Entrenamiento de sistemas de IA en el ámbito sanitario: interacciones entre el reglamento general de protección de datos y el reglamento de inteligencia artificial

Training of AI systems in the healthcare sector: interactions between the general data protection regulation and the artificial intelligence act

Paola Zouak Lara
Contratada predoctoral FPU en el Departamento de Derecho Civil
Universidad de Granada[1]

Recibido:12.06.2025 / Aceptado:25.07.2025
DOI: 10.20318/cdt.2025.9903

Resumen: El entrenamiento de sistemas de inteligencia artificial en el ámbito sanitario plantea complejas interacciones normativas entre el Reglamento General de Protección de Datos (RGPD) y el Reglamento de Inteligencia Artificial (RIA). Mientras el RGPD regula exclusivamente la consideración de tratamiento de datos personales y posee una regulación estricta, el RIA principalmente impone requisitos para sistemas de alto riesgo, categoría en la que se incluyen muchas aplicaciones sanitarias. Esta convergencia normativa exige una evaluación rigurosa del ámbito de aplicación de ambos instrumentos, una perspectiva técnica para comprender como funciona el entrenamiento de la IA y un balance que garantice simultáneamente la protección de los derechos fundamentales y la innovación tecnológica responsable en el sector salud.

Palabras clave: Inteligencia artificial, Derecho sanitario, protección de datos personales, extraterritorialidad.

Abstract: The training of artificial intelligence systems in the healthcare sector raises complex regulatory interactions between the General Data Protection Regulation (GDPR) and the Artificial Intelligence Regulation (AI Act). While the GDPR strictly governs the processing of personal data, the AI Act primarily sets requirements for high-risk systems, a category that includes many healthcare applications. This regulatory convergence demands a thorough assessment of the scope of both instruments, a technical understanding of AI training processes, and a balanced approach that ensures both the protection of fundamental rights and responsible technological innovation in the health sector.

Keywords: Artificial intelligence, Health law, Personal data protection, Extraterritoriality.

[1] Trabajo realizado en el marco del Proyecto de I+D+I financiado por el MICIN «Robótica, Inteligencia Artificial y Mayores: oportunidades y desafíos» (PID2023-1514410B-I00), dirigido por Inmaculada Sánchez Ruiz de Valdivia y María del Carmen García Garnica. PID2023-151441OB-I00 y en el marco del Contrato FPU del Ministerio de Ciencia, Innovación y Universidades.

I. **Introducción**

1. La Inteligencia artificial (IA) está teniendo un gran impacto en diversos sectores de nuestra sociedad. Sin embargo, por reciente que parezca, es un fenómeno que consta de una larga trayectoria y cuyo término se acuñó por primera vez en la Conferencia de Darthmouth en 1956 por el informático John McCarthy, quien investigó junto a un grupo de científicos las posibilidades de que las máquinas adquirieran comportamientos inteligentes[2]. En esa misma época, Arthur Samuel creó *checkers*, el primer programa de ajedrez con autonomía propia capaz de mejorarse a sí mismo con el entrenamiento y el uso, lo cual desembocó en 1997 en la creación de Deep Blue, otro programa de ajedrez que consiguió derrotar en una partida a Gary Kasparov, el mejor jugador de ajedrez de aquel momento[3]. Con estos someros ejemplos se busca visibilizar acerca de los avances que está suponiendo la IA y sus múltiples aplicaciones sociales, centrando nuestra atención en el ámbito sanitario.

2. Una de las capacidades desarrolladas en la inteligencia artificial es la toma de decisiones de forma automatizada, es decir, decisiones que realiza un sistema informático sin la intervención directa de una persona, y cuyo funcionamiento se basa en algoritmos, inteligencia artificial y aprendizaje automático.

3. Sin embargo, a pesar de las múltiples ventajas que presenta la IA en el ámbito sanitario y que posteriormente se enunciarán, también surgen una serie de dificultades o inconvenientes durante su entrenamiento, lo cual puede redundar en un servicio deficitario o sesgado, capaz de poner en riesgo las previsiones establecidas en 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[4] (Reglamento general de protección de datos o RGPD). De manera adicional, dado el gran entramado normativo que la Unión Europea ha ido creando en los últimos años, se hace necesaria una aclaración sobre el ámbito de aplicación de los diferentes instrumentos, su compatibilidad y la casuística a la que se pueden enfrentar en concreto con el 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 o RIA[5]).

4. Por todo ello, el objeto de la investigación es el entrenamiento de la IA que se utiliza en el ámbito sanitario y la normativa que lo regula principalmente: RGPD y RIA. Mientras que el objetivo del estudio es identificar la compatibilidad o incompatibilidad de ambos instrumentos normativos y proponer algunas reformas que puedan servir para mejorar los servicios de salud. Para ello utilizaremos una metodología propia de las ciencias jurídicas, de tipo teorética, analizando tanto la doctrina como la legislación y jurisprudencia más relevante a nivel europeo para esclarecer el panorama normativo actual y a la vez se propondrá un enfoque técnico basado en las principales necesidades que tienen los

[2] E. Soria Olivas., M.A. Sánchez- Montañés Isla, et. al, *Sistemas de Aprendizaje Automático*, RA-MA, Madrid, 2023, p. 17.

[3] R. Herrera de las Heras, *Aspectos legales de la inteligencia artificial: personalidad jurídica de los robots, protección de datos y responsabilidad civil*, Dykinson, 2022, pp. 11-14.

[4] DOUE-L-119/1, de 27 de abril de 2016.

[5] DOUE-L- de 13 de junio de 2024.

ingenieros informáticos a la hora de elaborar sus propios sistemas de IA para que entendamos los retos a los que se enfrentan e intentemos darle respuesta.

II. **La inteligencia artificial, el machine learning y el análisis de datos en el ámbito sanitario**

1. **El concepto de IA del RIA**

5. Para comenzar este apartado se hace necesario otorgar una definición de qué debe entenderse por inteligencia artificial, lo cual no es sencillo ya que debe ser un concepto que englobe una tipología de tecnología que se encuentra en constante actualización. Incluso la propia Unión Europea ha ido variando dicha definición, pasando por la dada en un primer momento por la Comisión Europea en el año 2018[6], continuando por la otorgada por el Alto Grupo de Expertos de la Comisión en 2019[7], la aportada por el Parlamento Europeo en la Resolución sobre recomendaciones a la Comisión en 2020[8], hasta la finalmente incorporada en el RIA[9]. Todo ello refleja la gran complejidad de esta tarea que, sin embargo, resulta crucial porque la definición jurídica delimitará lo que deberá entenderse comprendido o no por los diversos instrumentos jurídicos y que, por lo tanto, redundará en una concreta protección u obligación para los responsables[10]. Por ello, a la vista de la multiplicidad de definiciones legislativas, debemos tomar la definición de sistema de IA aportada por el RIA que la define como un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales. Esta definición hace que todo aquello que se salga de la misma no quede bajo el amparo del RIA.

2. **El análisis de datos como herramienta de entrenamiento**

6. Sin embargo, a pesar de haber otorgado la definición legal de IA, lo cierto es que para entender exactamente qué es la IA se hace necesario desgranar el concepto, yendo más allá y comprendiendo su funcionamiento, realizando una aproximación técnica que nos permita comprender los entresijos del programa que queremos analizar. La inteligencia artificial se fundamenta en el uso de algoritmos, los

[6] En la Comunicación de la Comisión dirigida al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre Inteligencia Artificial para Europea COM (2018) 237, se señalaba que "el término IA se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción –con cierto grado de autonomía– con el fin de alcanzar objetivos específicos. Los sistemas basados en la IA pueden consistir simplemente en un programa informático (p. ej. asistentes de voz, programas de análisis de imágenes, motores de búsqueda, sistemas de reconocimiento facial y de voz), pero la IA también puede estar incorporada en dispositivos de hardware (p. ej. robots avanzados, automóviles autónomos, drones o aplicaciones del internet de las cosas)."

[7] El Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial de la Comisión Europea, en su *A definition of AI: main capabilities and disciplines*, de 8 de abril de 2019 estableció que: "En lo siguiente utilizaremos el término *sistema de IA* para referirnos a cualquier componente, software y/o hardware basado en IA. En concreto, los sistemas de IA suelen estar integrados como componentes de sistemas más grandes, en lugar de ser sistemas independientes."

[8] La Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, (2020/2012(INL)), art. 4 establecía que se entendería por IA: " un sistema basado en programas informáticos o incorporado en dispositivos físicos que manifiesta un comportamiento inteligente al ser capaz, entre otras cosas, de recopilar y tratar datos, analizar e interpretar su entorno y pasar a la acción, con cierto grado de autonomía, con el fin de alcanzar objetivos específicos."

[9] El art. 3 del RIA establece que un sistema de IA es: un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

[10] L. Cotino Hueso, *¿Qué es «inteligencia artificial» para el reglamento?: Análisis, delimitación y aplicaciones prácticas*, Aranzadi, 2024, pp. 114-115.

cuales son secuencias finitas de reglas formales que, a partir de un *input*, permiten ejecutar una serie de operaciones lógicas previamente definidas y generar un resultado[11].

7. El paso siguiente es abordar el concepto de *machine learning* o aprendizaje automático, una rama de la inteligencia artificial que permite a los ordenadores aprender a partir de datos sin necesidad de una programación explícita previa. Su funcionamiento se apoya en proporcionar al algoritmo datos de entrada, a partir de los cuales se construye un modelo capaz de realizar predicciones y clasificaciones sobre nuevas observaciones, incluso si estas no han sido previamente conocidas por el algoritmo. Este proceso forma parte de lo que se conoce como minería de datos, que implica la recopilación y depuración de los datos de entrada[12]. Para llevar a cabo este entrenamiento del algoritmo debe existir un científico de datos que se dedique a programar, a elegir los datos pertinentes y a supervisar dicho entrenamiento. Nos centramos concretamente en el *machine learning* o aprendizaje automático[13] porque la mayoría de los sistemas inteligentes que se utilizan en el ámbito de la sanidad utilizan este tipo de forma de entrenamiento para conseguir utilidades tales como el procesamiento de imágenes[14], la realización de intervenciones, la predicción de resultados o los seguimientos remotos de pacientes[15]. A día de hoy la IA que utiliza aprendizaje automático no solamente sirve de apoyo al diagnóstico que en última instancia emite el médico, sino que sirve para optimizar la atención que se le presta al paciente[16]. Reconocida la importancia del uso de la IA en el ámbito sanitario, uno de los aspectos fundamentales que sirve de piedra angular para mejorar el servicio a los pacientes consiste en la calidad de los datos utilizados para entrenar a los modelos de IA. La calidad del modelo que se cree va a depender de la representatividad de los datos que se introduzcan durante el entrenamiento.

8. Habiendo señalado las principales utilidades que presenta la IA en el ámbito sanitario, procederemos a ilustrar cómo se comienza a entrenar al sistema de IA para identificar los principales problemas a los que se enfrentan los programadores y la regulación a la que se somete todo este procedimiento.

