Revista de Derecho Civil
http://nreg.es/ojs/index.php/RDC
ISSN 2341-2216
vol. XII, núm. 3 (julio-septiembre, 2025)
Estudios, pp. 175-206

ENTRE LA INNOVACIÓN Y EL DERECHO: LA ADECUACIÓN DE LOS *DEATHBOTS* AL REGLAMENTO DE IA

Idoia Landa Reza
Profesora Ayudante Doctora de Derecho Civil
Universidad del País Vasco

TITLE: *Between innovation and law: the compliance of deathbots with the ai act*

RESUMEN: La inmortalidad ha constituido uno de los sueños de toda sociedad. Con la llegada de la inteligencia artificial se crea una batalla entre la naturaleza humana y la ficción, pero también entre la innovación y el derecho. En este contexto, cabe preguntarse si la creación de *deathbots* o avatares mediante el volcado de datos de las personas fallecidas, con el objetivo de simular su permanencia en la tierra, respeta el contenido del reglamento europeo de inteligencia artificial. Así, se evaluará si, en función de la clasificación del reglamento, esta práctica debe ser prohibida o, por el contrario, puede estar permitida bajo ciertos parámetros. Este trabajo, por tanto, se centrará en estudiar las implicaciones jurídicas de emular una conversación con un difunto.

ABSTRACT: *Immortality has been one of the dreams of every society. With the arrival of artificial intelligence, a battle is created between human nature and fiction, but also between innovation and law. In this context, it is worth asking whether the creation of deathbots or avatars by dumping data of deceased people, with the aim of simulating their permanence on earth, respects the content of the European artificial intelligence regulation. Thus, it will be evaluated whether, based on the regulation's classification, this practice should be prohibited or, on the contrary, allowed under certain parameters. This work will therefore focus on studying the legal implications of emulating a conversation with the deceased.*

PALABRAS CLAVE: *robot póstumo*, protección de datos personales, inteligencia artificial, duelo.

KEY WORDS: *deathbots, data protection, artificial intelligence, grief.*

---

1. INTRODUCCIÓN

El avance de la inteligencia artificial[1], comúnmente conocida como IA, ha hecho posible

[1] En palabras de BARRIO ANDRÉS, la inteligencia artificial es sin duda el habilitador por excelencia en la transformación digital y su potencial es enorme. En este mismo sentido, HERRERA DE LAS HERAS remarca que el mundo del Derecho ha de prevalecer vigilante para poder adecuar las normas actuales a las nuevas circunstancias y necesidades. Véanse al respecto: BARRIO ANDRÉS, Moisés, *Manual de derecho digital*, Tirant lo Blanch, Valencia, 2024, p. 74; HERRERA DE LAS HERAS, Ramón, *Aspectos legales de la inteligencia artificial. Personalidad jurídica de los robots, protección de datos y responsabilidad civil*, Dykinson, Madrid, 2022, p. 11.

que se puedan crear representaciones digitales que simulan la presencia de una persona fallecida a partir de datos, videos y mensajes recopilados durante su vida. No se trata de ciencia ficción, sino una realidad. Estos avatares o *deathbots*, permiten que una representación digital del difunto continúe interactuando con sus seres queridos, emulando su voz y su personalidad.

Aunque el término «avatar» parezca reciente y haga recordar una película taquillera de los últimos años, su origen se encuentra en el hinduismo (del sánscrito *avatāra* cuyo significado es el «descenso»), y se refiere a la encarnación divina en la tierra. Se utiliza para describir la forma física que una deidad adopta para descender (de ahí el nombre del concepto) al mundo terrenal con el propósito de restaurar el *dharma* (el orden cósmico, la rectitud) y combatir las fuerzas del *adharma* (el caos o el desorden)[2].

Así, se trata de la manifestación de una deidad en el mundo terrenal, un descenso de lo divino a lo material para cumplir un determinado propósito. En lo que respecta al ámbito digital, un avatar es la representación gráfica de una persona en un entorno virtual[3]. A modo de metáfora, podría decirse que al igual que los dioses adoptan una forma física con el fin de interactuar con los humanos, los usuarios pueden crear su representación digital con el objetivo de relacionarse en el mundo online. Sin perjuicio de lo anterior, hoy en día no es necesario que la persona en cuestión esté viva, también se puede realizar un avatar de una persona ya fallecida.

Por su parte, el concepto *deathbot* es el resultado de sumar la palabra *death* (muerte el inglés) y *bots* (que a su vez proviene de la palabra «robot», aplicaciones informáticas que efectúan automáticamente tareas en Internet, imitando así el comportamiento humano). Asimismo, es común emplear el término *griefbot*, una combinación de las palabras *grief* («dolor») y *bot* (abreviatura de «robot»), haciendo referencia explícita al posible uso de estos sistemas de inteligencia artificial como herramienta para aliviar el sufrimiento de los familiares en el proceso de duelo. Si bien el término *bot* (en singular) o *bots* (en plural) no esté tan interiorizado en la sociedad actual, sí que lo está una vertiente suya: los *chatbots*. Los *chatbots* son un tipo de *bot* que han sido creados para mantener una «conversación» con los humanos[4].

En pocas palabras, el presente término hace referencia al hecho de mantener una

[2] Véase al respecto: MCENTEE, Rory, *Theology without walls. An interspiritual approach*, en M. JL., *Theology without walls*, Routledge, Nueva York, 2020.
[3] RAE, avatar. Disponible en: https://dle.rae.es/avatar
[4] KURPICZ-BRIKI, Mascha, *More than a chatbot. Language models demystified*, Springer, Cham, 2023, p. 2.

conversación con un sistema de inteligencia artificial que emula ser una persona ya fallecida, pudiendo nombrarse como robots póstumos o simuladores de identidad. Con el objetivo de ampliar su clasificación desde una perspectiva técnica, se ha de introducir el concepto de la Inteligencia Artificial Generativa (*generative AI* o *GENAI*), un campo de la IA que crea nuevo contenido tras ser entrenado con grandes cantidades de datos. Justamente, el término «generativa» se refiere a la capacidad de la IA para producir resultados novedosos en lugar de simplemente reproducir, categorizar, procesar y analizar entradas. Puede generar cualquier cosa desde imágenes, audio y vídeos, hasta texto en lenguaje natural e incluso codificación informática[5].

A su vez, dentro de la categoría de IA generativa, se identifica el subgrupo grandes modelos de lenguaje (*Large Language Models* o LLMs), son un subtipo de IA generativa especializados en comprender y generar texto. Estos modelos avanzados de inteligencia artificial son diseñados para comprender y generar texto en lenguaje natural[6] basándose en redes neuronales profundas. Por tanto, imitan la actividad humana en términos de comprensión y generación de texto[7]. Los *deathbots* no son un modelo de lenguaje en sí mismo, pero se pueden basar en los grandes modelos de lenguaje para operar. Se trata de un sistema de IA generativa que emula la personalidad de una persona fallecida, basándose en grandes cantidades de datos y redes neuronales que imitan el funcionamiento de la mente humana.

Aunque estos sistemas utilizan modelos de IA generativa, su aplicación está restringida a un propósito específico: emular conversaciones con personas fallecidas**.** Esto los diferencia de los modelos de uso general[8] como *ChatGPT*[9] o *Gemini*, que tienen aplicaciones más amplias. Los modelos de uso general son versátiles y pueden aplicarse

[5] KA YUK CHAN, Cecilia, y COLLOTON, Tom, *Generative AI in higher education. The ChatGPT effect*, Routledge, Nueva York, 2024, p. 9.

[6] PAASS, Gerhard y GIESSELBACH, Sven, *Foundation models for natural language processing: pre-trained language models integrating media*, Springer, Cham, 2023, p. 33.

[7] En este sentido: KUCHARAVY, Andrei; PLANCHEREL, Octave; MULDER, Valentin; MERMOUD, Alain y LENDERS, Vicent, *Large language models in cybersecurity. Threats, exposure and mitigation*, Springer, Cham, 2024, p. 3.

[8] Según el Considerando 95 del RIA, el concepto de modelos de IA de uso general debe definirse claramente y diferenciarse del concepto de sistemas de IA con el fin de garantizar la seguridad jurídica. La definición debe basarse en las características funcionales esenciales de un modelo de IA de uso general, en particular la generalidad y la capacidad de realizar de manera competente una amplia variedad de tareas diferenciadas.

[9] Véase al respecto: SEJNOWSKI, Terry, *ChatGPT and the future of AI: the deep language revolution*, The Mit press, Cambridge, Massachusetts, 2024; VAN DER SLOOT, Bart, *Regulating the synthetic society. Generative AI, Legal questions and societal challenges*, Hart Publishing, Oxford, 2024, p. 15.

en múltiples contextos[10], mientras que los *deathbots* están diseñados para un propósito concreto.

En lo que respecta al funcionamiento de estos sistemas, de un modo simple puede indicarse que el mismo usuario de la aplicación realiza un volcado de información de la persona fallecida. Los programas son «alimentados» por videos, audios, mensajes y otros datos que permitan crear la representación digital más real del difunto[11]. Estos datos son procesados y utilizados para entrenar un modelo de IA que identifica patrones en la escritura, el tono, el vocabulario, las expresiones y hasta los emoticonos que solía utilizar.

Tras el volcado de datos que realiza el mismo usuario, el sistema de IA aprende cómo la persona fallecida estructuraba sus pensamientos, cómo respondía en diferentes contextos y qué tipo de frases utilizaba con mayor frecuencia. Utilizando técnicas de procesamiento del lenguaje natural, el sistema interpreta las preguntas o comentarios del usuario y genera respuestas que imitan la forma en que la persona fallecida probablemente habría respondido. También es posible copiar el patrón que seguía la voz del fallecido. A partir de grabaciones de voz, el sistema puede recrear su tono y modulación, permitiendo que las respuestas del *chatbot* no solo sean escritas, sino también habladas. Esto crea una experiencia aún más inmersiva y emocionalmente impactante para el usuario.

El caso de *Meeting You* es uno de los ejemplos más conocidos del uso de la inteligencia artificial para emular interacciones con personas fallecidas. Presentado en un documental surcoreano de 2020, relata la experiencia real de Jang Ji-sung, una madre que, a través de la realidad virtual, pudo «reencontrarse» con su hija Nayeon, fallecida en 2016. Mediante técnicas avanzadas de modelado 3D e inteligencia artificial, los desarrolladores crearon un avatar sorprendentemente realista que imitaba su voz, gestos y expresiones, ofreciendo una experiencia profundamente inmersiva y conmovedora. Mientras algunos lo consideraron una vía para la sanación emocional, otros advirtieron sobre los riesgos de prolongar el sufrimiento y la falta de consentimiento del fallecido.

