning: algoritmos capaces de enseñarse a sí mismos tareas), la inteligencia aumentada (augmented intelligence: colaboración entre humanos y máquinas) o la robótica con IA (IA integrada en robots)*», apartado 2.1.); no obstante, es posible concretar su objetivo fundamental en «*la investigación y el desarrollo de la automatización de comportamientos inteligentes*» (Continúa: *como razonar, recabar información, planificar, aprender, comunicar, manipular, observar e incluso crear, soñar y percibir*): Vid. Dictamen del Comité Económico y Social Europeo sobre la «*Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el Consumo, el empleo y la sociedad, de 31 de mayo y 1 de junio de 2017, apartado 2.1.*

¹⁵ Vid. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y social europeo y al Comité de las Regiones «*La construcción de una economía de los datos europea*», COM (2017) 9 final, de 10 de enero de 2017: «*La economía de los datos mide la repercusión global del mercado de los datos —es decir, el mercado en que se intercambian datos digitales como productos o servicios derivados de los datos brutos— en el conjunto de la economía. Implica la generación, recogida, almacenamiento, procesamiento, distribución, análisis, elaboración, entrega y explotación de los datos que hacen posibles las tecnologías digitales*».

Comisión Europea. Los datos personales y la IA conformarían la base esencial de la *personalidad virtual* de todo ciudadano europeo.¹⁷ La Comisión es consciente de esta relación y vela por garantizar la coherencia de la Propuesta con la regulación vigente en materia de protección de datos.¹⁸ En este sentido, podríamos identificar a la IA como uno de los medios de obtención de datos personales, de forma que la defensa de estos justifica en parte ya la regulación de aquella.¹⁹ La IA utiliza parte de los datos recopilados para *tomar decisiones* o *actuar* de una determinada manera; los datos son, podríamos decir, *la gasolina* con la que se mueve la IA,²⁰ con la que después desarrolla un comportamiento autónomo e *inteligente*. Este *comportamiento inteligente*, su diseño, aplicación y consecuencias, es el núcleo principal de la Propuesta de regulación,²¹ de forma que controlar y depurar el uso

¹⁶ Vid. Libro Blanco.

¹⁷ Sobre lo que hemos llamado *personalidad virtual*, más conocido como *habeas data* sería interesante ver a Fanni, Simona (2020) op. cit., pp. 200 a 224.

¹⁸ Regulado, como se ha recordado ya por el Reglamento (UE) *general de protección de datos* 2016/679, de 27 de abril de 2016 en la Unión Europea y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

¹⁹ Peguera Poch, Miquel (2020): “En búsqueda de un marco normativo para la Inteligencia Artificial” en Cerrillo i Martínez, Agustí et Peguera Poch, Miquel (Coords.) *Retos de la inteligencia artificial*. Cizur Menor: Aranzadi, pp. 41 a 56, vid. pp. 41 y 42.

²⁰ «La IA requiere el uso de grandes cantidades y variedades de datos de diferentes fuentes, la conformación de los respectivos regímenes de pertenencia y circulación afecta la capacidad de las empresas para implementar de manera efectiva procesos computacionales innovadores y consolidar posiciones de poder en un mercado»; reglas en virtud de las cuales el *software* procesa datos y toma de decisiones: Ottolia, Andrea (2018): *Derecho, big data e inteligencia artificial*. Valencia: Tirant lo Blanch, pp. 8 y 9. Puede desprenderse esta idea de los datos como *el alimento de la inteligencia artificial* en el interesante análisis elaborado por Cotino Hueso, Lorenzo. (2019) “Riesgos e impactos del big data, la inteligencia artificial y la robótica. Enfoques, modelos y principios de la respuesta del derecho” en *RGDA* (nº 50), 37 pp.

²¹ Con *comportamiento inteligente* nos referimos «a la capacidad de percibir el entorno mediante sensores, procesar los datos recogidos, determinar a partir de la información obtenida cuál es la mejor opción para lograr los objetivos definidos por quien ha diseñado el sistema, y llevarla a la práctica; (...) de hecho, en versiones más avanzadas, el sistema es capaz de “aprender” y de calibrar el resultado de su acción, determinar su grado de éxito y perfeccionar sus reglas para tomar futuras decisiones»: vid. Peguera Poch, Miquel (2020): “En búsqueda de un marco normativo para la

de datos sensibles o personales por parte de la IA es una de las principales motivaciones para regular estas técnicas. Lo que a nivel jurídico interesa en esta cuestión es que la obtención y el uso de esos datos suscite confianza y se asiente en valores y derechos fundamentales, como la dignidad humana y la protección de la privacidad.²²