9. El primer paso que deben dar los programadores es escoger el proyecto, decidiendo qué tipo de sistema necesitan crear y su finalidad principal. Posteriormente se procede a la elección de los

---

[11] A. Palma Ortigosa, *Decisiones automatizadas y protección de datos: Especial atención a los sistemas de inteligencia artificial*, Dykinson, 2022, p. 37.

[12] J. J. Beunza Nuin J.J., y E. Condés Moreno, "Conceptos", en J.J. Beunza Nuin, et al. *Manual práctico de inteligencia artificial en entornos sanitarios*, Elsevier, 2023, pp. 4- 9.

[13] Sobre este punto profundizan: J.J. Beunza Nuón, "Algoritmos disponibles en la práctica sanitaria", en BEUNZA NUÓN J.J. et al., Manual práctico de inteligencia artificial en entornos sanitarios, Elsevier, 2023, pp. 19- 23; Ficco M. y D'Angelo G., Artificial Intelligence Techniques for Analysing Sensitive Data in Medical Cyber-Physical Systems, *Springer*, 2025.

[14] En esta línea, se pueden identificar los siguientes casos:

a) BioMind, que es una aplicación de inteligencia artificial desarrollada por el Artificial Intelligence Research Centre for Neurological Disorders del Hospital Beijing Tiantan, fue entrenada con miles de imágenes recogidas en el propio hospital para detectar tumores y hemorragias cerebrales mediante TAC. Para evaluar su efectividad, en 2018 se organizó un concurso de diagnóstico frente a los 15 principales especialistas chinos en este campo. En la primera ronda, la IA acertó el 87% de los casos en 15 minutos, mientras que los médicos lograron un 66% en 30 minutos. En una segunda ronda, la IA alcanzó un 83% en 3 minutos, y los médicos un 63% en 20 minutos.

b) En el Massachusetts General Hospital de Boston, el equipo del Computer Science and Artificial Intelligence Laboratory diseñó un algoritmo utilizando 60.000 mamografías del hospital. Esta IA destaca por su capacidad de prever el desarrollo del cáncer de mama con hasta cinco años de antelación. Mientras los métodos actuales alcanzan una precisión del 18%, la IA logró un 31%.

c) En Valladolid, un grupo de investigación ha desarrollado un sistema automatizado para diagnosticar la retinopatía diabética a partir de imágenes del fondo de ojo. Para ello, se entrenó una red neuronal multicapa con 564 imágenes, obteniendo una precisión del 84%.

d) En el ámbito de las enfermedades psiquiátricas, se entrenó un algoritmo supervisado con textos y audios procedentes de las redes sociales Facebook y Twitter, permitiendo diagnosticar trastorno bipolar con una precisión que oscila entre el 90% y el 98%.

e) En ginecología, se ha implementado un algoritmo no supervisado basado en k-means clustering —una técnica de agrupamiento usada en minería de datos— que permite clasificar a pacientes con cáncer de ovario a partir de imágenes de TAC y muestras patológicas de 364 mujeres, ofreciendo una clasificación más precisa y fiable que la tradicional.

[15] F. Ramón Fernández, "Diagnóstico médico por robots y responsabilidad civil", *Lex Medicinae*, n.º42, 2024, p. 18.

[16] I. Alkorta Idiakez, *La regulación de los productos sanitarios con Inteligencia Artificial*, Tirant lo Blanch, 2025, p. 16.

datos y su clasificación, ya que con estos datos se entrenará posteriormente al sistema. Una vez se han identificado y clasificado dichos datos se continúa con la fase de preprocesado de datos y su limpieza, siendo ésta la fase más tediosa y a la vez importante, ya que supone el núcleo duro del entrenamiento. La pregunta que nos puede surgir en este punto es, ¿y cómo se consiguen dichos datos? Pues lo cierto es que se recurre a la minería de datos o *data mining*, que es una técnica que permite extraer una serie de información de ciertos datos mediante la observación de relaciones, ciertos patrones o semejanzas que no se ven a simple vista pero que sirven para interrelacionar los datos introducidos[17]. Traducido a un lenguaje no técnico, se trataría de encontrar el valor subyacente en un conjunto de datos que a priori no presentan ningún tipo de relación entre sí, desgranando su valor y estableciendo conexiones.

10. En la fase de preprocesado se realiza la limpieza de datos, otorgándole a cada dato una variable y un valor, eliminando los datos incorrectos y atípicos, que se identifican porque normalmente se salen de los umbrales máximos y mínimos establecidos[18]. Lo que se pretende con este procedimiento es que los datos estén perfectamente clasificados para facilitar el entrenamiento y que no existan errores posteriormente. Para poder limpiar esos datos, los programadores deben aplicar ciertas operaciones técnicas muy complejas. En el caso de que se esté trabajando con imágenes, por ejemplo, se aplicarían técnicas de procesado de imágenes para intentar reducir o eliminar el llamado "ruido", que referido a los datos se trata de ciertos errores que se pueden haber dado en el etiquetado, o por introducir datos defectuosos[19]. Por ejemplo, si se está trabajando con imágenes de cáncer de hígado, ruido sería introducir una imagen de un estómago. Por lo tanto, el programador debe eliminar dicha imagen para que cuando se introduzca dicho dato, el sistema no confunda un hígado con un estómago.

11. Las técnicas de procesamiento de datos han experimentado una evolución significativa, impulsada por sistemas avanzados capaces de gestionar volúmenes masivos de información sin necesidad de preprocesamiento manual por parte del programador. Estos sistemas integran herramientas automáticas de detección, reconocimiento y transformación de datos. Dentro de este conjunto de técnicas se incluye la eliminación de anomalías, la conversión de datos que provienen de diferente fuente, el etiquetado de datos…

12. Una vez se tienen los datos debidamente clasificados el programador debe elegir cuál es el algoritmo adecuado para poder cumplir el objetivo pretendido con su sistema de IA. En este punto nos encontramos con diferentes tipos de algoritmos:

- Algoritmo de aprendizaje supervisado. Este tipo de algoritmo se entrena con datos de entrada (introducidos) y de salida (el dato que va a emitir el sistema de IA) que están etiquetados y clasificados de manera previa. Al habérsele indicado al sistema de IA lo que significa cada dato, éste es capaz de encontrar similitudes y relaciones y lo reconoce al instante, ya que sus imágenes de muestra estaban catalogadas con anterioridad.
- Algoritmo de aprendizaje no supervisado. Este tipo de algoritmo no contiene datos previamente etiquetados y clasificados, sino que se le permite a la propia IA que extraiga patrones comunes de entre los datos introducidos, de modo que ésta misma aprende a ver las similitudes y llega a la misma conclusión que si los datos no hubieran estado clasificados.
- Algoritmo de aprendizaje por refuerzo. Este tipo de algoritmo no se basa en la introducción de datos, sino en un método de ensayo y error del propio sistema, de modo que cuando da una respuesta correcta se lo premia y cuando emite un resultado erróneo se le aplica un castigo, haciendo que vaya aprendiendo en función de la respuesta que recibe del exterior.

[17] R. Martínez Martínez, "Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo", *Revista catalana de dret públic*, n.º 58, 2019, p. 75.

[18] E. Soria Olivas; M.A. Sánchez- Montañés Isla, et. al. *Sistemas de Aprendizaje Automático*, RA-MA… *op cit*. p. 27.

[19] A. Palma Ortigosa, "Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos", *Revista General de Derecho Administrativo*, n.º 5, 2019, pp. 7-8.

3. Problemas que plantean los sistemas de IA en el entrenamiento

13. La última etapa del diseño consiste en probarlo y desplegar el sistema, pero no resulta relevante para este estudio. Como podemos observar, la clave para que un sistema de IA funcione correctamente es que los datos que se introduzcan sean correctos y estén debidamente clasificados. Pero, si la cuestión parece tan sencilla, ¿cuáles son los verdaderos problemas a los que se enfrentan los programadores y dónde reside la dificultad? Los ingenieros informáticos normalmente refieren tres problemas a los que se enfrentan diariamente[20].

14. En primer lugar, nos encontramos con una cantidad insuficiente de datos. Cuando se está implementado un sistema de IA cuya finalidad es lanzarlo al mercado, lo que se pretende es que sea lo más certero posible y para ello es necesario que en los bancos de datos de la empresa existan millones de imágenes debidamente etiquetadas para el entrenamiento del sistema. Cuantos más patrones se tengan mejor funcionará el modelo. Sin embargo, hay que tener en cuenta que no solo es relevante el número de datos sino la calidad de los mismos, para que el sistema sea seguro y fiable. En este contexto hay quienes plantean que una buena opción para poder gozar de tales cantidades sería la creación de espacios de datos abiertos, es decir, espacios donde se aporten datos que pueden ser reutilizados con una cierta seguridad común[21].

15. Esta idea se asemeja bastante a lo que ha propuesto la UE en el Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847[22], que busca crear unas grandes piscinas de datos cuya propiedad sea de la UE y que puedan ser utilizadas por todos los países de la UE, proporcionando datos de los diferentes países cuyo control corresponde a un representante que debe ser nombrado por cada país. El control, la protección y el uso de los datos en vez de recaer en empresas privadas de diversa índole pasaría a ser de parte de la UE, que se prevé que se convierta en un ente garantista con un papel activo en la protección de datos. De este modo, los datos de esos grandes bancos de la UE podrían ser utilizados y reutilizados por las empresas que lo soliciten siempre que cumplan con los requisitos estipulados en la normativa[23].

16. En segundo lugar, nos encontramos con los datos no representativos. Además de poseer una cantidad adecuada de datos, la calidad de los mismos goza de una gran importancia, ilustrémoslo con un ejemplo. Si estamos diseñando un sistema que sirva para procesar imágenes y detectar cuándo un pulmón tiene cáncer y le hemos introducido imágenes de pulmones sanos y pulmones con cáncer y al finalizar el entrenamiento la tasa de acierto es de un 97% podríamos decir que ha sido todo un acierto. Sin embargo, ¿qué pasaría si al introducirle una imagen de un solo pulmón, pongamos por ejemplo el izquierdo, no reconoce ninguna lesión cuando esta es patente? Se podría haber cometido un error, por ejemplo, haber entrenado al sistema exclusivamente con imágenes de pulmones derechos, pero no izquierdos. ¿Es un pulmón? Sí, pero el modelo estaba acostumbrado a identificar la imagen por la forma concreta del pulmón, sin fijarse en otras características para acotar el camino y facilitar el reconocimiento, por lo que el modelo no serviría porque posee un sesgo muestral, que se produce cuando ciertos miembros de una población tienen menos o más posibilidades de ser incluidos por diversas razones, pensemos por ejemplo raza, sexo, edad… Además del llamado sesgo muestral también nos podemos encontrar con el ruido muestral, derivado de las propias diferencias inherentes a los individuos, lo cual nos lleva a la conclusión de que para que el resultado emitido por la IA sea coherente, es necesario que el conjunto de datos de entrenamiento sea lo suficientemente grande, ya que cuanto más grande sea mejores serán los patrones que se pueden extraer.

---

[20] e. soria olivas, m.a. sánchez- montañés isla, et. al. *Sistemas de Aprendizaje Automático*, RA-MA… op cit. p. 114.