[10] PRESNO LINERA destaca a los modelos fundacionales (actualmente modelos de IA generativa) como la gran novedad de Reglamento de Inteligencia Artificial, ya que su regulación no estaba prevista ni en la propuesta de la Comisión ni en la orientación general del Consejo. Véase: PRESNO LINERA, Miguel Ángel, «La propuesta de Ley de Inteligencia Artificial Europea», *Revista de las Cortes Generales* (2023), núm. 116, p. 114.

[11] O'CONNOR, Mórna y KASKET, Elaine, «What grief isn't: Dead grief concepts and their digital-age revival», en M.T.; B.C.; A.S; y G. J. (Eds.), *Social media and technology across the lifespan,* Springer Nature, Nueva York, 2022, pp. 115-130.

Aunque el presente es un trabajo jurídico y no una reflexión filosófica, resulta esencial abordar los dilemas éticos y humanos, ya que su comprensión es fundamental para realizar un análisis jurídico exhaustivo de la adecuación de los deathbots al Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) [12], en adelante RIA. En este sentido, la creación y puesta en el mercado de estos sistemas puede interpretarse como una forma de comercialización del dolor y el sufrimiento humano o, dicho de otra manera, la capitalización del luto. Las empresas que desarrollan estas tecnologías ofrecen a los familiares la posibilidad de «mantener vivos» a sus seres queridos de forma virtual, lo cual podría interpretarse como una explotación económica del proceso de duelo. Esto es, un modelo de negocio basado en la prolongación del duelo[13].

Las empresas que desarrollan estas tecnologías pueden beneficiarse de la debilidad de quienes atraviesan una pérdida, ofreciendo servicios que, lejos de facilitar la aceptación de la muerte, pueden perpetuar la dependencia emocional y comercial del usuario. Nadie quiere experimentar la pérdida por segunda vez, y estos avatares o *deathbots*, al imitar la forma de hablar, la personalidad, la voz o los gestos del fallecido, pueden generan un apego prolongado que interfiera con el proceso natural del duelo. En lugar de ayudar a aceptar la ausencia, estas simulaciones pueden atrapar a los usuarios en una relación ilusoria, dificultando el cierre emocional y fomentando una conexión que nunca se rompe del todo.

Además de la dependencia emocional derivada de la interacción con estas tecnologías, se crea una dependencia hacia la empresa que ofrece dicho servicio. Estas empresas introducen un esquema de monetización basado en la suscripción, donde el acceso a la representación virtual de un ser querido está condicionado a pagos recurrentes. Por ende, el duelo deja de ser un proceso íntimo y personal para convertirse en un

[12] DOUE núm. 1689, de 12/07/2024.

[13] El luto se divide en cinco etapas: negación, ira, negociación, depresión y aceptación. En la etapa de la negación, la persona se resiste a aceptar la realidad de la pérdida. La mente crea una barrera protectora para evitar enfrentar el dolor de manera inmediata. En este contexto, interactuar con una simulación de una persona fallecida prolongaría la presente etapa. La tecnología ofrece una presencia artificial del fallecido, lo cual puede retrasar, en la mayoría de los casos, la aceptación de la muerte. Véase al respecto: KLÜBER-ROSS, Elisabeth y KESSLER, David, *Sobre el duelo y el dolor*, Luciérnaga Cas, Barcelona, 2016.

mercado. La memoria del fallecido se transforma en un bien comercializable, sujeto a estrategias de fidelización que explotan la fragilidad emocional del usuario.

La frontera entre lo que es éticamente aceptable y lo inaceptable se difumina cuando las emociones humanas y la tecnología se mezclan de esta forma. Lo que podría ser percibido como un consuelo momentáneo, puede transformarse en una distorsión de la percepción de la realidad. En el documental «La inmortalidad artificial» de la cineasta ANN SHIN se plantea si es posible, o incluso deseable, alcanzar una forma de inmortalidad mediante la inteligencia artificial[14]. La propuesta se sitúa en un punto de confluencia entre el progreso tecnológico y la naturaleza humana, cuestionando las consecuencias de intentar trascender los límites biológicos que definen nuestra existencia.

Según queda reflejado, aunque esta tecnología parece ofrecer una solución a la finitud, en realidad no es más que una simulación, lo que pone en evidencia la brecha entre lo humano y lo artificial. Intentar trascender las limitaciones de las personas a través de máquinas puede resultar deshumanizante, pues nuestra identidad está definida por la mortalidad, la vulnerabilidad y el sentido que estas otorgan a la vida. El documental también advierte sobre los efectos de la simulación de personas fallecidas en el proceso de duelo. Así, se indica que, aunque esta tecnología puede brindar consuelo temporal, corre el riesgo de prolongar innecesariamente la aceptación de la pérdida, dificultando el cierre emocional y la adaptación a la ausencia.

Este fenómeno suscita diversas preguntas jurídicas y éticas acerca del uso y control de los datos en un contexto que va más allá de la vida física del individuo, así como el impacto psicológico de esta emulación en quienes interactúan con ella. En primer lugar, es fundamental esclarecer si la normativa de protección de datos personales autoriza a los familiares del difunto a utilizar los datos del fallecido para llevar a cabo su emulación digital. Asimismo, es necesario evaluar la compatibilidad de los *deathbots* con el RIA, que establece un marco normativo para el uso de sistemas de IA. Para ello, se analizará en qué tipología de sistema de IA se encuentran: sistemas prohibidos, sistemas de alto riesgo, sistema de riesgo limitado, sistemas de riesgo mínimo o IA generativa.

En este sentido, surge la pregunta de si la creación y utilización de *deathbots* debe quedar bajo la responsabilidad de los individuos que, guiados por sus propios intereses

[14] SHIN, Ann, «La inmortalidad artificial», disponible en: https://www.youtube.com/watch?v=s8RayNMLQBA

y deseos, deciden preservar la imagen de un ser querido, o si, por el contrario, es necesario establecer límites regulatorios que protejan la integridad emocional y psicológica de los posibles usuarios. Es decir, si su uso debe quedar a la merced de la responsabilidad individual o si, por el contrario, debe ser regulado estrictamente, e incluso prohibido, como medida de protección.

2. APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES

Si bien la personalidad jurídica se pierde con la muerte, el fallecimiento de la persona no hace que los datos personales de la misma desaparezcan. En el mismo sentido, la huella digital perdura tras la muerte. Este hecho platea varios problemas. Por una parte, la problemática relativa a la protección de datos personales del fallecido; por otra, la relativa a la gestión y destino *mortis causa* de su contenido digital[15].

Aunque el Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos o RGPD)[16], manifiesta que la norma no es de aplicación para la protección de datos personales de las personas fallecidas, los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas[17]. Es en este contexto donde entra en juego la normativa española, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)[18].

La LOPDGDD regula las citadas materias en dos artículos distintos: los datos personales en el artículo 3 (dentro del Título 1 «disposiciones generales») y el contenido digital en el artículo 96 (dentro del Título X «garantías de los derechos digitales»)[19]. Dado que el derecho a la protección de datos personales es un derecho fundamental recogido en el artículo 18.4 de la CE, su regulación se realiza mediante una ley orgánica.

En base al artículo 3 de la LOPDGDD, las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse al responsable o

[15] PÉREZ VALLEJO, Ana María y VIVAS TESÓN, Inmaculada, *La transmisión mortis causa del patrimonio intelectual y digital*, Aranzadi, Pamplona, 2022, p. 213.
[16] DOUE L 119/1, de 04/05/2016.
[17] Considerando 27 del RGPD.
[18] BOE núm. 294, de 06/12/2018.
[19] Como el derecho a la protección de datos personales es un derecho fundamental y exige ley orgánica, el artículo 3 LOPDGDD tiene tal carácter, mientras que el artículo 96 LOPDGDD se considera ley ordinaria (Disposición final 1ª LOPDGDD).

encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión salvo que el interesado haya realizado una manifestación contraria en vida. Es decir, se contempla la posibilidad de que los familiares, herederos o pareja del fallecido puedan acceder a esos datos en los casos en que el fallecido no haya dejado instrucciones claras al respecto. Por tanto, el citado artículo se centra en el acceso a los datos personales del difunto, no en su transferencia o uso posterior.

Por su parte, el artículo 96 de la LOPDGDD se refiere al acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas, esto es, a la gestión de los contenidos digitales tras el fallecimiento del interesado[20]. Los servicios de la sociedad de la información representan una actividad por vía electrónica y normalmente a cambio de una prestación económica. En base al artículo 2.b) de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)[21], cualquier persona física o jurídica que suministre un servicio de la sociedad de la información es un prestador de servicio. Así, por ejemplo, los motores de búsqueda o las redes sociales se clasifican dentro de la indicada definición.

En relación con los contenidos digitales, estos no se limitan a ser bienes en su sentido tradicional, ya que la actividad del usuario en la red puede tener tanto un valor patrimonial como no patrimonial. Desde el momento en que se accede a Internet, se deja un rastro que evidencia la presencia en el entorno digital, reflejando distintos aspectos de la identidad y actividad del usuario[22].

El término «contenido digital» se puede utilizar para describir archivos (por ejemplo, archivos alojados en servicios de alojamiento en la nube), sitios web, dominios, criptomonedas, cuentas electrónicas (banca online o servicios de pago), cuentas de correo electrónico, cuentas de redes sociales y servicios de suscripción (como las cuentas de *Netflix*, *HBO* o *Spotify*). En cuanto a los archivos, la norma alude exclusivamente a aquellos contenidos digitales que estén siendo gestionados por

[20] MARTÍNEZ MARTÍNEZ, Nuria, «Reflexiones en torno a la protección *post mortem* de los datos personales y la gestión de la transmisión mortis causa del patrimonio digital tras la aprobación de la LOPDGDD», *Derecho Privado y Constitución* (2019), núm. 35, pp. 178 y 207.
[21] DOUE núm. 178, de 17 de julio de 2000.
[22] NAVAS NAVARRO, Susana, «Herencia y protección de datos de personas fallecidas: a propósito del mal denominado testamento digital», *Revista de derecho privado* (2020), núm. 1, p. 64 y ss.

prestadores de servicios de la sociedad de la información, por lo que se entiende que los archivos deben de estar en la nube, no en un soporte físico[23]. Los haberes digitales susceptibles de valoración económica son parte del caudal relicto. En cambio, el contenido digital de carácter personal queda excluido de la herencia[24].