Lo dicho hasta ahora permite apreciar que existe una estrecha relación entre los sistemas de IA y otras materias o asuntos fuertemente protegidos ya por la Unión Europea, lo cual va a influir en las características y contenido de esta futura regulación. Controlar los efectos derivados del uso de datos protegidos por la IA no es la única finalidad de la Propuesta de Reglamento, también hay una relación especial entre IA y la protección de consumidores, la regulación sobre seguridad de los productos, la no discriminación e igualdad de género y la Carta de los Derechos Fundamentales de la Unión, a la que pretende atender de manera especial el futuro Reglamento.²³ De todos ellos destacaría en este sentido la afectación del uso de la IA a la regulación en materia de seguridad de productos. Desde el momento en que un producto puede incorporar sistemas de IA, la Propuesta de Reglamento pretende modificar y completar la regulación vigente en la materia introduciendo el análisis específico de aquellos sistemas en los procedimientos de evaluación de la conformidad de estos productos.²⁴

2. POR QUÉ REGULAR LA INTELIGENCIA ARTIFICIAL

La IA ofrece indiscutiblemente numerosas ventajas tanto para el ser humano como para la sociedad: esta puede aportar una amplia gama de beneficios económicos y sociales. Mediante IA se pueden crear *patrones dinámicos de tendencias de futuro*, que aportan *predictibilidad* y un *apoyo en la toma de decisiones*, lo que puede cambiar nuestra forma de relacionarnos, de vender, comprar, diseñar...²⁵ Al mejorar la

Inteligencia Artificial” en Cerrillo i Martínez, Agustí et Peguera Poch, Miquel (Coords.) op. cit.

²² Vid. Libro blanco.

²³ Vid. p. 4 de la Propuesta.

²⁴ Ibidem.

²⁵ «Se puede conocer mejor al cliente, al mercado, personalizar los productos y servicios, mejorar el márketing y la publicidad, tener una mejor visión estratégica y de

predicción, la optimización de las operaciones, la asignación de recursos y la personalización de la prestación de servicios, el uso de la IA *puede apoyar resultados social y ambientalmente beneficiosos y proporcionar ventajas competitivas clave a las empresas y a la economía europea, lo que será esencial en ámbitos o sectores de gran impacto, como el del cambio climático, el medio ambiente y la salud, el sector público, las finanzas, la movilidad, los asuntos de interior y la agricultura.*²⁶ En otro plano, la IA se ha demostrado útil también para contribuir a la lucha contra la delincuencia, la ciberdelincuencia y el terrorismo,²⁷ sin olvidar las distintas aplicaciones que esta puede tener para el sector público y, en especial, para las Administraciones Públicas, a las que puede servir como instrumento auxiliar en la toma de sus decisiones; unas decisiones que pueden verse, cuando menos, agilizadas²⁸ o, incluso, acotadas en su eventual discrecionalidad.

No obstante, dicho lo anterior, la IA al mismo tiempo puede generar una serie de riesgos y problemas que deben ser abordados. Como reconoce la propia Comisión ciertas características de la IA, como la opacidad de muchos algoritmos, plantean riesgos específicos y potencialmente elevados²⁹ que pueden generar daños tanto *«materiales (para la seguridad y la salud de las personas, con consecuencias como la muerte, y menoscabos al patrimonio) como inmateriales (pérdida de privacidad, limitaciones del derecho de libertad de expresión, dignidad*

negocio, crear nuevos servicios y productos, y obtener nuevos ingresos, mejorar y agilizar la toma de decisiones, prever el comportamiento»: Sáiz, Carlos (Coord.): (2017) *Código de buenas prácticas en protección de datos para proyectos de Big Data*. Madrid: AEPD e ISMS Forum, pp. 6-7.

²⁶ Vid. p. 1 de la Propuesta.

²⁷ *«AI can help to fight crime and terrorism, and enable law enforcement to keep pace with the fast developing technologies used by criminals and their cross-border activities»:* Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: *Fostering a European approach to Artificial Intelligence*, COM (2021) 205 final de 21 de abril de 2021, p. 3.

²⁸ Vid. nota 24 y Cerrillo i Martínez, Agustí (2020): “El impacto de la inteligencia artificial en las Administraciones públicas: estado de la cuestión y una agenda” en Cerrillo i Martínez, Agustí et Peguera Poch, Miquel (Coords.) op. cit., pp. 75 a 92, vid. pp. 79 y 80.

