InDret
4.2024

Editorial

Una lectura del Reglamento de Inteligencia Artificial desde el derecho privado

-

El pasado doce de julio el Diario Oficial de la UE publicaba finalmente el Reglamento 2024/1689, por el que se establecen normas armonizadas en materia de inteligencia artificial. El Reglamento de IA –uno de los hitos legislativos de la anterior Comisión von der Leyen y acaso la norma con mayor poder simbólico para reflejar las líneas generales de política regulatoria europea sobre mercados y tecnologías digitales– llegaba tras más de tres años de debates, presiones y negociaciones. Sus 180 considerandos, 113 artículos y 13 anexos recogen, en casi 150 páginas, un marco legal armonizado que, a pesar de su carácter fragmentario, va a acabar condicionando el desarrollo y uso en los próximos años de modelos, sistemas y herramientas de inteligencia artificial en Europa.

El Reglamento de IA es esencialmente una norma de seguridad de producto, con un claro componente de derecho público regulatorio, cuyo objetivo es establecer normas armonizadas para el desarrollo, la comercialización, puesta en servicio y el uso de sistemas de IA en función de las características y riesgos que presentan. Como norma de seguridad de producto, sus reglas se basan, principalmente, en un sistema de evaluación de la conformidad, acreditación y vigilancia del mercado propio del denominado Nuevo Marco Legislativo, con la intervención intensa de agentes como las autoridades notificantes, los organismos de evaluación de conformidad y los organismos notificados.

Un resumen a vuelapluma del Reglamento da buena cuenta de su carácter de derecho público. El Reglamento distingue cuatro niveles de riesgo con consecuencias jurídicas diversas. En primer lugar, identifica un riesgo no permitido: se prohíben, por sus efectos nocivos en la salud y en los derechos fundamentales, determinadas prácticas como el uso de sistemas y técnicas de IA deliberadamente manipuladoras o engañosas o que exploten sujetos vulnerables, el uso de sistemas para finalidades de clasificación social (*social scoring*), y algunos usos para la categorización e identificación biométricas y para la inferencia de emociones en los ámbitos laboral y educativo, entre otras (art. 5 RIA). En segundo lugar, el Reglamento identifica un nivel de riesgo alto: la mayoría de sus normas se dirigen a regular los sistemas de IA de alto riesgo (arts. 6-49 RIA), cuyos desarrollo y funcionamiento se sujetan a un conjunto de deberes y especificaciones técnicas que alcanzan a aspectos tales como la implementación de sistemas de gestión de riesgos, la gobernanza de

los datos, la conservación de registros, la elaboración de documentación, la transparencia y comunicación de información y la supervisión humana. El Reglamento de IA atribuye el cumplimiento de estos y otros deberes a los diferentes agentes que participan en la cadena de valor que desde el entrenamiento y desarrollo de modelos desemboca en la fabricación de sistemas de IA y en la prestación de servicios relacionados con estos. Sujetos como los proveedores de los sistemas de IA de alto riesgo, los responsables de su despliegue y otros, tales como importadores, distribuidores y representantes, habrán de asumir un conjunto de obligaciones, que incluyen, entre otras, deberes de sometimiento al proceso de evaluación de conformidad antes de la introducción del sistema en el mercado o puesta en servicio, elaboración de evaluaciones de impacto, deberes de vigilancia y retirada del mercado o deberes de cooperación con las autoridades. En tercer lugar, el Reglamento de IA identifica un nivel de riesgo relevante: algunos sistemas, en función de sus usos y de sus características, pueden afectar a quienes interactúan con ellos sin saberlo y, en efecto, el Reglamento prevé deberes de información y transparencia para que, por ejemplo, los proveedores de sistemas de IA destinados a interactuar directamente con personas físicas, por ejemplo, un *chatbot*, se aseguren de que estas conocen que no están interactuando con otra persona física; o que los responsables del despliegue de un sistema de IA que genere o manipule imágenes o contenidos de audio o vídeo que constituyan una ultrasuplantación (*deepfake*) harán público que estos contenidos o imágenes han sido generados o manipulados de manera artificial (art. 50 RIA). También incluye el Reglamento un conjunto de normas sobre modelos de inteligencia artificial de propósito general, como los modelos de aprendizaje profundo utilizados en el ámbito de la IA generativa (arts. 51-56 RIA). En algunos supuestos, los riesgos que comportarán podrán tener una dimensión sistémica y, por ello, se elevan los deberes que se imponen a los proveedores de estos modelos. En cuarto lugar, puede identificarse un nivel de riesgo residual: para aquellos sistemas de IA no cubiertos en el resto de niveles, el Reglamento persigue el cumplimiento voluntario de deberes de seguridad y el fomento y la adopción de códigos de conducta no obligatorios (arts. 96-97 RIA).