En base al citado artículo 96 de la LOPDGDD, podrán acceder a contenidos digitales gestionados por prestadores de servicios de la sociedad de la información de la persona fallecida: las personas vinculadas al fallecido por razones familiares o de hecho y sus herederos; el albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello; en el caso de los menores sus representantes legales o, en el marco de sus competencias, el Ministerio Fiscal; y, en el caso de que el fallecido fuese una persona con discapacidad, el designado para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo que prestase.

En este sentido, CÁMARA LAPUENTE se ha manifestado en contra de la amplia legitimación que otorga la normativa por defecto, siendo preferible que la legitimación para ejercer esas facultades provenga del difunto[25]. Siguiendo esta línea, GINEBRA MOLINS afirma que permitir la intervención concurrente de tantas personas legitimadas *ex lege* identificadas de manera tan imprecisa e indeterminada, bastando un vínculo con el fallecido por razones familiares o de hecho salvo prohibición expresa, y con facultades tan amplias puede resultar excesivo. Por ello, la autora defiende la regla de no acceso[26].

Como se viene indicando, tanto el artículo 3 como el artículo 96 de la LOPDGDD se refieren a un acceso *post mortem* (a datos personales o contenido digital del difunto), pero no establecen un marco para el volcado de dichos datos o dicho material a terceras empresas. Los dos artículos objeto de análisis legitiman automáticamente a ciertas personas para acceder a los datos personales o contenido digital de la persona fallecida, pero no realizan ninguna referencia sobre su posible transferencia.

[23] MORALEJO IMBERNÓN, Nieves, «El testamento digital en la nueva Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales», *Anuario de derecho civil* (2020), p. 255.
[24] PÉREZ VALLEJO, Ana María y VIVAS TESÓN, *La transmisión mortis causa del patrimonio intelectual y digital*, *op*. *cit*., p. 635.
[25] CÁMARA LAPUENTE, Sergio, «La sucesión mortis causa en el patrimonio digital», *El notario del siglo XXI* (2019), núm. 84, pp.421-422.
[26] GINEBRA MOLINS, María Esperança, «Voluntades digitales: disposiciones mortis causa», en AA.E. y CL.S., *El derecho privado en el nuevo paradigma digital*, Dykinson, Madrid, 2020. pp. 233-234.

Esta diferencia en el contenido resulta especialmente relevante en el contexto de los *deathbots*, dado que en esta práctica el usuario ya cuenta con los datos personales del difunto. No accede, sino que es el encargado de realizar el volcado de la información personal a la empresa creadora del sistema de inteligencia artificial, quién posteriormente alimentará al sistema de IA con el objetivo de crear la versión digital de la persona fallecida.

En otras palabras, el usuario no está solicitando acceso a los datos del difunto a una entidad o sistema, sino que ya posee dichos datos, que podrían ser la información personal almacenada en archivos o incluso contenidos previos de interacciones con la persona fallecida como los mensajes de un chat. En este escenario, el usuario actúa como responsable del volcado de esa información a la empresa desarrolladora del sistema de inteligencia artificial, en lugar de depender de un acceso regulado o autorizado a esos datos. Esta práctica carece de un marco normativo específico en la LOPDGDD.

Este hecho refleja una dinámica diferente, el usuario no está accediendo directamente a los datos de la persona fallecida bajo la voluntad del difunto o los términos de la ley, sino que los está proporcionando directamente a la empresa, lo cual cambia la perspectiva jurídica. El usuario realiza un contrato de servicio con la empresa creadora del *deathbot*, para lo cual ha de realizar el volcado de datos del difunto a la misma. En este contexto, la normativa sobre protección de datos podría considerarse insuficiente para cubrir este tipo de situaciones, ya que el control de los datos no se realiza de manera formal por parte de los legitimados, sino por el propio usuario que, en su deseo de recibir una «respuesta» del ser querido, asume un rol proactivo en la transferencia y uso de dichos datos.

La creación de la representación digital del difunto que implique un volcado de sus datos personales no está explícitamente contemplada en la normativa de protección de datos personales. En consecuencia, en lo que concierne a la transferencia de los datos tras el fallecimiento del titular, nos encontramos ante un claro vacío normativo, lo que genera incertidumbre e inseguridad jurídica. Todo ello refleja la necesidad de crear un marco jurídico que regule de manera expresa el destino de los datos personales tras el fallecimiento del titular de estos.

Sin perjuicio de lo anterior, no debe quedar en el olvido que con esta práctica también se realiza un tratamiento de los datos personales del usuario del sistema de IA. Es este

usuario final quien crea la cuenta que permite utilizar el sistema, por tanto, también se realiza un tratamiento de sus datos personales[27]. Por ello, se ha de respetar el contenido de la normativa de protección de datos personales. La base legal que se sigue para realizar este tratamiento es precisamente el consentimiento del usuario del sistema de IA. Así, el proveedor del *griefbot* debe solicitar el consentimiento tras informar adecuadamente, entre otras cuestiones, sobre la finalidad del tratamiento y sus derechos al usuario.

Para la creación de la cuenta, el usuario deberá proporcionar una serie de datos personales corrientes, como su nombre y dirección de correo electrónico. El tratamiento de esta información se basa en el artículo 6 del RGPD. En este caso, la justificación legal aplicable sería el consentimiento del usuario (artículo 6.1.a) del RGPD) o la ejecución de un contrato en caso de que la plataforma requiera estos datos para la prestación del servicio (artículo 6.1.b) del RGPD).

No obstante, el propósito principal del sistema es permitir que el usuario recree conversaciones con un ser querido fallecido. En este contexto, es previsible que el usuario comparta una gran cantidad de datos personales de carácter sensible, como información sobre su salud o creencias religiosas. Estos datos pertenecen a las categorías especiales de datos personales definidas en el artículo 9 del RGPD, cuyo tratamiento está generalmente prohibido, salvo que se cumpla una excepción específica. Dado que la recopilación y procesamiento de estos datos sensibles es inherente al funcionamiento del sistema, la base legal aplicable deberá ser el consentimiento explícito del artículo 9.2.a) del RGPD. Asimismo, la plataforma deberá adoptar medidas de seguridad adecuadas para proteger la información sensible proporcionada por el usuario.

3. CLASIFICACIÓN DEL RIESGO SEGÚN EL REGLAMENTO DE INTELIGENCIA ARTIFICIAL

El Reglamento de Inteligencia Artificial de la Unión Europea surgió como una respuesta a la necesidad de establecer un marco legal que regule el desarrollo y uso de la IA de manera segura, ética y transparente. El camino comenzó el 9 de diciembre de 2023 mediante el acuerdo provisional del Consejo de la Unión Europea y el Parlamento Europeo sobre el Reglamento de Inteligencia Artificial[28]. Tras ser adoptado

[27] AGUSTINOY, Albert, «Griefbots: la resurrección artificial del fallecido». Disponible en: https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/griefbots-resurreccion-artificial-fallecidos (última consulta: 30/01/2025).

[28] CONSEJO DE LA UNIÓN EUROPEA., «Reglamento de Inteligencia Artificial: el Consejo y el Parlamento alcanzan un acuerdo sobre las primeras normas del mundo en materia de inteligencia artificial»,

formalmente el 21 de mayo de 2024 por el Consejo de la Unión Europea, el 13 de junio del mismo año se procedió a su firma. Finalmente, se publicó el 12 de julio de 2024 con una *vacatio legis* de veinte días, aunque según el artículo 113, no será del todo aplicable hasta agosto del 2027.

En cuanto a la aplicación territorial del RIA, en base a su artículo 2, es de aplicación a los proveedores que comercialicen o pongan en servicio sistemas de IA en la Unión, independientemente de que dichos proveedores estén establecidos en la Unión o en un tercer país; así como a los usuarios de los sistemas de IA ubicados en la Unión; y a los proveedores y usuarios de sistemas de IA que estén ubicados en un tercer país, cuando el resultado producido por el sistema se utilice en la Unión. Esto es, si el sistema creador de la representación digital del difunto es ofrecido a usuarios en la UE, la normativa europea de IA es de aplicación. Esto se debe a los principios de extraterritorialidad que también se identifica en el RGPD, con estas cautelas se evitan fugas de aplicación derivadas de la deslocalización de proveedores y usuarios[29].

El RIA se centra en los riesgos asociados a su uso, estableciendo un marco normativo que clasifica los sistemas según su nivel de peligro. Tal y como se indicaba en el Libro Blanco sobre Inteligencia Artificial de la Comisión Europea, este enfoque basado en el riesgo resulta importante para asegurar que la intervención reguladora sea proporcionada. Se requiere de criterios claros para establecer diferencias entre las distintas aplicaciones de IA, en especial para determinar si entrañan un riesgo elevado o no. Incluso cuando se considere que una aplicación de IA no entraña un riesgo elevado, esta debe seguir estando sujeta a las normas vigentes en la UE[30].

3.1. *Sistemas de IA prohibidos*

El artículo 5 del RIA es uno de los ejes principales de la norma, dado que fija los límites que la Unión Europea quiere establecer al uso de la inteligencia artificial[31]. El objeto de regulación no es la tecnología en sí, sino los efectos que la misma pueda producir. Quedan proscritos aquellos efectos que atenten contra los intereses y valores humanos

consilium.europa.eu, 9 de diciembre de 2023. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/

[29] GAMERO CASADO, Eduardo, «El enfoque europeo de inteligencia artificial», *Revista de derecho administrativo* (2021), núm. 20, p. 277.

[30] COMISIÓN EUROPEA, «Libro blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza», 2020, p.22. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065

[31] Las prohibiciones han entrado en vigor el 2 de febrero de 2025 (considerando 179 del RIA).

y socaven los principios constitucionales occidentales[32]. Así, la Unión Europea prohíbe determinados usos de una tecnología concreta, cuyos efectos sobre los derechos de las personas se consideran contrarios a los valores y a los postulados éticos en lo que esta se sustenta. Por todo ello, tal y como se refleja en el considerando 26, se considera necesario prohibir determinadas prácticas de IA por no ser aceptables. Estas prácticas se regulan en el indicado artículo 5 en ocho supuestos concretos[33]:

a) Sistemas que se sirvan de técnicas subliminales, manipuladoras o engañosas.

b) Sistemas que exploten la vulnerabilidad de una persona o un determinado colectivo.

c) Sistemas que evalúen o clasifiquen a personas físicas o grupos de personas atendiendo a su comportamiento social, características o personalidad.

d) Sistemas que sirvan para valorar o predecir el riesgo de que una persona física cometa un delito.

e) Sistemas que creen o amplíen bases de datos de reconocimiento facial.

f) Sistemas de reconocimiento de emociones en el trabajo y centros educativos.

g) Sistemas de categorización biométrica para deducir la raza, opinión política, afiliación sindical, convicción religiosa, vida sexual u orientación sexual.

h) Sistemas de identificación biométrica remota en tiempo real en espacios de acceso público.