²⁹ Vid. COM (2021) 205 final, op. cit.

humana, discriminación en el acceso al empleo, etc.)» de gran relevancia.³⁰ Estos riesgos y daños, como reconocen las instituciones europeas, no pueden ser atendidos por la legislación vigente de forma adecuada³¹ y afectan en general a niveles esenciales, tanto jurídicos como económicos, y en concreto a aspectos principales tales como son los derechos fundamentales y la seguridad, las cuestiones relativas a la responsabilidad civil,³² las garantías en la actuación de la Administración Pública y la Administración de justicia o también, obviamente, a nivel cibernético o de ciberseguridad.³³

Este escenario, de grandes ventajas y arriesgados inconvenientes, es el que pretende ordenar la Unión Europea diseñando un marco jurídico que permita alcanzar un equilibrio con el que preservar el liderazgo tecnológico de Europa, pero garantizando que los europeos puedan beneficiarse de estas nuevas tecnologías de forma segura y fiable, de acuerdo con los valores, derechos fundamentales y principios de la Unión.³⁴ *Excelencia y confianza* son los dos grandes fines que estableció la Comisión Europea para esta regulación de la IA;³⁵ una regulación que, en definitiva, no pretende sino complementar la existente sobre elementos que irremediablemente se ven o se verán afectados por la IA con un conjunto de normas armonizadas aplicables al diseño, el desarrollo y la utilización de determinados sistemas de IA de alto riesgo.³⁶

De este modo, encontramos ámbitos especialmente vulnerables a estos riesgos derivados del *mal uso* de la IA en materia de responsabilidad civil, contratos públicos y privados, privacidad e,

³⁰ Vid. Libro Blanco, p. 13.

³¹ Vid. COM (2021) 205 final, op. cit.

³² «Siendo los principales aquellos que pueden afectar «a la aplicación de las normas diseñadas para proteger los derechos fundamentales (como la protección de los datos personales y la privacidad, o la no discriminación) y la seguridad, así como a las cuestiones relativas a la responsabilidad civil»: Libro blanco.

³³ Risks emerging from human-robot collaboration, cyber risks with safety implications, and autonomous machines: vid. COM (2021) 205 final, op. cit.

³⁴ Vid. p. 3 y art. 1 de la Propuesta.

³⁵ Vid. COM (2018) 237 final op. cit.

³⁶ Vid. p. 4 de la Propuesta.

incluso, a nivel administrativo.³⁷ Unos riesgos que se combatirán imponiendo una mayor transparencia y claridad a los sistemas de actuación de la IA o, incluso, la asistencia o seguimiento humano de los mismos, así como limitando su uso en determinados ámbitos.³⁸

2.1. Riesgos de la IA para los derechos fundamentales

Los riesgos derivados del uso de esta inteligencia no humana recaen especialmente sobre la protección y garantía de derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea; específicamente la Comisión habla en este sentido de posibles repercusiones para el derecho a la dignidad humana, el respeto de la vida privada y familiar y la protección de datos de carácter personal, la no discriminación y la igualdad entre hombres y mujeres, libertad de expresión y de reunión, el derecho a la tutela judicial efectiva y a un juez imparcial, la presunción de inocencia y los derechos de la defensa, así como el principio general de buena administración. Asimismo, podrían verse directamente afectados los derechos de los trabajadores, de los consumidores, los derechos del niño y la integración de las personas discapacitadas y el derecho a un nivel elevado de protección del medio ambiente y la mejora de su calidad.³⁹ Para la defensa de todos ellos, la Comisión reconoce una inevitable restricción a la libertad de empresa, la propiedad intelectual y la libertad de las artes y de las ciencias; ahora bien, esta limitación será proporcionada y limitada *al mínimo necesario para prevenir y reducir riesgos graves para la seguridad y violaciones probables de los derechos fundamentales*.⁴⁰

Estos posibles daños, advertidos por la propia Comisión, proceden del uso de datos realizado la IA. La toma de decisiones por

³⁷ Vid. COM (2021) 205 final, op. cit.

³⁸ Vid. art. 14 y Título IV de la Propuesta.

³⁹ Vid. pp. 12 y 13 de la Propuesta. Es posible leer un estudio profundo de los efectos de la IA en alguno de estos derechos en Cerrillo i Martínez, Agustí et Peguera Poch, Miquel (Coords.) op. cit., especialmente sobre su afectación a los derechos de los trabajadores (Fernández García, Antonio, pp. 125 a 142), empleados públicos (Galindo Caldés, Ramón, pp. 93 a 110), en materia de justicia penal (Blacells, Marc, pp.145 a 160 y Vilalta Nicuesa, Aura Esther, pp. 161 a 179) y propiedad intelectual (Xalabarder, Raquel, pp. 205 a 224 y Seuba, Xavier, pp. 241 a 254).

