



Giusella Finocchiaro

El nuevo derecho de la Inteligencia Artificial



Palestra Europa

EL NUEVO DERECHO DE LA INTELIGENCIA ARTIFICIAL

GIUSELLA FINOCCHIARO

EL NUEVO DERECHO DE LA INTELIGENCIA ARTIFICIAL

Traducción de
Mayté Chumberiza Tupac Yupanqui
Hilda Rojas Sinche

PALESTRA EUROPA

LIMA-MADRID

2025

EL NUEVO DERECHO DE LA INTELIGENCIA ARTIFICIAL
Giusella Finocchiaro

Primera edición, mayo 2025

Traducción de la obra original de la autora:
Diritto dell'intelligenza artificiale, Bologna: Zanichelli Editore, 2024.

© 2025: GIUSELLA FINOCCHIARO

© 2025: Palestra Jurídica S. L.

Calle Sepúlveda, 135 - Bº Iz, 28011, Madrid, España

Telf. (+34) 691626018

europa@palestraeditores.com

www.palestraeuropa.es

© 2025: Palestra Editores S. A. C.

Plaza de la Bandera 125, Pueblo Libre, Lima, Perú

Telf. +511 6378902 – 6378903

palestra@palestraeditores.com

www.palestraeditores.com

© De la traducción: MAYTÉ CHUMBERIZA TUPAC YUPANQUI, HILDA ROJAS SINCHE

Impresión y encuadernación:

IVERSO IMPRESIÓN

MAYO, 2025

Cuidado de estilo y edición:

MAYTÉ CHUMBERIZA TUPAC YUPANQUI

HILDA ROJAS SINCHE

Diagramación:

JOHN PAOLO MEJÍA GUEVARA

Depósito Legal: M-11252-2025

ISBN: 979-13-87545-16-1

Tiraje: 500 ejemplares

Impreso en España – Printed in Spain

Creemos que el conocimiento jurídico de calidad es una herramienta para transformar nuestras sociedades. Cada ejemplar que llega a tus manos contribuye a la construcción de una comunidad académica más crítica, rigurosa e inclusiva. Adquiriendo este libro, estás apoyando el trabajo de autores y autoras comprometidos con el desarrollo del pensamiento jurídico contemporáneo. Desde **Palestra Europa**, agradecemos tu apoyo a la edición independiente y a la difusión del saber jurídico.

PARA DERECHOS DE REPRODUCCIÓN, COPIA O ESCANEADO DE FRAGMENTOS, POR FAVOR CONTACTA CON CEDRO (CENTRO ESPAÑOL DE DERECHOS REPROGRÁFICOS) A TRAVÉS DE WWW.CONLICENCIA.COM O LLAMANDO AL 91 702 19 70 / 93 272 04 47.

CONTENIDO

PREFACIO	9
----------------	---

Capítulo 1

LA REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL	11
1. El objeto de la normativa	11
2. El contexto geopolítico.....	16
3. El enfoque adoptado por el legislador europeo	24
4. Cuestiones críticas.....	26

Capítulo 2

ASPECTOS REGLAMENTARIOS DE LA INTELIGENCIA ARTIFICIAL.....	33
1. La situación actual.....	33
2. Las normas dictadas en el mundo.....	35
3. El Reglamento Europeo sobre Inteligencia Artificial en el punto de mira.....	37
4. Conclusiones.....	38

Capítulo 3

REGLAMENTO EUROPEO SOBRE INTELIGENCIA ARTIFICIAL: EL MODELO BASADO EN LA GESTIÓN DE RIESGOS	41
1. El contexto geopolítico.....	41
2. El riesgo de la retórica y la necesidad de un nuevo modelo	42

3. El modelo europeo	49
4. Conclusiones.....	70

Capítulo 4

INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS.....	73
1. Sobre el método	73
2. La inteligencia artificial y el planteamiento del legislador europeo.....	77
3. Mercado digital y protección de datos	82
4. Los principios fundamentales	85
4.1. Datos personales y anónimos	85
4.2. Calidad de los datos	88
4.3. Decisiones automatizadas y derecho de explicación	90
4.4. Finalidad del tratamiento	93
4.5. Responsabilidad	94
5. Conclusiones.....	97

Capítulo 5

EL CONTRATO EN LA ERA DE LA INTELIGENCIA ARTIFICIAL.....	101
1. Introducción	101
2. Método	103
3. La identificación de las partes.....	106
4. La imputación de la voluntad.....	116
5. El objeto del contrato.....	123
6. La forma del contrato.....	124

7. Limitación de autonomía del incumplimiento	126
8. Conclusiones sobre los <i>contratos inteligentes</i>	127

Capítulo 6

INTELIGENCIA ARTIFICIAL Y RESPONSABILIDAD	131
---	-----

1. Sobre el método: verificación de la necesidad de una intervención legislativa	131
2. El papel del legislador europeo	136
3. La inteligencia artificial y sus implicaciones jurídicas	142
4. Retórica	145
5. Nuevas cuestiones relativas a la responsabilidad	147

Capítulo 7

INTELIGENCIA ARTIFICIAL Y DERECHOS DE AUTOR. SUGERENCIAS	155
--	-----

Capítulo 8

INTELIGENCIA ARTIFICIAL EN EL PODER JUDICIAL	165
--	-----

1. El escenario	165
2. El marco reglamentario actual	173
3. Jurisprudencia	183
4. Conclusiones: ¿sustituirá la inteligencia artificial al juez y al abogado?	187

Capítulo 9

RESPONSABILIDAD DE LAS PLATAFORMAS Y PROTECCIÓN DE LOS CONSUMIDORES	195
---	-----

1. Desde la Directiva 2000/31/CE	195
2. ... a la necesidad de la Unión Europea de recuperar el espacio reglamentario	198

3.	El modelo de responsabilidad adoptado en la Ley de Servicios Digitales y el paradigma usuario-consumidor.....	203
4.	Las obligaciones introducidas por la DSA.....	205
5.	Protección del consumidor: un sistema compuesto.....	210

PREFACIO

Este volumen se ha escrito para responder rápidamente a la necesidad didáctica de proporcionar a los estudiantes del curso *Derecho de Internet y de los Medios Sociales* de la Universidad de Bolonia material actualizado sobre el tema de la inteligencia artificial. Se trata de una antología de obras ya publicadas, convenientemente revisadas.

La inteligencia artificial, que ya forma parte de nuestra vida cotidiana, también es un tema de estudio necesario para los abogados, sobre todo si están especializados en el ámbito digital.

Finalmente, deseo extender mi agradecimiento a la abogada Giorgia Bianchini, quien colaboró conmigo en los temarios y la revisión de los escritos.

Bolonia, 31 de julio de 2024

CAPÍTULO I

LA REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL*

1. EL OBJETO DE LA NORMATIVA

Una reflexión sobre la regulación de la inteligencia artificial requiere, en primer lugar, una definición del objeto de la regulación.

Definir la inteligencia artificial es una tarea difícil y, de hecho, muchas definiciones se han sucedido, especialmente en los últimos años, cuando el tema ha recibido una atención general¹. Por ejemplo, se puede citar la contenida en la Comunicación de la Comisión Europea de 25 de abril de 2018, según la cual el término “se refiere a sistemas que muestran un comportamiento inteligente analizando

* Este capítulo incorpora, con algunas adaptaciones y actualizaciones, el artículo publicado en *Rivista Trimestrale di Diritto Pubblico*, 2022, 1085 y ss.

¹ Para algunas reflexiones sobre la definición de inteligencia artificial por los informáticos, véanse las contribuciones de Gabrielli, “Dalla logica al Deep Learning: una breve riflessione sull’intelligenza artificiale”, 21 y ss.; de Rovati, “Il processo di apprendimento algoritmico e le applicazioni nel settore legale”, 31 y ss. y de Tomassini, “L’intelligenza artificiale: quali prospettive?”, 43 y ss. Todas ellas se encuentran en el volumen *XXVI Lezioni di diritto dell’intelligenza artificiale*, ed. Ruffolo (Giappichelli, 2020).

su entorno y realizando acciones, con cierto grado de autonomía para alcanzar objetivos específicos”².

Más reciente aún es la definición, también de origen europeo, contenida en el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024. A partir de esta, se establecen normas armonizadas sobre la inteligencia artificial, las cuales se consignaron en la Ley de la IA, donde se define dicha tecnología como “un sistema automatizado diseñado para funcionar con distintos niveles de autonomía y que puede tener capacidad de adaptación tras su despliegue y que, con fines explícitos o implícitos, deduce de la entrada que recibe cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales”³.

² Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, 2018, *Inteligencia artificial para Europa*, COM (2018) 237, 1, <https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:52018DC0237>. Mayor definición ofrece el informe del Centre for European policy studies (CEPS), *Artificial Intelligence: Ethics, Governance and Policy Challenges*, ed. Renda (CEPS, 2019), consultado el 24 de junio de 2024, <https://www.ceps.eu/ceps-events/artificial-intelligence-ethics-governance-and-policy-challenges/> y presentado en Assonime el 25 de marzo de 2019, que se refiere a la inteligencia artificial como “el uso de técnicas hechas por el hombre (significado latino de *artificialis*) para replicar la capacidad de ‘leer dentro’ de la realidad”, 4.

³ Apartado 1 del art. 3 del Reglamento. Esta definición difiere de la propuesta inicial de la Comisión. En el proceso legislativo que condujo a la aprobación final del Reglamento, se siguió la noción ya establecida en el seno de la Organización para la Cooperación y el Desarrollo Económico (OCDE). Recogida en los *Principios de IA* de la OCDE de 2019, la definición de la OCDE también se ha ido modificando con el tiempo y, finalmente, quedó establecida en los siguientes términos: “Un sistema de IA es un sistema basado en máquinas que, por objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los distintos sistemas de IA varían en sus niveles de autonomía y adaptabilidad tras su despliegue”.

Sin embargo, incluso después de más de setenta años, el método adoptado por Turing en su famoso ensayo de 1950 sigue siendo más convincente: en lugar de definir qué es la inteligencia, lo cual es una tarea muy difícil, conviene comparar los resultados de un proceso. Si el proceso se califica de inteligente cuando lo realiza un ser humano, entonces, puede calificarse de inteligente si lo realiza una máquina⁴. De este modo, para simplificar, según Turing, la inteligencia artificial puede definirse como la ciencia de hacer que los ordenadores ejecuten tareas que requieren inteligencia cuando las realizan los humanos⁵.

Así, OCDE, *Explanatory memorandum on the updated OECD Definition of an AI System* (2024), consultado el 21 de junio de 2024, https://www.oecd.org/en/publications/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en.html.

⁴ Hace referencia al método del Juego de Imitación, desarrollado por Alan Turing, considerado el padre fundador de la informática y la inteligencia, al que el autor dedica el primer párrafo de su obra “Computing Machinery and Intelligence”, *Mind* LIX, no. 236 (1950): 433-460, <https://academic.oup.com/mind/article-abstract/LIX/236/433/986238>. La *prueba* fue ideada por Turing para determinar si una máquina es capaz de pensar, es decir, capaz de establecer conexiones, enlazar ideas y expresarlas. La *prueba* se basa en la evaluación de capacidad de un ordenador para imitar el comportamiento de un ser humano: si el resultado es positivo, debe considerarse que la máquina es capaz de pensar de forma equivalente o, en cualquier caso, indistinguible de un ser humano. La pregunta “¿pueden pensar las máquinas?” fue considerada sin sentido por el propio Turing.

El nacimiento de la inteligencia artificial se remonta a la Conferencia de Dartmouth (Hannover, New Hampshire) de 1956. El texto de la propuesta con la que los organizadores de la conferencia abordaron los principales temas del campo de investigación, incluidas las redes neuronales, la teoría de la computabilidad, la creatividad, así como el procesamiento y reconocimiento del lenguaje natural, data de 1955. Véase McCarthy, Minsky, Rochester y Shannon, “A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence”, *AI Magazine* 27, no. 4 (2006): 12-14. Consultado el 20 de junio de 2024. aaai.org/ojs/index.php/aimagazine/article/view/1904/1802.

⁵ Alan Turing afirmaba lo siguiente: “La idea que subyace a los ordenadores digitales puede explicarse diciendo que estas máquinas están pensadas para realizar

Siguiendo un enfoque contrafáctico, se puede utilizar el método propuesto por Floridi⁶ y evitar definir la inteligencia artificial como “la reconozco cuando la veo”.

En cualquier caso, sea cual sea la definición que se adopte, se debe advertir del peligro de antropomorfizar la inteligencia artificial, lo cual puede partir de su propia definición. En efecto, el término “inteligencia” es condicionante e induce a pensar en un ser inteligente.

Aquí se utiliza una metáfora⁷: la aplicación de la inteligencia artificial se comporta como si fuera inteligente. Pero es necesario ser plenamente consciente tanto de las ventajas como de los límites en el uso de metáforas a fin de evitar que la metáfora sustituya a la realidad⁸. De no ser así, el uso del término “inteligencia” podría llevar a la suposición implícita de una subjetividad de la aplicación de la inteligencia artificial, de forma que se condicione subrepticamente cualquier razonamiento sobre la subjetividad jurídica desde el principio.

cualquier operación que pudiera realizar un ordenador humano”, “Computing Machinery...”, 436.

⁶ Floridi, *Etica dell'intelligenza artificiale* (Raffaello Cortina, 2022), 40 y ss.

⁷ He desarrollado el tema de la metáfora como herramienta cognitiva también en el ámbito del Derecho en mi “Firma digitale”, en *Commentario del Codice Civile Scialoja-Branca*, Bolonia-Roma, ed. Galgano (Zanichelli, 2000) y, luego, en “La metafora e il diritto nella normativa sulla cosiddetta ‘firma grafometrica’”, *Diritto dell'informazione e dell'informatica* 29, no. 1 (2013): 1-16.

Sobre la metáfora en la jurisprudencia digital véase Morelli y Pollicino, “Metaphors, Judicial Frames and Fundamental Rights in Cyberspace”, *American Journal of Comparative Law* 68, no. 3 (2020): 616-646 y “The Metaphors of the Net. Lenguaje figurado, encuadramiento judicial y protección de derechos fundamentales en el ciberespacio: comparando modelos”, *Revista AIC* (2018).

⁸ Galgano, *Le insidie del linguaggio giuridico. Saggio sulle metafore nel diritto* (Il Mulino, 2010).

Si, por tanto, la aplicación de la inteligencia artificial es tal cuando conduce a resultados a los que podría conducir la inteligencia humana, el objeto de regulación es claramente amplísimo: cualquier proceso que pueda calificarse de inteligente podría ser objeto de regulación.

Llegados a este punto, se plantea la cuestión de si es conveniente que el legislador adopte un enfoque dirigido a regular la inteligencia artificial en su conjunto o, por el contrario, a regular las aplicaciones de la inteligencia artificial en sectores específicos o materias concretas. La primera opción es la adoptada por el Reglamento Europeo sobre Inteligencia Artificial, el cual, de hecho, tiene un enfoque regulador horizontal. La segunda es la preferida por algunas organizaciones internacionales en las que se ha considerado preferible regular las aplicaciones de la inteligencia artificial o, más concretamente, sus efectos en ámbitos específicos.

El tema fue ampliamente debatido en el *UNI-DROIT-UNCITRAL Joint Workshop on Smart Contracts, Artificial Intelligence and Distributed Ledger Technology*, que se celebró en Roma en la sede del Instituto Internacional para la Unificación del Derecho Privado (UNIDROIT) los días 6 y 7 de mayo de 2019. Este evento tenía como objetivo evaluar si eran necesarias intervenciones regulatorias a nivel internacional en relación con los *contratos inteligentes*, la inteligencia artificial y la tecnología de libro mayor distribuido.

Las conclusiones del taller fueron que debía adoptarse un enfoque doble: por un lado, defensivo —por así decirlo—, dirigido a adaptar las herramientas existentes a las nuevas tecnologías, y, por otro lado, proactivo, destinado a dictar algunas normas sencillas para facilitar el desarrollo de las tecnologías en algunos ámbitos limitados. En esa ocasión, también se puso de manifiesto que uno de los pocos ámbitos en los que es deseable una intervención reguladora es el de la responsabilidad por los daños causados por las aplicaciones de inteligencia artificial.

Un razonamiento similar podría llevarse a cabo en relación con otros sectores específicos, distintos del contractual. Por ejemplo, con respecto a la protección de los datos personales tratados por sistemas de inteligencia artificial; o con respecto a las aplicaciones en el sector sanitario; o con respecto a la administración pública y, en particular, al delicado perfil de transparencia del algoritmo utilizado en la toma de decisiones; o incluso en la administración de justicia; o en el sector del derecho penal; o en el ámbito de los derechos de autor⁹.

La cuestión fundamental que subyace a la elección de uno u otro enfoque es la relativa a la finalidad de la regulación: si se quiere dictar nuevas normas para un fenómeno nuevo o, por el contrario, limitar la intervención reguladora para superar o eliminar las barreras legales al uso de la tecnología.

Este dilema siempre se ha planteado en el diálogo entre el derecho y la tecnología con diferentes resultados, y, por supuesto, también se plantea aquí.

Entre las razones que condujeron a la regulación europea, se encuentran las geopolíticas, las cuales abordaremos en breve.