Aunque sean técnicamente posibles, la ley prohíbe dichos usos, lo cual refleja una postura contraria a dejar todo en manos de una responsabilidad individual. Este enfoque busca equilibrar la innovación tecnológica con la protección de derechos fundamentales, la seguridad y el bienestar público. Por ello, podría manifestarse que la regulación de la inteligencia artificial actúa como un freno a los posibles abusos, reconociendo que ciertos usos pueden ser realmente perjudiciales para los individuos o la sociedad en su conjunto.

Tras realizar el listado de todos los sistemas prohibidos, en lo que respecta a los *deathbots*, es de interés desarrollar la idea de la manipulación. De acuerdo con el considerando 29 del RIA, se entiende por prácticas de manipulación, aquellas técnicas

[32] HERNÁNDEZ RAMOS, Mario, «El marco jurídico regulatorio europeo de la inteligencia artificial. La relación de complementariedad entre el reglamento de la UE y la convención marco del consejo de Europa», *Revista Española de Derecho Europeo* (2024), 92, p. 17.

[33] BARRIO ANDRÉS, Moisés, *Comentarios al Reglamento Europeo de Inteligencia Artificial*, La Ley, Madrid, 2024, pp. 184-185.

que pueden utilizarse para persuadir a las personas de que adopten comportamientos no deseados, o para engañarlas, empujándolas a tomar decisiones de una manera que perjudica su autonomía, su toma de decisiones y su capacidad de elegir libremente. Con dicho objetivo, se utilizan componentes subliminales como estímulos de audio, imagen o vídeo que la persona no pueda percibir, así como otras técnicas manipulativas o engañosas[34].

El reglamento prohíbe los sistemas de IA que puedan alterar la decisión final del usuario a través de sistemas que influyan en su comportamiento, ya sea persuadiéndolo a adoptar conductas no deseadas o induciéndolo a tomar decisiones que, en condiciones normales, no tomaría. Así, el concepto de manipulación del RIA se refiere a las prácticas que modifican la voluntad del usuario mediante técnicas que pueden ser engañosas, coercitivas o persuasivas. En cambio, la interacción con los *dethtbots* no busca modificar las decisiones del usuario. Su función se centra en permitir una interacción emocional con la recreación de una persona fallecida, lo que, si bien puede generar un gran impacto en los sentimientos del usuario, no se alinea directamente con la definición de manipulación establecida en la normativa.

Aun siendo cierto que estos sistemas pueden afectar emocionalmente al usuario, este efecto no es equiparable a la manipulación prohibida por el RIA, dado que el objetivo o efecto no es modificar su voluntad ni inducirlo a elecciones que de otra forma no tomaría. En otras palabras, la manipulación emocional que realizan los *deathbots* al emular una conversación con la persona fallecida no se encuentra dentro de la definición de manipulación de la normativa.

En lo que concierne al concepto de la vulnerabilidad del artículo 5.1.b) del RIA, se prohíbe la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que exponga alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra.

El indicado artículo se refiere a «alguna de las vulnerabilidades», pero en realidad solo contempla la edad, la discapacidad y una situación social o económica específica, una opción legislativa criticable. En este mismo sentido, se ha de hacer referencia expresa a

[34] Ibidem., p. 194.

la «metáfora de las capas», la cual es utilizada para criticar la visión esencialista de la vulnerabilidad (característica inherente a cierto grupo de personas) y defender que se trata de una condición compleja y cambiante. La vulnerabilidad no es una etiqueta fija, las capas superpuestas pueden modificarse según la situación del individuo, ciertas capas pueden ser temporales mientras que otras perduran en el tiempo. La existencia y relación de estas capas hacen que la vulnerabilidad de una persona aumente[35].

Respecto al factor de la edad, ha sido introducido con el objetivo de reflejar la vulnerabilidad de los menores y las personas mayores. Cabría argumentar que, aunque no se mencione explícitamente en el RIA, el factor de la edad también abarca el concepto de la brecha digital[36]. En la mayoría de los casos, la brecha digital afecta a personas mayores que no han crecido en un entorno digital, lo cual les provoca tener más dificultad a la hora de comprender lo que implica utilizar la IA.

En cuanto a la discapacidad como factor de vulnerabilidad, el considerando 29 del RIA indica que el presente concepto ha de interpretarse de acuerdo a la Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los requisitos de accesibilidad de los productos y servicios[37]. El considerando 3 de la indicada directiva hace referencia expresa a la Convención de las Naciones Unidas sobre los Derechos de las Personas con Discapacidad adoptada el 13 de diciembre de 2006, manifestando que dentro del concepto de «personas con discapacidad» se incluyen a aquellas que tengan deficiencias físicas, mentales, intelectuales o sensoriales a largo plazo que, al interactuar con diversas barreras, puedan impedir su participación plena y efectiva en la sociedad, en igualdad de condiciones con las demás.

Comúnmente se identifican cuatro tipos de discapacidad: discapacidad física o motora (movilidad reducida o enfermedades motoras), discapacidad sensorial (problemas sensoriales como trastornos oculares o auditivos), discapacidad intelectual (limitaciones en las funciones mentales). La definición de discapacidad abarca desde pequeñas dificultades en el funcionamiento hasta grandes impactos en la vida de una persona[38]. Cada situación de discapacidad es única, por ser el resultado de diversos factores (contexto físico, mental, cultural y social de cada persona). No se trata

[35] LUNA, Florencia, «Elucidating the concept of vulnerability: Layers not labels», *International journal of feminist approaches to bioethics*, vol. 2, (2009), núm.1, p. 121.
[36] Véase al respecto: SÁNCHEZ VALLE, María y ABAD ALCALÁ, Leopoldo (coord.), *Mayores (des) conectados. Estudio sobre la brecha digital*, Dykinson, Madrid, 2024.
[37] DOUE núm. 151, de 07/07/2019.
[38] ORGANIZACIÓN MUNDIAL DE LA SALUD, «Informe mundial sobre la discapacidad», 2011, p. 48. Disponible en: https://iris.who.int/handle/10665/75356

solamente de la condición médica, sino de un fenómeno complejo donde influyen múltiples elementos.

Aplicando la ya citada «metáfora de las capas», la discapacidad se puede visualizar como una superposición de distintos niveles de influencias que afectan a la realidad individual. En el centro se encuentra la persona con su capacidad y limitaciones. A su alrededor, se dibujan diversas capas que van desde el entorno familiar (un entorno seguro que permita el apoyo necesario o la falta de ella) y el entorno físico (como la accesibilidad o la falta de ella) hasta factores legales y culturales (normas, valores o creencias sobre las personas con discapacidad). Por ello, dos personas que cuenten con la misma condición pueden situarse en dos contextos muy diversos. Esta interacción entre las capas que rodean a las personas con discapacidad también influye en su vulnerabilidad frente a la inteligencia artificial, sin embargo, el RIA no hace ninguna referencia al respecto.

La prohibición del artículo 5.1.b) del RIA tiene como objetivo evitar que los sistemas de IA exploten las barreras a las que se enfrentan las personas con discapacidad. Sin embargo, podría manifestarse que, en cuanto a la discapacidad, este apartado se aleja de la idea de la manipulación y el perjuicio, centrándose en dos objetivos: evitar la discriminación y fomentar la accesibilidad a los sistemas de IA. Esto es, por una parte, que las personas no sufran una discriminación algorítmica[39]; y por otra parte, que los desarrolladores de sistemas de IA tomen medidas específicas para hacer que sus productos sean accesibles para las personas con discapacidad[40]. Todo ello resalta la necesidad de diseñar sistemas de IA en base a algoritmos con datos representativos, reflexionar sobre las diversas necesidades de las personas con discapacidad y garantizar la accesibilidad digital.

[39] Existe una relación directa entre los sistemas de IA y los sesgos algorítmicos. Estos pueden surgir de los datos con lo que se entrenan los sistemas o de decisiones tomadas durante su diseño. Los sesgos algorítmicos pueden perpetuar y ampliar desigualdades existentes, afectado a grupos vulnerables. Véase al respecto: ITURMENDI RUBIA, José Miguel, «Inteligencia artificial y derechos humanos. Desafíos y oportunidades en la era digital», *Deusto Journal of Human Rights* (2024), núm. 14, p. 17; En el mismo sentido, VALLE ESCOLANO afirma que la discriminación de las personas con discapacidad producto de la IA y del uso de algoritmos en particular, tiene su origen en datos deficientes y/o poco representativos, o sacados de contexto; en la falta de transparencia de la tecnología (que dificulta detectar los efectos discriminatorios); en la fuerza de las discriminaciones históricas; en la ausencia de puesta en valor de su protagonismo o intervención en multitud de áreas y contextos; y, finalmente, en el incumplimiento de la obligación de realizar ajustes razonables, que incrementa las desventajas para las personas con discapacidad y el consiguiente aumento de su vulnerabilidad. Véase al respecto: VALLE ESCOLANO, Raquel, «Inteligencia artificial y derechos de las personas con discapacidad: el poder de los algoritmos», *Revista Española de Discapacidad*, vol. 11 (2023) núm.1, p. 19.

[40] Véase al respecto: MARTÍNEZ TORÁN, Manuel y ESTEVE SENDRA, Chele, «Accesibilidad digital y discapacidad», *Revista Española de Discapacidad*, vol. 10 (2022), núm.2.

El RIA introduce un último factor de vulnerabilidad: una situación social o económica concreta. Aunque el texto legal no proporciona una definición precisa, el considerando 29 menciona la pobreza o la pertenencia a minorías étnicas o religiosas como ejemplos. La interpretación tradicional del presente término se centra en las condiciones estructurales que afectan a una persona o a un grupo, como la pobreza, la exclusión social o la pertenencia a minorías marginadas. Estas condiciones suelen estar ligadas a factores materiales y sistémicos que limitan el acceso a recursos, oportunidades y derechos.