⁴⁰ Ibidem

cualquier humano puede ser errónea y subjetiva, algo que no evita la IA, de hecho, *esta misma subjetividad puede tener efectos mucho más amplios y afectar y discriminar a numerosas personas sin que existan mecanismos, como los de control social, que rijan ese comportamiento.*⁴¹ La opacidad de algunos de los algoritmos o métodos utilizados por la IA puede dificultar el conocer, y lo que puede ser en ciertos puntos más importante, el probar, el modo en que se ha alcanzado una solución y, en su caso, un perjuicio a un tercero; y es que *a medida que se van automatizando comportamientos humanos mediante sistemas expertos que aprenden del entorno y toman sus propias decisiones sin que el individuo que los plantea conozca de antemano el criterio o procedimiento a seguir, se van generando situaciones de vulnerabilidad en la seguridad y derechos de las personas.*⁴² Reducir esa opacidad y los sesgos vulneradores de derechos fundamentales que pueden surgir del uso de sistemas de IA es uno de los grandes objetivos que se marcará la futura Ley de IA.⁴³

3.2. Los riesgos de la IA y los sistemas tradicionales de responsabilidad civil

La nueva realidad que se nos anuncia con planteamientos como el que nos ocupa traerá consigo un conjunto de nuevos riesgos y daños; riesgos y daños especiales, pues se desarrollarán en el mundo virtual o procederán de este. Esto tendrá repercusiones directas en los sistemas de responsabilidad civil, unos sistemas que, tal y como están configurados en la actualidad, no serían aplicables a un escenario como el anunciado. Como bien advierte NÚÑEZ ZORRILLA, nuestro ordenamiento jurídico presenta una serie de carencias ante esta nueva materia, especialmente a nivel de responsabilidad, que deben ser resueltas. Y es que en general el sistema de responsabilidad civil vigente parte de entender que el daño procede de una acción realizada por un ser libre y plenamente consciente

⁴¹ Vid. Libro blanco.

⁴² Navas Navarro, Susana et ali. (2017) op. cit., p.35. Este aprendizaje del que se habla ante la IA hace que no puedan preverse ni anticiparse en la fase de diseño muchos de los riesgos o consecuencias derivados de este uso de la IA, algo a lo que también hizo referencia la Comisión y propone abordar en la futura regulación: vid. Libro Blanco.

⁴³ Vid. pp. 12 y 13 de la Propuesta.

de sus actos (existe culpa) sobre la base de un juicio de previsibilidad y evitabilidad (*sensu contrario*, esto actúa como causa eximente de la responsabilidad),⁴⁴ elementos que en ningún caso se cumplirían ante las acciones desarrolladas por estas inteligencias no humanas. Este nuevo contexto exigiría crear o adaptar los sistemas de responsabilidad civil vigentes y objetivarlos, en estos casos, al máximo.⁴⁵

Una de las mejores opciones sería, en opinión del propio Parlamento Europeo y de la doctrina, la de adaptar la regulación en materia de responsabilidad por productos defectuosos,⁴⁶ superando los obstáculos que *la opacidad, la conectividad y la autonomía de los sistemas imponen a la hora de establecer la trazabilidad de acciones perjudiciales específicas de los sistemas de IA hasta una intervención humana específica*, haciendo responsables a las diferentes personas que participen en toda la cadena de valor que crean, mantienen o controlan el riesgo asociado al sistema de IA.⁴⁷

2.2. Los riesgos generados por la IA y su uso por la Administración Pública

La actual relación entre IA y la Administración Pública debe atenderse desde dos puntos de vista distintos: por un lado, la protección que debe ejercer la Administración de los derechos e intereses generales ante los riesgos de derivados de la IA y, por otro, el propio uso de esa IA por parte de la Administración Pública.

Las previsiones recogidas en la Propuesta de Reglamento en este sentido se limitan a establecer la obligación de cada Estado miembro de designar, por un lado, lo que denomina *autoridad notificante*, que estará encargada de velar por los procedimientos y seguimientos específicos de control de estos sistemas de IA y, por otro, de una autoridad nacional

⁴⁴ Vid. Núñez Zorrilla, María del Carmen (2019): *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*. Madrid: Reus, pp. 21 a 23.

⁴⁵ *Ibidem*, p. 22.

⁴⁶ Vid. Resolución del Parlamento Europeo, de 20 de octubre de 2020, sobre un régimen de responsabilidad civil en materia de inteligencia artificial y Gómez Ligüerre, Carlos et García Micó, Tomás. (2020): “Liability for Artificial Intelligence and other emerging technologies” en INDRET (1), p. 502.