[21] j. lozano carrillo, "La Inteligencia Artificial necesita datos de calidad y seguros", *Revista jurídica: Región de Murcia*, n.º. 54, 2024, p. 160.

[22] DOUE-L-2025-80382.

[23] m. Recuero Linares, "El uso secundario de datos de salud electrónicos: el futuro Reglamento del Espacio Europeo de Datos de Salud y su interacción con la protección de datos personales", *Indret: Revista para el análisis del Derecho*, nº. 2, pp. 5-7.

17. Finalmente nos podemos encontrar con un problema que puede resultar contradictorio y es el sobreajuste, consistente en que el sistema ha sido tan minuciosamente entrenado que no es capaz de establecer comportamientos generalizados, ya que solamente se ciñe a un rango muy concreto de individuos o conductas. Se podría decir que el sistema confunde el ruido muestral con la verdadera información y se hace necesario de nuevo reajustarlo.

18. Fuera de todos estos problemas a los que se tienen que enfrentar los ingenieros, debemos como juristas conocer cuáles son los instrumentos normativos que acotan o ponen límite a la libertad creativa y empresarial de las empresas tecnológicas que se dedican a la creación de sistemas inteligentes, para saber cuál es el rango de maniobra con el que cuentan estos especialistas. En concreto, para ceñirnos a la materia objeto de estudio analizaremos tanto el RIA como el RGPD, que son los dos principales Reglamentos cuyo ámbito de aplicación y regulación debe quedar totalmente claro y que resultan imprescindibles cuando se habla de entrenamiento de IA con datos. Antes de adentrarnos en el estudio de esta cuestión específica resulta imprescindible señalar una serie de principios que deben ser tenidos en cuenta a la hora de tratar los datos para entrenar al sistema inteligente, como son el de licitud lealtad y transparencia, recogido en el art. 5.1.a del RGPD, que asegura que no se lleven a cabo prácticas engañosas o que se coloque a un individuo en una posición de desventaja; la exactitud de los datos, plasmada en el art. 5.1.d del RGPD que exige la eliminación de información inexacta o duplicada que pueda generar resultados sesgados; el principio de minimización, recogido en el art. 5.1. c del RGPD que establece que el tratamiento de datos se limite a los fundamentales para cumplir con la finalidad específica que se pretende abarcar. Teniendo en cuenta estos principios, procedemos a analizar los principales instrumentos normativos reguladores del entrenamiento de la IA.

III. La regulación de la IA en el Reglamento de Inteligencia Artificial

19. Habiendo estudiado cómo se realiza el proceso para entrenar a un sistema inteligente cabe realizar ahora un acercamiento a cómo ha planteado la Unión Europea el reto de la regulación de la IA en el RIA, ya que esto servirá de cota y límite a la actividad de los programadores y empresarios de sistemas de IA.

20. Debemos partir de la base de que actualmente a nivel mundial podríamos distinguir principalmente dos tendencias por lo que respecta a la regulación de la IA: por una parte nos encontramos con países que optan por una regulación imperativa cuya finalidad es proteger al ciudadano para evitar los riesgos a los que se enfrenta por el uso de la IA, lo cual puede conllevar a una limitación del desarrollo tecnológico ya que las empresas deben hacer frente a una gran cantidad de requisitos, obligaciones e imposiciones de todo tipo; por otra parte nos encontramos con países que optan por una desregulación total, cuya finalidad es favorecer la innovación y el desarrollo tecnológico empresarial, dejando de lado las vulnerabilidades a las que se encuentran expuestos sus futuros clientes, lo cual hace que el mercado se pueda transformar en una jungla cuyas normas impuestas sean las de la empresa de turno con más poder[24]. Cabe señalar igualmente que cuando hablamos de una ausencia de regulación no nos estamos refiriendo literalmente a una falta completa de positivación, sino a una forma de legislar basada en normas de *soft law*, materializada en códigos de conducta, buenas prácticas, guías o recomendaciones generales que no imponen deberes reales u obligaciones a los responsables de la IA.

1. Países que optan por la ausencia de regulación

21. Comenzando con los países que optan por un modelo liberal de ausencia de regulación nos encontramos con Estados Unidos, que ha sido el pionero en esta categoría y ha ido arrastrando al resto

[24] A.J. Tapia Hermida, "Claves de la Ley europea de inteligencia artificial: Reglamento (UE) 2024/1689 de 13 de junio de 2024", *La Ley Unión Europea*, n.º. 133, 2025, pp. 2-3.

de países que se han unido a este tipo de desregulación. El 23 de enero de 2025 el actual presidente de EEUU dictó la *Executive Order 14179-Removing Barriers to American Leadership in Artificial Intelligence*[25]. En esta norma se pone de manifiesto que Estados Unidos ha estado durante mucho tiempo a la cabeza de la innovación en materia de IA y para ello plantea la necesidad de que se sigan desarrollando sistemas de IA libres de barreras o fronteras ideológicas. Para ello, recalca que, concretamente, la finalidad de esta norma es revocar la *Executive Orden 14110 of 30 October 2023*[26] dictada por el anterior presidente Joe Biden, cuyo objetivo era establecer un marco normativo integral para el desarrollo y el uso fiable y ético de la IA en EEUU. Esta orden anterior, con estructura de un código de buenas prácticas, configuraba una serie de principios rectores y planeaba la creación de la autoridad del *Chief AI Officer*, encargado de coordinar políticas éticas para utilizar la IA. De este modo se pretende volver al panorama anterior de total libertad de emprendimiento y experimentación instaurado en el ámbito empresarial.

22. Siguiendo esta misma línea nos encontramos con el caso de Uruguay, que en 2020 aprobó la Estrategia de Inteligencia Artificial para el Gobierno Digital[27], que enumera una serie de principios que se deben tener en cuenta para realizar el diseño, desarrollo y despliegue de los sistemas de IA. No se queda atrás el gobierno de Colombia, que ha llevado a cabo una frenética labor legislativa, dictando el Plan estratégico para la transferencia de conocimiento en Inteligencia Artificial[28], la Hoja de Ruta para la Adopción Ética y Sostenible de la Inteligencia Artificial[29] y la Política Nacional para la Transformación Digital e Inteligencia Artificial[30].

23. Por su parte, Argentina en 2023 publicó las Recomendaciones para una Inteligencia Artificial fiable, cuya finalidad es garantizar el desarrollo responsable de la IA, dirigiendo sus indicaciones al sector público principalmente en materia de ética. Este documento destaca por compartir el mismo enfoque centrado en el ser humano que comparten otros documentos como la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO[31] o los Principios Asilomar[32]. Este tipo de enfoque pretende respetar en todo el ciclo de vida del sistema de IA tanto los valores fundamentales como los derechos humanos, la privacidad, la equidad y la justicia social.

24. En esta misma línea se encuentra China, que ha optado por un enfoque si bien centralizado, con tintes de *soft law*, al caracterizarse por la emisión de directrices, recomendaciones y políticas cuyo objetivo es asegurar una correcta implementación de la IA. La norma más importante sin duda es el Reglamento de Síntesis Profunda[33], que resulta aplicable a los servicios disponibles para la ciudadanía China y que exige a los proveedores de servicios de IA la realización de controles de seguridad y registro de los algoritmos de forma pública si prevén que los servicios pueden tener un efecto relevante en la población. Además, esta norma impone un deber de transparencia, de modo que obliga a revelar cuándo el contenido ha sido generado artificialmente y qué tipo de datos han sido tenidos en cuenta para entrenar el modelo[34]. Esta norma, con ciertos tintes europeos se aplica tanto a los proveedores de servicios, los técnicos de soporte, los usuarios y las plataformas en línea, imponiendo obligaciones de ciberseguridad, protección de datos, auditoría de algoritmos, registros y verificación de datos.

---

[25] Disponible en: https://www.presidency.ucsb.edu/node/376009

[26] Disponible en: https://www.congress.gov/crs-product/R47843

[27] Disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Estrategia%20IA%20-%20versi%C3%B3n%20espa%C3%B1ol.pdf

[28] Disponible en: https://minciencias.gov.co/sites/default/files/upload/noticias/hoja_de_ruta_adopcion_etica_y_sostenible_de_inteligencia_artificial_colombia_0.pdf

[29] Disponible en: https://minciencias.gov.co/sites/default/files/upload/noticias/hoja_de_ruta_adopcion_etica_y_sostenible_de_inteligencia_artificial_colombia_0.pdf

[30] Disponible en: http://hdl.handle.net/20.500.12324/36742

[31] Disponible en: https://www.unesco.org/es/articles/recomendacion-sobre-la-etica-de-la-inteligencia-artificial

[32] Disponible en: https://philarchive.org/archive/MORVPD-2

[33] Disponible en: https://tinyurl.com/4zrrxjyn

[34] M. Pérez Ugena, "Análisis comparado de los distintos enfoques regulatorios de la inteligencia artificial en la Unión Europea, EE. UU., China e Iberoamérica", *Anuario Iberoamericano de Justicia Constitucional*, vol. 28, n.º. 1, 2024, pp. 145-147.

2. Países que optan por la regulación

25. En el otro extremo de países que optan por una visión reguladora y proteccionista nos encontramos con México, que estaba en trámites de promulgar la Ley para la Regulación Ética de la Inteligencia Artificial y la Robótica en 2023[35], cuyo objetivo es crear un organismo denominado Consejo Mexicano de Ética para la Inteligencia Artificial y Robótica, que se pretende usar como plataforma de intercambio de propuestas futuras legislativas entre los diferentes operadores del sistema y como organismo revisor del cumplimiento de las normas y redacción de informes de control. Esta norma prevé ciertas prácticas prohibidas de la IA, como aquellas que puedan derivar en manipulación social discriminación o violación de principios fundamentales. Sin embargo, en 2024 se ha aprobado la Ley Federal que regula la IA[36], con el mismo enfoque de riesgo que ya proponía la versión anterior.

26. Por su parte, Chile presentó en 2023 el Proyecto de Ley sobre robótica, inteligencia artificial y tecnologías conexas[37], cuya finalidad es realizar una clasificación de los diferentes sistemas de IA en función de su riesgo, dividiéndolos en IA prohibida e IA de alto riesgo. De manera complementaria también cuenta con la Política Nacional de Inteligencia Artificial, que consta de diez objetivos que se deben poner en marcha durante el uso de un sistema inteligente, como son: fomentar e impulsar la productividad económica de la IA para llegar a niveles iguales o superiores al promedio de crecimiento económico para países OCDE por el impacto de IA; impulsar la construcción de certezas regulatorias sobre los sistemas de IA que permitan su investigación, desarrollo e implementación, respetando los derechos fundamentales; desarrollar herramientas para el uso ético de inteligencia artificial en el Estado; impulsar programas de capacitación para funcionarios públicos sobre el uso ético de IA en este sector; promover y articular la discusión sobre gobernanza de la IA y cooperación internacional en América Latina y El Caribe; colaborar e incidir activamente en la discusión de gobernanza y estándares a nivel internacional; fomentar el uso de IA para combatir la crisis climática; fomentar el uso de energías renovables no convencionales en el desarrollo de la IA; fomentar la participación de mujeres en áreas de investigación y desarrollo relacionadas a la IA para alcanzar un nivel igual o mayor al promedio OCDE; fomentar la participación de mujeres en áreas de IA en la industria hasta alcanzar, al menos, un valor igual o superior al promedio OCDE y velar porque el impacto de la automatización no perjudique por género y que la creación de empleo sea equitativa; y fomentar la inclusión y no discriminación en la implementación de sistemas de IA.