El Reglamento de IA complementa este régimen de clasificación de niveles de riesgo con normas sobre espacios controlados de pruebas o *regulatory sandboxes* (arts. 57-63 RIA); sobre gobernanza pública, que prevén la creación de organismos europeos como la Oficina de IA y la designación de autoridades nacionales (arts. 64-70 RIA); sobre vigilancia poscomercialización, intercambio de información y vigilancia del mercado (arts. 72-94); y sobre infracciones y sanciones (arts. 99-101 RIA). Las reglas de gobernanza y los instrumentos de investigación y sanción siguen a los establecidos en otros reglamentos europeos como el Reglamento General de Protección de Datos y el Reglamento de Servicios Digitales.

A pesar de la evidente naturaleza de derecho público del Reglamento de IA, son muchas las implicaciones para diferentes ámbitos del derecho privado, que los juristas dedicados al derecho de daños, contratos o la propiedad no pueden ignorar sin más. Sin ningún ánimo de exhaustividad, ni de profundidad, los párrafos que siguen describen algunas interacciones del nuevo texto del Reglamento de IA con cuestiones propias del derecho privado.

El Reglamento de IA no se ocupa de normar la responsabilidad civil por daños y perjuicios causados durante el desarrollo y uso de modelos y sistemas de inteligencia artificial, ni tampoco de establecer una pretensión indemnizatoria para su compensación en este ámbito. Con arreglo al considerando 9, el Reglamento se aplica sin perjuicio de las demás normas vigentes en la Unión y en los EE.MM. y, en particular, del derecho general de daños y del derecho de responsabilidad

del fabricante por productos defectuosos. En buena medida, esta opción legislativa responde a la elaboración durante la tramitación del Reglamento de IA de dos instrumentos normativos independientes para las cuestiones relacionadas con la reparación de los daños: la Directiva sobre responsabilidad por los daños causados por productos defectuosos, aprobada recientemente y pendiente de publicación en el DOUE, y la Propuesta de Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial, cuyo futuro como derecho vigente es punto menos que incierto. Que la reparación de los daños y perjuicios causados por modelos y sistemas de inteligencia artificial quede fuera del Reglamento no comporta que este no sea una pieza más –y fundamental– del complejo engranaje del derecho de daños en este sector: el remedio indemnizatorio no puede desligarse de otros mecanismos que, juntamente, contribuyen a que los riesgos que generan determinadas actividades peligrosas no se acaben concretando o se concreten en menos ocasiones en daños. Así, *ex ante* la regulación de las especificaciones técnicas para hacer a los sistemas de IA de alto riesgo más seguros y las limitaciones de entrada en el mercado sin contar con las pertinentes evaluaciones de conformidad y, *ex post*, los deberes de vigilancia postcomercialización y el derecho sancionador, si funciona razonablemente bien, habrán de prevenir muchos daños, reducir el protagonismo de las acciones indemnizatorias y mitigar los costes privados y sociales de los pleitos de responsabilidad civil.