⁴⁷ Resolución del Parlamento Europeo, de 20 de octubre de 2020 op. cit.

competente para la supervisión y seguimiento que controle, de forma objetiva, el cumplimiento de los requisitos exigidos a todos los intervinientes en la cadena de creación y uso de sistemas de IA; en caso de que sea la propia Administración la que haga uso de dichos sistemas, será el Supervisor Europeo de Protección de Datos quien, conforme se establece en la Propuesta, supervise esa actuación.⁴⁸ Las funciones otorgadas a la *autoridad nacional competente* y a la *autoridad notificante* podrán recaer sobre el mismo ente u organismo salvo que el Estado miembro decida lo contrario.⁴⁹

La forma en que se propone ejercer este control supone, para parte de la doctrina, la adopción en esta materia de un principio que, siendo propio del ámbito medioambiental, es gestor de riesgos desconocidos como los que se avecinan con el desarrollo de estas nuevas inteligencias no humanas: estamos haciendo referencia al principio de precaución.⁵⁰ El recurso al principio de precaución sólo se produce en la *hipótesis de riesgo potencial*, de forma que aunque no pueda demostrarse por completo la existencia de un riesgo –en este caso, para la protección de los derechos fundamentales afectados por la IA-, no pueda cuantificarse su amplitud o no puedan determinarse sus efectos debido a la insuficiencia o al carácter no concluyente de los datos científicos, se justificaría la prohibición del uso o puesta en servicio, en este caso, de un sistema de IA.⁵¹ En ningún caso el principio de precaución legitimaría la toma de una decisión arbitraria, sino que permitiría excepcionar en un caso puntual el régimen jurídico vigente y esperar, hasta determinar la existencia o no de un riesgo potencial para los derechos fundamentales, a permitir el uso y distribución del sistema de IA cuestionado.⁵² En todo

⁴⁸ Art. 59 de la Propuesta.

⁴⁹ Arts. 30 y 59.2 de la Propuesta.

⁵⁰ Vid. Cerrillo i Martínez, Agustí (2020): “El impacto de la inteligencia artificial en las Administraciones públicas: estado de la cuestión y una agenda” en Cerrillo i Martínez, Agustí et Peguera Poch, Miquel (Coords.) op. cit. p. 76.

⁵¹ Vid. Comunicación de la Comisión sobre el recurso al principio de precaución, COM (2000) 1 final, de 2 de febrero de 2000.

⁵² Esteve Pardo describe el principio de precaución como «*un estado de excepción declarado por la ciencia*» en Esteve Pardo, José (2009): *El desconcierto del Leviatán. Política y derecho ante las incertidumbres de la ciencia*. Madrid: Marcial Pons, pp. 144 y ss. Dicho esto, para profundizar en la cuestión en referencia exclusiva a los sistemas de IA vid. Boix Palop, Andrés (2020): “Los algoritmos son reglamentos: la necesidad

caso, la Propuesta de Reglamento exigirá que la decisión tomada por la autoridad pública sea recurrible por cualquier legitimado.⁵³

Por otro lado, lo que sí se echa en falta en la Propuesta de Reglamento que analizamos a continuación es una referencia específica al uso de estas inteligencias por parte de los poderes públicos, más allá de la autoridad que ejercerá su control,⁵⁴ debido a los efectos –más importantes aún– que esta actuación podría tener en los derechos fundamentales de los ciudadanos europeos. En España, como ocurre en otros Estados miembros, las Administraciones o poderes públicos tienen reconocida legalmente la facultad de llevar a cabo parte de su actuación de forma automatizada, es decir, sin que medie la decisión humana, lo que da cabida al uso de sistemas de IA por parte de la Administración Pública española.⁵⁵ La cuestión está en que este reconocimiento general no hace referencia a ámbitos concretos de actuación de la Administración y, como se podrá imaginar, el uso de este tipo de sistemas no generaría los mismos riesgos ante procedimientos reglados o discrecionales. En los primeros, aquellos procedimientos en los que existe una solución única una vez atendidos los requisitos correspondientes en cada caso, la principal cuestión estaría, como bien aprecia de la Sierra Morón en que *«el individuo disconforme con el resultado que quiera recurrir el acto correspondiente podrá tener interés en conocer la configuración del algoritmo, así como su correcta aplicación en el supuesto concreto»* y la Administración deba atender dicha reclamación.⁵⁶ Problema distinto surgiría cuando la decisión del órgano público cuente con un margen de apreciación discrecional. En este caso la doctrina presenta más cautelas a la hora de aceptar el uso de la IA; un uso que en opinión de la

de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones” en *Revista de Derecho Público: Teoría y Método* (Vol.1), pp. 223 a 270.