27. Finalmente nos encontramos con el caso de Brasil, que tiene la Ley 2338/2023[38] aprobada el 10 de diciembre de 2024 que establece una serie de reglas que deben cumplir los sistemas inteligentes para ser considerados como IA fiable, respetando los derechos de propiedad intelectual y generales de los ciudadanos. Lo llamativo de esta normativa es que es la primera en todo el continente americano en regular aspectos como la responsabilidad civil, estableciendo que el proveedor o el operador del sistema que cause un daño material o moral debe repararlo independientemente del grado de autonomía que posea el sistema, pero realiza una distinción: cuando se trate de un sistema de alto riesgo el proveedor responderá objetivamente dependiendo de su participación en la conducta dolosa; cuando se trate de un sistema de un sistema de bajo riesgo se establece un sistema de responsabilidad por culpa, aplicándose la inversión de la carga de la prueba. En esta ley se contempla también la creación de sandboxes, que son entornos donde se puede practicar, ensayar y probar modelos de IA antes de implementarla definitivamente.

28. Por otra parte, Brasil cuenta también con la Estrategia de Brasil para la Inteligencia Artificial[39], cuyos objetivos principales son: contribuir a la elaboración de principios éticos para el desarrollo y el uso de la IA responsable; promover inversiones sostenidas en investigación y desarrollo de IA;

[35] Disponible en: https://www.senado.gob.mx/66/gaceta_comision_permanente/documento/135000

[36] Disponible en: https://sil.gobernacion.gob.mx/Archivos/Documentos/2024/04/asun_4729480_20240402_1712079223.pdf

[37] Disponible en: https://www.camara.cl/verDOC.aspx?prmID=72777&prmTipo=FICHAPARLAMENTARIA&prmFICHATIPO=DIP&prmLOCAL=0

[38] Disponible en: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233

[39] Disponible en: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial

eliminar las barreras a la innovación en IA; empoderar y formar profesionales para el ecosistema de IA; estimular la innovación y el desarrollo de la IA brasileña en un entorno internacional; y promover un entorno cooperativo entre entidades públicas y privadas, centros de industria e investigación para el desarrollo de la Inteligencia Artificial.

3. El caso de la Unión Europea

29. En abril de 2021, la Comisión Europea propuso el primer proyecto europeo que regulaba la IA cuyo rasgo distintivo fue el enfoque basado en el riesgo, vertebrado en una estructura piramidal. Por ello, la Unión Europea se convirtió y actualmente es la primera potencia en adoptar un enfoque claramente regulacionista y proteccionista con los derechos de los usuarios. Esta propuesta de la Comisión se materializó el pasado 12 de julio de 2024 en el RIA, y se caracteriza por realizar una distinción entre los diversos tipos de sistemas de IA que en función de su categoría se someterán a unas normas armonizadas u otras. Esto supone un cambio de paradigma, debido a que esta perspectiva supone variar la tendencia a adoptar una regulación uniforme para todas las formas de IA de la UE[40]. Esto pone de manifiesto que este instrumento tiene un carácter generalista, buscando abordar el uso de los sistemas de IA de un modo global y no especializado, sin distinguir entre las diversas materias o sectores que se pueden ver implicados.

30. La finalidad principal del Reglamento es crear unas mejores condiciones para el uso y desarrollo de la IA, creando un entorno donde se erradiquen las prácticas discriminatorias y permitiendo que la IA se convierta en una tecnología segura, transparente, trazable y respetuosa.

31. Por lo que respecta a otras temáticas relacionadas con la inteligencia artificial es importante señalar que el RIA exclusivamente se ciñe a clasificar los diferentes tipos de IA y establecer obligaciones para los responsables y el sistema de sanciones. Con respecto a la responsabilidad y los daños causados por los sistemas inteligentes estas materias estaba previsto que se regularan en un instrumento normativo diferente. Por ello nos encontramos en un primer momento con dos instrumentos que iban a regularla[41]:

- Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo (Directiva de productos defectuosos[42])
- Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA de 2022[43])

32. Con respecto a la Propuesta de Directiva de responsabilidad en materia de IA esta solo establecía aspectos procesales, no regulando la responsabilidad en sí, y derivaba a los regímenes de responsabilidad por culpa que establecieran los diferentes Estados Miembros. Tenía previsto el ejercicio de acciones contra cualquier causante del daño, ya fuera proveedor, distribuidor o importador por cualquier tipo de daño resarcible. Se trataba de una norma de armonización mínima que daba un amplio margen de discrecionalidad a los Estados. En base a esta propuesta se entendía por afectado por el daño cualquier persona que podía reclamar cualquier tipo de daño, pero siempre orientado a los producidos por los sistemas clasificados según el Reglamento de IA como de alto riesgo[44]. Este proyecto tenía como objetivo

[40] J. C. Fernández Rozas, "La Ley de Inteligencia Artificial de la Unión Europea: un modelo para innovaciones radicales, responsables y transparentes basadas en el riesgo", La *Ley Unión Europea*, nº 124, 2024, pp. 12-13.

[41] C. Muñoz García, *Regulación de la inteligencia artificial en Europa: Incidencia en los regímenes jurídicos de protección de datos y de responsabilidad por productos*, Tirant lo Blanch, Valencia, 2023, p. 194.

[42] DOUE-L-2024-81701, de 18 de noviembre de 2024

[43] COM (2022) 496 final de 28 de septiembre de 2022

[44] M.L. Atienza Navarro, ¿Son necesarias reglas especiales para los daños causados por Inteligencia Artificial? en I. Herbosa Martínez, y D. Fernández de Retana Gorostizagoiza, (dirs.), *Derecho e inteligencia artificial. El jurista ante los retos de la era digital*, Aranzadi, Navarra, 2023, p. 403.

facilitar la carga de la prueba y la relación de causalidad de los daños causados por sistemas inteligentes, introduciendo la presunción de causalidad, e incorporando medidas que favorecían la obtención de la prueba y la identificación de las personas responsables para evitar la opacidad a la que a veces se enfrentaban las víctimas cuando el sistema inteligente era de caja negra.

33. Por su parte, la Directiva de productos defectuosos establece normas de responsabilidad objetiva y resulta aplicable tanto a sistemas de IA como a productos físicos que lleven incorporados sistemas de IA. Exclusivamente prevé la acción de reclamación frente al fabricante o productor aparente y da vía a la exención de responsabilidad.

34. Lo relevante de este asunto es que, como se puede observar, a pesar de haber sido publicadas ambas propuestas en 2022, solo la Directiva de productos defectuosos ha visto la luz a finales del año pasado. ¿Qué ha pasado con la Propuesta de Directiva de responsabilidad en materia de IA?

35. Pues bien, a pesar de la a priori férrea posición europea que siempre ha abogado por una protección ferviente de la ciudadanía frente a las injerencias que podían llevar a cabo las grandes compañías y empresas tecnológicas, en el último año parece que la UE ha optado por dar un cambio de rumbo a su línea de actuación, auspiciada por la nueva administración llevada a cabo por el Gobierno de los Estados Unidos, que apuesta abiertamente por la desregulación[45]. A principios del año 2025, los días 10 y 11 de febrero tuvo lugar en París la Cumbre sobre Inteligencia Artificial, momento que aprovechó la Unión Europea para anunciar que su nuevo objetivo respecto a la inteligencia artificial es ponerse a la cabeza y estar a la altura de la carrera competitiva empresarial, para ser una firme competidora de potencias tales como China y Estados Unidos. En ese mismo momento retiró la propuesta de Directiva sobre responsabilidad en materia de IA, lo que supone que la Propuesta que llevaba parada ya tres años, ha desaparecido por completo del horizonte legislativo europeo, dejando descolgada parte de la regulación que estaba planeada.

4. Ámbito de aplicación del Reglamento

A) Ámbito competencial

36. En primer lugar, con respecto al ámbito competencial, el RIA se aplica únicamente a las materias que están dentro del ámbito de aplicación de la legislación europea sin interferir en la competencia de los respectivos Estados Miembros. Por ello, quedan excluidos del ámbito competencial materias tales como la IA con fines militares o de defensa, investigación o innovación[46].

B) Ámbito material

37. Con respecto al ámbito material, este Reglamento no constituye una mera guía con recomendaciones o estipulaciones de carácter blando, sino que establece las diversas responsabilidades de los sujetos y las consecuencias por su incumplimiento. Para conseguir que efectivamente se cumpla lo estipulado cuenta con diversas herramientas: abundantes mecanismos de control como autoridades de control del mercado, con potestad para comprobar e intervenir (art. 70), controles y procedimientos de autorización para la creación de los denominados sistemas de alto riesgo (art. 5); sanciones severas en caso de incumplimiento (art. 99) y multas administrativas (art. 100 y 101).

[45] M. barrio andrés, "El cambio de paradigma de la regulación global de la inteligencia artificial" *Derecho Digital e Innovación. Digital Law and Innovation Review*, n.º. 23, p. 1.

[46] J. C. fernández rozas, "La Ley de Inteligencia Artificial de la Unión Europea: un modelo para innovaciones radicales, responsables y transparentes basadas en el riesgo…" *op cit*. p. 18

C) Ámbito territorial

38. Más interesante, controversial y complejo resulta sin duda el ámbito territorial de este instrumento jurídico. El artículo 2.1 del RIA cobra una importancia singular al delimitar el ámbito de aplicación subjetivo y territorial del Reglamento, ya que concreta quiénes van a estar sujetos a las obligaciones que el instrumento contempla, expresándose en los siguientes términos: "El presente Reglamento se aplicará a: a) los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA o que introduzcan en el mercado modelos de IA de uso general en la Unión, con independencia de si dichos proveedores están establecidos o ubicados en la Unión o en un tercer país; b) los responsables del despliegue de sistemas de IA que estén establecidos o ubicados en la Unión; c) los proveedores y responsables del despliegue de sistemas de IA que estén establecidos o ubicados en un tercer país, cuando los resultados de salida generados por el sistema de IA se utilicen en la Unión; d) los importadores y distribuidores de sistemas de IA; e) los fabricantes de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca; f) los representantes autorizados de los proveedores que no estén establecidos en la Unión; g) las personas afectadas que estén ubicadas en la Unión."

39. Por lo tanto, atendiendo a la literalidad del precepto, tanto los proveedores como los usuarios y sistemas de IA que estén en la UE o en terceros países se encuentran vinculados por el Reglamento cuando la información de salida del sistema de IA se utilice en la UE. Esto significa que el Reglamento tiene un carácter transfronterizo y extraterritorial, que debe ser analizado con detenimiento. Esta concepción de la extraterritorialidad en materias relacionadas con el mundo virtual "no físico" surgió por primera vez con el Reglamento General de Protección de Datos (que posteriormente comentaremos), cuyo artículo 3.2 prevé la aplicación del Reglamento al tratamiento de datos personales de interesados que residan en la Unión por parte del responsable o encargado no establecido en la Unión cuando se ofrecen, dirigen o personalizan los servicios a personas físicas dentro de la UE[47].