Siguiendo esta visión tradicional, el luto, situación por la que atraviesa el usuario de los *deathbots*, quedaría fuera del término situación socioeconómica, por tratarse de un estado emocional particular que se deriva de una pérdida, no una condición estructural. En otras palabras, aunque el duelo afecte al bienestar emocional de una persona, en el sentido del RIA no constituye una vulnerabilidad socioeconómica. Por ende, según esta limitada interpretación que parece seguir la normativa, los *griefbots* no podrían ser identificados como sistemas de IA a prohibir. No obstante, podrían explorarse interpretaciones más amplias que consideren el impacto del luto en la vulnerabilidad frente a la IA.

En esta misma línea, se ha defendido que la vulnerabilidad ha de ser interpretada como una característica intrínseca de todas las relaciones entre la IA y los humanos, que se manifiesta dependiendo de las diferentes características de diseño y modos de interacción. Esto es, que la implementación de los propios sistemas de IA puede crear o exacerbar la vulnerabilidad. Debido a factores como el contexto de uso, el modo de interacción, la autonomía del sistema de IA y la apariencia física del sistema pueden contribuir a determinar el grado en que los usuarios pueden volverse vulnerables al interactuar con los sistemas. Por ello, se propone que este significado diferente de vulnerabilidad se integre dentro del concepto de «situación social específica» del artículo 5.1.b) del RIA. Así, no solo se protegería a los grupos tradicionalmente vulnerables, sino que también reconocería otras nuevas formas de vulnerabilidad que nacen de la interacción entre la IA y los seres humanos[41].

Más allá de las características del usuario, es importante destacar la noción de «finalidad o efecto» que introduce el artículo 5.1.b) del RIA. No solo se prohíbe aquél sistema de IA que haya sido diseñado con la idea de alterar el comportamiento humano, sino también aquel que produzca dicho efecto. La norma no requiere que el

[41] GALLI, Federico, y NOVELLI, Claudio, «The many meanings of vulnerability in the AI Act and the one missing», *BioLaw Journal* (2024), núm. 1, p. 71.

sistema de IA tenga el objetivo principal de modificar el comportamiento de una persona con un efecto perjudicial para la misma, es suficiente con conseguir dicho efecto. Por tanto, el artículo 5.1.b) del RIA prohíbe la explotación de la vulnerabilidad con el objetivo o efecto de alterar el comportamiento de manera perjudicial.

Ambos elementos son necesarios para que se considere que un sistema de IA está explotando una vulnerabilidad de una persona o grupo específico: la modificación del comportamiento y perjuicio o riesgo de perjuicio[42]. El sistema ha de tener la finalidad o el efecto de alterar el comportamiento de una persona o un colectivo. Es decir, ha de influir en las decisiones o acciones de la persona o grupo determinado. Esta alteración, debe producir o ser razonablemente probable que produzca un perjuicio. Un claro ejemplo sería un sistema de recomendación de créditos que, tras analizar la vulnerabilidad socioeconómica de una persona (por ejemplo, pobreza y baja educación financiera), personaliza las ofertas para influir su decisión, de una manera que pueda crear un perjuicio significativo como el endeudamiento excesivo.

A diferencia de los sistemas de IA diseñados para manipular el comportamiento financiero de una persona vulnerable, en principio, el propósito de los *deathbots* es distinto[43]. Ahora bien, no cabe duda de que, al interactuar con un sistema que reproduce la forma de hablar o hasta la voz de un ser querido fallecido, el usuario puede sentirse atrapado en una ilusión que no solo prolonga su proceso de duelo, sino que también lo aleja de la aceptación emocional de la realidad. Como resultado, en la práctica, se puede genera una dependencia hacia el producto[44]. Es más, el usuario puede sentir una presión emocional de seguir abonando el servicio para no perder la

[42] En las Directrices éticas para una IA fiable elaborada por el Grupo independiente de expertos de alto nivel sobre inteligencia artificial, se identifican ciertos principios éticos entre los que cabe destacar el principio de prevención del daño. Según se indica, los sistemas de IA no deberían provocar daños (o agravar los existentes) ni perjudicar de cualquier otro modo a los seres humanos. Esto conlleva la protección de la dignidad humana, así como de la integridad física y mental. Todos los sistemas y entornos de IA en los que operan estos deben ser seguros. También deberán ser robustos desde el punto de vista técnico, y debería garantizarse que no puedan destinarse a usos malintencionados. Las personas vulnerables deberían recibir mayor atención y participar en el desarrollo y despliegue de los sistemas de IA. Por tanto, en relación directa con el derecho a la dignidad humana, los sistemas de IA no deben provocar daños ni perjudicar de ningún modo a los seres humanos. Esto conlleva la protección de la integridad física y mental. Véase al respecto: GRUPO INDEPENDIENTE DE EXPERTO DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL, «Directrices éticas para una IA fiable», 8 de abril de 2019. Disponible en: https://digital-strategy.ec.europa.eu/es/library/ethics-guidelines-trustworthy-ai; HERNÁNDEZ LÓPEZ, José Manuel, *Reglamento de inteligencia artificial*, Bosch, Barcelona, 2024, p. 16.

[43] Esta tecnología podría ser utilizada con un fin ilícito que pueda implicar diversas infracciones dentro del Código Penal: la suplantación de identidad (art. 401 del CP) o el fraude (art. 248 y ss del CP), entre otras cuestiones.

[44] FABRY, Regina E. y ALFANO, Mark, «The affective scaffolding of grief in the digital age: the case of deathbots», *Topoi*, vol. 43 (2024), núm. 3, pp. 757-769.

«interacción» con su ser querido, lo que, en última instancia, crearía una manipulación que perjudicaría emocional y económicamente a la persona en cuestión. No ha de quedar en el olvido que la finalidad última de la empresa que proporciona el servicio es la creación de un negocio rentable[45].

Sin perjuicio de lo anterior, aunque puedan generar una dependencia emocional[46] y consecuencias económicas negativas para el usuario, realizando una interpretación estricta del artículo 5 del RIA, actualmente estos sistemas no estarían prohibidos.

3.2. *Sistemas de IA de alto riesgo*

La clasificación de los sistemas de IA de alto riesgo se realiza en el artículo 6 del RIA. Estos sistemas no están prohibidos, pero se sujetan a una serie de restricciones y a mecanismos de control *ex ante* y *ex post* mediante los que garantizar la aplicación efectiva del RIA. Se trata de una luz naranja en el semáforo, se pueden implantar siempre que se reúnan los requisitos que el propio Reglamento establece[47].

Por una parte, el sistema deberá estar destinado a ser un componente de seguridad de un producto que entre en el ámbito del anexo I del RIA o que dicho sistema sea en sí mismo un producto. Por otro lado, existirá la obligación de realizar una evaluación de conformidad antes de su introducción o puesta en servicio en el mercado. Además de dichos sistemas de IA, también se considerarán de alto riesgo los sistemas de IA contemplados en el anexo III[48].

En el indicado anexo se identifican 25 sistemas dentro de ocho distintos ámbitos (biometría; infraestructuras críticas; educación y formación profesional; empleo, gestión de los trabajadores y acceso al autoempleo; acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de estos servicios y prestaciones; garantía del cumplimiento del Derecho, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable; migración, asilo y gestión del control fronterizo, en la medida en que su uso esté permitido por el Derecho de la

[45] En este sentido: ÖHMAN, Carl y FLORIDI, Luciano, «The political economy of death in the afe of information: a critical approach to the digital afterlife industry», *Minds & machines*, vol. 27, núm. 4, pp. 639-662.

[46] LINDEMANN, Nora Freya, «The ethical permissibility of chatting with the dead: Towards a normative framework for Deathbots», *Publications of the Institute of Cognitive Science*, vol. 1 (2022), pp. 52 y 54.

[47] GAMERO CASADO, Eduardo, «El enfoque europeo de inteligencia artificial», *op. cit.*, p. 279.

[48] MIGUEZ MACHO, Luís, y TORRES CARLOS, Marcos, «Sistemas de IA prohibidos y sistemas de IA de alto riesgo», en BA. M., *El reglamento europeo de Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2024, pp. 60-61.

Unión o nacional aplicable; administración de justicia y procesos democráticos).

Ahora bien, no es estrictamente necesario que un sistema de IA esté listado en el Anexo III para ser considerado de alto riesgo en el marco del Reglamento de IA. Lo realmente importante es si el sistema genera un riesgo significativo para la salud, la seguridad o los derechos fundamentales de las personas, independientemente de si está mencionado en el anexo. Este anexo contiene ejemplos específicos de áreas y aplicaciones de IA que se consideran de alto riesgo debido a su impacto potencial. Además de los sistemas ya mencionados en el Anexo III, el resto de los sistemas de IA deberán ser evaluados individualmente para determinar si presentan un riesgo significativo, incluso si no están específicamente mencionados en el anexo.

Esto es, el artículo 6 del RIA no ha de ser interpretado como un *numerus clausus*, sino como un *numerus apertus*. Esto se puede hacer bajo la premisa de que un sistema de IA tiene el potencial de causar un perjuicio a la salud, seguridad o derechos fundamentales de las personas. En base al artículo 7 del RIA, la Comisión Europea tiene la capacidad de modificar y actualizar la lista en función de los riesgos emergentes. Esto implica que no se limita a los ejemplos específicos del Anexo III, sino que permite la inclusión de nuevos sistemas de IA de alto riesgo a medida que se identifican riesgos adicionales para la salud, seguridad o los derechos fundamentales.

En esta misma línea, MIGUEZ MACHO y TORRES CARLOS manifiestan que el RIA no contiene una enunciación taxativa de los sistemas de inteligencia artificial que se consideran de alto riesgo, sino que establece una metodología dinámica para su determinación, basada en remisiones a otras normas y a evaluaciones de riesgo que esos sistemas pueden representar para los derechos fundamentales, la salud y la seguridad[49]. Por ende, la clasificación de un sistema de IA dentro de la categoría de alto riesgo se basa en su potencial para causar un daño al usuario. Un sistema de IA no se considerará de alto riesgo si no presenta un riesgo importante de causar perjuicios a la salud, seguridad o derechos fundamentales[50]. Cuando un sistema de IA afecta negativamente alguno de estos aspectos, debe ser clasificado dentro de esta categoría.

[49] *Ibidem*, p. 61.