⁵³ Art. 45 de la Propuesta

⁵⁴ Recuérdese el art. 59.8 de la Propuesta.

⁵⁵ En España este es el caso del artículo 41 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

⁵⁶ De la Sierra Morón, Susana (2021): “Control judicial de los algoritmos: robots, administración y estado de derecho” en *Lefebvre* (11 de junio de 2021): <https://elderecho.com/control-judicial-de-los-algoritmos-robots-administracion-y-estado-de-derecho>

mayoritaria debería estar limitado a los casos de discrecionalidad técnica –que no política- y siempre que existiese lo que han denominado una *reserva de humanidad*,⁵⁷ algo que, con otras palabras (habla de *vigilancia humana*) la Propuesta de Reglamento exigiría únicamente para los sistemas de IA de alto riesgo.⁵⁸ Quizás, todo sistema de IA utilizado por el poder público debería ser considerado como de alto riesgo. A este respecto, resulta necesario traer a colación la reciente jurisprudencia del Consejo de Estado italiano en este asunto de la que se deduce que, incluso ante una decisión discrecional podría resultar aplicable la IA siempre y cuando se pudiese mantener un requisito esencial del acto como es la motivación del mismo y esta se haga con transparencia y no discriminación, de forma que podría tener que hacerse público el funcionamiento del algoritmo utilizado para tomar dicha decisión y poder justificarse su resultado.⁵⁹

3. BREVE ANÁLISIS DE LA PROPUESTA LEGISLATIVA PARA REGULAR LA INTELIGENCIA ARTIFICIAL DE LA UNIÓN EUROPEA

La Propuesta para una regulación del Parlamento Europeo y el Consejo por la que se establecen normas armonizadas sobre la inteligencia artificial, en el momento en que se están escribiendo estas líneas, se encuentra en plena tramitación, concretamente en la primera lectura del procedimiento legislativo ordinario.⁶⁰

Dicho lo anterior, tenemos información suficiente como para determinar el carácter y características generales que tendrá esta futura regulación, sin perjuicio de las cautelas que debemos mantener ante los

⁵⁷ Cerrillo i Martínez, Agustí (2020): “El impacto de la inteligencia artificial en las Administraciones públicas: estado de la cuestión y una agenda” en Cerrillo i Martínez, Agustí et Peguera Poch, Miquel (Coords.) op. cit. pp. 80 y 81.

⁵⁸ Vid. art. 14 de la Propuesta.

⁵⁹ La doctrina destaca y analiza sus sentencias nº 2270, de 8 de abril y nº8472, de 13 de diciembre ambas de 2019 vid. Cerrillo i Martínez, Agustí (2020): “El impacto de la inteligencia artificial en las Administraciones públicas: estado de la cuestión y una agenda” en Cerrillo i Martínez, Agustí et Peguera Poch, Miquel (Coords.) op. cit. pp. 81 y 82 o De la Sierra Morón, Susana (2021) op. cit.

⁶⁰ Art. 294 TFUE.

posibles cambios que puedan sucederse a lo largo de la tramitación de la norma.

El primer punto que debemos determinar es que el texto de la Propuesta, aunque habla de *establecer normas armonizadas*,⁶¹ presenta un Reglamento; un Reglamento peculiar. En principio, la Directiva es la norma europea que permite ofrecer una regulación armonizada en los 27, obligando únicamente en cuanto al resultado que deba conseguirse con una determinada regulación, pero dejando a la elección de las autoridades nacionales la forma y el modo de alcanzar esos objetivos.⁶² Un Reglamento, por su parte, impone una regulación unificada en los ordenamientos internos de todos los estados miembros sin dejar, en principio, margen de apreciación o adaptación a los legisladores internos. Lo que ocurre es que, cada vez con más frecuencia, las fronteras entre las Directivas y los Reglamentos se están disipando, especialmente en materias complejas como las que nos ocupa. A través de estos *nuevos* Reglamentos, la Unión impone *más que unos mínimos* a los Estados miembros, pero les deja a estos cierto margen para desarrollar o adaptar parte del contenido de la norma. Este parece ser el caso de la Propuesta cuyo análisis que nos ocupa. Observamos esta peculiaridad, especialmente, al analizar la entrada en vigor y *aplicación* del futuro Reglamento: de forma excepcional, pues es algo más propio de las Directivas, en el artículo 85 de la Propuesta se distingue entre entrada en vigor y aplicabilidad de la norma; es decir, entre el momento en que la norma despliega obligaciones (para los Estados miembros) y el momento en que es plenamente aplicable y obligatoria, en un momento posterior. Ni siquiera es uniforme la Propuesta en este aspecto: el art. 85 habla de la adquisición de vigencia pasado los 20 días tradicionales de *vacatio legis*, mientras que el contenido de la regulación será plenamente aplicable pasados dos años con carácter general, salvo en aspectos concretos en los que se habla de tres meses o un año.⁶³ Esta práctica es peculiar, pero la

⁶¹ Vid. apartado 2 de la Propuesta, pp. 6 a 8.