40. A pesar de que el RGPD supusiera un primer acercamiento a la extraterritorialidad digital, el RIA propone una aplicación mucho más amplia, como señala el considerando 21 "Con el objetivo de garantizar la igualdad de condiciones y la protección efectiva de los derechos y libertades de las personas en toda la Unión, las normas establecidas en el presente Reglamento deben aplicarse a los proveedores de sistemas de IA sin discriminación, con independencia de si están establecidos en la Unión o en un tercer país, y a los responsables del despliegue de sistemas de IA establecidos en la Unión." En este sentido, el art. 3.1 del RIA, de forma parecida a lo que establece el art. 3.2 del RGPD prevé la aplicación del Reglamento a los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA con independencia de si están ubicados dentro o fuera de la UE, al igual que los responsables del despliegue de sistemas de IA siempre que los resultados de salida generados por el sistema de IA se utilicen en la Unión.

41. Sin embargo, respecto de la interpretación de este precepto nos encontramos con dos corrientes: la primera, que defiende que se debe interpretar literalmente, de modo que el RIA tiene vocación de ser aplicado a cualquier sujeto que con voluntad o no despliegue efectos con sus productos en la UE y otra vertiente, que interpreta que el art. 3.1 del RIA debe interpretarse como que se aplica solamente cuando el proveedor de los servicios y sistemas de IA ha dirigido voluntariamente sus actividades a la UE y no en todo caso.

42. Comenzando con la primera teoría, para algunos autores, mientras que el RGPD tiene vocación de ser aplicado cuando el sujeto fuera de la UE busca dirigir sus actividades dentro de la UE, el RIA se aplica incluso cuando el proveedor o el responsable del despliegue no tenía intenciones de dirigir sus actividades a la UE[48].

[47] M. Barrio Andrés, "El efecto Bruselas del Reglamento Europeo de inteligencia artificial", OTROSÍ*: Revista del Colegio de Abogados de Madrid*, nº2, 2024, p. 47.

[48] *Ibid*, p. 48.

43. Para poder entenderlo mejor realizaremos un ejemplo práctico: La empresa 1, con sede en Argentina dedicada a crear un software capaz de procesar imágenes de cerebros y detectar Alzheimer en estadios tempranos vende dicho software a la empresa 2, que tiene su sede en Japón y se dedica a incluir dicho software en un dispositivo electrónico sanitario. Cuando la empresa japonesa realiza una tirada lo suficientemente numerosa de aparatos decide abrir una sucursal en Sevilla para comenzar a comercializar este invento novedoso. Pues bien, según lo que estipula el propio RIA, la empresa argentina (1), sería responsable del despliegue del sistema de IA, ya que el software es considerado un contenido y sistema de IA según el art. 3.1. Por otra parte, la actividad que está llevando a cabo la empresa 1 sería un resultado de salida. Aunque pueda parecer extraño, en virtud del comentado art. 2.1.c), el RIA le resultaría aplicable a la empresa argentina que no ha tenido ningún contacto directo con Europa ni ha pretendido expandir su invento en territorio europeo. La doctrina señala que, para evitar este tipo de situaciones, la única opción que le quedaría a la empresa 1 sería incluir una cláusula contractual en la que ésta prohíba a su cliente (empresa 2 japonesa) comercializar su producto en la UE [49].

44. Como se puede observar, este efecto expansivo del RIA lleva a que toda empresa del mundo que trabaje como proveedora de servicios tecnológicos o responsable de despliegue de cualquier tipo de sistema de IA se vea abocada a que se le aplique el RIA en función del comportamiento de la empresa compradora. Se podría considerar, por lo tanto, que dicho Reglamento tiene una vis expansiva excesivamente amplia que puede dar lugar a problemas futuros.

45. Con respecto a la segunda teoría, recordemos, consistente en que el RIA solo se aplica cuando existe una cierta voluntad de conexión con la UE, la doctrina[50] pone de manifiesto que Internet es un medio global sin fronteras pero que este hecho no resulta suficiente como para interpretar que el art. 3 del RIA haga que se pueda aplicar el RIA cuando los sistemas de IA desarrollados por proveedores sitos en terceros Estados sean accesibles por clientes en Europa. Para sustentar esta teoría se basan en la necesidad de que existan criterios de conexión, que hacen que el RIA solo se pueda aplicar cuando los proveedores lleven a cabo actividades que presenten una conexión o vinculación estrecha con la UE, produciendo efectos en el mercado o dirigiendo sus actividades. Para esta rama doctrinal, la interpretación contraria, es decir, la aplicación masiva del RIA supondría una gran inseguridad jurídica de los operadores que no podrían determinar cuándo estarían obligados a cumplir los requisitos del RIA y sus obligaciones ya que no tendrían la posibilidad de saber los actos que van a llevar a cabo las empresas a las que les venden dichos productos y, por otra parte, supondría una aplicación injustificada en situaciones que no tienen ningún tipo de vinculación con la UE.

46. Sea como fuere, llegados a este punto puede surgirnos la duda de qué ha podido llevar a la UE a redactar un artículo tan sumamente amplio o, más bien, a buscar esa extraterritorialidad en la aplicación del RIA. La respuesta se basa en dos razones fundamentales. La primera es que si no se aplica de manera extensiva el Reglamento no habría forma de garantizar una protección integral de los derechos fundamentales de los ciudadanos europeos, ya que solamente quedarían protegidos si la empresa distribuidora del sistema inteligente operase en la UE, lo cual realistamente no es verídico. En segundo lugar, la vocación de extraterritorialidad garantiza que los proveedores de sistemas de IA puedan competir en situación de igualdad, ya que las obligaciones que se les impone son las mismas independientemente de donde estén sitos. Si el RIA solo se aplicase a las empresas con sede en Europa, esto pondría a los terceros Estados en una situación de ventaja frente a las empresas europeas que deberían cumplir con todo el entramado obligacional de la norma y haría que, con el tiempo, las empresas europeas buscasen establecerse en territorio extracomunitario a pesar de operar en Europa por tal de evadir los requisitos del RIA.

47. Sin embargo, se ha de tener en cuenta que una gran desventaja de la extraterritorialidad radica precisamente en ese trato igualitario que puede llevar a las empresas a pensar que como independien-

[49] *Ibid* p. 48.

[50] A. López-Tarruella Martínez, "El futuro Reglamento de Inteligencia Artificial y las relaciones con terceros Estados", *Revista electrónica de estudios internacionales (REEI)*, nº 45, 2023, p. 6.

temente de donde estén situadas van a tener que cumplir con el Reglamento si quieren operar en Europa, podría ser nuestro territorio prescindible dentro de su mercado, lo cual provocaría un desabastecimiento de servicios digitales e inteligentes, convirtiéndose nuestro continente en un cementerio tecnológico.

48. Este tipo de argumentación ha llevado a la doctrina a crear el término "efecto Bruselas", referido a la emigración de empresas europeas a terceros Estados con el fin de evitar la aplicación de la normativa tan exigente que se requiere en Europa. En el caso del RIA hay quienes consideran que ya se está dando el referido efecto, ya que si un proveedor quiere incluir datos extraídos de ciudadanos europeos para entrenar a su sistema de IA debe cumplir con las exigencias del RIA[51]. Por lo tanto, resultaría complejo que si esa misma empresa quiere ofrecer sus servicios en terceros Estados tenga que entrenar a sus sistemas exclusivamente con datos extraídos de pacientes fuera de la UE para poder comercializarlos fuera de Europa, ya que supondría una bifurcación del mismo sistema de IA en función de la población a la que vaya dirigido, lo cual repercutiría gravemente en la economía y el presupuesto de la empresa tecnológica[52].

49. Si bien algunos autores, como Bradford defienden que en ningún caso podría darse un abandono empresarial de las compañías tecnológicas en Europa por el gran volumen humano y económico que supone el continente, López-Tarruella en cambio apunta que en 2024 OpenAi lanzó una IA generativa con capacidad de conversión de textos a vídeos en todo el mundo, salvo en Europa; lo mismo ocurre con Apple Intelligence. Según este autor, esa huida de la UE no se debe a una falta de recursos económicos sino a un temor a las posibles sanciones a las que se pueden enfrentar si no cumplen con la normativa europea del RIA[53]. Siguiendo de nuevo a López-Tarruella otra desventaja de considerar esa aplicación extraterritorial es y un sistema tan encorsetado de obligaciones es la presión ejercida sobre las empresas con un volumen de negocios mediano o pequeño, ya que no cuentan con recursos suficientes como para poder ponerse al día de las obligaciones que se les exigen y que suponen un gran coste económico, tales como la redacción de códigos de buenas prácticas internos, la creación de *sandboxes*, la contratación de personal específico de control, etc.

D) Competencia de las autoridades nacionales de control

50. Otro aspecto relevante que contempla el RIA en el art. 70 es la creación de unas autoridades nacionales de control para supervisar que se cumplen las obligaciones previstas en el Reglamento que deben ser designadas por los Estados miembros. Una de las funciones que tiene precisamente esa autoridad de vigilancia del mercado, según estipula el art. 85 es la de tramitar las reclamaciones que cualquier persona física y jurídica puede presentar cuando considera que se ha infringido lo dispuesto en el Reglamento. Para estas autoridades de vigilancia, el art. 3 del RIA adquiere un nuevo carácter, ya que se convierte en una norma de competencia internacional, pero no en el sentido jurídico tradicional, sino de competencia de las autoridades administrativas internacionales nombradas por cada Estado para poder conocer de las reclamaciones que las personas les presenten en relación con un incorrecto cumplimiento del Reglamento. Por ello, estas autoridades deberán justificar su competencia acudiendo precisamente al art. 3 y no al Reglamento (UE) Nº 1215/2012 del Parlamento Europeo y del Consejo de 12 de diciembre de 2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (RBIbis[54]).

[51] A. Bradford, *Digital Empires: The Global Battle to Regulate Technology*, OUP, Oxford, 2023, pp. 397-398.

[52] A. López-Tarruella Martínez, "Claroscuros del "efecto Bruselas" del Reglamento de Inteligencia Artificial", *Revista Española de Derecho Internacional*, vol. 77, n.º.1, 2025, p. 239.

[53] En concreto, el art. 99 del RIA establece en su apartado tercero que si no se respeta la prohibición de las prácticas de IA referidas en el art. 5 las multas pueden llegar hasta los 35 millones de euros, y si el infractor es una empresa hasta el 7% de su volumen de negocios mundial. En el caso de incumplimiento de las obligaciones no referidas en el art. 5 las multas pueden llegar a 15 millones o el 3% del volumen de negocios mundial total.

[54] DOUE-L-351/1, de 20 de diciembre de 2012.