[50] Tal y como se manifiestan en las Directrices sobre Inteligencia Artificial y Protección de Datos del Consejo de Europa, la protección de la dignidad humana y la salvaguarda de los derechos humanos y las libertades fundamentales son esenciales al desarrollar y adoptar aplicaciones de IA que puedan tener consecuencias para las personas y la sociedad. Véase al respecto: CONSEJO DE EUROPA, «Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data», 2019. Disponible en: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

El perjuicio a la salud se refiere a los riesgos que un sistema de IA puede representar para la salud física o mental de las personas. En este contexto, la salud mental es un aspecto crucial, especialmente cuando se trata de sistemas de IA que interactúan con usuarios de manera directa. Según la OMS, la salud mental es un estado de bienestar físico, mental, emocional y social, determinado por la interacción del individuo con la sociedad. Se define por las condiciones en las que las personas nacen, crecen, viven, trabajan y envejecen, y no puede considerarse aisladamente de la realización de los derechos humanos y las libertades fundamentales. La salud mental y el bienestar deben abordarse de forma holística, aplicando enfoques multisectoriales que implique, entre otras cuestiones, la aplicación de la ley[51]. Siguiendo esta última afirmación, el RIA también ha de ser interpretado y aplicado teniendo en consideración la salud mental y el bienestar de los usuarios de los sistemas de IA.

Debemos recordar que el derecho a la salud, consagrado en el artículo 25 de la Declaración Universal de Derechos Humanos (DUDH)[52] y el artículo 43 de la Constitución española[53] es un derecho fundamental que posee el siguiente contenido: derecho a la acción del Estado, derecho a las prestaciones sanitarias y derecho a la protección jurisdiccional[54]. Si un sistema de IA atenta contra este derecho fundamental, su clasificación como sistema de alto riesgo no solo será necesaria, sino también una obligación en cumplimiento del marco normativo vigente.

Cuando un sistema de IA es identificado de alto riesgo, el RIA introduce entre los artículos 9 y 15 medidas estrictas para garantizar la seguridad, transparencia y equidad. Estos requisitos abarcan siete aspectos: gestión de riesgos; gobernanza de datos; documentación técnica; conservación de registros; transparencia; supervisión humana; precisión, solidez y ciberseguridad. Según el artículo 8.2 del RIA, los proveedores serán responsables de garantizar que su producto cumpla plenamente todos los requisitos aplicables.

El artículo 9 del RIA obliga a realizar un proceso continuo durante todo el ciclo de vida

[51] ORGANIZACIÓN MUNDIAL DE LA SALUD Y NACIONES UNIDAS., «Salud mental, derechos humanos y legislación. Orientación práctica», 2024, p. 9. Disponible en: https://iris.who.int/bitstream/handle/10665/379200/9789240098169-spa.pdf?sequence=1

[52] *«Toda persona tiene derecho a un nivel de vida adecuado que le asegure, así como a su familia, la salud y el bienestar, y en especial la alimentación, el vestido, la vivienda, la asistencia médica y los servicios sociales necesarios; tiene asimismo derecho a los seguros en caso de desempleo, enfermedad, invalidez, viudez, vejez u otros casos de pérdida de sus medios de subsistencia por circunstancias independientes de su voluntad».*

[53] *«Se reconoce el derecho a la protección de la salud».*

[54] ESCRIBANO COLLADO, Pedro, *El derecho a la salud*, Universidad de Sevilla, Sevilla, 2015, p. 45.

del sistema de IA que requerirá revisiones y actualizaciones sistemáticas con el objetivo de identificar y determinar los riesgos conocidos y otros riesgos que puedan surgir. Cuando los sistemas de IA de alto riesgo utilicen técnicas que impliquen el entrenamiento con datos, estos deberán de cumplir ciertos criterios de calidad. Por otra parte, en base al artículo 11 del RIA, es esencial la gestión y acreditación documental del sistema. En este mismo sentido, se ha de garantizar un nivel de trazabilidad para poder comprobar el funcionamiento del sistema. En cuanto a la obligación de transparencia, los sistemas de IA de alto riesgo deben ser acompañados de instrucciones de uso correspondientes en un formato digital o de otro tipo adecuado, las cuales incluirán información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los responsables del despliegue[55]. El artículo 14 del RIA establece que los sistemas de IA de alto riesgo deben diseñarse y desarrollarse de tal forma que puedan ser vigilados de manera efectiva por personas físicas con la finalidad de prevenir o reducir los riesgos para la salud, la seguridad o los derechos fundamentales. Por último, el artículo 15 del RIA dispone que los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que alcancen un nivel adecuado de precisión, solidez y ciberseguridad[56].

Si se acredita que el uso de los *deathbots* genera o existe una gran posibilidad de que genere un impacto negativo en la salud mental del usuario, creando angustia, confusión o dependencia, el sistema deberá ser clasificado como categoría de alto riesgo incluso si no está explícitamente mencionado en el Anexo III. A pesar de que en este momento no existen pruebas científicas definitivas que demuestren de manera irrefutable el impacto negativo de estos sistemas en la salud mental de los usuarios, debido a que los *deathbots* se acaban de incorporar al mercado, este trabajo, en previsión del posible daño, realiza una interpretación del sistema conforme al RIA. Cabe destacar que esta previsión no debe considerarse como un juicio definitivo, sino como una anticipación jurídica de lo que podría ocurrir.

En relación con los *deathbots*, destacan tres principales medidas: la supervisión humana, la etiqueta de «creado por inteligencia artificial» resultado de la obligación de transparencia y la ciberseguridad. La supervisión humana ha de ser integrada en cada fase del ciclo de vida del sistema, desde su diseño y configuración hasta su despliegue y

[55] En base al considerando 13 del RIA, el concepto de «responsable del despliegue» debe interpretarse como cualquier persona física o jurídica, incluida cualquier autoridad pública, órgano u organismo, que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional.

[56] MIGUEZ MACHO, Luís, y TORRES CARLOS, Marcos, «Sistemas de IA prohibidos y sistemas de IA de alto riesgo», en BA. M., *El reglamento europeo de Inteligencia Artificial*, *op. cit.,* pp. 62-69.

uso continuado, con el fin de prevenir efectos perjudiciales en los usuarios. Este control es el reflejo de la prohibición de llevar a cabo un determinado tratamiento automatizado de datos[57] sin la supervisión humana debido al riesgo que representa el tratamiento[58]. Así, se han de establecer protocolos estrictos para que no generen respuestas manipuladoras o dañinas. Con dicho objetivo, se deben introducir mecanismos de control y auditoría periódicos para detectar y mitigar posibles efectos negativos en la salud mental de los usuarios. Estos controles deben incluir evaluaciones sobre la duración de la interacción, signos de aislamiento social o el duelo patológico o demasiado prolongado en el tiempo, estableciendo criterios claros para la intervención y el ajuste del sistema cuando sea necesario.

En lo que respecta a la ya citada obligación de transparencia, los proveedores[59] del sistema de IA deberán dar al usuario unas instrucciones de uso[60] que incluyan información concisa, completa, correcta, clara, accesible y comprensible antes de comenzar con la interacción. Asimismo, es indispensable que se introduzcan avisos claros en cada interacción con el sistema de IA para recordar al usuario que no está hablando con su ser querido, sino con una construcción basada en datos que el mismo ha aportado al sistema. Esto es, los usuarios deben saber en todo momento que están interactuando con una simulación creada por inteligencia artificial, y no pueden llegar a olvidarlo. No es suficiente con introducir dicho aviso al comienzo de la interacción, debe estar presente en todo momento.

Una forma eficaz de lograr el indicado objetivo es introducir una etiqueta clara y grande en el mismo chat, en ningún modo podrá ser algo sutil o difícilmente apreciable,

[57] En este sentido, el artículo 22 del RGPD recoge el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Aunque el citado artículo hable de derecho, el artículo 22, apartado 1, establece una prohibición general de las decisiones basadas únicamente en el tratamiento automatizado. Por ende, el responsable del tratamiento debe garantizar que cualquier supervisión de la decisión sea significativa, en vez de ser únicamente un gesto simbólico. Véase al respecto: GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, «Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679», 2017. Disponible en: https://www.aepd.es/documento/wp251rev01-es.pdf

[58] OBREGÓN FERNÁNDEZ, Aritz, y LAZCOZ MORATINOS, Guillermo, «La supervisión humana de los sistemas de inteligencia artificial de alto riesgo. Aportaciones desde el Derecho Internacional Humanitario y el Derecho de la Unión Europea», *Revista electrónica de estudios internacionales* (2021), núm. 42, p. 7.

[59] Según el artículo 3.3 del RIA se entiende por proveedor «*una persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente*».

[60] Artículo 3.15 del RIA: «*información facilitada por el proveedor para informar al responsable del despliegue, en particular, de la finalidad prevista y de la correcta utilización de un sistema de IA*».

porque en dicho caso no se estaría respetando la obligación de transparencia. El hecho de que la etiqueta de «creado por inteligencia artificial» o «respuesta generada mediante inteligencia artificial» esté visible constantemente asegurará que los usuarios sean conscientes de la naturaleza de la interacción.

En relación con la ciberseguridad, tal y como se ha manifestado anteriormente, el usuario comparte gran cantidad de datos, de los cuales, un porcentaje significativo corresponde a datos sensibles. Teniendo en cuenta que el usuario pretende recrear una conversación con su ser querido, compartirá con el sistema de IA las novedades de su vida, sus preocupaciones y decisiones a tomar. Toda esta información es de gran interés para los ciberdelincuentes. Por ende, es indispensable adoptar medidas de seguridad robustas que hagan frente a los ciberataques.

El verdadero desafío radica en verificar que los sistemas de IA realmente cumplen con los requisitos establecidos en el RIA, lo cual constituye el núcleo de la evaluación de conformidad. El mismo considerando 125 del RIA indica que es importante desarrollar un procedimiento adecuado de evaluación de la conformidad de los sistemas de IA de alto riesgo en el que participen organismos notificados[61], denominado «evaluación de la conformidad de terceros». No obstante, se limita el alcance de las evaluaciones externas de la conformidad a los sistemas de IA de alto riesgo que no están asociados a productos. Así, el proveedor es quien, por norma general, debe llevar a cabo la evaluación de la conformidad de dichos sistemas bajo su propia responsabilidad, con la única excepción de los sistemas de IA que están destinados a utilizarse para la biometría.