Sea como fuere, las potenciales reclamaciones privadas por daños derivados del funcionamiento y uso de modelos y sistemas de inteligencia artificial de alto riesgo exigirán en muchos casos identificar infracciones de deberes de seguridad establecidos en el propio Reglamento de IA y valorar si estas pueden servir por si solas para acreditar la negligencia de los demandados en el pleito. Este parece ser el modelo defendido por la Comisión en su Propuesta de Directiva de Responsabilidad Civil e Inteligencia Artificial. El artículo 4 de esta define la culpa del demandado como *"el incumplimiento de un deber de diligencia establecido por el Derecho de la Unión o nacional destinado directamente a proteger frente a los daños que se hayan producido"* y especifica luego determinados incumplimientos normativos que *per se* pueden presumirse negligentes. En cuanto a los proveedores de sistemas de IA de alto riesgo u otros sujetos que se equiparan al proveedor, el art. 4.2 prevé los siguientes supuestos de infracciones normativas del Reglamento de IA: a) incumplimiento de los criterios de calidad sobre datos de entrenamiento (*training data*), validación o prueba; b) incumplimiento de los requisitos de transparencia; c) diseño o desarrollo del sistema sin que permita una vigilancia efectiva por parte de personas físicas durante el funcionamiento del sistema de IA; d) diseño o desarrollo del sistema que, en atención a su finalidad, no ofrezca niveles adecuados de precisión, solidez y ciberseguridad; e) falta de adopción inmediata de medidas correctoras necesarias para poner el sistema de IA en conformidad después de detección de incidentes o para retirarlo del mercado. También el artículo 10.2.b) de la nueva Directiva sobre responsabilidad por los daños causados por productos defectuosos señala que *"[s]e presumirá el carácter defectuoso del producto cuando se cumpla alguna de las siguientes condiciones: [...] b) el demandante demuestre que el producto no cumple los requisitos obligatorios de seguridad del producto establecidos en el Derecho de la Unión o nacional que tienen por objeto proteger contra el riesgo del daño sufrido por la persona perjudicada"*. Habrá de verse cómo operarán en la práctica estas presunciones de negligencia –que, en buena medida, recuerdan a doctrinas propias del *common law* como la *negligence per se*– y de defecto de producto y cómo los diferentes criterios de imputación objetiva y, en particular, la identificación del

ámbito de protección objetivo y subjetiva de la norma que establece deberes de seguridad, servirán para limitar su papel.

La identificación de diferentes deberes de seguridad en el Reglamento de IA también servirá para delimitar esferas de control entre los varios participantes en la cadena de valor de la inteligencia artificial. Entre el momento en que empiezan a compilarse grandes bases de datos que servirán para entrenar un modelo, hasta que este se pone en servicio y se utiliza el sistema basado en aquel, puede intervenir una pluralidad de sujetos, que complicará a menudo la atribución de responsabilidad civil por daños y perjuicios. El establecimiento de diferentes obligaciones para diferentes grupos de operadores –principalmente, de los proveedores de los sistemas y de los responsables de su despliegue– habrá de contribuir a facilitar esta tarea. En cualquier caso, no podrá ignorarse la posibilidad de acudir a normas y doctrinas nacionales sobre solidaridad u otras modalidades de la obligación de reparar los daños y perjuicios, especialmente, cuando los diferentes operadores estén situados en jurisdicciones diferentes. Además, los organismos de evaluación de conformidad de los sistemas de IA de alto riesgo y los organismos notificados podrán llegar a responder en algunos casos (véase, entre otras, STJUE de 16 de febrero de 2017, asunto C-219/15, *Elisabeth Schmitt c. TÜV Rheinland LGA Products GmbH*). De hecho, el propio Reglamento obliga ya a los primeros a suscribir un seguro de responsabilidad adecuado para sus actividades de evaluación de la conformidad, salvo que la potencial responsabilidad civil sea asumida por el Estado miembro en que estén establecidos o que sea la propia administración pública la que se encargue de la evaluación de la conformidad (art. 31.9 RIA). En el derecho español, demandar junto a un proveedor privado de un sistema de IA a un organismo público de evaluación de conformidad o a un organismo notificado obligará a acudir a la jurisdicción contencioso-administrativa y a la regulación de la responsabilidad patrimonial.