51. Precisamente por tratarse de una autoridad administrativa, la única disposición que van a poder aplicar es su propia ley, es decir, el RIA, no pudiendo planteárseles la aplicación de algún Derecho extranjero de un tercer Estado, ya que se trata de una relación estructural *forum-ius*[55]. Además de esta especialidad, igual que ocurre con el RGPD, el RIA prevé la aplicación de la normativa europea y no la de un Estado en concreto. Lo mismo ocurre con la competencia de las autoridades de control, que se otorga de manera general y no para cada autoridad en concreto (ya que estas serán elegidas por los diferentes Estados). Por estas características especiales puede surgir la duda de cómo se solventaría una cuestión cuando la controversia está relacionada con diferentes Estados miembros, es decir, cuál es la autoridad de control que debería actuar. Para responder a este interrogante habría que acudir de nuevo al art. 85, que establece una competencia territorial de esta figura, de modo que se podría entender que sería competente la autoridad donde el actor de la acción tiene su residencia habitual o donde se le produjo el daño[56].

E) Aplicación del RIA como norma de policía por los tribunales

52. Una última perspectiva que debemos analizar del RIA es su aplicación por los órganos jurisdiccionales. Esto se debe a que en el seno de una prestación de servicio de un sistema de IA puede que se produzca algún tipo de daño del que se derive responsabilidad extracontractual o algún tipo de incumplimiento del contrato de servicios. En esta amplia casuística podría existir la posibilidad de que el RIA sea invocado como norma que sustenta la demanda. Concretamente, al tratarse de litigios civiles, por lo que respecta a la competencia judicial internacional de cualquier órgano judicial de un Estado Miembro, éste deberá determinarla según lo dispuesto en el RBI bis, y por lo que respecta a la ley aplicable, dependerá del petitum de la demanda: si se trata de una controversia relacionada con responsabilidad extracontractual, será de aplicación el Reglamento (CE) Nº 864/2007 del Parlamento europeo y del Consejo de 11 de julio de 2007 relativo a la ley aplicable a las obligaciones extracontractuales (RRII[57]); mientras que si el litigio versa sobre un incumplimiento contractual, habrá que aplicar el Reglamento (CE) nº 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (RRI[58]).

53. En estos casos, el RIA sería aplicable igualmente, pero en su vertiente de ley de policía. La ley de policía se puede definir en virtud del art. 9.1 del RRI como una disposición cuya observancia un país considera esencial para la salvaguarda de sus intereses públicos, cualquiera que sea la ley aplicable al contrato. Se puede entender que el RIA es una norma de policía ya que el propio considerando primero señala que "una de las finalidades del Reglamento es asegurar un nivel elevado de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, proteger frente a los efectos perjudiciales de los sistemas de IA en la Unión, así como brindar apoyo a la innovación". Al considerar el RIA como una norma de policía, esto llevaría a su aplicación preferente frente al Derecho material que sea aplicable que surja por la aplicación de la correspondiente norma de conflicto. En consecuencia, incluso cuando el Derecho aplicable sea el de un tercer Estado, el tribunal competente debería aplicar el RIA con preferencia[59]. Sobre este aspecto resulta relevante mencionar la STJUE de 21 de enero de 2019, As. C-148/18, Agostinho Da Silva Dekra Claims Services Portugal SA[60], que concretó por primera vez cuáles eran las circunstancias que debían darse para que la aplicación de la ley designadas por las partes quedara descartada por las normas de policía. En esta sentencia el

[55] A. López-Tarruella Martínez, "El futuro Reglamento de Inteligencia Artificial y las relaciones con terceros Estados…" *op cit*. p. 8.

[56] Ibid. p. 9.

[57] DOUE-L-199/40, de 11 de julio de 2007.

[58] DOUE-L-2008-81325, de 4 de julio de 2008.

[59] López-Tarruella Martínez, A. "El futuro Reglamento de Inteligencia Artificial y las relaciones con terceros Estados…" *op cit*. p. 10.

[60] ECLI:EU:C:2019:84

TJUE mantiene una interpretación restrictiva de la noción de leyes de policía[61], en la línea del Abogado General, argumentando que se trata de disposiciones que suponen una excepción a la ley previamente designada por la norma de conflicto de los Reglamentos Roma I y Roma II. Una interpretación extensiva y más flexible impediría conseguir los objetivos que tiene el instrumento en cuestión (la ley de policía)[62]. Para poder apreciar cuándo nos encontramos ante una norma con la consideración de ley de policía es necesario, según el TJUE verificar que la disposición se ha adoptado por el legislador con la finalidad de proteger intereses públicos especialmente importantes. Como herramienta para responder a esta cuestión se debe analizar la estructura general de la norma, los objetivos y las circunstancias que han motivado su promulgación. En segundo lugar, es necesario asegurarse de que la disposición constituye una expresión de los principios fundamentales del ordenamiento en cuestión. Finalmente, el último requisito hace referencia a que la aplicación de la disposición sea absolutamente imprescindible para poder proteger el interés del caso en concreto. Añade la doctrina, que una pista para poder averiguar si una norma posee la cualidad de ley de policía puede ser el hecho de que contenga sanciones en caso de incumplimiento, no siendo este un requisito fijo, ya que, dentro del ámbito legislativo de cada uno de los países, cada Estado es soberano para establecer qué normas dentro de su ordenamiento van a poseer el carácter de policía[63]. Por otro lado, otros indicativos de que nos encontramos ante normas de policía puede ser la idea de orden social que imponen dichas normas; que se trate de normas que regulen los efectos que las relaciones entre particulares producen dentro del propio Estado o las normas que regulan la sociedad civil[64].

54. Yendo incluso más allá, si abogamos por la teoría antes mencionada sobre el ámbito de aplicación territorial determinado por la vinculación estrecha con la UE y no de manera general, nos encontramos con que solamente se podrá entender aplicable el RIA en su vertiente de norma de policía cuando entren en juego o puedan verse lesionados los objetivos que pretende el Reglamento. Sobre esta cuestión se ha pronunciado ya el Tribunal de Justicia de la Unión Europea (TJUE) en su sentencia de 24 de septiembre de 2019, Google France, C-507/17[65], que se podría aplicar por analogía de la siguiente forma: en la sentencia se llega a la conclusión de que la normativa sobre el derecho al olvido se puede aplicar cuando afecta a un interesado en sede europea, es decir, cuando la búsqueda se realiza desde una dirección IP localizada en uno de los Estados Miembros sujetos a la normativa concreta. En nuestro caso podría aplicarse de modo parecido, es decir, cuando el daño o la injerencia se produzca a un ciudadano que se encuentre establecido en alguno de los Estados Miembros en los que resulta aplicable el RIA. De hecho, la aplicación de las leyes de policía constituye un elemento recurrente en la regulación de las relaciones internacionales. Esta realidad se manifiesta con mayor claridad en el ámbito digital, donde la defensa de los intereses europeos solo puede asegurarse mediante la aplicación de normas imperativas de este tipo.

IV. El Reglamento General de Protección de Datos como freno al uso de datos

55. Habiendo visto cómo la UE ha contemplado la regulación de la IA, procede ahora aclarar porqué se relaciona habitualmente el RIA con el RGPD y cuál es la jerarquía exacta entre ellos. Cuando se habla de IA desde el inicio de la creación del sistema, pasando por todas sus etapas se deben implementar una serie de medidas tanto técnicas como organizativas para garantizar que están protegiendo

[61] Esta misma visión restrictiva de las normas de policía ya había sido puesta de manifiesto por el TJUE en las sentencias: de 23 de noviembre de 1999, Arblade, C-369/96 y C-376/96, ECLI:EU:C:1999:755; de 9 de noviembre de 2000, Ingmar, C-381/98, ECLI:EU:C:2000:605; de 6 de octubre de 2009, Asturcom, C-40/08, ECLI:EU:C:2009:615 ; de 17 de octubre de 2013, UNAMAR, C-184/12, ECLI:EU:C:2013:663.

[62] M. Vixaina Miquel, "La ley aplicable a la determinación del alcance de la indemnización de los daños morales sufridos por víctimas indirectas de accidentes de tráfico: ¿son los "criterios de equidad" una "ley de policía" según el art. 16 del Reglamento Roma II? (STJUE de 5 de septiembre de 2024, as. C-86/23, E.N.I, Y.K.I c. Huk-Coburg-allgemeineversicherung ag)" *Crónica de Derecho Internacional Privado*, núm. 48, 2024, p. 501.

[63] E. C. Torralba Mendiola, "La aplicación de las leyes de policía contenidas en Directivas de la Unión Europea. El ejemplo de la regulación de la cadena alimentaria" *REDI*, vol. 75, núm. 1, 2023, p. 144.

[64] A. L. Calvo Caravaca, et al, *Tratado de derecho internacional privado*, Tirant lo Blanch, Valencia, 2022, pp. 504-506.

[65] ECLI:EU:C:2019:772

los datos que se usan para el entrenamiento del programa. Las más habituales son la obtención del consentimiento informado y libre de las personas que ceden dichos datos, la transparencia sobre cómo se van a utilizar dichos datos. Esto se debe a que los sistemas de IA son al fin y al cabo sistemas de procesamiento de información, por lo que los datos van íntimamente ligados al desarrollo y el éxito del sistema inteligente[66]. Esas grandes cantidades masivas de datos es lo que comúnmente se denomina *big data* y son esenciales para entrenar los modelos mediante algoritmos de *machine learning* capaces de encontrar correlaciones entre la información introducida.

56. A pesar de que puedan existir datos que se utilicen para el entrenamiento de la IA que no sean personales, la realidad refleja que la gran mayoría de ocasiones los datos utilizados tienen la consideración de datos personales, por lo que será de aplicación el RGPD. Por lo tanto, el RGPD estará presente en todo el ciclo de vida del sistema de IA. Comenzando con la fase de entrenamiento del modelo, posteriormente la de validación, a la que se le introducirán datos sobre situaciones reales para evaluar la calidad del modelo y su correcto funcionamiento. En algunas ocasiones los datos que se introducen en la fase de validación pueden ser diferentes a los datos introducidos durante el entrenamiento, por ejemplo, porque la empresa haya externalizado el servicio de validación a una segunda empresa que certifique la calidad del mismo.

1. Ámbito de aplicación

A) Ámbito material

57. El principal objetivo que presenta este Reglamento aparece recogido en el art. 2.1 y es proteger los derechos y libertades fundamentales de las personas físicas, en concreto el derecho a la protección de datos personales. Este instrumento normativo tiene vocación de ser aplicado al tratamiento automatizado de datos personales y al no automatizado de datos personales contenidos o destinado a ser incluidos en un fichero (art. 2.1). Al igual que ocurre con el RIA, el RGPD se aplica exclusivamente a los datos personales que se traten en el ejercicio de una actividad comprendida en el ámbito de aplicación del Derecho de la Unión (art. 2.2.a).

B) Ámbito territorial

58. Con respecto al ámbito territorial, como hemos mencionado anteriormente, el RGPD fue un instrumento pionero, al prever por primera vez en un instrumento sobre temática digital una aplicación extraterritorial. La intención del legislador según la doctrina es que la protección en materia de datos viajase allí donde se movían los datos, para que no quedaran desprotegidos los usuarios ante el movimiento ingente de cantidades de datos a nivel mundial[67]. En este sentido, el art. 3 prevé que se aplique al tratamiento de datos personales en el contexto de actividades de un establecimiento del responsable, independientemente de que el tratamiento tenga lugar en la Unión o no cuando las actividades de tratamiento estén relacionadas con alguno de los siguientes elementos: la oferta de bienes o servicios a los interesados que se encuentran en la Unión, independientemente de si la contraprestación requiere pago y cuando el tratamiento esté relacionado con el control del comportamiento.