⁶² Art. 288 TFUE.

⁶³ Art. 85 de la Propuesta: «*Entrada en vigor y aplicación: 1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea. 2. El presente Reglamento se aplicará a partir de [veinticuatro meses tras la entrada en vigor del Reglamento]. 3. No obstante lo dispuesto en el apartado 2: a) el título III, capítulo 4, y el título IV se aplicarán a partir de [tres meses tras la entrada en*

Unión Europea la viene aplicando precisamente en la regulación de materias conexas a la que nos ocupa como es la Protección de Datos,⁶⁴ lo que otorga también cierta coherencia a este marco normativo liderado por ese Reglamento (UE) 2016/679, de 27 de abril de 2016, general de protección de datos o el más reciente y general Reglamento (UE) 2021/694, de 29 de abril de 2021, por el que se establece el Programa Europa Digital.

La Propuesta organiza, por el momento, al futuro Reglamento en doce Títulos y 85 artículos, con varios Anexos. El contenido se divide entre los dos grandes objetivos que tiene la Unión Europea en esta normativa: tanto ofrecer un escenario en el que uso se los sistemas de IA sea fiable y seguro para los derechos de los ciudadanos europeos (en especial en los Títulos I, II, III, IV, VIII y IX), como garantizar una posición de vanguardia para Europa en esta materia y el establecimiento de ese Mercado Único Digital, provechoso y seguro (Título V, principalmente). De todo ello, merecería mención destacada lo siguiente:

La Propuesta de Reglamento organiza su regulación sobre los sistemas de IA en atención al riesgo que se desprenda de su uso: este puede ser bajo o mínimo, alto o inaceptable. Para los sistemas de IA de bajo riesgo la Propuesta básicamente recomienda que sus proveedores se sumen voluntariamente a los distintos códigos de conducta, códigos de buenas prácticas, que para el resto propone en el art. 69, así como alguna obligación específica de transparencia. En el polo opuesto, en el que encontramos los sistemas de riesgo inaceptable, lo que hace la Propuesta es, directamente, prohibirlos. El art. 5 de la Propuesta recoge las prácticas de IA que estarían prohibidas por la Unión Europea por ser altamente susceptibles de vulnerar valores y derechos fundamentales protegidos por la Unión, así como de ejercer una manipulación general de la población y, especialmente, de sectores más vulnerables.

vigor del presente Reglamento]; b) el artículo 71 se aplicará a partir de [doce meses tras la entrada en vigor del presente Reglamento]. El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro».

⁶⁴ Lo mismo que inmediatamente antes ocurre en el art. 99 del Reglamento (UE) general de protección de datos 2016/679, motivo por el cual se justifica la existencia de la Ley Orgánica española 3/2018: «Entrada en vigor y aplicación: 1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea. 2. Será aplicable a partir del 25 de mayo de 2018. El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro».

El grueso de la regulación recogida por la Propuesta de Reglamento se lo llevan los sistemas de IA de alto riesgo. En general, para poder ser permitidos, deben cumplirse unos fuertes requisitos horizontales durante toda su vida útil (arts. 8 a 15), requisitos específicos impuestos a sus proveedores (arts. 16 a 23 y 25), fabricantes de productos (art. 24), importadores (arts. 26 y 28), distribuidores (arts. 27 y 28) y usuarios (arts. 28 y 29). Dentro de los requisitos generales destacaríamos la que hemos llamado antes *reserva de humanidad*, en definitiva, una vigilancia humana (art. 14) que todo sistema de alto riesgo debe poder permitir. En este sentido, serán esenciales también las previsiones generales sobre las normas, evaluaciones, certificaciones y registro que deberá cumplir todo sistema de IA de alto riesgo para entrar al mercado europeo (arts. 40 a 51).

Dentro de estos sistemas de alto riesgo, la Propuesta de Reglamento parece querer diferenciar, por su uso especial y características, a los sistemas de identificación biométrica remota (aquellos destinados a identificar a personas físicas a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia: art. 3.36); unos sistemas a los que considera en todo caso de alto riesgo y, con carácter general, prohibidos (art. 5.1.d) y 5.2). El uso excepcional de estos sistemas de identificación biométrica estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente (art. 5.3) y sometido a controles especiales de transparencia (art. 52).