Es probable que los tribunales que resuelvan pleitos sobre la reparación de daños y perjuicios causados por sistemas de IA hayan de pronunciarse sobre el argumento esgrimido con frecuencia por demandados según el cual estos no deberían responder por cuanto fueron escrupulosos en el cumplimiento de todos los deberes impuestos por la normativa sobre seguridad de producto. Se trata de la defensa de *regulatory compliance*, en buena medida, el reverso de la negligencia *per se*. El éxito de alegaciones en este sentido es poco probable. El Reglamento de IA ha de considerarse una normativa de mínimos en materia de deberes de seguridad para los sistemas de IA de alto riesgo, especialmente, en un campo tan dinámico y con altos niveles de innovación en estos momentos como la inteligencia artificial. Además, el Reglamento no impide la aplicación de otras normas de seguridad de producto, especialmente, cuando los sistemas de IA se utilizan como componente de seguridad de un producto o constituyen un producto con arreglo a la legislación europea sobre armonización. También, el Reglamento ya prevé otras fuentes como actos delegados de la Comisión, códigos de buenas prácticas, códigos de conducta o estándares técnicos armonizados, que completarán y concretarán los niveles de seguridad que habrán de respetar los sistemas de IA. Además, en relación con los *regulatory sandboxes*, el Reglamento de IA prevé que el cumplimiento normativo podrá únicamente evitar la imposición de multas administrativas, pero no la responsabilidad civil. En este sentido, el artículo 57.12 RIA establece que *"[l]os proveedores y proveedores potenciales que participen en el espacio controlado de pruebas para la IA responderán, con arreglo al Derecho de la Unión y nacional en materia de responsabilidad, de cualquier daño infligido a terceros como resultado de la experimentación realizada en el espacio controlado de pruebas. Sin embargo, siempre que los proveedores potenciales respeten el plan*

específico y las condiciones de su participación y sigan de buena fe las orientaciones proporcionadas por la autoridad nacional competente, las autoridades no impondrán multas administrativas por infracciones del presente Reglamento […]".

En relación con el derecho de daños, el Reglamento también prevé que el número de personas afectadas y el nivel de los daños que hayan sufrido y las acciones emprendidas por el operador de un sistema de IA para mitigar los perjuicios sufridos por las personas afectadas serán considerados como factores para decidir la imposición de sanciones administrativas y su cuantía (arts. 99.7 y 101.1 RIA).

El Reglamento de IA también tendrá repercusiones para el derecho de contratos y, en especial, para el derecho de consumo. Los deberes de seguridad impuestos a los operadores de sistemas de IA de alto riesgo afectarán, entre otros, a la contratación bancaria y de seguros. El Anexo III del Reglamento atribuye la condición de sistemas de alto riesgo a los destinados a ser utilizados para evaluar la solvencia de personas físicas o establecer su calificación crediticia, salvo los sistemas de IA utilizados al objeto de detectar fraudes financieros, y a los sistemas destinados a la evaluación de riesgos y la fijación de precios en relación con las personas físicas en el caso de los seguros de vida y de salud. Los primeros se consideran de alto riesgo porque, señala el Reglamento, al decidir si determinados individuos pueden acceder a recursos financieros o servicios esenciales como la vivienda, la electricidad y los servicios de telecomunicaciones, pueden llegar a excluir a determinadas personas o colectivos y perpetuar patrones históricos de discriminación por motivos de origen racial o étnico, género, discapacidad, edad u orientación sexual, o generar nuevas formas de discriminación. Los segundos se consideran de alto riesgo ya que, según el Reglamento, pueden afectar de un modo considerable a los medios de subsistencia de las personas y, si no se diseñan, desarrollan y utilizan debidamente, pueden vulnerar sus derechos fundamentales y tener graves consecuencias para la vida y la salud de las personas, como la exclusión financiera y la discriminación. Entre otras obligaciones, compañías de seguros, bancos y otras entidades financieras habrán de cumplir con los requisitos impuestos por el Reglamento de IA relativos a la gestión de riesgos, la calidad y la pertinencia de los conjuntos de datos utilizados, la documentación técnica y la conservación de registros, la transparencia y la comunicación de información a los responsables del despliegue, la supervisión humana, la solidez, la precisión y la ciberseguridad. En cualquier caso, cuando los responsables del despliegue de estos sistemas de alto riesgo sean entidades financieras sujetas a requisitos relativos a su gobernanza, sus sistemas o sus procesos internos, podrán cumplir con algunos deberes de seguridad ajustándose a lo establecido en la normativa sobre servicios financieros. También los centros de enseñanza privada podrán quedar cubiertos por la normativa de seguridad del Reglamento si utilizan sistemas de IA para, por ejemplo, determinar la admisión en sus programas o para evaluar a los estudiantes. El Reglamento también alcanzará algunas tareas en la provisión de servicios médicos que empleen sistemas de IA.