2. EL CONTEXTO GEOPOLÍTICO

En el Reglamento sobre Inteligencia Artificial, la Unión Europea (UE) ha optado por un enfoque normativo horizontal, aunque el Parlamento Europeo ha adoptado una serie de resoluciones relativas a la inteligencia artificial en relación con ámbitos específicos, por

⁹ Cada uno de estos temas, junto con otros, se profundiza en los dos volúmenes editados por Ruffolo, *XXVI Lezioni di diritto...*. Véase también Abriani y Schneider, *Diritto delle imprese e intelligenza artificiale* (Il Mulino, 2021) y Tampieri, *L'intelligenza artificiale e le sue evoluzioni. Civil law perspectives* (Wolters Kluwer Cedam, 2022).

ejemplo, con respecto a la ética¹⁰, la responsabilidad¹¹ y los derechos de autor¹². Como se afirma en el informe adjunto¹³, “el interés de la UE es preservar el liderazgo tecnológico de la UE”. Sin embargo, si se examina más de cerca, la UE no ostenta un liderazgo tecnológico en el ámbito de la inteligencia artificial, ya que no se encuentra entre los principales productores mundiales¹⁴. Más bien, como se aclara en el mismo informe¹⁵, se trata de “proteger la soberanía digital de la UE y explotar sus instrumentos y poderes reguladores para dar forma a reglas y normas de alcance mundial”. Este es el

¹⁰ Resolución del Parlamento Europeo del 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre el marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas, 2020/2012(INL).

¹¹ Resolución del Parlamento Europeo del 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad para la inteligencia, 2020/2014(INL).

¹² Resolución del Parlamento Europeo del 20 de octubre de 2020, sobre los derechos de propiedad intelectual para el desarrollo de tecnologías de inteligencia artificial, 2020/2015(INI).

¹³ Página 7 del informe.

¹⁴ “Según un informe reciente del Banco Europeo de Inversiones, existe un déficit de inversión de 10 000 millones de euros en la UE en el ámbito de las tecnologías de IA y *blockchain*. El 80% de las inversiones anuales mundiales en estas tecnologías se concentran en Estados Unidos y China, mientras que Europa solo invierte el 7% del total”. Así, Serri, “L’Europa in ritardo sull’AI: politica industriale e diritti”, *Aspenia* no. 94 (2021): 246 y ss. De nuevo, según el *Informe sobre el Índice de Inteligencia Artificial 2024* de la Universidad de Stanford, en 2023, Estados Unidos vio cómo las inversiones en IA alcanzaban los 67 200 millones de dólares, casi 8,7 veces más que China, el segundo mayor inversor. Además, mientras que la inversión privada en IA en China y la Unión Europea, incluido el Reino Unido, ha disminuido un 44,2% y un 14,1%, respectivamente, desde Estados Unidos se ha experimentado un aumento del 22,1%. El informe está disponible en https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf (consultado el 21 de junio de 2024).

¹⁵ Página 15 del informe.

objetivo declarado por la presidenta de la Comisión Europea desde su toma de posesión.

En el contexto geopolítico¹⁶, por tanto, la estrategia de la UE consiste en posicionarse como líder en la producción de legislación y hacer que el modelo europeo se convierta en una referencia mundial y pueda ser adoptado en otras regiones del mundo (el llamado “efecto Bruselas”)¹⁷.

No competimos con China y Estados Unidos en producción tecnológica, sino en regulación. El objetivo es afirmar una “soberanía digital” europea, como se dice en el informe, que sea a la vez externa, hacia los otros dos actores mundiales, e interna, hacia los Estados nacionales europeos. Por un lado, se trata de afirmar un nuevo modelo y, por otro, de evitar la fragmentación.

En este sentido, se confirma el diseño estratégico del legislador europeo, cuyo fin, en este caso, es construir un mercado único digital europeo y cuya estructura normativa se articula fundamentalmente en cuatro ámbitos: en primer lugar, el de la protección de datos personales, con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 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”, ahora más conocido como “GDPR”—, así como el de la valorización de los datos previsto en la Ley de Datos¹⁸, la Ley de Gobernanza

¹⁶ Para una reflexión sobre las principales orientaciones jurídicas del mercado digital, véase Finocchiaro, Balestra y Timoteo, eds., *Major Legal Trends in the Digital Economy* (Il Mulino, 2022).

¹⁷ Sobre el tema, en su totalidad, véase Bradford, *The Brussels Effect: How the European Union Rules the World* (Universidad de Oxford, 2020).

¹⁸ Se trata del Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo del 13 de diciembre de 2023: “Relativo a normas armonizadas sobre el acceso y el uso equitativos de los datos y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de datos)”. Disponible

de Datos¹⁹ y el Reglamento sobre el Espacio Europeo de Datos de Salud²⁰; en segundo lugar, el de los servicios digitales y el mercado digital, con la Ley de Servicios Digitales²¹ y la Ley de Mercados Digitales²²; en tercer lugar, la relativa a la identidad digital, con la revisión del Reglamento e-IDAS de 2014²³; y, por último, la relativa a la inteligencia artificial, con el reciente reglamento y la propuesta de Directiva que pretende adaptar las normas sobre responsabilidad

en <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R2854> (consultado el 10 de junio de 2024).

- ¹⁹ Se trata del Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo del 30 de mayo de 2022: “Relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento sobre gobernanza de datos)”. Disponible en <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CE-LEX:32022R0868> (consultado el 10 de junio de 2024).
- ²⁰ Se trata del Reglamento del Parlamento Europeo y del Consejo “sobre el Espacio Europeo de Datos Sanitarios”, aprobado por el Parlamento Europeo el 24 de abril de 2024. En el momento de redactar este documento, está pendiente la aprobación del texto por el Consejo. El texto aprobado por el Parlamento está disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_EN.pdf (consultado el 10 de junio de 2024).
- ²¹ Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo del 19 de octubre de 2022: “Relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento sobre servicios digitales)”. Disponible en <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065> (consultado el 10 de junio de 2024).
- ²² Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo del 14 de septiembre de 2022: “Sobre mercados equitativos y competitivos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento sobre el mercado digital)”. Disponible en <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022R1925> (consultado el 10 de junio de 2024).
- ²³ Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo del 11 de abril de 2024: “Por el que se modifica el Reglamento (UE) 910/2014 con respecto al establecimiento del marco europeo para una identidad”. Disponible en <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32024R1183> (consultado el 10 de junio de 2024).

civil extracontractual a la inteligencia artificial, es decir, la *Directiva sobre responsabilidad en materia de IA*²⁴.

Dentro de este diseño, no sólo se salvaguardan los derechos fundamentales²⁵, sino también los “valores” europeos, y este último término se menciona varias veces en el reglamento para subrayar que el modelo desarrollado no es sólo normativo, sino cultural. La intención es dejar claro que no se trata sólo de normas jurídicas, sino también de la cultura que esas normas expresan.

El modelo adoptado en Estados Unidos, con las necesarias simplificaciones que se recogen en este resumen, es un modelo de corregulación basado en la *antirreglamentación*. En octubre de 2023, el presidente Biden emitió una *Executive Order on the Safe, Secure, and Trustworthy Development and Use Artificial Intelligence*, cuyos principios habían sido compartidos con los principales productores de inteligencia artificial en agosto del mismo año. Entretanto, las autoridades antimonopolio, tras haber implicado a las grandes tecnológicas en numerosas investigaciones²⁶, habrían iniciado una

²⁴ Comisión Europea, Dirección General de Justicia y Consumidores. *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)*. COM (2022) 496 final, 28 de septiembre de 2022. Disponible en <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CE-LEX:52022PC0496> (consultado el 10 de junio de 2024).

²⁵ Se hace referencia expresa a los siguientes derechos consagrados en la Carta de los Derechos Fundamentales de la Unión Europea: el derecho a la dignidad humana (art. 1), el respeto de la vida privada y la protección de los datos de carácter personal (arts. 7 y 8), la no discriminación (art. 21), y la igualdad entre mujeres y hombres (art. 23).

²⁶ Los procedimientos más recientes incluyen el anunciado por el Departamento de Justicia de EE. UU. en marzo de 2024, centrado en las prácticas de Apple destinadas a hacer menos probable el cambio a dispositivos de la competencia, o el iniciado en 2023 por la *Comisión Federal de Comercio de EE. UU.* contra Amazon, relativo a sus estrategias para mantener una posición dominante en el mercado. Otras iniciativas del Departamento de Justicia y la Comisión Federal

investigación contra algunos de los principales actores del mercado de la producción de sistemas de IA²⁷.

El modelo chino, en cambio, parece dirigista y basado en el capitalismo de Estado. Ciertamente, China se caracteriza por ser cada vez más activa también en la producción normativa: en el ámbito de la protección de datos personales, baste recordar la Ley de Protección de Datos Personales (“Pipl”) en vigor desde el 1 de noviembre de 2021²⁸, la Ley de Seguridad de Datos (“Dsl”) en vigor desde el 1 de septiembre de 2021²⁹ y la Ley de Ciberseguridad (“Csl”) en vigor desde el 1 de junio de 2021³⁰. Y, desde una perspectiva estratégica, la reciente creación de la Bolsa de Datos de Shanghai (“Sde”) también aspira a crear el Modelo Shanghai para la compraventa de datos. El Modelo de Shanghai tiene la ambición de resolver los problemas que dificultan hoy en día la circulación de datos y de presentarse como un modelo de referencia mundial

de Comercio afectaron a Google y Meta. *La defensa de la competencia* también se ha centrado en Big Tech en la UE, con la Comisión comprometida, al menos desde 2017, en más de un caso, contra Google, Meta, Amazon y Apple. Entre los más recientes, está el que llevó a multar Apple con más de 1800 millones de euros en marzo de 2024 por abusar de su posición dominante en la distribución de aplicaciones de música en *streaming*. Según la reconstrucción de la Comisión, Apple impidió a los desarrolladores de aplicaciones de *streaming* de música informar a los usuarios de iOS de la disponibilidad de servicios alternativos más baratos y proporcionar instrucciones sobre cómo suscribirse a estos servicios.

²⁷ “El Departamento de Justicia y la Comisión Federal de Comercio acuerdan repartirse la responsabilidad de investigar a tres grandes actores de la industria de la inteligencia artificial”, titulaba el *New York Times* el 5 de junio de 2024, en un artículo disponible en <https://www.nytimes.com/2024/06/05/technology/nvidia-microsoft-openai-antitrust-doj-ftc.html> (consultado el 18 de junio de 2024).

²⁸ Ley de Protección de Datos Personales de la República Popular China, 20 de agosto de 2021.

²⁹ Ley de Seguridad de Datos de la República Popular China, 10 de junio de 2021.

³⁰ Ley de Ciberseguridad de la República Popular China, 6 de noviembre de 2016.

para eliminar los riesgos de inseguridad. Dentro de la producción normativa que específicamente se enfoca en la inteligencia artificial, se encuentra la publicación de los *Principios de Beijing sobre IA*, publicados en 2019 por la Academia de Beijing de Inteligencia Artificial (BAAI); los *Principios para desarrollar una IA responsable para la Inteligencia Artificial de Nueva Generación*, publicados en 2019 por el Comité de Expertos en Gobernanza de la IA de Nueva Generación; y, posteriormente, de las *Disposiciones de Gestión de Recomendaciones Algorítmicas*, publicadas en diciembre de 2021; las *Disposiciones de Síntesis Profunda*, publicadas en noviembre de 2022; y las *Medidas Provisionales para la Administración de Servicios de Inteligencia Artificial Generativa*, publicadas en julio de 2023. A estas iniciativas se sumó el proyecto de Ley de Inteligencia Artificial que se publicó en mayo de 2023.

Por lo tanto, como siempre, la estrategia regulatoria también persigue objetivos geopolíticos tratando de ampliar el ámbito de aplicación de la normativa europea. El artículo 2, de hecho, utiliza una técnica análoga a la empleada por el artículo 3 del Reglamento (UE) 2016/679³¹ y establece que el reglamento se aplica a

³¹ En efecto, el art. 3 del Reglamento (UE) 2016/679 dispone lo siguiente: “El presente reglamento se aplica al tratamiento de datos personales efectuado en el marco de las actividades de un establecimiento por un responsable o un encargado del tratamiento, independientemente de que el tratamiento se lleve a cabo o no en la UE. El presente reglamento se aplicará al tratamiento de datos personales de interesados situados en la UE, efectuado por un responsable o un encargado del tratamiento que no esté establecido en la UE, cuando las actividades de tratamiento se refieran: a) a la oferta de bienes o a la prestación de servicios a dichos interesados en la UE, con independencia de que se exija o no un pago por parte del interesado, o b) a la supervisión de su comportamiento, en la medida en que dicho comportamiento tenga lugar en la UE”. Sobre el ámbito de aplicación territorial del Reglamento (UE) 2016/679, Catanzariti, “Art. 3”, en *Codice della privacy e data protection*, eds. D’orazio, Finocchiaro, Pollicino y Resta, (Giuffrè, 2021), 143 y ss.; Czerniawski y De Hert, “Expanding the European data protection scope beyond territory: Article 3 of the General

los proveedores que comercialicen o pongan en servicio sistemas de inteligencia artificial o modelos de IA para fines generales en la UE, con independencia de que estén establecidos en la UE o en un tercer país, así como a los usuarios³² de sistemas de IA con lugar de establecimiento o situados en UE, y a los proveedores y usuarios de sistemas de IA con lugar de establecimiento o situados en un tercer país, cuando el producto producido por el sistema se utilice en la UE³³.

Data Protection Regulation in its wider context”, *Int. Data Priv. Law* 6, no. 3 (2016): 230 y ss.; Finocchiaro, “Il quadro d’insieme sul regolamento europeo sulla protezione dei dati personali” y Spangaro, “L’ambito di applicazione materiale della disciplina del Regolamento europeo 679/2016”, en *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, N.º 101*, ed. Finocchiaro (Zanichelli, 2019), 1 y ss. y 27 y ss., respectivamente; Reccia, “Art. 3”, en *GDPR e normativa privacy. Commentario*, eds. Belisario, Riccio y Scorza (Ipsos, 2018), 18 y ss.

³² He traducido con *users* la palabra *deployer*, el cual está presente en inglés también en el texto italiano del reglamento. El término designa a la persona física o jurídica, autoridad, agencia u otro organismo que utiliza un sistema de AI bajo su propia autoridad, excepto cuando el sistema se utiliza en el curso de una actividad personal no profesional. Así, apartado 4 del artículo 3 del reglamento.

³³ El Considerando 21 y Considerando 22 también se expresan claramente en este sentido. El Considerando 21 establece lo siguiente: “A fin de garantizar la igualdad de condiciones y la protección efectiva de los derechos y libertades de las personas en toda la UE, las normas establecidas en el presente reglamento deben aplicarse de forma no discriminatoria a los proveedores de sistemas de IA, con independencia de que estén establecidos en la UE o en un tercer país, y a los *implantadores* de sistemas de IA establecidos en la UE”. El Considerando 22 estipula lo siguiente: “Habida cuenta de su naturaleza de sistemas digitales, determinados sistemas de IA deben entrar en el ámbito de aplicación del presente reglamento incluso cuando no se comercialicen, pongan en servicio o utilicen en la UE [...] Para evitar que se eluda el presente reglamento y garantizar la protección efectiva de las personas físicas establecidas en la UE, el presente reglamento también debe aplicarse a los proveedores y a los *implantadores* de sistemas de IA establecidos en un tercer país, en la medida en que el producto generado por dichos sistemas se utilice en la UE”.

3. EL ENFOQUE ADOPTADO POR EL LEGISLADOR EUROPEO

El enfoque adoptado por el legislador europeo para la regulación de la inteligencia artificial es, como ya se ha mencionado, un enfoque horizontal. La limitación inherente a este planteamiento es que, al no tratarse de normas destinadas a resolver problemas concretos o a colmar determinadas lagunas del ordenamiento jurídico, deben ser necesariamente aplicables a cualquier sector, ya sea el sanitario o el financiero. Por lo tanto, no se trata de normas *ad hoc* para resolver un problema concreto o eliminar obstáculos jurídicos, sino de disposiciones generales para esbozar un marco global, es decir, un marco de referencia en el que funcionarán los sistemas de inteligencia artificial, incluso los que están por venir.

El reglamento parte de una página en blanco y esboza un método para hacer frente a los problemas que en abstracto podría crear cualquier aplicación de la inteligencia artificial y que el legislador europeo pretende evitar. Entre los peligros identificados por el Consejo y el Parlamento Europeo y mencionados en la exposición de motivos que acompaña a la propuesta de reglamento³⁴, se insta a hacer frente a “la falsabilidad, la facticidad, un cierto grado de imprevisibilidad y el comportamiento parcialmente autónomo de algunos sistemas de IA”.

El reglamento adopta un modelo de gestión de riesgos basado en la clasificación de los sistemas de inteligencia artificial en cuatro categorías según el riesgo que presenten: sistemas con riesgo inaceptable, sistemas de alto riesgo, sistemas de bajo riesgo y sistemas de riesgo mínimo³⁵.

³⁴ Página 2 del informe.

³⁵ Véanse la página 14 de la exposición de motivos que acompaña al proyecto de reglamento y el Considerando 26 del reglamento, que reza así: “A fin de introducir un conjunto proporcionado y eficaz de normas vinculantes para los sistemas de IA, conviene utilizar un enfoque basado en el riesgo claramente

En primer lugar, se prohíben los sistemas que presenten un riesgo inaceptable.