59. En este punto la doctrina[68] ha señalado el sentido que se le debe dar concretamente a este artículo, entendiendo que el Reglamento es aplicable cuando el responsable proyecta ofrecer servicios

[66] M. Pérez-Ugena Coromina, Protección de datos en la aplicación de sistemas de inteligencia artificial, *Parlamento y Constitución. Anuario*, n.º 25, 2024, p. 210.

[67] A. Ortega Giménez, "La extraterritorialidad del nuevo Reglamento europeo de Inteligencia Artificial", *Revista jurídica: Región de Murcia*, n.º 54, 2024, pp. 122-124.

[68] P. A. Miguel Asensio, "Competencia y derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea", *Revista española de derecho internacional*, vol. 69, 2017, n.º 1, p. 84.

a los interesados que se encuentran en un Estado miembro. En este sentido no se podría valorar como suficiente el hecho de que el servicio online se encuentre en una lengua accesible para los ciudadanos de la Unión, sino que se hace necesaria la concurrencia de otros factores que den a entender de manera inequívoca la intención del responsable de dirigir sus actividades directamente a los países de la Unión, como que se usen varias lenguas oficiales, o monedas, o se presten servicios específicos para ciudadanos residentes o se mencione directamente a los clientes o usuarios de países específicos. Siguiendo la jurisprudencia más clásica del TJUE, contenida en la STJUE de 7 de diciembre de 2010, *caso Pammer y Hotel Alpenhof*, C-585/08[69], ente los indicios más relevantes de que existe esa intencionalidad se encuentra la mención de que ofrezca sus servicios o bienes en un Estado miembro, la publicidad dirigida a consumidores domiciliados en ese Estado, la mención de números de teléfono con un prefijo concreto, o el uso de un nombre comercial específico[70].

2. Previsiones generales e interacción con el RIA

60. Ahora bien, ¿cómo establece el RGPD que deben tratarse los datos que se van a usar para entrenar al sistema de IA? El art. 5 del RGPD recoge una serie de principios que se deben tener en cuenta: los datos se deben tratar de forma lícita, leal, transparente; se deben recoger con unos fines determinados, explícitos, legítimos, adecuados, pertinentes y limitados al uso para el que fueron recogidos, sin posibilidad de ser tratados ulteriormente con fines distintos a los iniciales; deben ser exactos, actualizados y mantenidos de forma que permitan la identificación de los interesados durante el tiempo concreto estipulado. Si nos referimos concretamente a los datos en el ámbito sanitario, estos tienen la consideración de datos sensibles según el art. 9, lo que hace que para que su tratamiento sea lícito deba existir un consentimiento previo por parte del paciente.

61. Siendo esto así y recordando que nuestro objeto de estudio es el entrenamiento de IA con datos en el ámbito sanitario, debemos dejar de lado cuestiones interesantes como las decisiones individuales automatizadas o la creación de perfiles de los pacientes (art. 22), que se salen de nuestro ámbito de estudio ya que no versan concretamente sobre el entrenamiento de la IA. Llegados a este punto habremos observado que el RGPD realiza pocas previsiones sobre los límites para poder entrenar a la IA y, desde el punto de vista de los ingenieros de datos, que se encuentran lejanos al mundo jurídico, una serie de principios generales que deben regir el tratamiento no ilustran con claridad cómo deben actuar durante el entrenamiento de su programa. Sobre este aspecto resulta especialmente llamativa la reciente publicación por parte de la Comisión Europea de la plantilla obligatoria derivada del art. 53.1 del RIA que recogía la obligación de los proveedores de modelos de IA de propósito general de divulgar públicamente los datos utilizados para su entrenamiento. De este modo lo que anteriormente se venía haciendo de modo voluntario por algunas empresas al estar establecido en códigos de buenas prácticas, ahora se convierte en una obligación legal cuya entrada en vigor es el 2 de agosto de 2025. Además de los datos de entrenamiento deberán publicar información general sobre el modelo, si los datos se han obtenido de bases públicas, privadas, webs, datos sintéticos, etc, además del tipo de procesamiento que se ha aplicado. De incumplirse dicha obligación se plantean multas de hasta quince millones de euros o el tres por ciento de la facturación global anual del proveedor. Con respecto a las fechas más relevantes de este documento, el 2 de agosto de 2027 es el plazo límite para modelos ya comercializados antes del 2 de agosto de 2025 y el 2 de agosto de 2026 es el inicio del régimen de supervisión y sanción por parte de la AI Office.

62. Es por ello que, en ocasiones pueden surgir daños derivados de infracciones del RGPD que deben ser reparadas, ahora bien, en la gran mayoría de ocasiones los responsables no serán estos inge-

[69] ECLI: EU:C:2010:740

[70] A. Ortega Giménez, "El impacto extraterritorial del Reglamento europeo de inteligencia artificial", *Anuario de la Facultad de Derecho*, nº 17, 2024, p. 227.

nieros cuya única función es experimentar, probar, entrenar y lanzar la IA, sino los responsables del tratamiento de datos, que son los que deben cumplir con las previsiones del RGPD a la hora de seleccionar los datos y posteriormente guardarlos o eliminarlos para que no existan intromisiones.

63. Para responder a esta necesidad de cubrir los daños, el Reglamento General de Protección de Datos prevé su art. 82, relativo al derecho a la indemnización y la responsabilidad del encargado del tratamiento de datos. Recientemente la STJUE de 11 de abril de 2024, *asunto Juris* 724/21[71] ha tratado precisamente cuáles son los requisitos para poder solicitar una indemnización y el sistema de funcionamiento de la responsabilidad en caso de error de una persona que actúa bajo la autoridad del responsable un litigio que versaba sobre un abogado que pedía responsabilidad a una empresa de base de datos jurídica por no haber respetado su derecho de oposición[72].

64. La primera cuestión prejudicial que plantea el tribunal alemán en este caso es la referida a si es posible considerar la mera infracción del RGPD como un daño o perjuicio inmaterial que da lugar a su respectiva indemnización, por conferir un derecho subjetivo o si es necesario que se produzca un daño independiente. En este sentido señala el TJUE que para que del art. 82 del RGP surja un derecho a indemnización es necesario que concurran tres requisitos:

– La existencia de un daño y perjuicio material o inmaterial
– La infracción del RGPD
– La relación de causalidad entre los daños y la infracción

65. Por lo tanto, la mera infracción del RGPD no puede constituir por sí sola un daño o perjuicio indemnización, siendo necesario probar los daños sufridos.

66. En segundo lugar, con respecto a la responsabilidad en caso de error, el responsable en este litigio pretendía ser declarado no culpable por no ser responsable del hecho causante de los daños, ya que en virtud del art. 82.3 el responsable del tratamiento puede quedar exento de responsabilidad si demuestra que no es en modo alguno responsable del hecho que ha causado los daños y perjuicios. En este caso el responsable alegaba que el culpable de la infracción había sido una persona que trabajaba en su equipo, pero no él directamente. El TJUE en este caso establece que el régimen de responsabilidad que aparece recogido en el Reglamento es un régimen de responsabilidad por culpa, recayendo la carga de la prueba en el responsable, que es el que debe desvirtuar la presunción de participación en la infracción. Por lo tanto, alegar exclusivamente que la persona que tenía a su cargo no había seguido sus indicaciones no es hecho suficiente para quedar exento de responsabilidad, ya que el TJUE exige que el responsable del tratamiento debe tomar medidas para garantizar que cualquier persona que trabaja bajo sus órdenes siguen sus instrucciones y respetan el RGPD.

67. Por lo tanto, de esta sentencia podemos extraer varias cuestiones relevantes para las personas que trabajan en el ámbito de la IA, entrenando sistemas mediante la introducción de datos:

– La mera infracción de un precepto del RGPD no hace que surja ningún tipo de responsabilidad
– Para que exista derecho a indemnización hace falta un daño material o inmaterial, una infracción demostrada y una relación de causalidad
– El régimen de responsabilidad del RGPD es por culpa
– La carga de la prueba recae en el responsable del tratamiento
– El responsable del tratamiento de datos debe responder por los daños causados por las personas que actúan bajo su supervisión

[71] ECLI:C:2024:288

[72] p. a. miguel asensio, "Determinación de la indemnización por daños derivados de infracciones del Reglamento General de Protección de Datos: STJ 3ª 11 abril 2024, asunto, C-741/21: juris", *La Ley Unión Europea*, nº 125, 2024, p. 5.

- El responsable de datos debe tomar medidas para que su equipo siga sus instrucciones
- Para que el responsable de datos se exima de responsabilidad debe demostrar que no existe relación causal entre el incumplimiento de sus obligaciones y los daños que haya sufrido la víctima

68. Habiendo visto cuáles son las principales previsiones que realiza el RGPD sobre preceptos relativos al entrenamiento y tratamiento de datos personales, procedemos a estudiar cuál es la jerarquía con respecto al RIA.

69. Lo cierto es que el propio RIA realiza de manera constante referencias al RGPD en todo lo relacionado con los datos personales. En concreto, el considerando 3 recoge que el Reglamento contiene normas específicas para proteger a las personas y sus datos personales, restringiendo el uso de sistemas de IA para identificación biométrica remota y el uso de IA para realizar evaluaciones de riesgo.

70. Por otro lado, el RIA también contempla la plena aplicación del RGPD siempre que exista un tratamiento de datos (hecho que ocurre en el entrenamiento de la IA) y lo hace en el considerando 10 en los siguientes términos: "El presente Reglamento no pretende afectar a la aplicación del Derecho de la Unión vigente que regula el tratamiento de datos personales, incluidas las funciones y competencias de las autoridades de supervisión independientes competentes para vigilar el cumplimiento de dichos instrumentos. Tampoco afecta a las obligaciones de los proveedores y los responsables del despliegue de sistemas de IA en su papel de responsables o encargados del tratamiento de datos derivadas del Derecho de la Unión o nacional en materia de protección de datos personales en la medida en que el diseño, el desarrollo o el uso de sistemas de IA impliquen el tratamiento de datos personales. También conviene aclarar que los interesados siguen disfrutando de todos los derechos y garantías que les confiere dicho Derecho de la Unión, incluidos los derechos relacionados con las decisiones individuales totalmente automatizadas, como la elaboración de perfiles".

71. Por otro lado, el considerando 157 recoge que el RIA se entiende sin perjuicio de las competencias, funciones, poderes e independencia de las autoridades u organismos públicos nacionales pertinentes que supervisan la aplicación del Derecho de la UE que protege los derechos fundamentales, incluidos los organismos de igualdad y las autoridades de protección de datos[73].