El Reglamento de IA, según lo establecido en su artículo 2.9, se ha de entender sin perjuicio de las normas establecidas por otros actos jurídicos de la Unión relativos a la protección de los consumidores. Las interacciones entre el Reglamento y la normativa de consumo serán diversas. Por ejemplo, el RIA no se encarga directamente de la personalización de ofertas, servicios y contratos, de la publicidad personalizada o de la utilización de sistemas de recomendación. Por ello, deberá ponerse en relación con lo previsto, entre otros instrumentos, en los artículos 6 de la la Directiva 2011/83/UE, de 25 de octubre de 2011, sobre los derechos de los consumidores, y

26 y 17 del Reglamento de Servicios Digitales. En cualquier caso, cuando para estas tareas se utilicen sistemas de IA calificados como de alto riesgo, deberán seguirse los criterios sobre gobernanza de datos establecidos en el artículo 10 RIA destinados a asegurar la calidad de los conjuntos de datos utilizados en su entrenamiento, validación y prueba. Hay una preocupación clara para mitigar los posibles sesgos que puedan afectar a la salud y la seguridad de las personas, a sus derechos fundamentales o generar algún tipo de discriminación. Con tal finalidad, podrán tratarse incluso datos de categorías especiales (art. 10.5 RIA).

Tampoco ofrece el Reglamento una regulación completa sobre prácticas desleales con consumidores en el ámbito de la inteligencia artificial. Con todo, trasluce una preocupación por la transparencia y el suministro suficiente de información a las personas que interactúen con sistemas de IA, especialmente en las relaciones de consumo, en las cuales la utilización de asistentes virtuales y de instrumentos de marketing emocional es cada vez más frecuente. En este sentido, el artículo 50.1 RIA obliga a los proveedores de *chatbots* y otros sistemas de IA destinados a interactuar directamente con personas físicas a diseñarlos y desarrollarlos de forma que estas estén informadas de que están interactuando con un sistema de IA, excepto cuando resulte evidente desde el punto de vista de una persona razonablemente informada, atenta y perspicaz, teniendo en cuenta las circunstancias y el contexto de utilización; y el artículo 50.2 RIA obliga a los responsables del despliegue de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica no prohibidos por el artículo 5 a informar de su funcionamiento. Además, si se emplean sistemas de IA de alto riesgo que tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas, el artículo 26.11 RIA impone a los responsables de su despliegue un deber de información a los individuos expuestos a aquellos. En el ámbito de las prácticas desleales con consumidores, el Reglamento también complementa las normas ya promulgadas en materia de patrones oscuros o *dark patterns* en instrumentos como el Reglamento de Servicios Digitales, el Reglamento de Datos o la Directiva 2011/83/UE, de 25 de octubre de 2011, sobre los derechos de los consumidores (tras su modificación por la Directiva (UE) 2023/2673 en lo relativo a los contratos de servicios financieros celebrados a distancia), con dos prohibiciones relativas a técnicas manipuladoras o engañosas y técnicas de aprovechamiento de vulnerabilidades de un individuo o de un colectivo. Por una parte, el artículo 5.1.a) RIA proscribe *"la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas"*. Por otra parte, el artículo 5.1.b) RIA prohíbe *"la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra"*. De las diferencias entre los requisitos establecidos en el Reglamento de IA y demás normas europeas sobre patrones oscuros, y de los problemas de compatibilidad y coherencia entre ellas, ya ha