En cambio, para los sistemas de IA de bajo riesgo, se estipulan ciertas obligaciones de transparencia y se fomenta la adopción de códigos de conducta.

Una gran parte del reglamento se dedica a establecer requisitos y obligaciones detallados para los sistemas de IA de alto riesgo, que están sujetos a un procedimiento de evaluación de la conformidad *ex ante* que finaliza con el marcado CE. Un papel decisivo lo desempeñarán las normas técnicas que elaborarán los organismos del sector, a los cuales el legislador europeo confía, por tanto, un considerable poder regulador³⁶.

Por último, el reglamento aborda los denominados *modelos fundacionales*, los que han sido muy debatidos y no se trataron inicialmente en el proyecto de reglamento.

También, en este caso, el legislador europeo opta por una disciplina basada en el riesgo, de manera que se prevé un régimen diferenciado en función de si el modelo da lugar o no a un riesgo sistémico³⁷.

definido. Dicho enfoque debe adaptar la tipología y el contenido de estas normas a la intensidad y el alcance de los riesgos que pueden generar los sistemas de IA. Por lo tanto, es necesario prohibir determinadas prácticas de IA inaceptables, establecer requisitos para los sistemas de IA de alto riesgo y obligaciones para los operadores pertinentes, así como obligaciones de transparencia para los sistemas de IA sancionados³⁷.

Para más información sobre este modelo basado en el riesgo y lo que se ofrece para cada nivel de riesgo, consulte el capítulo 4 de este volumen.

³⁶ Resta, ¿“Cosa c’è di ‘europeo’ nella proposta di regolamento UE sull’Intelligenza Artificiale?”, *Diritto dell’informazione e dell’informatica* XXXVI, no. 2 (2022): 323 y ss.; Veale y Zuiderveen Borgesius, “Demystifying the Draft EU Artificial Intelligence Act”, *Computer Law Review International* 22, no. 4 (2021): 97 y ss.

³⁷ Sobre la definición de “modelos de IA de propósito”, y el punto de las obligaciones y requisitos para estos modelos, véase el capítulo 4 de este volumen.

4. CUESTIONES CRÍTICAS

El Reglamento Europeo sobre Inteligencia Artificial se propone como modelo de referencia mundial. Se repite a menudo que es el primer acto normativo³⁸ que pretende regular todo el sector, pero, como se ha escrito, Estados Unidos y China ya han emitido normativas al respecto. Además, varias organizaciones internacionales están llevando a cabo proyectos para regular ámbitos específicos de aplicación de la inteligencia artificial³⁹, considerando que, en muchos casos, el nivel adecuado de identificación de las normas sólo puede ser internacional.

El modelo europeo, como ya se ha dicho, es un modelo basado en la gestión de riesgos que parte de la clasificación de cuatro posibles categorías de riesgo para, a continuación, determinar los métodos para frenar los distintos riesgos asociados a ellas: en el caso más grave, prohibir los sistemas; en el caso de sistemas de alto riesgo, adoptar un procedimiento complejo y articulado para la gestión y el seguimiento continuo de los riesgos; y, en el caso de bajo riesgo, establecer obligaciones de transparencia.

Es ciertamente apreciable que la UE se haya preguntado por los problemas que plantea la inteligencia artificial y haya intentado intervenir. Sin embargo, algunas críticas son inevitables⁴⁰.

³⁸ Pero informa Floridi, “The European Legislation on AI: A Brief Analysis of its Philosophical Approach”, *Philos. Technol.* 34 (2021): 216 y ss., la US National AI Initiative Act, que se convirtió en ley el 1 de enero de 2021.

³⁹ UNIDROIT ha formulado principios sobre “activos digitales y Derecho privado”. La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-TRAL) adoptó en julio de 2024 una ley modelo sobre contratos celebrados y ejecutados mediante sistemas automatizados. El Instituto de Derecho Europeo está elaborando “Principios rectores y reglas modelo sobre contratos algorítmicos”.

⁴⁰ Para una lectura crítica, véase Abriani y Schneider, *Diritto delle imprese...*, 107 y ss; Floridi, “The European Legislation on AI...”; Restà, “Cosa c’è di ‘europeo’...”;

En primer lugar, el sistema esbozado en el reglamento parece rígido. La clasificación de los sistemas de inteligencia artificial en los distintos tipos de riesgo estará inevitablemente sujeta a revisión, tal como prevé el propio reglamento. Se desarrollarán nuevos sistemas, aún inéditos y se crearán nuevos métodos de aplicación de los sistemas ya previstos, lo que modificará el nivel de riesgo.

Por supuesto, el Reglamento Europeo sobre Inteligencia Artificial no es el primer caso en el que el legislador europeo construye un modelo basado fundamentalmente en la gestión de riesgos. De hecho, el caso más reciente e importante es el ya mencionado reglamento europeo 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. Pero, en este último acto, el sistema de gestión de riesgos va acompañado del *principio de responsabilidad*, es decir, el principio según el cual el responsable del tratamiento debe adoptar las medidas adecuadas para aplicar los principios y disposiciones del reglamento en función de las características específicas del tratamiento, así como aportar pruebas de haber llevado a cabo esta actividad. Esto permite una adaptación continua del modelo de gestión de riesgos por el propio responsable del tratamiento⁴¹.

Así, en el GDPR, es el responsable del tratamiento quien debe gestionar y evaluar el riesgo, mientras que, en el actual reglamento europeo, es el legislador quien decide qué sistemas

Tampieri, *L'intelligenza artificiale...*, 48 ss; Veale y Borgesius, "Demystifying the Draft EU...". Véase también Ahmed, Rengers, Harkens, Li, Maclaren, Piselli, Smuha y Yeung, *How the EU can achieve legally trustworthy AI: a response to the European Commission's proposal for an Artificial Intelligence Act*, que contiene los comentarios formulados por El Legal, Ethical & Accountable Digital Society (LEADS) Lab de la Universidad de Birmingham, disponible en papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991 (consultado el 18 de junio de 2024).

⁴¹ También abordo este tema en los capítulos 3 y 4 de este volumen.

son de alto riesgo y cómo se debe tratar el riesgo que suponen. Además, se parte de una definición muy amplia de sistema de inteligencia artificial.

Por tanto, un primer punto crítico a señalar es que las aplicaciones de inteligencia artificial, incluso las futuras, se regulan desde la perspectiva del presente y que, por tanto, el sistema no es suficientemente dinámico para seguir los desarrollos posteriores de la inteligencia artificial.

En segundo lugar, hay que tener en cuenta que un modelo de gestión de riesgos conlleva cargas administrativas muy importantes: elaboración de planes, certificaciones, notificaciones, producción de documentación y *branding*, cuyo coste será asumido por las empresas con independencia de su tamaño y del perfil concreto de aplicación de la IA en consideración.

Este error, es decir, adoptar la misma solución para temas y ámbitos muy diferentes entre sí, ya se ha cometido en otros sectores de la organización, por ejemplo, lo que respecta a la normativa sobre el tratamiento de datos personales, que, de hecho, se ha replanteado más recientemente con el *principio de responsabilidad* para permitir modular las medidas que deben adoptarse en función de las características específicas del caso.

Naturalmente, las obligaciones establecidas por el legislador europeo tendrán efectos diferentes según a quien se apliquen. Es de suponer que las grandes empresas no tendrán problemas para ocuparse de la documentación, la certificación, el marcado y otras cargas. En cambio, las pequeñas empresas y, en particular las empresas emergentes, verán cargas económicas muy pesadas e importantes como resultado de las obligaciones establecidas por el legislador europeo. Inevitablemente, las cargas y los costes de la protección diferirán en función de a quien vayan dirigidos. El legislador europeo deja en manos de los Estados miembros la creación de espacios de

experimentación normativa (*sandboxes*), y la adopción de medidas de apoyo a las pequeñas y medianas empresas⁴².

Por tanto, una segunda cuestión crítica es la adopción de un enfoque formal, oneroso e indiferenciado.

Sin embargo, desde un punto de vista sustantivo, la cuestión más importante es saber si el reglamento da respuesta a los peligros, desde la discriminación al sectarismo, que subyacen en su propia génesis, así como si protege adecuadamente los derechos y valores europeos, desde la dignidad personal a la protección de datos personales, a los que apela constantemente.

La protección proporcionada por el legislador europeo es general y abstracta, y consiste en el mismo modelo de gestión de riesgos que el reglamento, con las prohibiciones incluidas en el mismo. No existen nuevos instrumentos que la persona, individualmente o incluso colectivamente organizada, pueda utilizar para que la protección sea más eficaz, rápida o eficiente. Los instrumentos de protección, por tanto, dada la materia, serán en su mayoría los ya previstos por el RGPD, como el derecho de acceso, el derecho a la supresión de datos y el derecho a la portabilidad. Los principios sustantivos aplicables serán también los previstos en el Reglamento (UE) 2016/679 relativo a la protección de datos: calidad de los datos, exactitud, minimización, pertinencia, limitación del almacenamiento, integridad y confidencialidad.

⁴² Este riesgo no parece atenuarse con medidas como el art. 11 del reglamento, según el cual la Comisión Europea define un formulario simplificado de documentación técnica “que responde a las necesidades de las pequeñas empresas y microempresas”, o el art. 62, apartado 2, que exige que, al fijar las tasas de evaluación de la conformidad, “se tengan en cuenta los intereses y necesidades específicos de las PYME proveedoras, incluidas las emergentes, reduciendo dichas tasas en proporción a su tamaño, al tamaño de su mercado y a otros indicadores pertinentes”.

Se pospone el tratamiento de la cuestión de fondo, más delicada, de la formulación de un nuevo modelo de responsabilidad. La cuestión ya había sido prevista por la Comisión, que había planteado la posible configuración de la subjetividad jurídica de las aplicaciones de inteligencia artificial⁴³. En el reglamento objeto de examen, sólo se indica que el proveedor de un sistema de IA de alto riesgo está llamado a garantizar que el sistema cumple los requisitos. La citada propuesta de *Directiva sobre responsabilidad en materia de IA*, publicada el 28 de septiembre de 2022, sigue un enfoque de armonización mínima, limitándose a armonizar únicamente las normas sobre responsabilidad por culpa que regulan la carga de la prueba de quienes solicitan una indemnización por daños causados por sistemas de IA.

Hasta la fecha, la normativa europea, aparte de su valor estratégico en el contexto geopolítico, que es su fundamento, define esencialmente un marco administrativo para la comercialización de productos de inteligencia artificial. No obstante, el marco general deberá completarse con reglamentos y normas técnicas que tendrán una importancia fundamental y se actualizarán continuamente.

Desde un punto de vista sustantivo, el reglamento se limita a prohibir los sistemas de inteligencia artificial que entrañen un riesgo inaceptable y a afirmar un “derecho a presentar una denuncia” y un “derecho a examinar los procesos individuales de toma de decisiones”⁴⁴ para, luego, remitir, implícita o explícitamente, a los principios generales que hoy están en el centro del derecho europeo, de la dignidad a la transparencia y la protección de los

⁴³ Véase el apartado 59, letra f), de la Resolución del Parlamento Europeo del 16 de febrero de 2017, con recomendaciones destinadas a la Comisión en relación con las normas de Derecho sobre robótica, 2015/2103(INL).

⁴⁴ Estos derechos se afirman en la sección 4 del capítulo IX dedicado a los “Recursos”, en los arts. 85 y 86.

datos personales. Sin embargo, no se prevén formas concretas de aplicarlos a los sistemas de inteligencia artificial, ni formas nuevas y más eficaces de proteger al individuo.

Si la UE quiere realmente proteger los derechos fundamentales y los valores europeos, y convertirlos de hecho en una referencia mundial, no puede limitarse a proporcionar una certificación cuyas reglas técnicas serán establecidas por los organismos de normalización. Si quiere afirmar un liderazgo europeo a escala mundial, debe ir más allá del enfoque organizativo y de gestión, y abordar las cuestiones de fondo verdaderamente pendientes. Entre estos se encuentran, los problemas que requieren algo más que soluciones meramente formales y que deben abordarse con determinación para completar la regulación de la inteligencia artificial. Incluyen, sin duda, la definición de un método nuevo y general de responsabilidad por los daños causados por las aplicaciones de inteligencia artificial, que vaya más allá del planteamiento de armonización mínima del reglamento y de la propuesta de Directiva; el desarrollo de nuevas soluciones jurídicas que permitan, respetando plenamente los derechos fundamentales, el flujo de datos personales y no personales hacia las aplicaciones de inteligencia artificial; y la identificación de nuevos instrumentos eficaces y rápidos de protección contra la discriminación. Se trata de un compromiso de naturaleza muy diferente sobre derechos sustantivos y sobre instrumentos para hacerlos efectivos, el cual debe completar el marco normativo y que sólo la UE en este momento histórico podría abordar.

CAPÍTULO 2

ASPECTOS REGLAMENTARIOS DE LA INTELIGENCIA ARTIFICIAL*

1. LA SITUACIÓN ACTUAL

El Reglamento Europeo de Inteligencia Artificial ha llegado al final de un largo viaje que comenzó en 2018. La conclusión de los trabajos y la publicación del reglamento el 12 de julio de 2024 eran muy esperadas en Europa.

Por supuesto, un fenómeno nuevo puede requerir una disciplina reguladora, pero a menudo las normas ya existen. Ahora bien, las normas no sólo sirven, por supuesto, para regular, sino también para tranquilizar. No es casualidad que las empresas que producen inteligencia artificial también las invoquen para infundir confianza en el mercado potencial y estimular así el crecimiento.

Por otra parte, en general, siempre se hace hincapié en los peligros de la inteligencia artificial y rara vez nos detenemos a considerar sus oportunidades, que también son enormes. Baste pensar

* Este capítulo incorpora, con algunas adaptaciones y actualizaciones, el artículo publicado en *Aspenia* (2024): 122 y ss.

en las que han madurado en el ámbito médico con la lectura de informes ecográficos y el reconocimiento de tumores, por ejemplo.

Sin embargo, con mucha más frecuencia, se hace hincapié en los peligros de la nueva tecnología: desde la pérdida de puestos de trabajo hasta el riesgo de las *fake news*, pasando por la amenaza de condicionar la democracia. Ciertamente, existen peligros, pero también importantes beneficios y, en cualquier caso, no cabe duda de que tendremos que convivir con la inteligencia artificial.

El gran temor procede, en parte, de nuestra cultura y de las producciones artísticas, literarias y cinematográficas que precedieron a la defensa de la inteligencia artificial. Baste mencionar *2001: Odisea del espacio* y la producción literaria de Asimov, cuyas leyes de la robótica fueron incluso mencionadas en un texto de la UE, en la Resolución del Parlamento Europeo de 16 de febrero de 2017¹. El peligro que se percibe como mayor es que esta nueva tecnología se rebele contra el hombre, según lo que se ha llamado el complejo de Frankenstein, llamado así por el protagonista de la famosa novela de Mary Shelley.

La urgencia de regular se ha convertido ahora en política y ha abandonado el ámbito técnico-jurídico en el que se había debatido hasta ahora. Las reuniones y declaraciones se sucedieron a un ritmo vertiginoso. Desde la trilateral Italia-Francia-Alemania², pasando por la Declaración del G7, acompañada del Código de Conducta

¹ Véase la letra t) de la Resolución del Parlamento Europeo del 16 de febrero de 2017, relativa a las recomendaciones a la Comisión sobre normas de Derecho civil en materia de robótica, 2015/2103(INL).

² La referencia es a la reunión celebrada en octubre de 2023 entre los representantes de los tres países para “dar un nuevo impulso a la cooperación industrial en sectores estratégicos, con especial atención a la inteligencia artificial”. Así, el comunicado ministerial, disponible en <https://www.mimit.gov.it/it/notizie-stampa/italia-germania-e-francia-enhance-industrial-cooperation-on-artificial-intelligence> (consultado el 21 de junio de 2024).

y Directrices para las Empresas que Desarrollan Sistemas Avanzados de IA³, hasta la *Orden Ejecutiva* de Biden⁴, en la cumbre de Bletchley Park⁵. El nivel de discusión ha cambiado: de ser técnico, para juristas o informáticos, el debate sobre las normas ha pasado a ser político, con una aceleración repentina, como ocurrió con la llegada del ChatGPT, que hizo de la inteligencia artificial un tema de discusión en nuestra vida cotidiana. Y ahora son muchos los gobiernos que reclaman el liderazgo. En poco tiempo, el fenómeno de la inteligencia artificial ha atraído la máxima atención política en todos los países del mundo.

Ahora, se trata de dictar las reglas de la inteligencia artificial equilibrando riesgos y oportunidades.

2. LAS NORMAS DICTADAS EN EL MUNDO

En Europa, el debate sobre la disciplina de la inteligencia artificial comenzó hace mucho tiempo. Ya en diciembre de 2018, se publicó el primer borrador de las *Directrices éticas para una IA fiable*

³ En octubre de 2023, los líderes del G7 acordaron la dirección a seguir en el campo de la IA, inaugurando el *Proceso de IA de Hiroshima*. El compromiso de los líderes se renovó posteriormente en *Trento*, con la *Declaración de Trento sobre IA* de marzo de 2024. La Declaración de Hiroshima, el Código de Conducta y las empresas que desarrollan sistemas avanzados de IA están disponibles en <https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-code-conduct-advanced-ai-systems>, mientras que la Declaración de Trento está disponible en <https://assets.innovazione.gov.it/1710610112-trento-ai-declaration.pdf> (consultada el 21 de junio de 2024).