Dicho lo anterior, se identifican dos distintas formas de realizar la evaluación de conformidad de los sistemas de IA de alto riesgo: evaluación interna (autoevaluación realizada por el propio proveedor) y evaluación externa (evaluado por un organismo notificado independiente), siendo destaca la primera por la norma. En palabras de ALKORTA IDIAKEZ[62], aunque esta solución puede agilizar el proceso de cumplimiento, plantea interrogantes sobre su imparcialidad y rigor. Para garantizar la fiabilidad de las autoevaluaciones, es necesario establecer salvaguardias adecuadas, como las inspecciones aleatorias por parte de los organismos de vigilancia, que equilibren la eficiencia con un cumplimiento estricto.

[61] Se entienden por organismos notificados las entidades designadas por los Estados miembros para llevar a cabo la evaluación de conformidad de los sistemas de IA de alto riesgo. El artículo 31 del RIA regula los requisitos relativos a los organismos notificados.

[62] ALKORTA IDIAKEZ, Itziar, «La regulación de los productos sanitarios con Inteligencia Artificial», Tirant lo Blanch, Valencia, 2025, p. 132.

Si bien se ha realizado un esfuerzo significativo en regular los sistemas de IA de alto riesgo, el RIA, al establecer y reforzar la autoevaluación, permite a los proveedores eludir la obligación de llevar a cabo una evaluación de conformidad adecuada. Atendiendo al nivel de riesgo que implican estos sistemas de IA, se debería de optar por la evaluación externa en todo caso o, al menos, como propone acertadamente la autora mencionada, realizar inspecciones aleatorias continuas.

3.3. *Sistemas de IA de riesgo limitado*

Aunque los sistemas de IA son comúnmente clasificados dependiendo de sus riesgos en cuatro categorías (riesgo inaceptable, alto riesgo, riesgo limitado y riesgo mínimo), el RIA solo regula expresamente en su articulado los sistemas de IA de riesgo inaceptables y los sistemas de IA de alto riesgo. En este sentido, el RIA no regula directamente los sistemas de IA de riesgo limitado, sino que los menciona de forma indirecta en el considerando 132 al indicar que, determinados sistemas de IA destinados a interactuar con personas físicas o a generar contenidos pueden plantear riesgos específicos de suplantación o engaño, con independencia de si cumplen las condiciones para ser considerados como de alto riesgo o no. Por consiguiente, el uso de estos sistemas debe estar sujeto, en determinadas circunstancias, a obligaciones de transparencia específicas.

Dado que el indicado considerando se refiere a la obligación de transparencia, la norma deriva a su artículo 50, el cual impone obligaciones de transparencia no solo para los sistemas de IA de alto riesgo, sino también para determinados sistemas de IA. Así se configura la categoría de sistemas de IA de riesgo limitado[63]. Esta obligación de transparencia comprende el deber de informar a los usuarios de que su contenido se ha generado mediante IA para que puedan tomar decisiones con conocimiento de causa sobre su uso posterior[64]. Por ende, el RIA impone ciertos requisitos de transparencia, exigiendo que los sistemas de inteligencia artificial que interactúen con humanos deban informar del hecho que estos están hablando y relacionándose con un sistema[65] y no con una persona.

[63] RAZQUÍN LIZEAGA, Martín María, «Sistemas de IA prohibidos, de alto riesgo, de limitado riesgo, o de bajo o nulo riesgo», *Revista de privacidad y derecho digital* (2024), núm. 34, p. 229.

[64] CONSEJO EUROPEO, «Reglamento de inteligencia artificial». Disponible en: https://www.consilium.europa.eu/es/policies/artificial-intelligence/

[65] En este sentido: SIMÓN CASTELLANO, Pere, «Taxonomía de las garantías jurídicas en el empleo de los sistemas de inteligencia artificial», *Revista de derecho político* (2023), núm. 117, p. 175.

Los robots de conversación han sido identificados como un claro ejemplo de sistemas de IA de riesgo limitado[66], ya que, en la mayoría de los casos, su función es interactuar con los usuarios mediante respuestas automatizadas sin representar un peligro significativo. Nos estaríamos refiriendo a *chatbots* de atención al cliente o asistentes virtuales (como *Siri* o *Alexa*). No obstante, aunque ciertos *bots* conversacionales pueden ser integrados en la indicada categoría, esta clasificación no ha de ser automática. La evaluación de su nivel de riesgo debe considerar factores como el propósito, su nivel de autonomía y el impacto que sus respuestas pueden generar en los usuarios. En este contexto, los *deathbots* no son un simple subgrupo de la categoría *chatbot* diseñados para mantener conversaciones y responder a consultas. El término general de *chatbot*, como sistema diseñado para interactuar con humanos mediante texto o voz, no llega a refleja ni la complejidad ni el potencial impacto emocional de los sistemas que emulan una conversación con un ser querido que ha fallecido.

Aunque técnicamente los *deathbots* son un tipo específico de *chatbot*, difieren en su propósito, ya que no buscan dar una respuesta general (las obras más conocidas de un autor, qué visitar en un país etc.), sino recrear la identidad de alguien que ha fallecido. En otras palabras, los *deathbots* no son simples *chatbots* de reglas predefinidas, sino que utilizan IA generativa para crear conversaciones en tiempo real con base en la gran cantidad de datos que ha proporcionado el usuario. Sin embargo, esta interacción busca emular un nuevo contacto con un ser querido que ha fallecido.

Por consiguiente, a la hora de aplicar el RIA, no todos los robots de conversación han de ser categorizados automáticamente como sistemas de riesgo limitado, se han de analizar las características de cada sistema. Este es un punto crucial, ya que clasificar de manera directa y sin una evaluación adecuada podría llevar a conclusiones erróneas que no reflejan correctamente el impacto o los riesgos de cada tecnología. Este enfoque de análisis de características garantiza que el RIA se aplique de manera justa y efectiva.

Siguiendo esta argumentación, en la relación entre usuario y robot de conversación que simula la identidad de una persona fallecida, la obligación de transparencia del proveedor de los sistemas de IA de riesgo limitado no es suficiente para garantizar el bienestar emocional del usuario. Si bien la transparencia es fundamental para que el usuario tome decisiones informadas sobre el uso del sistema, no cubre todos los

[66] NOVELLI, Claudio; CASOLARI, Federico; ROTOLO, Antonino; TADDEO, Mariarosaria y FLORIDI, Luciano, «AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act», *Digital Society*, vol. 3 (2024), núm. 13, p. 6.

aspectos necesarios para asegurar que la experiencia no ponga en riesgo su salud mental. La información sobre la naturaleza del sistema (es decir, que el usuario sepa que está interactuando con una máquina y no con un ser humano) es importante, pero no aborda de manera integral los potenciales efectos emocionales y psicológicos que pueden surgir durante la interacción.

Este escenario reafirma la necesidad de cumplir todas las obligaciones aplicables a los sistemas de IA de riesgo alto (artículos 9-15 del RIA) a fin de garantizar una gestión adecuada del bienestar emocional de los usuarios. Entre las obligaciones, en el caso particular de los *deathbots* cabe destacar la ya indicada supervisión humana.

4. CONCLUSIÓN

Abogando por un enfoque preventivo que busque salvaguardar el bienestar de los usuarios y teniendo en cuenta el impacto potencialmente negativo en la salud mental de quienes optan por mantener a sus seres queridos virtualmente presentes, se podría llegar a pensar que los *deathbots* son sistemas de IA de riesgo inaceptable y, por tanto, prohibidos.

Sin embargo, en base al artículo 5 del RIA, su prohibición no estaría jurídicamente justificada. Tal y como se ha argumentado, los conceptos actuales de manipulación y vulnerabilidad no aplican al presente caso. En cuanto a la manipulación, aunque estos sistemas pueden afectar emocionalmente al usuario, este efecto no es equiparable a la manipulación prohibida por el RIA, dado que el objetivo o efecto no es modificar su voluntad ni inducirlo a elecciones que de otra forma no tomaría. Por su parte, aunque el duelo afecte al bienestar emocional de una persona, en el sentido del RIA no constituye un tipo de vulnerabilidad. Por ende, no pueden ser identificados como sistemas de IA a prohibir.

Dejando atrás los sistemas de IA prohibidos y pasando a la categoría de riesgo alto, aunque no está científicamente demostrado en este momento el daño que estos sistemas puedan generar en la salud mental de los usuarios, su potencial riesgo es patente. Por lo tanto, si se acredita que este riesgo es real o que efectivamente provocan un daño, deberán ser identificados como sistemas de IA de alto riesgo.

El artículo 6 del RIA indica que, si el sistema de IA está destinado a ser un componente de seguridad de un producto que entre en el ámbito del Anexo I del RIA o que dicho sistema sea en sí mismo un producto, será de riesgo alto. Igualmente, también se consideran de alto riesgo los sistemas de IA contemplados en el Anexo III. No obstante,

no ha de comprenderse que este último anexo incorpora una lista cerrada de sistemas, debiendo poner el foco en el potencial riesgo para la salud, seguridad y derechos fundamentales.

Siguiendo esta afirmación, los proveedores de estos sistemas deberán introducir todas las medidas que regula el RIA entre sus artículos 9 y 15. Como se ha indicado anteriormente, en el caso particular de los *deathbots,* destacan tres medidas a adoptar: la supervisión humana, la transparencia y la ciberseguridad. Estas medidas no solo cumplen con las obligaciones legales, sino que también son esenciales para proteger el bienestar de los usuarios y garantizar que el uso de la inteligencia artificial se realice de manera ética, responsable y segura.

En esta línea, como se ha señalado previamente, se pone en duda la adecuación del sistema de autoevaluación para los sistemas de IA de alto riesgo debido a su falta de supervisión externa. Sin una validación externa independiente, el proceso de autoevaluación corre el riesgo de ser insuficiente para garantizar el cumplimiento riguroso de los estándares establecidos. Por ende, se ha de optar por la evaluación externa en todo caso o, al menos, implementar inspecciones aleatorias continuas que inciten a los proveedores a cumplir de manera rigurosa con los requisitos establecidos.

El análisis que se ha llevado a cabo ha demostrado que no todos los robots de conversación deben ser clasificados automáticamente dentro de esta categoría. Los robots de conversación que simulan la identidad de una persona fallecida tienen el potencial de generar un impacto emocional negativo y complejo en los usuarios, un aspecto que no debe ser subestimado. En consecuencia, el impacto de estos sistemas es significativamente mayor de lo que su clasificación como riesgo limitado podría sugerir.

Retomando el planteamiento inicial, es fundamental subrayar que no se debe dejar todo en manos de la responsabilidad individual de los usuarios. Los sistemas de inteligencia artificial, especialmente aquellos que tienen un impacto directo en la salud mental, no han de depender únicamente del discernimiento o la precaución de cada individuo para evitar daños potenciales.