advertido el reciente informe de la Comisión sobre *digital fairness* y control de adecuación de la normativa sobre consumo.

Finalmente, el artículo 86 del Reglamento prevé un derecho a la explicación de decisiones tomadas individualmente, que constituye la única pretensión individual de este instrumento normativo que puede hacerse valer por una persona en un ámbito contractual o extracontractual. Con arreglo al art. 86.1 RIA, *"[t]oda persona que se vea afectada por una decisión que el responsable del despliegue adopte basándose en los resultados de salida de un sistema de IA de alto riesgo que figure en el anexo III, con excepción de los sistemas enumerados en su punto 2* [i.e. sistemas de IA destinados a ser utilizados como componentes de seguridad en la gestión y el funcionamiento de las infraestructuras digitales críticas, del tráfico rodado o del suministro de agua, gas, calefacción o electricidad]*, y que produzca efectos jurídicos o le afecte considerablemente del mismo modo, de manera que considere que tiene un efecto perjudicial para su salud, su seguridad o sus derechos fundamentales, tendrá derecho a obtener del responsable del despliegue explicaciones claras y significativas acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada".* Este derecho de explicación difiere, de nuevo, tanto en sus condiciones de ejercicio como en su contenido y facultades de otros derechos reconocidos, por ejemplo, en los artículos 13.2.f), 14.2.g) y 22 del Reglamento General de Protección de Datos y 18.8 de la Directiva (UE) 2023/2225, de 18 de octubre de 2023, relativa a los contratos de crédito al consumo. Varios autores ya han examinado los diferentes ámbitos de aplicación y las posibilidades de comptatibilidad entre ellos.

El Reglamento también contiene unas pocas normas relativas a los derechos de propiedad intelectual. El artículo 54 RIA impone a los proveedores de modelos de IA de uso general (*General Purpose Artificial Intelligence Models o GPAIMs*) la obligación de establecer directrices para cumplir con el derecho de la UE en materia de derechos de autor y, en particular, para respetar las reservas de derechos expresadas por sus titulares; y la obligación de elaborar y poner a disposición del público un resumen suficientemente detallado del contenido utilizado para entrenar el GPAIM, de acuerdo con el modelo que facilite la Oficina de IA. La Propuesta inicial de Reglamento de IA de 21 de abril de 2021 no contenía ninguna norma referida a derechos de propiedad intelectual. Durante el otoño de 2022, con la popularización de aplicaciones de IA generativa y, en especial, de ChatGPT, surgieron las primeras iniciativas para regular estos sistemas capaces de generar textos, imágenes, sonidos, videos y otros contenidos a partir de las instrucciones o *prompts* introducidos por sus usuarios. El Consejo de la UE propuso entonces incluir en el Reglamento de IA normas especiales dirigidas a los "sistemas de IA de uso general", pero tampoco sin regular aspectos relacionados con los derechos de autor. A partir de las reacciones de algunos titulares de derechos, incluyendo autores y editores, que señalaban que sus obras se empleaban sin autorización para entrenar los modelos de IA subyacentes a estos sistemas, el Parlamento Europeo propuso incluir obligaciones relativas a la documentación y puesta a disposición pública de un resumen suficientemente detallado sobre los contenidos protegidos por derechos de autor que se hubieran empleado como datos de entrenamiento, que finalmente, se incorporaron a la versión final.