⁴ Se trata, por supuesto, de la *Orden Ejecutiva sobre el Desarrollo y Uso Seguro y Fidedigno de la Inteligencia Artificial* ya mencionada en el capítulo 1.

⁵ En noviembre de 2023, líderes de 28 países participaron en la *Cumbre sobre la Seguridad de la IA* iniciada por el Reino Unido, que se celebró en Bletchley Park y concluyó con la firma de la *Declaración de Bletchley sobre la seguridad de la IA*, disponible en <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration.es-419> (consultado el 21 de junio de 2024).

elaboradas por el Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial, designado por la Comisión Europea. Luego, en 2021, se presentó la primera propuesta de la Ley de IA, el Reglamento Europeo sobre Inteligencia Artificial, que luego fue aprobado y publicado en el Diario Oficial el 12 de julio de 2024: estos son los tiempos de la democracia europea. Ciertamente, el debate europeo de los últimos años ha contribuido a definir las cuestiones principales y, por tanto, muchos de los conceptos clave identificados en los principios y normas aprobadas se hacen eco del debate europeo: como la importancia de salvaguardar los derechos de la persona, que deben estar en el centro, la transparencia, la seguridad y muchos otros. Pero ahora Europa ya no corre sola y avanza hacia una coordinación internacional con muchos líderes potenciales.

En primer lugar, se encuentra Estados Unidos, que optó por un enfoque corregulador. De hecho, la *Orden Ejecutiva* del presidente Biden, emitida el 30 de octubre de 2023, fue precedida en julio del mismo año por un comunicado de la Casa Blanca en el que se informaba que siete grandes empresas estadounidenses productoras de IA (Amazon, Anthropic, Google, Inflection, Meta, Microsoft y Open AI) se habían comprometido voluntariamente con los principios fundamentales en el desarrollo de la IA de seguridad, que son los de protección y confianza. Estos principios, ya desarrollados en esa comunicación, constituyen la base de la *Orden Ejecutiva*, que los retoma y articula.

No olvidemos tampoco las iniciativas chinas, donde se incluyen los principios sobre inteligencia artificial de la Academia de Inteligencia Artificial de Pekín en 2019 y los nuevos principios sobre inteligencia artificial, *Medidas provisionales para la administración de servicios de inteligencia artificial generativa* en 2023.

Por tanto, puede decirse que, mientras en el caso del reglamento de la UE sobre protección de datos personales el conocido GDPR

Europa llegó primero y produjo el llamado “efecto Bruselas”, en este caso, que otros países ya han regulado el fenómeno y Europa sí ha condicionado el debate con la discusión que precedió a la promulgación del reglamento.

3. EL REGLAMENTO EUROPEO SOBRE INTELIGENCIA ARTIFICIAL EN EL PUNTO DE MIRA

La Ley Europea de IA dicta las condiciones de acceso al mercado de los sistemas de IA. Se trata de un enfoque basado en el riesgo, que prohíbe la introducción en el mercado de sistemas con un riesgo inaceptable (por ejemplo, sistemas de puntuación social) y, para la mayoría de los sistemas clasificados como de alto riesgo, permite su introducción en el mercado bajo determinadas condiciones.

Conviene recordar que la Ley de IA no regula todas las cuestiones que plantea la inteligencia artificial, sino que determina, como ya se ha dicho, las condiciones de acceso al mercado. Otras cuestiones jurídicas, por ejemplo, la responsabilidad por los daños causados por los sistemas de IA, la protección los derechos de autor y de la propiedad intelectual, la protección de la intimidad y los datos personales no están regulados por la Ley de IA. Sin embargo, es importante subrayar que esto no significa en absoluto, como a veces se afirma, que exista un vacío legal: hoy en día, ya se pueden tomar decisiones sobre la base de las normas existentes, como demuestra el hecho de que ya se hayan tomado muchas decisiones en todo el mundo sobre las cuestiones mencionadas.

Por supuesto, puede y debe debatirse si las normas actuales son adecuadas o si deben replantearse: esta reflexión se refiere, por ejemplo, a la autoría, la responsabilidad y la protección de datos personales, pero este es un debate que continuará al margen de la Ley de IA.

4. CONCLUSIONES

Nos encontramos en un momento crucial para establecer las normas que guíen el desarrollo de la IA y para lograr la coordinación mundial imprescindible para que estas normas sean eficaces en la protección de los derechos fundamentales.

Sin embargo, también es necesario encontrar un nuevo enfoque para ciertas cuestiones abiertas, que requieren un replanteamiento de los paradigmas culturales, incluso antes que las normas. Basta pensar en la responsabilidad, autenticidad y la gestión de los datos personales. De hecho, en lo que respecta a la responsabilidad, cuando los sistemas de IA producen resultados que no pueden predecirse *a priori*, sería necesario concebir un nuevo modelo que prescinda de la malicia, la culpa e incluso la búsqueda del error, y que asigne la responsabilidad civil sobre la base de un sistema de reparto de riesgos entre los distintos actores del sistema. En cuanto a la gestión de los flujos de datos, hay que encontrar un modelo de circulación de datos que supere la lógica de la propiedad. En efecto, los datos, personales y no personales se reutilizan y no son bienes “rivales”. La propiedad, en cambio, es por naturaleza un derecho exclusivo. Por tanto, es necesario pasar de la lógica de la propiedad, inadecuada en el contexto de la circulación de datos, a la del uso. La licencia parece ser el modelo de contrato más adecuado en este caso.

Una vez más, en lo que respecta al uso de los datos, no es adecuado a los tiempos en que vivimos pensar que podemos gestionar los grandes flujos de datos personales con el consentimiento individual. Por lo tanto, también aquí es necesario pensar en un nuevo modelo que se centre en las garantías que debe ofrecer el sistema y potenciar las bases jurídicas para el tratamiento de datos distintas del consentimiento.

Por último, en lo que respecta a las obras creadas por la inteligencia artificial, la cuestión es si el modelo autorial actual es

adecuado o si debe elaborarse un paradigma autorial diferente, como ha ocurrido en otras épocas.

Queda entonces abierta la cuestión de la gobernanza: toda regulación conlleva también un modelo organizativo, que luego determina en gran medida su eficacia. Ciertamente, es necesaria una supervisión de la difusión de las aplicaciones de inteligencia artificial, que lleve a cabo actividades de supervisión, coordinación y apoyo, pero también de coordinación entre los distintos sujetos competentes, de forma que se evite una peligrosa fragmentación⁶. En efecto, la inteligencia artificial es, por su propia naturaleza, transversal, pero es esencial que un sujeto pueda coordinar eficazmente a todos los demás y liderar así una estrategia tanto a escala nacional como europea.

⁶ La Ley de IA establece un sistema de gobernanza complejo y articulado, que comprende esencialmente, además de las autoridades nacionales, es decir, al menos una autoridad de notificación y una autoridad de vigilancia del mercado, una serie de organismos europeos: la Oficina IA, a través de la cual la Comisión Europea “desarrolla” sus competencias y capacidades en el ámbito de la IA (así, art. 64 del reglamento), el Comité Europeo de IA, compuesto un representante de cada Estado miembro y que constará de dos subgrupos. En primero lugar, un Foro Consultivo “para proporcionar conocimientos y apoyo al Comité y a la Comisión” (art. 67 del reglamento) y, en segundo lugar, un Grupo de Expertos Científicos Independientes.

CAPÍTULO 3

REGLAMENTO EUROPEO SOBRE INTELIGENCIA ARTIFICIAL: EL MODELO BASADO EN LA GESTIÓN DE RIESGOS*

1. EL CONTEXTO GEOPOLÍTICO

Una reflexión sobre el Reglamento Europeo de Inteligencia Artificial no puede prescindir de algunas consideraciones necesariamente sintéticas sobre el escenario geopolítico actual. El mercado de las nuevas tecnologías y, en concreto, de la inteligencia artificial es, sin duda, un mercado global sin barreras geográficas. La acción reguladora, en cambio, se caracteriza por las fronteras de los Estados nacionales o de instituciones supranacionales, como la UE. Por otra parte, este contraste entre el carácter eminentemente nacional del derecho y la dimensión global del fenómeno a regular, que hoy aparece en toda su evidencia en el esfuerzo por regular las

* Este capítulo recoge, con las oportunas adaptaciones y actualizaciones, el artículo publicado en *Information and Computer Law* (2022): 303 y ss., bajo el título “La propuesta de Reglamento sobre Inteligencia Artificial: el modelo europeo basado en la gestión de riesgos”.

consecuencias jurídicas de aplicaciones de la inteligencia artificial, ha caracterizado desde el principio el problema de las fuentes del derecho en Internet¹.

En la actualidad, el mercado parece dividirse básicamente en tres zonas de influencia: Europa, Estados Unidos y China.

El modelo adoptado en Europa es el modelo normativo: se trata no sólo de regular y reglamentar los nuevos fenómenos, las nuevas tecnologías y los nuevos bienes, sino también de promover el llamado “efecto Bruselas”, es decir, proponer el modelo europeo como referencia mundial².

El modelo adoptado en Estados Unidos, teniendo que simplificar aquí en aras de la brevedad, es un modelo corregulador, basado en la defensa de la competencia.

El modelo chino, por su parte, parece ser un modelo dirigista basado en el capitalismo de Estado, caracterizado recientemente por una importante producción normativa en el ámbito de la protección de datos personales, pero también específicamente de la IA y por algunas elecciones estratégicas precisas, como la creación de la Shanghai Data Exchange (SDE), la bolsa de Shanghai para el intercambio de datos³.

2. EL RIESGO DE LA RETÓRICA Y LA NECESIDAD DE UN NUEVO MODELO

Como es bien sabido, regular la tecnología es muy difícil. El principio de neutralidad tecnológica, actualmente establecido en

¹ Remito a mi obra “Lex Mercatoria and electronic commerce. The Law Applicable to Contracts Concluded on the Internet”, *Contratto e Impresa* (2001): 571-610, donde se ofrece amplia bibliografía.

² Para un análisis más detallado, remítase a lo ya explicado en el capítulo 1 de este volumen.

³ Véase nuevo el capítulo 1 de este volumen.

el ámbito internacional, es el resultado de un complejo debate. Según este, que se ha afirmado en la elaboración de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI)⁴, la ley debe permanecer neutral con respecto a la tecnología, absteniéndose de encontrar la solución técnica para aplicar los principios jurídicos afirmados. En otras palabras, la norma jurídica no debe referirse a un nivel de seguridad predefinida o una tecnología específica, sino que debe limitarse a dictar la finalidad que debe alcanzarse sin indicar las modalidades técnicas para su consecución⁵.

A la hora de legislar sobre inteligencia artificial, hay que tener en cuenta otras dos cuestiones críticas que pueden afectar a la actuación del legislador. La primera es el miedo: el temor a que las aplicaciones de inteligencia artificial puedan tomar decisiones de forma autónoma e, inspiradas en la literatura de ciencia ficción, puedan volverse contra los seres humanos y actuar de forma imprevista. Estos temores tienen su origen en la difícil previsibilidad de los resultados de los procesos de *machine learning*. Hay que ser consciente de este condicionamiento, así como del de la retórica, porque el miedo conduce, en este caso, a controlar la ansiedad. Los

⁴ El principio de neutralidad tecnológica ya fue afirmado por la CNUDMI en la Ley Modelo sobre Comercio Electrónico de 1996. Sobre este punto, véase mi “Il ruolo dell’UNCITRAL nello sviluppo della disciplina sul commercio elettronico”; Castellani, “I testi dell’UNCITRAL in materia di diritto del commercio elettronico”; y Ratti, “La Convenzione sull’uso delle comunicazioni elettroniche: le principali disposizioni”, en *Diritto dell’informatica*, ed. Delfini Finocchiaro (Utet Giuridica, 2014), respectivamente, 63-70, 43-62 y 71-107.

⁵ El principio de neutralidad tecnológica fue adoptado por el legislador europeo, por ejemplo, en el Reglamento (UE) 910/2014, el denominado Reglamento e-IDAS, cuando introdujo definiciones de firma electrónica y firma electrónica avanzada no referidas a tecnologías específicas. Por otra parte, no puede decirse que la noción de firma electrónica reconocida vinculada a niveles de seguridad predeterminados sea “tecnológicamente neutra”.

legisladores impulsados, o al menos condicionados, por el miedo tienen la necesidad de controlarlo todo dictando normas extremadamente detalladas; tomando una instantánea de lo que existe sin permitir que las normas evolucionen con el tiempo; entrando en detalles; abandonando la neutralidad técnica que, internacionalmente, es el principio fundamental al que hay que referirse. No se puede permitir que las sugerencias inducidas por las grandes obras artísticas sobre el tema, las cuales también se mencionaron en la Resolución del Parlamento Europeo de 2017 sobre las Tres Leyes de la Robótica de Asimov⁶, así como en la cinematografía y otros desarrollos artísticos, alimenten temores infundados. Esto podría llevar a la necesidad de un control absoluto y generar así el riesgo de regular en detalle lo que aún no se conoce del todo y que necesita un modelo de regulación y unos principios firmes, un marco claro en el que desarrollarse, y no normas detalladas y cargas burocráticas. No hay que caer en el error de querer regular al detalle el proceso de toma de decisiones. La segunda cuestión crítica es la de la retórica: caer en ella y acabar convirtiendo las aplicaciones de la inteligencia artificial en materia jurídica sin que ello contribuya a un nuevo modelo de regulación. El riesgo es que el uso genérico del término

⁶ Véase la Resolución del Parlamento Europeo del 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre las disposiciones de Derecho civil en materia de robótica, 2018/C 252/25. En particular, la resolución afirma lo siguiente: “Las leyes de deben considerarse dirigidas a los diseñadores, fabricantes y usuarios de robots, incluidos los robots con autonomía incorporada y capacidad de autoaprendizaje, ya que dichas leyes no pueden convertirse en código máquina”. A continuación, se cita el texto de las leyes de Asimov, que, como es bien sabido, reza así: “(1) Un robot no puede dañar a la humanidad ni puede permitir que la humanidad sea dañada por su falta de acción. (2) Un robot debe obedecer órdenes dadas por seres humanos, siempre que dichas órdenes no contravengan la Primera Ley. (3) Un robot debe proteger su propia existencia, siempre que esta autodefensa no entre en conflicto ni con la Primera ni con la Segunda Ley”.

“inteligencia” lleve implícitamente a suponer que existe un “sujeto inteligente” y no aplicaciones tecnológicas que hacen cosas que, si las hicieran los humanos, se considerarían inteligentes, tomando prestada la lección de Turing⁷.

Ciertamente, se puede elaborar un modelo jurídico de responsabilidad basado en una síntesis o metáfora lingüística⁸, como es el caso del concepto de personalidad jurídica, incluso de la subjetividad jurídica en las aplicaciones de la inteligencia artificial, pero siempre que sea adecuado para regular mejor el fenómeno⁹. Es necesario que esta sea una elección precisa y no una mera consecuencia de

⁷ Turing, “Computing Machinery...”, 436. Véase el capítulo 1 de este volumen sobre este punto.

⁸ Sobre el uso de la metáfora como técnica jurídica y sus límites, véanse las buenas páginas de Galgano, *Le insidie del linguaggio giuridico...*

⁹ Sobre el reconocimiento de la personalidad jurídica, Pagallo, *The Laws of Robots. Crimes, Contracts, and Torts* (Springer, 2013); Sartor, “Cognitive automata and the law: electronic contracting and the intentionality of software agents”, *Artificial Intelligence Law* 17, no. 4 (2009): 253-290; Teubner, “Rights of Non-Humans? Electronic Agents and Animals as New Actors in Politics and Law”, *Journal of Law and Society* 33, no. 4 (2006): 497-521. Teubner profundiza en este tema en el volumen *Soggetti giuridici digitali? Sullo status privatistico degli agenti software* (Edizioni Scientifiche Italiane, 2019). En sentido contrario, véase Bertolini y Aiello, “Robot companions: A legal and ethical análisis”, *Information Society* 34, no. 3 (2018): 130-140; Bertolini, “Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules”, *Law, Innovation and Technology* 5, no. 2 (2013): 214-247; Coppini, “Robotica e intelligenza artificiale: questioni di responsabilità civile”, *Politica del diritto* 49, no. 4 (2018): 713-739; Toffoletto, “IoT e Intelligenza Artificiale: Le Nuove Frontiere della Responsabilità Civile e del Risarcimento”, *Questioni di Giustizia*, 13 de junio de 2018, notas al margen de la conferencia “Inteligencia artificial y perfiles de aplicación temprana: Justicia, IoT y trabajadores” (Aula Magna del Palacio de Justicia de Milán), 17 de abril de 2018. Véase también mi contribución, “La conclusione del contratto telematico mediante i “software agents”: un falso problema giuridico?”, *Contratto e Impresa* (2002): 500-509.

una subjetividad implícita y presupuesta, fruto de la retórica¹⁰, y que se defina el nuevo modelo jurídico¹¹.

¹⁰ He desarrollado estos argumentos más ampliamente en mi *Inteligencia Artificial y Responsabilidad*, en el capítulo 6 de este volumen.