El control del cumplimiento de estos requisitos se ejercerá, como ya se ha podido adelantar, por la autoridad pública designada al efecto por cada Estado miembro; aquí hablaríamos de la que el Reglamento denomina *autoridad notificante* (art. 30), que será la encargada de determinar los procedimientos de evaluación oportunos para garantizar el cumplimiento de la norma; también de la *autoridad nacional de supervisión* (art. 59), cuya función será supervisar la aplicación y ejecución del futuro Reglamento, así como representar a su Estado en el Comité Europeo de Inteligencia Artificial, -que se encargará de garantizar la uniformidad en la aplicación del Reglamento en el conjunto de los Estados miembros (arts. 56 a 58)-. Esta función podrá ser ejercida, como ya se ha señalado, por el Supervisor Europeo de Protección de Datos si el sistema de IA de alto riesgo es utilizado por un poder público (art. 59.8). La autoridad nacional de supervisión a su vez también podrá ejercer el cargo de *autoridad de vigilancia del mercado* (art. 63), que será

la encargada de conceder o no la debida autorización para la introducción en el mercado o la puesta en servicio en este de un sistema de IA de alto riesgo. Todas estas decisiones deberán ser susceptibles de recurso (art. 45).

Dicho esto, y al margen de las obligaciones de seguimiento habituales (Título VIII), de las sanciones previstas por su incumplimiento (Título X) y de las medidas en favor de la innovación en materia de IA (Título V) -segundo gran objetivo, recordemos, de este marco normativo-, resta por destacar una característica más de la Propuesta de Reglamento como es su firme voluntad de ofrecer una regulación *que resista al paso del tiempo*. En el contexto en el que se encuentra esta tecnología, de rapidísima evolución, es importante ofrecer un marco jurídico capaz de adaptarse con la máxima inmediatez a esos cambios, pues ello ofrece seguridad jurídica. Este es el papel que juegan los Anexos al Reglamento, cuyo contenido está preparado para que la Comisión periódicamente lo revise y adapte conforme se sucedan los avances tecnológicos.

BIBLIOGRAFÍA

Ai Hleg (2019): *A definition of AI: main capabilities and disciplines*. Brussels: European Commission.

Boix Palop, Andrés (2020): “Los algoritmos son Reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones” en *Revista de Derecho Público: Teoría y Método* (Vol.1), pp. 223 a 270.

Sáiz, Carlos (Coord.): (2017) *Código de buenas prácticas en protección de datos para proyectos de Big Data*. Madrid: AEPD e ISMS Forum.

Cerrillo i Martínez, Agustí et Peguera Poch, Miquel (Coords.) *Retos de la inteligencia artificial*. Cizur Menor: Aranzadi.

Cotino Hueso, Lorenzo (2019) “Riesgos e impactos del big data, la inteligencia artificial y la robótica. Enfoques, modelos y principios de la respuesta del derecho” en *RGDA* (nº 50), 37 pp.

De la Sierra Morón, Susana (2021): “Control judicial de los algoritmos: robots, administración y estado de derecho” en *Lefrebre* (11 de junio de 2021): <https://elderecho.com/control-judicial-de-los-algoritmos-robots-administracion-y-estado-de-derecho>.

Esteve Pardo, José (2009): *El desconcierto del Leviatán. Política y Derecho ante las incertidumbres de la ciencia*. Madrid: Marcial Pons.

Fanni, Simona (2020): “La inteligencia artificial y el cuerpo humano digital: a la búsqueda del habeas data” en *Ius et Scientia* (Vol. 6, nº 2), pp. 200 a 224.

García García, Sara (2021): "Construcción y aplicación de la llamada Ley Europea del Clima: el paso definitivo hacia la neutralidad climática y la energía verde en la Unión Europea". *La Ley. Unión Europea* (27), pp.

Gómez Ligüerre, Carlos et García Micó, Tomás (2020): “Liability for Artificial Intelligence and other emerging technologies” en *INDRET* (1).

Navas Navarro, Susana et ali. (2017): *Inteligencia artificial. Tecnología y derecho*. Valencia: Tirant lo Blanch.

Núñez Zorrilla, María del Carmen (2019): *Inteligencia artificial y responsabilidad civil. Régimen jurídico de los daños causados por robots autónomos con inteligencia artificial*. Madrid: Reus.

Ottolia, Andrea (2018): *Derecho, big data e inteligencia artificial*. Valencia: Tirant lo Blanch.

Rouhiainen, Lasse (2018): *Inteligencia artificial. 101 cosas que debes saber hoy sobre nuestro futuro*. Barcelona: Alienta Editorial.