En el texto del Reglamento de IA finalmente aprobado, destaca sobre todo el nuevo deber de los proveedores de los GPAIMs de respeto a las reservas de derechos de propiedad intelectual hechas por sus titulares, que tiene una relación directa con el límite de minería de textos y datos previsto en el artículo 4 de la Directiva (UE) 2019/790, de 17 de abril de 2019, sobre los derechos de autor

y derechos afines en el mercado único digital (y, en el derecho español, en el artículo 67 del Real Decreto-ley 24/2021, de 2 de noviembre, de transposición de directivas de la Unión Europea). Entre otras medidas, esta Directiva estableció dos excepciones o limitaciones a derechos de autor y derechos afines de carácter imperativo relacionadas con la minería de textos y datos (*Text and Data Mining*). Según el artículo 2.2. de la Directiva, la "minería de textos y datos" consiste en *"toda técnica analítica automatizada destinada a analizar textos y datos en formato digital a fin de generar información que incluye, sin carácter exhaustivo, pautas, tendencias o correlaciones"*.

La primera de las excepciones, prevista en el artículo 3 de la Directiva, está limitada a la minería de textos y datos con fines de investigación científica. En este sentido, establece un límite a los derechos de reproducción sobre obras y bases de datos originales y a los derechos *sui generis* sobre bases de datos, en relación con aquellas reproducciones y extracciones realizadas por organismos de investigación e instituciones responsables del patrimonio cultural con el fin de realizar, con fines de investigación científica, minería de textos y datos de obras u otras prestaciones a las que tengan acceso lícito. Hace pocas semanas, un tribunal alemán en Hamburgo se pronunciaba sobre la aplicación de este límite a algunas bases de datos de LAION, muy utilizadas en el campo de la IA generativa y, a pesar de que el Reglamento no es todavía aplicable en este punto, no se apartaba de sus orientaciones.

La segunda de las excepciones, prevista en el artículo 4 de la Directiva, es genérica y cubre todas aquellas reproducciones y extracciones de obras y otras prestaciones accesibles de forma legítima para actividades de minería de textos y datos con finalidades distintas a la investigación científica y, por tanto, incluyendo por ejemplo, aquellas actividades con fines comerciales. A diferencia de lo que ocurre con la excepción para fines de investigación científica, el artículo 4.3 de la Directiva señala que: *"[l]a excepción o limitación establecida en el apartado 1 se aplicará a condición de que el uso de las obras y otras prestaciones a que se refiere dicho apartado no esté reservado expresamente por los titulares de derechos de modo adecuado, como medios de lectura mecánica en el caso del contenido puesto a disposición del público en línea"*. En consecuencia, los titulares de derechos pueden oponerse a que sus obras u otras prestaciones puedan ser utilizadas para labores de minería de textos y datos mediante reserva expresa. En particular, si se trata de contenido difundido online, esta reserva podrá realizarse con medios de lectura mecánica. Se trata de un mecanismo de *opt-out*, que ahora el Reglamento de IA exige respetar.

Son muchas otras las cuestiones de derecho privado que se verán afectadas, en mayor o menor medida, por las normas del Reglamento de IA. Temas tales como los contratos entre diferentes integrantes de la cadena de valor de la inteligencia artificial, el ejercicio de los derechos individuales de protección de datos personales, las intromisiones en los derechos al honor, propia imagen e intimidad por la realización de *deepfakes*, la participación en ensayos y pruebas para evaluar el correcto funcionamiento de sistemas de IA, o los problemas de competencia relacionados con la adopción de códigos de conducta y buenas prácticas, no podrán tratarse sin ignorar las reglas –con frecuencia prolijas en detalles y remisiones y redactadas en un lenguaje más bien áspero– del Reglamento. Hace ya mucho tiempo que el derecho privado no puede hacerse ni estudiarse de espaldas al derecho regulatorio y al estado de los conocmientos científicos y técnicos de las materias sobre las que se proyecta. A las herramientas que empleamos quienes nos dedicamos al derecho privado se añade ahora una nueva pieza.

Antoni Rubí Puig