¹¹ La relación entre responsabilidad civil e inteligencia artificial se examina adecuadamente en la sección monográfica de la revista *Giurisprudenza Italiana*, dedicada al tema de inteligencia artificial y responsabilidad, titulada “Intelligenza Artificiale e diritto” dirigido por Ruffolo y Gabrielli no. 7 (2019): 1657-1660. En particular, véanse las contribuciones de Costanza, “L’intelligenza artificiale e gli stilemi della responsabilità civile”, *Dottrina e attualità giuridiche - Intelligenza Artificiale e diritto*, *Giurisprudenza Italiana* no. 7 (2019): 1686-1689, que identifica la responsabilidad en cabeza de la parte más próxima al hecho dañoso causado por la aplicación de la inteligencia artificial. El tema ha sido explorado también ampliamente por Franzoni, “La ‘vicinanza della prova’, quindi...”, *Contratto e Impresa* 2, no. 2 (2016): 360 y ss.; por Gambini, “Algoritmi e sicurezza: un’analisi giuridica”, *Giurisprudenza Italiana* 171, no. 7 (2019): 1726-1740, que aborda la cuestión de la seguridad en el ámbito de la inteligencia artificial examinando las soluciones ya existentes y adoptadas en el ámbito de los servicios de la sociedad de la información y del tratamiento automatizado de datos. También véase Ruffolo, “Intelligenza artificiale, machine learning e responsabilità da algoritmo”, *Giurisprudenza Italiana* no. 7 (2019): 1689-1704, que examina las posibilidades de identificar y calificar la responsabilidad de la inteligencia artificial a la luz del Código Civil, examinando también las hipótesis de reconocimiento de la personalidad jurídica. Con especial énfasis en la cuestión de la responsabilidad civil de los denominados *coches autónomos*, véase Calabresi y Al Mureden, *Driverless Cars. Intelligenza artificiale e futuro della mobilità* (Il Mulino, 2021) y Al Mureden, “Autonomous cars e responsabilità civile tra disciplina vigente e prospettive de iure condendo”, *Contratto e Impresa* 3 (2019): 895-924. El tema de la responsabilidad derivada de las aplicaciones de los sistemas de inteligencia artificial también se explora en profundidad en el volumen editado por Pizzetti, *Artificial intelligence, personal data protection and regulation* (Conseil de L’Europe, 2018) y, en particular, en la contribución de Bassini, Liguori y Pollicino, en *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, ed. Pizzetti no. 6 (2018), 333-371, en la que los autores ofrecen una panorámica de las diferentes orientaciones expresadas por la doctrina y la jurisprudencia en relación con la cuestión de la responsabilidad civil y penal derivada de cualquier daño causado por sistemas de inteligencia artificial; Massolo, “Responsabilità civile e IA”, en *Intelligenza*

Por ejemplo, en relación con el problema de la indemnización de los daños causados por la aplicación de la inteligencia artificial, hay que considerar que esta no dispondría de bienes con los que indemnizar los daños. Podría construirse un patrimonio reservado a la aplicación de inteligencia artificial, precisamente con el fin de permitir la indemnización de los daños¹². Sin embargo, si se quiere preservar un patrimonio para este fin, no es necesario construir el complejo edificio de la subjetividad de la aplicación. Se puede, sin embargo, construir un patrimonio reservado a la indemnización de este tipo de daños.

A diferencia de lo que ocurrió con la persona jurídica¹³, en este caso, parece que la atribución de subjetividad jurídica a las

artificiale, protezione dei dati personali e regolazione, eds. Pizzetti y Angelini, 373- 382, valora en cambio la idoneidad del marco jurídico nacional y europeo para regular las relaciones civiles en la era de la inteligencia artificial.

Para una revisión de las cuestiones planteadas, véase también el volumen editado por De Franceschi y Schulze, *Digital Revolution. New challenges for Law*, (C.H. Beck-Nomos, 2019), y en particular las contribuciones de Mazzini, “A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law”, 245-298, y de Mezzanotte, “Risk Allocation and Liability Regimes in the IoT”, 169- 189, ambos compiladas *Digital Revolution. New challenges for Law*, eds. De Franceschi y Schulze (C.H.Beck-Nomos, 2019). Véase Rachum y Twaig, “Whose Robot Is It Anyway? Liability for Artificial-Intelligence Based Robots”, *University of Illinois Law Review* 14, no. 22 (2020); Weber-Staiger, “New Liability Patterns in the Digital Era”, en *EU Internet Law*, eds. Synodinou, Jougoux, Marko y Prastitou (Springer, 2017): 197-214.

¹² Véase Pagallo, “Robotrust and legal responsibility”, *Knowledge, Technology & Policy* 23, no. 3 (2010): 367-379; Sartor, “Gli agenti software: nuovi soggetti del ciberdiritto?”, en *Contratto e Impresa* 18, no. 2 (2002): 465-499.

¹³ Véase Galgano, *Le insidie del linguaggio giuridico...*, quien atribuye a la metáfora el papel de simplificación lingüística de la complejidad de las relaciones jurídicas y, citando a su vez a D’Alessandro, *Personae giuridiche e analisi del linguaggio* (Giuffrè, 1989): 70 y ss., afirma lo siguiente: “La persona jurídica es, por tanto, un ente ‘detectable sólo en la escena jurídica verbalizada’, mientras que ‘en la escena real o existencial sólo existe un sujeto de derecho: el hombre’.

aplicaciones de IA es una construcción que aumenta la complejidad jurídica en lugar de disminuirla¹⁴. Sobre todo, la atribución de subjetividad a la aplicación de la inteligencia artificial no resuelve el problema más complejo: el de la identificación de los criterios de atribución de la responsabilidad, que parece ser el verdadero *quid* de la cuestión. De hecho, es necesario idear un nuevo modelo de responsabilidad que debería liberarse por completo de las condiciones subjetivas¹⁵ y ser más bien un modelo de asignación de riesgos¹⁶.

Sin embargo, una vez identificado el ámbito en el que el concepto de persona jurídica cumple su función, no se puede dejar de apreciar el valor de este concepto, que ninguna paráfrasis —‘por compleja e ingeniosa que sea’— podría sustituir; al contrario, debe considerarse como una ‘admirable creación original del lenguaje jurídico’, 49.

¹⁴ Véase Di Giovanni, “Attività contrattuale e intelligenza artificiale”, *Giurisprudenza Italiana* (2019): 1677-1686.

¹⁵ También presente en la Resolución del Parlamento Europeo de febrero de 2017, que, como observa Ruffolo, “Per i fondamenti di un diritto alla robotica self-learning; dalla maquinaria produttiva all’auto driverless: verso una ‘responsabilità da algoritmo’”, en *Intelligenza artificiale e responsabilità*, ed. Ruffolo (Giuffrè, 2017), 11-12. En este, se establece lo siguiente: “Parece no estar completamente exenta de una cierta centralidad del elemento subjetivo culposo como criterio de atribución de responsabilidad por lesiones causadas por robots *autodidactas*”. De hecho, el punto 59 f) de la resolución invita a la Comisión a considerar “el establecimiento de un estatuto jurídico específico para los robots a largo plazo, de modo que al menos los robots autónomos más sofisticados puedan ser considerados personas electrónicas responsables de indemnizar cualquier daño causado por ellos, así como el posible reconocimiento de la personalidad electrónica de los robots que toman decisiones autónomas o interactúan de forma independiente con terceros”.

¹⁶ He desarrollado más ampliamente estas consideraciones en mi *Inteligencia artificial y responsabilidad*, en el capítulo 6 de este volumen. Ciertamente, un principio que puede ser de gran utilidad es el basado en la *responsabilidad*. Sobre este punto, véase lo que ya se ha tratado en el capítulo 1 y lo que se explicará en el capítulo 4. Véase también Comandé, “Intelligenza artificiale e responsabilità tra «liability» e «accountability»”. Il carattere trasformativo dell’IA e il problema della responsabilità”, *Analisi Giuridica dell’Economia* no. 1 (2019): 169-188;

3. EL MODELO EUROPEO

El Reglamento Europeo de Inteligencia Artificial forma parte de un diseño estratégico, que se articula fundamentalmente en cuatro ámbitos ya mencionados: el de la protección de datos personales, con 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”, por ahora más conocido como “GDPR”; y el de la valorización de los datos aportados por la Ley de Datos¹⁷, por la Ley de Gobernanza de Datos¹⁸ y por el

Costanza, “L’intelligenza artificiale...”, 1689 y mi contribución, “L’accountability nel Regolamento Europeo”, en *Commentario del Codice Civile - Delle persone*, eds. Barba y Pagliantini (Utet Giuridica, 2019). A favor de un régimen de “responsabilidad objetiva”, véase Vladeck, “Machines without principals: liability rules and artificial intelligence”, en *Washington Law Review* 89, no. 1 (2014): 117-150, quien; sin embargo, aboga por la creación de una subjetividad pura de las aplicaciones autónomas. Para más detalles sobre la responsabilidad de la organización en su conjunto, en relación con la realización de actos *informáticos*, véase mi libro *I contratti informatici*, en *Trattato di diritto commerciale e di diritto pubblico dell’economia*, vol. XXII, ed. Galgano (CEDAM, 1997), en particular, 187. Finalmente, Calabresi ya habló de “responsabilidad de la empresa” en su obra “Some Thoughts on Risk Distribution and the Law of Torts”, *Yale Law Journal* (1961): 449-553.

¹⁷ Se trata del Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo del 13 de diciembre de 2023, “relativo a normas armonizadas acceso y el uso equitativo de los datos y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de datos)”, disponible en <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32023R2854> (consultado el 10 de junio de 2024).

¹⁸ Se trata del Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo del 30 de mayo de 2022, “relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento sobre gobernanza de datos)”, disponible en <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CE-LEX:32022R0868> (consultado el 10 de junio de 2024).

Reglamento sobre el Espacio Europeo de Datos de Salud¹⁹; la de servicios digitales y el mercado digital, con la Ley de Servicios Digitales²⁰ y la Ley de Mercados Digitales²¹; la relativa a la identidad digital, con la revisión del Reglamento e-IDAS de 2014²² y, por último, la inteligencia artificial, con el reciente Reglamento y la propuesta de Directiva que pretende adaptar las normas sobre responsabilidad civil extracontractual a la inteligencia artificial, la *Directiva sobre responsabilidad por IA*²³.

-
- ¹⁹ Se trata del Reglamento del Parlamento Europeo y del Consejo “sobre el Espacio Europeo de Datos Sanitarios”, aprobado por el Parlamento Europeo el 24 de abril de 2024. En el momento de redactar este documento, está pendiente aprobación del texto por el Consejo. El texto aprobado por el Parlamento está disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_EN.pdf (consultado el 10 de junio de 2024).
- ²⁰ Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo del 19 de octubre de 2022, “relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento sobre servicios digitales)”, disponible en <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065> (consultado el 10 de junio de 2024).
- ²¹ Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, “sobre mercados justos y competitivos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento sobre el mercado digital)”, disponible en <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022R1925> (consultado el 10 de junio de 2024).
- ²² Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo del 11 de abril de 2024, “por el que se modifica el Reglamento (UE) 910/2014 con respecto al establecimiento del marco europeo para una identidad”, disponible en <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32024R1183> (consultado el 10 de junio de 2024).
- ²³ Propuesta de Directiva del Parlamento Europeo y del Consejo, “relativa a la adaptación de las normas sobre responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad por inteligencia artificial)”, disponible en <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52022PC0496> (consultado el 10 de junio de 2024).

El objetivo estratégico es garantizar el establecimiento de un mercado único digital europeo y permitir a la Unión Europea “ser líder mundial en el desarrollo de una inteligencia artificial segura, fiable y ética”²⁴ también mediante el desarrollo de un modelo normativo. Los objetivos específicos son los siguientes:

- Garantizar que los sistemas de IA comercializados y utilizados en la Unión sean seguros y cumplan la legislación vigente sobre derechos fundamentales y los valores de la Unión;
- garantizar la seguridad jurídica para facilitar la inversión y la innovación en inteligencia artificial;
- mejorar la gobernanza y la aplicación efectiva de la legislación vigente sobre derechos fundamentales y requisitos de seguridad aplicables a los sistemas de IA;
- facilitar el desarrollo de un mercado único de aplicaciones de IA seguras y fiables y evitar la fragmentación del mercado”²⁵.

El Reglamento sobre Inteligencia Artificial es un texto muy complejo que consta de nada menos que 113 artículos²⁶.

²⁴ Así, el informe de la Comisión Europea que acompaña a la propuesta de reglamento, 2.

²⁵ Informe de la Comisión Europea que acompaña a la propuesta de reglamento.

²⁶ Sobre la propuesta de reglamento, véase Alpa, ¿“Quale modello normativo europeo per lintelligenza artificiale?”, *Contratto e Impresa* no. 4 (2021): 1003-10026; Ebers, “Standardizing AI - The Case of the European Commission’s Proposal for an Artificial Intelligence Act”, en *Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, eds. Dimatteo, Cannarsa y Poncibo (Cambridge, 2022); Floridi, “The European Legislation on AI...”, 215-222; Maccarthy y Propp, “Machines Learn That Brussels Writes the Rules: The EU’s New AI Regulation,” *Brookings Institution*, 9 de mayo de 2023, <https://www.brookings.edu/articles/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/>; McFadden, Jones, Taylor y Osborn, *Harmonising Artificial Intelligence. The role of standards in the EU AI Regulation* Harmonising Artificial Intelligence (Oxford Commission on AI y Good Governance, 2021); Mökander, Axente, Casolari y Floridi, “Conformity Assessments and Post-market Monitoring: A Guide to

Se optó por un enfoque horizontal, que abarca todos los sectores. Según la Comisión, se optó por una metodología que establece un marco reglamentario únicamente para los sistemas de IA de alto riesgo, con la opción de que todos los proveedores de sistemas de IA que no sean de alto riesgo sigan un código de conducta. “Los requisitos abarcarán los datos, la documentación y la trazabilidad, el suministro de información y la transparencia, la supervisión humana, así como la solidez y la precisión, y serán obligatorios para los sistemas de IA de alto riesgo. Las empresas que introduzcan códigos de conducta para otros sistemas de IA lo harán de forma voluntaria”²⁷.

Así pues, el reglamento regula la puesta en servicio y utilización de sistemas de inteligencia artificial en general, como se indica en el artículo 1, y no en un sector específico.

La definición de sistema de inteligencia artificial, coherente con este planteamiento, es extremadamente general²⁸. A los sistemas de inteligencia artificial se suman los modelos de IA para fines generales, los ya conocidos “modelos fundacionales”, cuya introducción en el mercado también está regulada por el reglamento²⁹.

the Role of Auditing in the Proposed European AI Regulation”, *Minds and Machines* (2021); Townsend, “Decoding the Proposed European Union Artificial Intelligence Act”, *Insights* 25, no. 20 (2021); Veale y Borgesius, “Demystifying the Draft EU...”, 97-112.

²⁷ Así, la exposición de motivos de la Comisión Europea que acompaña a la propuesta del reglamento, 11.

²⁸ Como se anticipó en el capítulo 1 de este volumen, la Ley de IA define un sistema de IA como “un sistema automatizado diseñado para funcionar con distintos niveles de autonomía y que puede mostrar adaptabilidad tras su despliegue y que, con fines explícitos o implícitos, deduce de la entrada que recibe cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales” (art. 3, N.º 1).

²⁹ Así, el artículo 1, letra e): “El reglamento [...] establece: [...] e) normas armonizadas para la comercialización de modelos de IA para usos generales”.

El modelo adoptado es uno basado en el riesgo, como ya se indicaba en la exposición de motivos del proyecto de reglamento, diferenciando entre usos de la IA que generan un riesgo inaceptable, un riesgo elevado, un riesgo limitado y un riesgo mínimo, respectivamente.

El legislador prevé que hay aplicaciones de la inteligencia artificial que deben prohibirse y las enumera en el artículo 5 del reglamento. Por ejemplo, prohíbe la puesta en marcha de sistemas que utilicen técnicas subliminales, así como la puesta en marcha de sistemas que exploten la vulnerabilidad de un grupo de personas.

En particular, por lo que se refiere a estas prácticas de inteligencia artificial, el legislador europeo inserta la consecución del objetivo como calificador de la aplicación prohibida: es decir, debe estar dirigida a alcanzar determinados objetivos, como distorsionar materialmente el comportamiento de forma que pueda esperarse razonablemente que cause un daño significativo³⁰.

³⁰ Las letras a) y b) del apartado 1 del art. 5 establecen lo siguiente: “Quedan prohibidas las siguientes prácticas de AI:

a) comercializar, poner en servicio o utilizar un sistema de IA que emplee técnicas subliminales que actúen sin el conocimiento de una persona, o técnicas intencionadamente manipuladoras o engañosas con el propósito o el efecto de distorsionar materialmente el comportamiento de una persona o grupo de personas menoscabar materialmente su capacidad de tomar una decisión con conocimiento de causa, llevándoles a tomar una decisión que de otro modo no habrían tomado, de forma que causen o sea razonablemente probable que causen un daño significativo a esa persona, a otra persona o a un grupo de personas;

b) la comercialización, puesta en servicio o utilización de un sistema de IA que explote las vulnerabilidades de una persona física o de un grupo específico de personas, debido a su edad, discapacidad o a una situación social o económica específica, con el objetivo o el efecto de distorsionar materialmente el comportamiento de esa persona o de una persona perteneciente a ese grupo de forma que cause o pueda esperarse razonablemente que cause a esa persona o a otra un daño significativo”.