El ejercicio de determinación del riesgo de los *deathbots* refleja la problemática que genera la interpretación y aplicación del RIA. El hecho de crear una norma a nivel europeo que regule los distintos riesgos de los sistemas de IA ha de ser identificado como un paso adelante y necesario, pero indiscutiblemente crea y creará problemas interpretativos.

Igualmente, es esencial crear una educación y conciencia social relativa a los riesgos que se derivan de la IA. La clave es la alfabetización digital, que permita a los usuarios comprender tanto el potencial de la tecnología como sus implicaciones éticas, jurídicas y psicológicas. La alfabetización digital no se refiere solo al hecho de saber adentrarse en el mundo virtual. En el contexto de la IA, implica entender cómo funcionan los algoritmos y cuáles son los riesgos y beneficios de interactuar con estos sistemas. No se ha de tener miedo a los avances tecnológicos, sino aprovechar sus beneficios y proteger a los usuarios de sus efectos negativos. No todo ha de quedar en manos de la responsabilidad individual.

5. BIBLIOGRAFÍA

AGUSTINOY, Albert, «Griefbots: la resurrección artificial del fallecido». Disponible en: https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/griefbots-resurreccion-artificial-fallecidos

ALKORTA IDIAKEZ, Itziar, «La regulación de los productos sanitarios con Inteligencia Artificial», Tirant lo Blanch, Valencia, 2025.

BARRIO ANDRÉS, Moisés, *Comentarios al Reglamento Europeo de Inteligencia Artificial*, La Ley, Madrid, 2024.

— *Manual de derecho digital*, Tirant lo Blanch, Valencia, 2024.

CÁMARA LAPUENTE, Sergio, «La sucesión mortis causa en el patrimonio digital», *El Notario del siglo XXI* (2019), núm. 84, pp. 375-432.

COMISIÓN EUROPEA, «Libro blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza», 2020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065

CONSEJO DE EUROPA, «Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data», 2019. Disponible en: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

CONSEJO DE LA UNIÓN EUROPEA, «Reglamento de Inteligencia Artificial: el Consejo y el Parlamento alcanzan un acuerdo sobre las primeras normas del mundo en materia de inteligencia artificial», *consilium.europa.eu*, 9 de diciembre de 2023. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/

CONSEJO EUROPEO, «Reglamento de inteligencia artificial». Disponible en: https://www.consilium.europa.eu/es/policies/artificial-intelligence/

ESCRIBANO COLLADO, Pedro, *El derecho a la salud*, Universidad de Sevilla, Sevilla, 2015.

FABRY, Regina E. y ALFANO, Mark, «The affective scaffolding of grief in the digital age: the case of deathbots», *Topoi*, vol. 43 (2024), núm. 3, pp. 757-769.

GALLI, Federico, y NOVELLI, Claudio, «The many meanings of vulnerability in the AI Act and the one missing», *BioLaw Journal* (2024), núm. 1, pp. 53-72.

GAMERO CASADO, Eduardo, «El enfoque europeo de inteligencia artificial», *Revista de derecho administrativo* (2021), núm. 20, pp. 268-289.

GINEBRA MOLINS, María Esperança, «Voluntades digitales: disposiciones mortis causa», en AA.E. y CL.S., *El derecho privado en el nuevo paradigma digital*, Dykinson, Madrid, 2020, pp. 209-238.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, «Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679», 2017. Disponible en: https://www.aepd.es/documento/wp251rev01-es.pdf

GRUPO INDEPENDIENTE DE EXPERTO DE ALTO NIVEL SOBRE INTELIGENCIA ARTIFICIAL, «Directrices éticas para una IA fiable», 8 de abril de 2019. Disponible en: https://digital-strategy.ec.europa.eu/es/library/ethics-guidelines-trustworthy-ai

HERNÁNDEZ LÓPEZ, José Manuel, *Reglamento de inteligencia artificial*, Bosch, Barcelona, 2024.

HERNÁNDEZ RAMOS, Mario, «El marco jurídico regulatorio europeo de la inteligencia artificial. La relación de complementariedad entre el reglamento de la UE y la convención marco del consejo de Europa», *Revista Española de Derecho Europeo*, 92, pp. 9-41.

HERRERA DE LAS HERAS, Ramón, *Aspectos legales de la inteligencia artificial. Personalidad jurídica de los robots, protección de datos y responsabilidad civil*, Dykinson, Madrid, 2022.

ITURMENDI RUBIA, José Miguel, «Inteligencia artificial y derechos humanos. Desafíos y oportunidades en la era digital», *Deusto Journal of Human Rights* (2024), núm. 14, pp. 11- 31.

KA YUK CHAN, Cecilia, y COLLOTON, Tom, *Generative AI in higher education. The ChatGPT effect*, Routledge, Nueva York, 2024.

KLÜBER-ROSS, Elisabeth y KESSLER, David, *Sobre el duelo y el dolor*, Luciérnaga Cas, Barcelona, 2016.

KUCHARAVY, Andrei; PLANCHEREL, Octave; MULDER, Valentin; MERMOUD, Alain y LENDERS, Vicent, *Large language models in cybersecurity. Threats, exposure and mitigation*,

Springer, Cham, 2024.

KURPICZ-BRIKI, Mascha, *More than a chatbot. Language models demystified*, Springer, Cham, 2023.

LINDEMANN, Nora Freya, «The ethical permissibility of chatting with the dead: Towards a normative framework for Deathbots», *Publications of the Institute of Cognitive Science*, vol. 1 (2022), pp. 52 y 54.

LINERA, Miguel Ángel, «La propuesta de Ley de Inteligencia Artificial Europea», *Revista de las Cortes Generales* (2023), núm. 116, pp. 81-133.

LUNA, Florencia, «Elucidating the concept of vulnerability: Layers not labels», *International journal of feminist approaches to bioethics*, vol. 2 (200), núm.1, pp. 121-139.

MARTÍNEZ MARTÍNEZ, Nuria, «Reflexiones en torno a la protección *post mortem* de los datos personales y la gestión de la transmisión mortis causa del patrimonio digital tras la aprobación de la LOPDGDD», *Derecho Privado y Constitución* (2019), núm. 35, pp. 169-212.

MARTÍNEZ TORÁN, Manuel y Esteve Sendra, Chele, «Accesibilidad digital y discapacidad», *Revista Española de Discapacidad*, vol. 10 (2022), núm.2, pp. 11-133.

MCENTEE, Rory, *Theology without walls. An interspiritual approach*, en M.JL., *Theology without walls*, Routledge, Nueva York, 2020, pp. 85-97.

MIGUEZ MACHO, Luís, y Torres Carlos, Marcos, «Sistemas de IA prohibidos y sistemas de IA de alto riesgo», en BA. M., *El reglamento europeo de Inteligencia Artificial*, Tirant lo Blanch, Valencia, 2024.

MORALEJO IMBERNÓN, Nieves, «El testamento digital en la nueva Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales», *Anuario de derecho civil* (2020), pp. 241-281.

NAVAS NAVARRO, Susana, «Herencia y protección de datos de personas fallecidas: a propósito del mal denominado «testamento digital»», *Revista de derecho privado* (2020), núm. 1, pp. 59-88.

NOVELLI, Claudio; CASOLARI, Federico; ROTOLO, Antonino; TADDEO, Mariarosaria y FLORIDI, Luciano, «AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act», *Digital Society*, vol. 3 (2024), núm. 13, pp. 1-13.

OBREGÓN FERNÁNDEZ, Aritz, y LAZCOZ MORATINOS, Guillermo, «La supervisión humana de los sistemas de inteligencia artificial de alto riesgo. Aportaciones desde el Derecho Internacional Humanitario y el Derecho de la Unión Europea», *Revista electrónica de estudios internacionales* (2021), núm. 42, pp. 1-29.

O'CONNOR, Mórna y KASKET, Elaine, «What grief isn't: Dead grief concepts and their digital-age revival», en M.T.; B.C.; A.S; y G. J. (Eds.), *Social media and technology across the lifespan,* Springer Nature, Nueva York, 2022, pp. 115-130.

ÖHMAN, Carl y FLORIDI, Luciano, «The political economy of death in the afe of information: a critical approach to the digital afterlife industry», *Minds & machines*, vol. 27 (2017), núm. 4, pp. 639-662.

ORGANIZACIÓN MUNDIAL DE LA SALUD Y NACIONES UNIDAS, «Salud mental, derechos humanos y legislación. Orientación práctica», 2024. Disponible en: https://iris.who.int/bitstream/handle/10665/379200/9789240098169-spa.pdf?sequence=1

ORGANIZACIÓN MUNDIAL DE LA SALUD, «Informe mundial sobre la discapacidad», 2011. Disponible en: https://iris.who.int/handle/10665/75356

PAASS, Gerhard y GIESSELBACH, Sven, *Foundation models for natural language processing: pre-trained language models integrating media*, Springer, Cham, 2023.

PÉREZ VALLEJO, Ana María y VIVAS TESÓN, Inmaculada, *La transmisión mortis causa del patrimonio intelectual y digital*, Aranzadi, Pamplona, 2022.

RAE, avatar. Disponible en: https://dle.rae.es/avatar

RAZQUÍN LIZEAGA, Martín María, «Sistemas de IA prohibidos, de alto riesgo, de limitado riesgo, o de bajo o nulo riesgo», *Revista de privacidad y derecho digital* (2024), núm. 34, pp. 172-235.

SÁNCHEZ VALLE, María y ABAD ALCALÁ, Leopoldo (coord.), *Mayores (des) conectados. Estudio sobre la brecha digital*, Dykinson, Madrid, 2024.

SEJNOWSKI, Terry, *ChatGPT and the future of AI: the deep language revolution*, The Mit press, Cambridge, Massachusetts, 2024.

SIMÓN CASTELLANO, Pere, «Taxonomía de las garantías jurídicas en el empleo de los sistemas de inteligencia artificial», *Revista de derecho político* (2023), núm. 117, pp. 153-196.

VALLE ESCOLANO, Raquel, «Inteligencia artificial y derechos de las personas con discapacidad: el poder de los algoritmos», *Revista Española de Discapacidad*, vol. 11 (2023), núm.1, pp. 7-28.

VAN DER SLOOT, Bart, *Regulating the synthetic society. Generative AI, Legal questions and societal challenges*, Hart Publishing, Oxford, 2024.

Fecha de recepción: 07.04.2025

Fecha de aceptación: 24.09.2025