72. Entrando en el cuerpo normativo, el art. 2.7 del RIA establece que el Derecho de la Unión en materia de protección de los datos personales, la intimidad y la confidencialidad de las comunicaciones se aplicará a los datos personales tratados en relación con los derechos y obligaciones establecidos en el Reglamento. Al estudiar este apartado en relación con el art. 2.8 del RIA que concreta que el RIA no afectará al RGPD, la doctrina[74] ha unido las interpretaciones contenidas en los considerandos y ha llegado a las siguientes conclusiones:

- El derecho a la intimidad y protección de datos personales debe quedar garantizado durante todo el ciclo de vida de la IA, debiendo respetarse el principio de minimización de datos y su protección (considerando 69).
- El RIA no afecta ni cambia las obligaciones de los proveedores y los responsables del despliegue de sistemas IA, ya que siguen siendo considerados responsables o encargados del tratamiento de datos (considerando 10).
- El RIA no es fundamento para el tratamiento de datos personales, ni aunque se traten de categorías especiales de datos (considerando 63).

[73] C. Fernández Hernández, *Guía práctica del Reglamento Europeo de Inteligencia Artificial. Manual de referencia para conocer, entender y aplicar la AI Act*, Aranzadi La Ley, Madrid, 2025, pp. 45-46.

[74] Ibid. p. 46.

– Los titulares de los datos personales siguen ostentando los derechos que les ofrecía el RGPD, en concreto el derecho a no ser objeto de una decisión automatizada o la elaboración de perfiles (considerando 63).
– La intencionalidad del RIA es facilitar la aplicación y el ejercicio de los derechos de los interesados que ya se encontraban antes garantizados por el Derecho de la UE (considerando 10).

73. Siendo así debemos considerar que no existe una jerarquía entre el RGPD y el RIA, sino una relación horizontal de igualdad basada en el ámbito material que se deba tratar. Esa complementariedad de ambas normas se puede observar en el art. 59 del RIA que prevé el tratamiento ulterior de datos personales para el desarrollo de determinados sistemas de IA en favor del interés público en el espacio controlado de pruebas de inteligencia artificial, proporcionando una base legal para que se puedan tratar los datos, dándoles un segundo uso a pesar de estar expresamente prohibido, por ser por razones de interés público, hecho que se permite de acuerdo con el art. 6.4 del RGPD y el art. 9.2.g[75]. Entre este tipo de sistemas de interés general el art. 59.1.a contempla los sistemas de salud pública, detección, diagnóstico, prevención y control, tratamiento de enfermedades y mejora de los sistemas sanitarios[76].

3. Desidentificación de datos personales para el entrenamiento de la IA

74. Como se ha mencionado antes respecto del tratamiento de datos en el RGPD, uno de los requisitos que se exige es el consentimiento por parte de la persona interesada para que se traten sus datos. Sin embargo, la realidad práctica es que el requisito de solicitar autorización expresa a cada uno de los pacientes para poder usar sus datos para entrenar al sistema de IA es totalmente inviable por falta de tiempo, logística y volumen de datos que se necesitan. En su lugar, una alternativa que llevan a cabo los ingenieros de datos es modificar dichos datos para que sean anónimos, de modo que no tengan la consideración de datos personales porque al realizarle modificaciones no es posible saber a qué paciente pertenecen[77].

75. El problema de anonimizar los datos es que si lo que se busca es asegurar que el riesgo de identificar al paciente se minimice, la utilidad de los datos también disminuye proporcionalmente, ya que los datos van a sufrir unas modificaciones que van a hacer que no se parezcan a la realidad, lo que disminuye la calidad. Entre las técnicas más habituales que se utilizan para anonimizar los datos nos encontramos con:

– Eliminación. Consistente en eliminar una cierta variable y sustituirla por una serie de valores nulos como por ejemplo xxxx.
– Generalización. Consistente en sustituir el valor de una variable por una expresión mucho más general, como por ejemplo sustituir el nombre de una ciudad por el de un país o la fecha de nacimiento por el año de nacimiento, de modo que el todo englobe a la parte concreta.
– Sustitución. Consistente en cambiar uno de los datos por otro siempre que no altere el resultado final, por ejemplo, sustituyendo el nombre de una persona por otro.
– Desplazamiento de fechas. Consistente en añadir un desfase entre diferentes fechas de manera constante para que exista una proporción que siempre se cumple y no se modifiquen matemáticamente los resultados.

[75] Este artículo permite el tratamiento levantando la prohibición de tratar datos personales cuando dicho tratamiento sea necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

[76] J. Jiménez López, El Reglamento de inteligencia artificial y el Reglamento General de Protección de Datos, en L. Cotino Hueso y P. Simón Castellano, *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea*, Aranzadi, 2024.

[77] J. J. Beunza Nuin y J. Bonis Sanz, "Protección de datos" en Beunza Nuin et al., *Manual práctico de inteligencia artificial en entornos sanitarios,* Elsevier, España, 2023, p. 131.

– Introducción de ruido estadístico. Consistente en seleccionar valores aleatorios y añadirlos a los valores normales.

76. A pesar de que existan todas estas técnicas posibles para aplicar a los datos de entrenamiento, los datos de salud son especialmente particulares y difíciles de desidentificar. Principalmente esto se debe a tres razones. La primera es que gran parte de la información en las historias clínicas de los pacientes se encuentra escrita en lenguaje natural, no estructurado, que complica la tarea de desidentificarlo, ya que el nombre del paciente puede aparecer por ejemplo entre otros datos dentro de la propia historia clínica. En segundo lugar, al tener las historias clínicas un relato temporal, es casi imposible poder eliminar o modificar las fechas, ya que es relevante el momento en el que han aparecido los síntomas, la forma de actuación, etcétera. Si en el proceso de desidentificación se modifica una fecha de forma errónea, el resto de historia clínica no tendrá coherencia y se estarían alterando los datos posteriores. Finalmente, algunos datos de salud son imposibles de desidentificar, ya que forman parte de la identidad del paciente, como la información genética o la forma de un cierto órgano o imagen de la parte del cuerpo.

V. Conclusiones

77. El uso de la inteligencia artificial en el campo médico ha generado importantes beneficios, al demostrar su utilidad en áreas como el análisis de imágenes, la realización de intervenciones mediante robots y la administración de tratamientos. Para poder realizar esos programas con inteligencia artificial se hace necesario el entrenamiento del programa con ingentes cantidades de datos que se han denominado Big Data realizando la técnica de la minería de datos.

78. Por otro lado, para que los datos que utilicen los ingenieros informáticos sean válidos de conformidad con el Reglamento General de Protección de Datos es necesario que cuenten con el consentimiento de las personas afectadas, sin embargo, se hace muy complicado que todos los pacientes tengan que dar su consentimiento cada vez que se realiza un procedimiento médico. Para ello el nuevo Reglamento del Espacio Europeo de Datos Sanitarios propone la cesión de grandes piscinas de datos a la Unión Europea que será la encargada de custodiarlos, facilitando de este modo la seguridad de los mismos, la interconexión entre Estados y un volumen adecuado para el entrenamiento de la IA. Sin embargo, a pesar de la puesta en marcha de dicho Reglamento siguen en el aire cuestiones como la correcta cognoscibilidad por parte de los pacientes que van a ceder sus datos sobre el fin de los mismos, la seguridad ante ciberataques de gran escala o la protección que van a recibir los pacientes mayores con dificultades para tener sistemas que hayan sido entrenados con datos de personas de avanzada edad específicamente.

79. La regulación de la inteligencia artificial en el mundo actualmente se puede dividir principalmente en dos sectores: Por una parte, el sector no regulacionista, siendo su máximo exponente Estados Unidos, que aboga por un libre desarrollo empresarial cuya ventaja principal es la inversión tecnológica en el sector privado y que se plasma en códigos de buena conducta o soft law con la desventaja de llevar a una desprotección a los usuarios. Por otra parte, nos encontramos con el sector regulacionista, cuyo máximo exponente es la Unión Europea que aboga por una normativa que impone un gran número de obligaciones y cuantiosas sanciones a las empresas con el fin de proteger al usuario frente a los intereses empresariales. Entre estas dos posiciones, parece mucho más adecuada la reguladora, debido a que su finalidad es la protección de lo intereses de los individuos sin frenar el avance del conocimiento o el desarrollo tecnológico. Para mejorar todavía más el abordaje de la regulación de la IA se propone limitar las obligaciones que se les imponen a los diversos sujetos que intervienen en la creación de un sistema de IA y un aumento de las sanciones por los daños o los incumplimientos causados esencialmente por falta de protección de los datos personales. Si se produjera una reducción de las obligaciones o de los controles tan técnicos y centrásemos la atención en resolver el principal problema que es la falta de datos seguros para trabajar que no estén supeditados a los intereses empresariales, el desarrollo tecnológico no se vería frenado.

80. El Reglamento de inteligencia artificial tiene un enfoque basado en el riesgo y divide la inteligencia artificial según sea prohibida, de alto riesgo o de riesgo medio/bajo. Lo más destacable con respecto a este Reglamento es su carácter extraterritorial, de modo que puede llegar a aplicarse a empresas fuera de la Unión Europea, pero cuyos resultados se desplieguen en territorio europeo, lo cual puede dar lugar a incoherencias legislativas internacionales que pueden llevar a las empresas tecnológicas que ni prestan ni dirigen sus servicios a la UE a la aplicación de dicho Reglamento por la venta de un producto que no estaba pensado para ser destinado a la UE en un primer momento. De forma colateral esto puede llevar a dichas empresas a evitar prestar sus servicios en la UE por el temor a que se les aplique una normativa muy estricta.

81. Por lo que respecta al Reglamento General de Protección de Datos este no contiene ninguna especificación con respecto al entrenamiento de la inteligencia artificial con datos pero sí que contiene una serie de principios que debe tener en cuenta el responsable de los datos. Sin embargo, todas estas especificaciones no tienen una forma de ser realmente aplicadas por las compañías y se plasman en el Reglamento con un carácter similar a los códigos de buena conducta, que enuncian valores tales como la equidad, la igualdad, la minimización, la justicia… valores que difícilmente van a ser aplicados en el ámbito del desarrollo de un producto tecnológico empresarial, ya que el principal interés de la compañía será obtener la mayor cantidad de datos posibles para perfeccionar el sistema, sin darle relevancia al modo en el que se han obtenido dichos datos. Por todo ello la idea que propone el Reglamento del Espacio Europeo de Datos de Salud podría llegar a ser positiva pero solo si se desarrollara más, en concreto su interrelación con la empresa privada.

82. Por todo ello la jerarquía entre el Reglamento de Inteligencia Artificial y el Reglamento de General de Protección de Datos es de carácter horizontal de modo que son complementarios y ninguno se aplica con prioridad frente al otro.

83. A la vista de los resultados se hace necesaria una reforma en materia de IA en sede europea, que, en vez de centrar su atención en una clasificación de los sistemas en función del riesgo, refunda los diferentes textos normativos en uno único con previsiones concretas que aseguren un abordaje integral de la cuestión. Para ello, sería necesario plantear una reforma del RIA exclusivamente, no siendo necesario para el RGPD, que por ahora resulta de una gran utilidad al imponer un sistema de protección del individuo con previsiones severas. Igualmente, sería oportuno revisar el amplísimo margen de aplicación extraterritorial de ambos Reglamentos, ya que en opinión de la doctrina más autorizada resulta excesivo.