También se prohíbe la comercialización y puesta en servicio de sistemas de puntuación social que atenten contra la dignidad humana³¹.

Asimismo, se prohíbe el uso de sistemas de identificación biométrica “en tiempo real” en espacios de acceso público, especialmente invasivos de los derechos y libertades de las personas afectadas, con fines policiales³². El punto crítico reside, por supuesto, en las excepciones previstas por el legislador, por ejemplo, para

³¹ En efecto, el art. 5, apartado 1, letra c), incluye entre las prácticas de IA prohibidas “la puesta en el mercado, encargo o utilización de sistemas de IA para evaluación o clasificación de personas físicas o grupos de personas durante un período de tiempo determinado sobre la base de su comportamiento social o de características personales o de personalidad conocidas, inferidas o previstas, cuando la puntuación social así obtenida conduzca a la concurrencia de uno o ambos de los siguientes supuestos:

- i) trato perjudicial o desfavorable de determinadas personas físicas o grupos de personas en contextos sociales no relacionados con los contextos en los que se generaron o recopilaban originalmente los datos;
- ii) trato perjudicial o desfavorable, injustificado o desproporcionado en relación con su comportamiento social o con la gravedad del mismo, a determinadas personas físicas o grupos de personas”.

³² Considerando 32: “El uso de sistemas de IA de identificación biométrica remota ‘en tiempo real’ de personas físicas en espacios de acceso público con fines policiales se considera especialmente intrusivo para los derechos y libertades de las personas afectadas, en la medida en que podría afectar a la intimidad de un amplio segmento de la población, hacer que se sientan constantemente vigiladas y desalentar indirectamente el ejercicio de la libertad de reunión y otros derechos fundamentales. Las imprecisiones técnicas de los sistemas de IA para la identificación biométrica a distancia de personas físicas pueden dar lugar a resultados sesgados y efectos discriminatorios. Estos posibles resultados sesgados y efectos discriminatorios son especialmente relevantes en relación con la edad, la etnia, la raza, el género o la discapacidad. La inmediatez del impacto y las limitadas oportunidades de realizar comprobaciones o correcciones adicionales en relación con el uso de tales sistemas que operan ‘en tiempo real’ también implican mayores riesgos con respecto a los derechos y libertades de las personas afectadas en el contexto de las actividades policiales o afectadas por ellas”.

los casos en que el uso de sistemas de identificación biométrica a distancia sea estrictamente necesario para “la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas”³³ o para “la prevención de una amenaza específica, sustancial e inminente para la vida o la integridad de las personas físicas o de una amenaza real y presente o real y previsible de un atentado terrorista”³⁴. Hubo un acalorado debate al respecto, ya que las excepciones, si son demasiado amplias, pueden acabar anulando lo prohibido en otras disposiciones.

El reglamento, a partir del artículo 6, clasifica los sistemas de inteligencia artificial como de alto riesgo. Establece que, si los sistemas de inteligencia artificial son sistemas de alto riesgo, deben cumplirse una serie de requisitos y debe realizarse una evaluación *ex ante* de conformidad. Los sistemas clasificados como de alto riesgo son los siguientes: los sistemas producidos o destinados a ser utilizados como componentes de seguridad de productos cubiertos por la legislación europea de armonización enumerada en el Anexo I del reglamento, cuando dicha legislación de armonización los someta a una evaluación de conformidad *ex ante* por terceros³⁵; otros sistemas independientes de AI con implicaciones para la salud, la seguridad y los derechos fundamentales, enumerados en el Anexo III del reglamento³⁶.

³³ Así art. 5(1)(h)(i).

³⁴ Así art. 5(1)(h)(ii).

³⁵ Se trata de los sistemas de alto riesgo contemplados en el apartado 1 del artículo 6.

³⁶ Se trata de los sistemas de alto riesgo contemplados en el apartado 2 del art. 6. El vínculo entre la clasificación del sistema y el riesgo para la salud, la seguridad y los derechos fundamentales queda bien reflejado en la excepción consagrada en el art. 6, apartado 3, según la cual “no se considerará de alto riesgo un sistema de AI contemplado el Anexo III cuando no presente un riesgo significativo de

Los requisitos que debe cumplir un sistema de inteligencia artificial de alto riesgo vienen dictados por el artículo 8 y siguientes.

Según el artículo 8, para garantizar el cumplimiento de estas obligaciones y requisitos, deben tenerse en cuenta tres elementos: la finalidad prevista del sistema de IA de alto riesgo, el “estado de la técnica generalmente reconocido en materia de IA y tecnologías relacionadas con la IA”, y el sistema de gestión de riesgos, que es objeto de la regulación específica establecida en el artículo 9.

En primer lugar, debe establecerse, implantarse, documentarse y mantenerse un sistema de gestión de riesgos, es decir, un proceso iterativo continuo, planificado y ejecutado a lo largo del ciclo de vida

perjuicio para la salud, la seguridad o los derechos fundamentales de las personas, ni siquiera en el sentido de no influir materialmente en el resultado del proceso de toma de decisiones”. Se establece que la excepción se aplica cuando: “a) el sistema de IA destinado a realizar una tarea de procedimiento limitada; b) el sistema de IA está destinado a mejorar el resultado de una actividad humana previamente realizada; c) el sistema de IA está destinado a detectar patrones de toma de decisiones o desviaciones de patrones de toma de decisiones anteriores y no está destinado a sustituir o influir en una evaluación humana previamente realizada sin una revisión humana adecuada; o d) el sistema de IA está destinado a realizar una tarea preparatoria para una evaluación pertinente para los casos de uso enumerados en el anexo” (art. 6, apartado 2). En cualquier caso, “un sistema de IA enumerado en el Anexo III se considera de alto riesgo cuando no plantee un riesgo significativo de perjuicio para la salud, la seguridad o los derechos fundamentales de las personas físicas” (art. 6, apartado 3, punto 3).

Entre los sistemas de alto riesgo incluidos en el Anexo III del figuran: los sistemas de identificación biométrica a distancia; los sistemas destinados a ser utilizados como componentes de seguridad en la gestión y explotación de infraestructuras digitales críticas, el tráfico por carretera o en el suministro de agua, gas, calefacción o electricidad; sistemas destinados a ser utilizados para determinar el acceso, la admisión o la asignación de personas a instituciones educativas y de formación profesional a todos los niveles; sistemas destinados a ser utilizados en contratación o selección trabajadores; sistemas de *calificación crediticia*; o sistemas destinados utilizados por una autoridad judicial en la investigación e interpretación de hechos y leyes, y en la aplicación de la ley a un conjunto concreto de hechos.

del sistema de IA de alto riesgo. Este debe incluir la identificación y el análisis de los riesgos conocidos y razonablemente previsibles asociados al sistema; la estimación y evaluación de los riesgos que puedan surgir cuando el sistema de IA de alto riesgo se utilice de acuerdo con su finalidad prevista y en condiciones razonablemente previsibles de uso indebido; la evaluación de cualquier otro riesgo derivado del análisis de los datos recogidos por el sistema de seguimiento poscomercialización; y la adopción de medidas de gestión de riesgos adecuadas que sean “apropiadas y específicas”³⁷.

Posteriormente, se identifican determinados criterios de calidad para los conjuntos de datos utilizados con fines de formación, validación y prueba en el contexto de los sistemas de IA de alto riesgo³⁸. En particular, estos conjuntos de datos deben estar sujetas a prácticas específicas de gobernanza y gestión³⁹, y ser pertinentes, suficientemente representativas y, “en la medida de lo posible”, exentas de errores, completas y estadísticamente adecuadas⁴⁰.

³⁷ Art. 9, apartados 1 y 2.

³⁸ Así, art. 10, apartado 1. Según las definiciones del art. 3, los “datos de entrenamiento” son datos “utilizados para entrenar un sistema de IA adaptando los parámetros que puede aprender” (29); los “datos de validación” son datos “utilizados para proporcionar una evaluación del sistema de IA entrenado y para afinar, otras cosas, los parámetros que no puede aprender y el proceso de aprendizaje con el fin, entre otras cosas, de evitar la inadaptación o la sobreadaptación” (30); los “datos de pruebas” son los datos utilizados para proporcionar una evaluación independiente del sistema de IA con el fin de confirmar su rendimiento previsto antes de su comercialización o puesta en servicio” (41).

³⁹ Así, el art. 10, apartado 2, identifica los ámbitos cubiertos por las prácticas de gestión. Entre ellos figuran: “a) las opciones de diseño pertinentes; b) los procesos de recopilación de datos y el origen de los datos, así como la finalidad original de la recopilación en el caso de los datos personales; c) las operaciones de tratamiento pertinentes para la preparación de datos, como la anotación, el etiquetado, la limpieza, la actualización, el enriquecimiento y la agregación”.

⁴⁰ Así, art. 10(3).

Además, se exige que, antes de comercialización o puesta en servicio del sistema de IA de alto riesgo, se elabore la documentación técnica pertinente, que tiene por objeto demostrar que el sistema de IA de alto riesgo cumple los requisitos establecidos en el reglamento, así como proporcionar a las autoridades y organismos competentes toda la información que necesiten para evaluar dicho cumplimiento⁴¹.

Además, los sistemas de IA de alto riesgo deben permitir, a nivel técnico, el registro automático de eventos, los llamados *logs*, a lo largo de su ciclo de vida para garantizar la trazabilidad del funcionamiento⁴², que deben ser suficientemente transparentes para permitir a los usuarios⁴³ interpretar el resultado y utilizarlo

⁴¹ Así, el art. 11, en el Anexo IV del reglamento para la determinación del contenido mínimo de la documentación técnica, se prevé que las pequeñas y medianas empresas, incluidas *las de nueva creación*, puedan presentar de forma simplificada algunos de los elementos de la documentación técnica especificados en el mismo y que la Comisión establezca un formulario simplificado de documentación técnica “que responda a las necesidades de las pequeñas empresas y microempresas”.

⁴² Así, el art. 12, que especifica cómo las capacidades de registro deben permitir, en particular, el registro de acontecimientos pertinentes para la identificación de situaciones que puedan hacer que el sistema presente un riesgo para la salud, la seguridad o la protección de los derechos fundamentales de las personas o suponga una modificación sustancial, y para facilitar el seguimiento posterior a la comercialización. Además, esta disposición identifica los datos que deben registrarse necesariamente con respecto a los sistemas de IA para la identificación biométrica, entre ellos, el registro del período de cada uso del sistema, la base de datos de referencia con la que el sistema ha verificado los datos de entrada, los datos de entrada para los que la búsqueda dio como resultado una coincidencia y el identificador de las personas físicas que participaron en la verificación de los resultados.

⁴³ También, en este caso, como en el capítulo 1 de este volumen, el término se utiliza en la traducción italiana, a pesar de que el texto italiano del reglamento emplea el término inglés *deployer*. Sobre la noción de *deployer*, ya indicada en el capítulo 1, véase también el resto de este capítulo.

adecuadamente⁴⁴. Teniendo esto en cuenta, los sistemas de IA de alto riesgo deben ir acompañados de instrucciones de uso, en un formato digital o no digital adecuado, que incluyan información concisa, completa, correcta, clara y pertinente que sea accesible y comprensible para los usuarios⁴⁵.

A continuación, los sistemas de IA de alto riesgo deben estar equipados con herramientas de interfaz hombre-máquina que permitan su supervisión por parte de personas físicas con el objetivo de prevenir o minimizar los riesgos para la salud, la seguridad o los derechos fundamentales⁴⁶. Por último, deben diseñarse y desa-

⁴⁴ Así, art. 13(1).

⁴⁵ Así, el art. 13(2) incluye, entre la información que debe facilitarse al usuario, lo siguiente: la identidad y los datos de contacto del proveedor y, en su caso, de su representante autorizado; las características, capacidades y limitaciones de funcionamiento del sistema de IA de alto riesgo, incluida la finalidad prevista; el nivel de precisión, solidez y ciberseguridad con respecto al cual se ha probado y validado el sistema de IA de alto riesgo; cualquier circunstancia conocida o previsible que pueda repercutir en el nivel previsto de precisión, solidez y ciberseguridad; cualquier circunstancia conocida o previsible, relacionada con uso del sistema de IA de alto riesgo de conformidad con su finalidad prevista o en condiciones razonablemente previsibles de uso indebido, que pueda plantear riesgos para la salud y la seguridad o los derechos fundamentales; en su caso, las capacidades y características técnicas del sistema de IA de alto riesgo relacionadas con el suministro de información pertinente para explicar sus resultados; en su caso, su rendimiento con respecto a las personas o grupos de personas sobre los que está previsto utilizar el sistema; en su caso, las especificaciones de los datos de entrada o cualquier otra información pertinente en términos de adecuación, validación y comprobación de conjuntos de datos, teniendo en cuenta la finalidad prevista del sistema de IA; en su caso, información que permita a los encargados de la implantación interpretar los resultados del sistema y utilizarlos de manera adecuada.

⁴⁶ Así, el art. 14 los riesgos que deben prevenirse o reducirse al mínimo para la salud, la seguridad o los derechos fundamentales son los “que puedan surgir cuando un sistema de IA de alto riesgo se utilice de acuerdo con su finalidad prevista o en condiciones de uso indebido razonablemente previsible, en particular cuando dichos riesgos persistan a pesar de la aplicación de otros requisitos

rollarse de forma que se alcance un nivel adecuado de precisión, robustez y ciberseguridad que perdure durante todo el ciclo de vida del sistema⁴⁷.

[del reglamento]”. Además, según el apartado 3 del art. 14, la vigilancia humana está garantizada mediante al menos una de las siguientes medidas: a) medidas identificadas e integradas en el sistema de IA de alto riesgo por el proveedor antes de su comercialización o puesta en servicio, cuando sea técnicamente posible; b) medidas identificadas por el proveedor antes de la comercialización o puesta en servicio del sistema de IA de alto riesgo, que sean adecuadas para su aplicación por el *encargado de la implantación*. De conformidad con el apartado 4 del art. 14, estas medidas, en función de las circunstancias, deberán permitir a la persona encargada de supervisar el sistema de IA de alto riesgo, entre otras cosas, a) comprender plenamente sus capacidades y limitaciones y poder supervisar debidamente su funcionamiento, de modo que puedan detectarse y tratarse los signos de anomalías, mal funcionamiento y rendimiento inesperado; b) ser consciente de una posible tendencia a confiar o depender excesivamente de forma automática de los resultados producidos por el denominado; (c) ser capaz de interpretar correctamente los resultados del sistema de inteligencia artificial de riesgo, teniendo en cuenta, por ejemplo, las herramientas y métodos de interpretación disponibles; (d) decidir, en cualquier situación concreta, no utilizar el sistema de inteligencia artificial de del sistema de inteligencia artificial de riesgo; y (d) decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o, de lo contrario, ignorar, anular o invertir la salida del sistema de IA de alto riesgo; y e) intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema botón de “parada” o un procedimiento similar que permita apagar el sistema de forma segura.

⁴⁷ Así, el art. 15 exige que los sistemas de IA de alto riesgo sean también resilientes con respecto a los errores, fallos o incoherencias que puedan producirse en el sistema o en el entorno en el que opera, en particular como resultado de su interacción con personas físicas u otros sistemas. Además, se exige que los sistemas de IA de alto riesgo que continúen su aprendizaje tras su comercialización o puesta en servicio se desarrollen de forma que se elimine o reduzca en la medida de lo posible el riesgo de que los resultados potencialmente distorsionados influyan en los insumos para futuras operaciones, los denominados “bucles de retroalimentación”, y que se garantice que dichos bucles estén sujetos a medidas de mitigación adecuadas. De nuevo, según el art. 15, apartado 5, los sistemas de IA de alto riesgo deben ser resistentes a los intentos de terceros no autorizados de modificar su uso o rendimiento aprovechando las vulnerabilidades

Otras obligaciones y requisitos para los sistemas de IA de alto riesgo se derivan de las disposiciones que establecen obligaciones específicas para quienes intervienen en la cadena de creación y uso de dichos sistemas.

Se trata del *proveedor* del sistema de IA, definido como la persona física o jurídica, autoridad pública, agencia u otro organismo que desarrolla o dispone el desarrollo de un sistema de inteligencia artificial o de un mecanismo de IA con vistas a colocar en el mercado bajo su propio nombre o marca, ya sea a cambio de una remuneración o de forma gratuita⁴⁸; del *implantador*, es decir, cualquier persona física o jurídica, autoridad pública, agencia u otro organismo que utilice un sistema de inteligencia artificial bajo su propia autoridad, a menos que el sistema se utilice en el curso de una actividad personal y no profesional⁴⁹; del c.d. *importador*,

del sistema. Por último, se espera que las soluciones técnicas para garantizar la ciberseguridad sean adecuadas a las circunstancias y riesgos pertinentes, mientras que las soluciones técnicas para hacer frente a las vulnerabilidades específicas de la IA deben incluir, en su caso, medidas para prevenir, detectar, responder, resolver y controlar los ataques que intenten manipular el conjunto de datos de entrenamiento (el llamado “envenenamiento de datos”); las entradas diseñadas para provocar que el modelo cometa un error (los llamados “ejemplos adversos”); los ataques o fallos contra la privacidad; y los ataques contra el rendimiento del sistema del modelo. El art. 15 cierra la sección 2 del capítulo III dedicándola expresamente a los requisitos de los sistemas de IA de alto riesgo.

⁴⁸ Así, el apartado 3 del art. 3. de la figura del *proveedor*. En el apartado 5 del art. 3, se identifica la del representante autorizado, es decir, cualquier persona física, o jurídica situada o establecida en la UE que reciba y acepte un mandato escrito del *proveedor* para cumplir y ejecutar en su nombre las obligaciones y procedimientos establecidos en el reglamento. Según el art. 22, antes de comercializar sus sistemas en el mercado de la Unión, los proveedores establecidos fuera de la UE deberán designar, mediante mandato escrito, a un representante autorizado establecido en la UE.

⁴⁹ Así, el apartado 4 del art. 3. Como ya se ha destacado en este volumen, la traducción italiana del reglamento conserva el término *deployer*, que puede entenderse como “usuario”.

es decir, toda persona física o jurídica situada o establecida en la UE que un sistema de inteligencia artificial que lleva el nombre o la marca de una persona física o jurídica establecida en un tercer país⁵⁰; y del *distribuidor*, es decir, toda persona física o jurídica de la cadena de suministro, distinta del proveedor o del importador, que comercializa un sistema de inteligencia artificial en el mercado de la UE⁵¹.

En el marco esbozado por el reglamento, el *proveedor* de un sistema de IA de alto riesgo está llamado, en primer lugar, a garantizar que el sistema cumple los requisitos descritos anteriormente⁵², así como, en caso de incumplimiento, adoptar inmediatamente las medidas correctoras necesarias para que el sistema sea conforme, retirarlo, inutilizarlo o recuperarlo, según proceda, informando de ello a los *distribuidores* y, en su caso, a los *instaladores*, al representante autorizado y al importador⁵³. La conformidad del sistema de IA de alto riesgo con el reglamento también deberá certificarse mediante un procedimiento de evaluación, que el *proveedor* garantizará que se lleve a cabo antes de su comercialización o puesta en servicio. Si el procedimiento de evaluación de la conformidad es satisfactorio, el *proveedor* deberá expedir una declaración de conformidad y colocar el marcado CE⁵⁴. En cualquier caso, *el proveedor* deberá demostrar la conformidad del sistema de AI de alto riesgo con los requisitos del reglamento cuando así se lo solicite una autoridad

⁵⁰ Así, el apartado 6 del art. 3

⁵¹ Así, el apartado 7 del art. 3

⁵² Así, art. 16(a).

⁵³ Así, art. 20.

⁵⁴ Así, el art. 16 (f), (g) y (h), que recuerda, en lo relativo al procedimiento de evaluación de la conformidad, la declaración de conformidad y el marcado. Véanse los arts. 43, 47 y 48.

nacional competente⁵⁵. Además, el proveedor deberá establecer y documentar un sistema de seguimiento poscomercialización que, proporcionado a la naturaleza de las tecnologías y los riesgos que plantea el sistema de IA, le permita evaluar su conformidad continua⁵⁶. Además, el *proveedor* está obligado a establecer un sistema de gestión de la calidad que, mediante políticas, procedimientos e instrucciones por escrito, garantice la conformidad del sistema de IA con el reglamento⁵⁷; a conservar la documentación del sistema

⁵⁵ Así, art. 16(k).

⁵⁶ Así, arts. 17(1)(h) y 72.

⁵⁷ Así, el art. 16(c) y el art. 17 dispone que el sistema de gestión de la calidad estará documentado de manera sistemática e incluirá al menos los siguientes elementos: a) una estrategia para el cumplimiento de la reglamentación, incluido el cumplimiento de los procedimientos de evaluación de la conformidad y los procedimientos para la gestión de los sistemas de IA de alto riesgo; b) las técnicas, los procedimientos y las intervenciones sistemáticas que se utilizarán para el diseño, el control del diseño verificación del diseño del sistema de IA de alto riesgo; c) los procedimientos de evaluación de la conformidad y los procedimientos para la gestión de los sistemas de IA; d) los procedimientos de examen, ensayo y validación que deben llevarse a cabo antes, durante y después del desarrollo del sistema de IA de alto riesgo y la frecuencia con que deben realizarse; e) las especificaciones técnicas, incluidas las normas, que deben aplicarse y, cuando las normas armonizadas pertinentes no se apliquen en su totalidad o no cubran todos los requisitos pertinentes del , los medios que deben utilizarse para garantizar que el sistema de IA de alto riesgo cumple los requisitos del reglamento; f) los sistemas y procedimientos, “lo que incluye su recopilación, análisis, etiquetado, almacenamiento, filtrado, prospección, agregación, conservación y cualquier otra operación relacionada con los datos que se lleve a cabo antes de la introducción en el mercado o puesta en servicio de sistemas de IA de alto riesgo”; g) el sistema de gestión de riesgos; h) el establecimiento, la aplicación y el mantenimiento de un sistema de seguimiento poscomercialización; i) los procedimientos relacionados con la notificación de incidentes graves y fallos de funcionamiento; j) la gestión de la comunicación con las autoridades nacionales competentes, incluidas las autoridades competentes sectoriales, que faciliten o apoyen el acceso a los datos; k) los sistemas y procedimientos para llevar registros; j) la gestión de la comunicación con las autoridades nacionales

de IA; a garantizar que el sistema es conforme con el reglamento del sistema⁵⁸; a conservar los registros generados automáticamente que estén bajo su control⁵⁹; y, antes de comercializar o poner en servicio el sistema de IA de alto riesgo, a registrarlo en la base de datos correspondiente de la Unión Europea, si se trata de un sistema de alto riesgo independiente⁶⁰. El *proveedor* también debe informar inmediatamente a las autoridades nacionales competentes de los Estados miembros en los que haya puesto a disposición el sistema de IA de alto riesgo y, en su caso, al organismo que haya expedido un

competentes, las autoridades competentes, incluidas las autoridades sectoriales, que faciliten o apoyen el acceso a los datos, los organismos notificados, otros operadores, los clientes u otras partes interesadas; k) los sistemas y procedimientos para conservar los registros y toda la información y documentación pertinentes; l) la gestión de los recursos, incluidas las medidas relacionadas con la seguridad del suministro; m) un marco de responsabilidad que defina las responsabilidades de la dirección y del resto del personal con respecto a todos los aspectos enumerados en el reglamento. En virtud de la subsección 2 del art. 17, la aplicación de estos aspectos es proporcional al tamaño de la organización de los proveedores, los cuales, en cualquier caso, deben cumplir el “grado de rigor y el nivel de protección necesarios para garantizar la conformidad de sus sistemas de IA de alto riesgo” con el reglamento.

⁵⁸ Así, el art. 18. Se hace referencia, entre otras cosas, a la documentación técnica mencionada en el art. 11, antes citado, y a la documentación sobre el sistema de gestión de la calidad.

⁵⁹ Así, el art. 19, apartado 1, reza lo siguiente: “Los proveedores de sistemas de inteligencia artificial de alto riesgo conservarán *los registros* [...] generados automáticamente por sus sistemas de inteligencia artificial de alto riesgo, en la medida en que dichos *registros* estén bajo su control. Sin perjuicio del Derecho de la UE o nacional aplicable, los *registros* se conservarán durante un período adecuado a la luz de la finalidad prevista del sistema de IA de alto riesgo, que será de al menos seis meses, salvo que el Derecho de la UE o nacional aplicable exija otra cosa, en particular el Derecho de la UE en materia de protección de datos personales y las obligaciones legales aplicables en virtud del Derecho de la UE o nacional”.

⁶⁰ Así, art. 16(i), art. 49, mientras que la base de datos de la UE se regula en el art. 71.

certificado para el sistema, si tiene conocimiento de que el sistema presenta un riesgo para la salud, la seguridad o la protección de los derechos fundamentales de las personas⁶¹, y a informar de cualquier incidente grave o funcionamiento defectuoso a las autoridades de vigilancia del mercado de los Estados miembros en los que se hayan producido tales incidentes o infracciones⁶².

Antes de comercializar un sistema de IA de alto riesgo, los *importadores* deben asegurarse de que el *proveedor* ha llevado a cabo el correspondiente procedimiento de evaluación de la conformidad y ha elaborado la documentación técnica pertinente. También, deben asegurarse de que el sistema lleva el marcado de conformidad necesario y va acompañado de la declaración de conformidad y las instrucciones de uso requeridas. Además, cuando el *importador* tenga motivos suficientes para creer que un sistema de IA de alto riesgo no cumple el reglamento, está falsificado o va acompañado de documentación falsificada, no deberá comercializarlo hasta que sea conforme y, si el sistema presenta un riesgo para la salud, la seguridad o la protección de los derechos humanos fundamentales, deberá informar de ello al *proveedor* y a las autoridades de vigilancia del mercado⁶³.

Obligaciones similares recaen, en cascada, sobre el *distribuidor*, quien, antes de comercializar un sistema de IA de alto riesgo, no sólo comprueba que el sistema lleva el marcado CE, la documentación técnica y las instrucciones de uso, sino, en general, que el *proveedor* y el *importador* han cumplido las obligaciones del reglamento⁶⁴.

De ello se derivan las obligaciones de los *implantadores* de utilizar los sistemas de IA de alto riesgo de acuerdo con las instrucciones

⁶¹ Así, art. 20(2).

⁶² Así, art. 73.

⁶³ Así, art. 23.

⁶⁴ Así, art. 24.

de uso, de supervisar el funcionamiento del sistema e informar al *proveedor* o *distribuidor*, y a la autoridad de vigilancia del mercado pertinente, y de suspender el uso del sistema si tienen motivos para creer que presenta un riesgo para la salud, la seguridad o la protección de los derechos fundamentales de las personas o si detectan un incidente grave o mal funcionamiento⁶⁵ y, en algunos casos, incluso realizar una evaluación de impacto sobre los derechos fundamentales⁶⁶.

Al término de este breve examen, cabe señalar que, en virtud del artículo 25, cualquier *distribuidor*, *importador*, usuario u otro tercero se considera *proveedor* a efectos del reglamento, y está sujeto a las obligaciones pertinentes: a) si pone su nombre o marca comercial en un sistema de IA de alto riesgo ya comercializado o puesto en servicio, sin perjuicio de los acuerdos contractuales que prevean un reparto diferente de las obligaciones; b) si introduce una modificación sustancial en el sistema de IA de alto riesgo ya comercializado o puesto en servicio, de modo que el sistema siga siendo un sistema de alto riesgo; c) si modifica la finalidad prevista de un sistema de IA, incluso de un sistema de uso general, ya comercializado o puesto en servicio y no clasificado como de alto riesgo, de modo que el sistema se convierta en tal. Cuando se produzcan estos casos, el *proveedor* que inicialmente comercializó o puso en servicio el sistema de IA de alto riesgo dejará de ser considerado como tal a

⁶⁵ Así, art. 26.

⁶⁶ Así, el art. 27. La evaluación se prevé para los implantadores que sean organismos del sector público o entidades privadas que presten servicios públicos y para los implantadores de sistemas de IA de alto riesgo “destinados a utilizarse en la evaluación de la solvencia de las personas físicas o a determinar su solvencia, con excepción de los sistemas de IA utilizados para detectar fraudes” y de los “destinados utilizarse en la evaluación de riesgos y la fijación de precios en relación con las personas físicas en el caso de los seguros de vida y los seguros de enfermedad” [Anexo III, p. 1]. III, [N.º 5(b) y (c)].

efectos del reglamento. También, para los sistemas de IA distintos de los sistemas de alto riesgo, se prevén ciertas obligaciones que se concretan en los requisitos mínimos de transparencia establecidos para determinados sistemas. Se trata, en particular, de los sistemas destinados a interactuar directamente con personas físicas y de los sistemas que generan contenidos sintéticos o *deep fakes*, imágenes o contenidos de audio, o vídeo generados o manipulados por la IA que se asemejan a personas, objetos, lugares u otras entidades o acontecimientos existentes y que podrían parecer falsamente auténticos o verdaderos⁶⁷. En el caso de los sistemas destinados a interactuar directamente con personas, estas deben ser informadas de que están interactuando con un sistema de IA⁶⁸, mientras que, para los sistemas que generan contenidos sintéticos, se espera que los *resultados* relevantes “estén marcados en un formato legible por máquina y detectable como generado artificialmente o manipulado”⁶⁹. De nuevo, para los sistemas que generan falsificaciones profundas, se espera que los usuarios hagan saber que el contenido

⁶⁷ Esta es la definición de *deep fake* del art. 3, apartado 60.

⁶⁸ “Salvo que resulte evidente desde la perspectiva de una persona física razonablemente informada, atenta y perspicaz, teniendo en cuenta circunstancias y el contexto de uso”, establece el art. 50, apartado 1, del reglamento. La disposición establece que la obligación tampoco se aplica “a los sistemas de AI autorizados por la ley para detectar, prevenir, investigar o enjuiciar delitos, sin perjuicio de las salvaguardias adecuadas para los derechos y libertades de terceros, a menos que dichos sistemas estén a disposición del público con el fin de denunciar un delito”.

⁶⁹ Así, el art. 50, apartado 2, según el cual “esta obligación no se aplica si sistemas de IA realizan una función estándar de ayuda a la edición o no alteran sustancialmente los datos de entrada proporcionados por el usuario o su semántica, o si están autorizados por la ley para averiguar, prevenir, investigar o perseguir delitos penales”

ha sido generado artificialmente o manipulado⁷⁰. Por último, las obligaciones de transparencia afectan a los usuarios de sistemas de reconocimiento de emociones, que, en este caso, se suman a las de los sistemas de alto riesgo al estar también incluidos en el Anexo III del reglamento, y a los usuarios de sistemas de categorización biométrica, también clasificados como de alto riesgo cuando la categorización se produce “sobre la base de atributos o características sensibles protegidos basados en la deducción de dichos atributos o características”. Los usuarios de estos sistemas están obligados a informar a las personas expuestas a ellos sobre el funcionamiento del sistema⁷¹.

El enfoque basado en el riesgo también informa la regulación de los modelos de IA de propósito general.

Según el artículo 3, N.º 63 del reglamento, un modelo de IA de propósito general es “un modelo de IA, incluso cuando dicho modelo de IA sea entrenado con grandes cantidades de datos mediante la autosupervisión a gran escala, que se caracteriza por una generalidad significativa y es capaz de realizar de forma competente una amplia gama de tareas distintas, independientemente de las formas en que el modelo se coloca en el mercado, y que puede integrarse en una variedad de sistemas o aplicaciones posteriores, con la excepción

⁷⁰ El apartado 4 del art. 50 extiende también a esta obligación la excepción prevista para los sistemas autorizados por la ley para averiguar, prevenir o investigar delitos. También establece que, si el contenido forma parte de “una obra o programa similar manifiestamente artístico, creativo, satírico o ficticio”, las obligaciones de transparencia se limitan a “la obligación de revelar la existencia del contenido generado o manipulado de forma adecuada, sin obstaculizar la exhibición o disfrute de la obra”.

⁷¹ Así, el art 50, apartado 3, estipula que la citada obligación “no se aplicará a los sistemas de IA utilizados para la categorización biométrica y el reconocimiento de emociones autorizados por la ley para la detección, prevención o investigación de infracciones penales, sin perjuicio de las garantías adecuadas para los derechos y libertades de terceros y de conformidad con el Derecho de la UE”.

de los modelos de IA utilizados para actividades de investigación, desarrollo o creación de prototipos antes de su comercialización”.

En este caso, el enfoque basado en el riesgo da lugar a un régimen diferenciado en función de si el modelo entraña o no un riesgo sistémico, definido como “un riesgo específico para las capacidades de alto impacto de los modelos de IA de propósito general, que tenga un impacto significativo en el mercado de la UE debido a su escala o a sus efectos negativos reales o razonablemente previsibles sobre la salud pública, la seguridad, los derechos fundamentales o la sociedad en su conjunto, que puedan propagarse a gran escala a lo largo de toda la cadena de valor”⁷². Si no existe este riesgo, los *proveedores* de modelos están sujetos a obligaciones como la aplicación de una política de cumplimiento de la legislación de la UE en materia de derechos de autor y la redacción de un resumen suficientemente detallado del contenido utilizado para la formación de modelos⁷³. Cuando, por el contrario, el modelo de propósito general plantea un riesgo sistémico, los *proveedores* están sujetos a obligaciones adicionales, que incluyen evaluar y mitigar los posibles riesgos sistémicos, rastrear, documentar y notificar a la Oficina Europea de IA los incidentes importantes, y garantizar un nivel adecuado de protección de la ciberseguridad del modelo y de su infraestructura física⁷⁴.

⁷² Así, art. 3(65). La clasificación de los modelos de propósito general como modelos con riesgo sistémico tiene lugar de conformidad con los criterios y procedimientos establecidos en los art. 51 y 52. Estos incluyen, en particular, el criterio de alta capacidad de impacto y la debatida presunción de que dicha capacidad corresponde a una cantidad acumulada de cómputo utilizada en el entrenamiento del sistema medida en operaciones de coma flotante (los denominados “FLOPS”) superior a 10.

⁷³ Así, art. 53.

⁷⁴ Así, art. 55.

4. CONCLUSIONES

El Reglamento Europeo sobre Inteligencia Artificial no es el primer caso en el que el legislador europeo construye un modelo basado fundamentalmente en la gestión de riesgos. El caso más reciente e importante es el reglamento europeo 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. Pero, como ya se ha dicho, en este último, el sistema de gestión de riesgos va acompañado del *principio de responsabilidad*, es decir, del principio introducido por ese mismo reglamento, según el cual el responsable del tratamiento debe adoptar las medidas adecuadas para aplicar los principios y disposiciones del reglamento en función de las particularidades del tratamiento y demostrar que ha llevado a cabo esta actividad⁷⁵. Este presupone que el responsable del tratamiento es el más indicado para gestionar y evaluar el riesgo.

En el Reglamento Europeo sobre Inteligencia Artificial, el planteamiento es diferente. Es el legislador quien decide qué sistemas son de alto riesgo y cómo debe tratarse el riesgo que plantean. Teniendo en cuenta que la definición de aplicaciones de inteligencia

⁷⁵ Sobre el principio de responsabilidad, permítanme remitirme a mis contribuciones “Il quadro d’insieme sul regolamento...”, “L’accountability nel Regolamento...” y “Il principio di accountability”, *Giurisprudenza Italiana* no. 12 (2019): 2778-2783. Véase también de Lucchini Guastalla, “Privacy e data protection: principi generali”, *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, ed. Emilio Tosi (Giuffrè, 2019), 58-92 y “Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori”, *Contratto e Impresa* (2018): 106-125; Malgieri, “Art. 5”, en *Codice della privacy e data protection*, eds. D’orazio, Finocchiaro, Pollicino y Resta (Giuffrè, 2021), 89-190; Mantelero, “Responsabilidad y riesgo en el Reglamento 2016/679 de la UE”, *Le nuove leggi civili* no. 1 (2017), 144-164; Resta, “Art. 5” y Siano, “Art. 24”, en *GDPR e normativa privacy. Commentario*, eds. Belisario, Riccio y Scorza (Ipsoa, 2018), 61-63 y 236-245, respectivamente. Véase también el capítulo 4 de este volumen.

artificial es muy amplia, parece crítico que estas se clasifiquen de forma rígida: cualquier desarrollo está obligado a incluirse en el marco definido por el legislador.

El problema radica en el peligro de que las aplicaciones de inteligencia artificial, incluso las futuras, se regulen con la perspectiva del actual presente y que, por tanto, el sistema no sea lo suficientemente dinámico como para seguir la evolución posterior de la inteligencia artificial.

Para gestionar este riesgo, la normativa europea impone una serie de obligaciones a quienes comercializan aplicaciones de inteligencia artificial, como certificaciones, avisos, presentación de documentación y marcado, que también son obligaciones de carácter administrativo. Este planteamiento tiene varios puntos críticos. El primero es la falta de neutralidad, como se ha ilustrado anteriormente. El otro punto crítico es el de prever, frente a una definición muy general de la inteligencia artificial, las mismas obligaciones para todo tipo de empresario, independientemente del tamaño de la empresa y de la criticidad de las actividades. Un modelo de este tipo tiene el gran defecto de tratar todas las aplicaciones de la inteligencia artificial de manera esencialmente homogénea, cuando las aplicaciones de la inteligencia artificial pueden ser muy diferentes entre sí y declinarse de maneras diferentes.

Este error ya se ha cometido en otros contextos, especialmente, en lo que respecta a las normas sobre el tratamiento de datos personales que, de hecho, se han replanteado en tiempos más recientes con el *principio de rendición de cuentas* para permitir modular las medidas que deben tomarse en función de las características específicas del caso.

La normativa europea tiene el mérito de ser un primer modelo organístico en este ámbito. Sin embargo, el modelo, basado en la gestión de riesgos, parece poco estimulante y demasiado costoso desde el punto de vista económico. Por otra parte, la reglamentación

européa corre de nuevo el riesgo de aislar a Europa. Es sin duda crucial en estos temas, así como en el mercado digital proponer y hacer valer un modelo, como ha hecho Europa en tantos otros casos, pero es igualmente importante trabajar en la cooperación internacional, es decir, intentar construir vías de diálogo, de cooperación —incluida la cooperación regulatoria— con otras regiones del mundo, porque construir un modelo aislado significa aislar a Europa. Utilizando una metáfora muy conocida, si construimos fortalezas, debemos recordar también tender puentes que las conecten con otros sistemas.

CAPÍTULO 4

INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS*

1. SOBRE EL MÉTODO

La inteligencia artificial y sus aplicaciones¹ constituyen el tema del momento². Afecta a la vida común bajo diversos perfiles: político, ético, sociológico y, por supuesto, como todo fenómeno social, también bajo el perfil jurídico.

* Este capítulo incorpora, con algunas adaptaciones y actualizaciones, el artículo publicado en *Giurisprudenza Italiana* (2019): 1670 y ss.

¹ En general, sobre el desarrollo actual de la inteligencia artificial y ciertos problemas, consúltense los siguientes informes: Stanford University Human-Centered Artificial Intelligence, *Artificial Intelligence Index Report 2024*; AI Now Institute At New York University, *Landscape. Confronting Tech Power 2023*, *AI Now Report 2019*, *AI Now Report 2018*; CEPS, *Artificial Intelligence....*

² Específicamente sobre el tema de este, véase Van Den Hoven van Genderen, “Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics”, *European Data Protection Law Review* 3, no. 3 (2017): 338 y ss; Kuner, Cate, Lynskey, Millard, Loideain y Svantesson, “Expanding the artificial intelligence-data protection debate”, *International Data Privacy Law* 8, no. 4 (2018): 289 y ss; Pizzetti, *Artificial intelligence...*

Como siempre, el método a adoptar sólo puede consistir en cuantificar el fenómeno de acuerdo con la normativa vigente e identificar las consecuencias de cualquier incumplimiento con el fin de verificar la posible necesidad de una legislación *ad hoc*.

Precisamente por el método, parece oportuno empezar hoy. De hecho, existe una tendencia generalizada, exaltada por los medios de comunicación, a una nueva regulación para cada nuevo fenómeno ilegal. La alarma social, que en muchos casos es absolutamente compartible, produce casi automáticamente la demanda de regulaciones *ad hoc*. Si bien es comprensible la exigencia de una declaración definitiva de la ilicitud del fenómeno con sus posibles consecuencias sancionadoras, la necesidad de dotar de una norma específica a cada nuevo caso parece ser el resultado de una carencia metodológica. Tal razonamiento puede entenderse si es llevado a cabo por no juristas, como resultado de una falta de competencia técnica, pero no puede justificarse si es realizado, en cambio, por juristas.

El jurista, en efecto, no puede limitarse a aplicar la norma al caso concreto que esboza, sino que debe utilizar la principal herramienta a su disposición que es la interpretación. Por lo tanto, no sólo debe aplicar las disposiciones pertinentes, sino también buscar respuestas en el ordenamiento jurídico, considerado en su complejidad. Si la correspondencia entre el caso y la norma fuera inequívoca, no se necesitarían conocimientos jurídicos. Cualquiera podría realizar esta sencilla tarea. Por el contrario, la visión sistemática y el método interpretativo son peculiares del trabajo del jurista, lo cual debería revalorizarse con orgullo.

Lamentablemente, nuestro legislador sucumbe cada vez con mayor frecuencia al clamor mediático y al halago del consenso que se recoge con una respuesta fácil, a través del conocido enfoque de la legislación de emergencia. El último acto en este sentido es

la disposición contenida en el apartado 3 del artículo 8³, Decreto Ley N.º 135, de 14 de diciembre de 2018 (más conocido como “decreto Simplifications”)⁴, que define la tecnología *blockchain* y las aplicaciones de los *contratos inteligentes*⁵.

Desde un punto de vista jurídico, la norma citada es errónea al menos por dos razones. En primer lugar, en el debate internacional, es ya un principio bien asentado el de la neutralidad tecnológica, en virtud del cual la norma jurídica debe ser tecnológicamente neutra

³ Esta disposición no figuraba en el texto original del decreto-ley citado, pero fue introducida por la Ley de Conversión N.º 12, de 11 de febrero de 2019 (en el Boletín Oficial N.º 36, de 12 de febrero de 2019).

⁴ Decreto Ley N.º 135, de 14 de diciembre de 2018, “Disposiciones Urgentes de Apoyo y Simplificación a las Empresas y a la Administración Pública”, publicado en la *Gazzetta Ufficiale della Repubblica Italianade*, 14 de diciembre de 2018, N.º 290.

⁵ “Las ‘tecnologías de libro mayor distribuido’ se definen como tecnologías de la información y protocolos que utilizan un libro mayor compartido, distribuido, replicable, accesible simultáneamente, descentralizado desde el punto de vista arquitectónico y basado en la criptografía, que permite el registro, la validación, la actualización y el almacenamiento tanto de datos no cifrados como de otros protegidos criptográficamente, no cifrados, inalterables. 2. Se define como ‘contrato inteligente’ un programa informático que funciona con tecnologías basadas en libros contables distribuidos y cuya ejecución vincula automáticamente a dos o más partes sobre la base de efectos predefinidos por ellas. Los contratos inteligentes cumplen el requisito de constar por escrito previa identificación informática de las partes interesadas, a través de un proceso que cuente con los requisitos establecidos por la Agencia para la Italia Digital mediante directrices que se adoptarán en el plazo de noventa días desde la entrada en vigor de la ley de conversión del presente decreto. 3. El almacenamiento de un documento electrónico mediante el uso de tecnologías basadas en registros distribuidos produce los efectos del sellado de tiempo electrónico a que se refiere el artículo 41 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014. En el plazo de noventa días desde la entrada en vigor de la ley de conversión del presente decreto, la Agencia Italia Digital identificará las normas técnicas que deben poseer las tecnologías basadas en registros distribuidos para producir los efectos a que se refiere el apartado 3”.

y, por tanto, no referirse a una tecnología concreta establecida en un momento histórico determinado. Las ventajas de la neutralidad tecnológica son evidentes: el derecho no condiciona el mercado, de forma que favorece tal o cual tecnología, no condiciona el desarrollo de la tecnología y no tiene por qué perseguirlo. El enfoque del derecho, en la neutralidad tecnológica, es “funcional”. No se centra en el “qué”, sino en el “cómo”. Legislar de este modo puede ser más difícil, porque no se regula el objeto, sino la función. Este principio fue afirmado, por ejemplo, por la CNUDMI en su reglamento sobre la firma electrónica, que se basa precisamente en los principios de “neutralidad tecnológica” y “equivalencia funcional”. De este modo, se establecen principios generales que pueden permanecer inalterados durante un cierto tiempo sin verse obligados por la evolución de las tecnologías⁶.

La norma italiana, por su parte, trata de describir la tecnología *blockchain* y las aplicaciones de los *contratos inteligentes* cristalizándolas.

Además, realiza otra operación innecesaria y, de hecho, perjudicial. Atribuye a los *contratos inteligentes*, después de haberlos definido inútilmente, según ese proceso contrario al principio de neutralidad tecnológica ilustrado anteriormente, la forma escrita, sólo si las partes se identifican según un proceso que será regulado por AgID⁷. Ahora bien, la identificación de las partes, según los principios generales, no es un requisito del contrato. Además, la forma escrita del documento informático es una cuestión ya ampliamente regulada por el Código de la Administración Digital⁸, que ciertamente no requiere mayor especificación.

⁶ Sobre este tema véase mi artículo, “Riflessioni su diritto e tecnica”, *Diritto dell'informazione e dell'informatica* 28, no. 4-5 (2012): 831 y ss.

⁷ En el momento de redactar este documento, las directrices siguen pendientes.

⁸ Decreto Legislativo N.º 82, de 7 de marzo de 2005, modificado y completado posteriormente por el Decreto Legislativo N.º 179, de 22 de agosto de 2016, y luego por el Decreto Legislativo N.º 217, de 13 de diciembre de 2017.

El tema que ocupa, inteligencia artificial y privacidad, debe enmarcarse por tanto en el contexto actual del desorden intelectual, y el objetivo que se perseguirá será racionalizar los requisitos y las respuestas normativas.

2. LA INTELIGENCIA ARTIFICIAL Y EL PLANTEAMIENTO DEL LEGISLADOR EUROPEO

La inteligencia artificial es ya una herramienta muy extendida, aunque todavía susceptible de gran expansión. Es, por tanto, una realidad y no una eventualidad futura. “La inteligencia artificial no es ciencia ficción: ya forma parte de nuestras vidas”⁹. Las aplicaciones de la inteligencia artificial son muchas, y algunos ejemplos son el procesamiento del lenguaje natural, el reconocimiento del habla, el agente virtual, el aprendizaje automático, el *hardware* optimizado para IA, la gestión de decisiones, el aprendizaje profundo, la biometría, la automatización de procesos robóticos y el análisis de textos¹⁰.

⁹ Esto es lo que dice la Comisión Europea en su *Comunicación al Parlamento, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Inteligencia Artificial para Europa*, COM (2018) 237 final, 25 de abril de 2018, 1.

¹⁰ Para una mayor discusión, véase mi contribución “Il contratto nell’era dell’intelligenza artificiale”, *Rivista Trimestrale di Diritto e Procedura Civile* 72 (2018): 441-460. Véase, además, algunos actos de fuente europea relevantes para la inteligencia artificial: Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión en relación con las normas de Derecho civil sobre robótica, 2015/2103(INL); Comunicación de la Comisión, *Plan de coordinación para la IA*, y anexo, *Plan coordinado para desarrollo y el uso de la inteligencia artificial “made in Europe”*, COM(2018) 795, de 7 de diciembre de 2018; Consejo de la Unión Europea, *Conclusiones de 11 de febrero de 2019 sobre el “Plan Coordinado sobre Inteligencia Artificial”*; Resolución del Parlamento Europeo, de 12 de febrero de 2019, relativa a una política industrial europea global sobre robótica e inteligencia artificial, 2018/2088 (INI).

La inteligencia artificial se basa en los datos. Una de las razones por las que, aunque ya se había estudiado ampliamente hace muchos años¹¹ y aunque ya estaba madura en muchos aspectos, aún no era una tecnología aplicable era la falta de una gran cantidad de datos disponibles.

Hoy en día, los datos están disponibles y a menudo son proporcionados por los propios usuarios, especialmente a través de las redes sociales y los motores de búsqueda. Facebook, Instagram y Google nos vienen inmediatamente a la cabeza, pero una cantidad aún mayor de datos está disponible en los grandes actores chinos de la web, como Ali Baba y Baidu, que nos parecen lejanos debido a la barrera lingüística que naturalmente nos separa.

Se calcula que hay miles de millones de usuarios que proporcionan datos a diario, de forma más o menos consciente, en todo el mundo¹².

¹¹ Como ya se ha señalado en este volumen, el nacimiento de la inteligencia artificial se remonta a la Conferencia de Dartmouth (Hannover, New Hampshire) de 1956. Véase el texto de la propuesta con la que los organizadores de la conferencia (así como los “padres fundadores” de esta tecnología) abordaron los principales temas del campo de investigación, incluidas las redes neuronales, la teoría computacional, la creatividad y el procesamiento y reconocimiento del lenguaje natural: McCarthy, Minsky, Rochester y Shannon, “A Proposal for the Dartmouth Summer Research Project...”, disponible en <https://aaai.org/ojs/index.php/aimagazine/article/view/1904/1802> (consultado el 20 de junio de 2024).

¹² Según *el Global Digital Report 2024* de We Are Social y Meltwater (conocidas agencias de gestión de redes sociales), hay 5350 millones de usuarios se conectarán a Internet en 2024, un aumento de 97 millones (1,8 %) en comparación con enero de 2018; 5000 millones de usuarios utilizarán los medios sociales, con un aumento total mundial de 266 millones (5,6 %) en comparación con el año pasado (el informe completo está disponible en <https://wearesocial.com/it/blog/2024/02/digital-2024-i-dati-glo-bali-5-billion-users-on-social-media/>, consultado el 19 de junio de 2024). También es interesante la visión ofrecida por Lori Lewis y Chadd Callahan, de *Cumulus Media*, sobre las actividades en

La IA se alimenta de datos¹³ y ahora los datos están ciertamente disponibles, a menudo incluso de forma gratuita. El nuevo petróleo, según la famosa metáfora de *The Economist*¹⁴, constituye el recurso de la nueva economía digital¹⁵. Está claro que el terreno de juego es, como mínimo, continental: Estados Unidos y China tienen los mayores mercados y las tecnologías más avanzadas y, por tanto, desempeñan el papel más importante. Europa pretende ser el tercer actor y consolidar el mercado digital europeo, pero el Estado individual no puede desempeñar ningún papel. La situación política, económica y, por lo tanto, legales son necesariamente europeos.

Los datos personales son, a la vez, el recurso en el que se basa la economía digital y el objeto del derecho a la protección de los

diversas plataformas web en el intervalo de un minuto en 2018. Por ejemplo, se constató que cada 60 segundos realizaron 3,7 millones de búsquedas en Google; 973 000 impactos en Facebook; 481 000 publicaciones en Twitter; 187 millones de correos electrónicos enviados; 38 millones de mensajes enviados a través del servicio de chat de WhatsApp; 4,3 millones de vídeos vistos en YouTube (este análisis, en forma de infografía, fue retomado por varios periódicos, entre ellos *Il Sole24Ore*, y está disponible en <https://www.infodata.ilssole24ore.com/2018/05/17/cosa-accade-inter-net-un-minute/>). Más reciente es “Data Never Sleeps 11.0”, la infografía de Domo, empresa especializada en soluciones de análisis de datos, según la cual en 2023 se realizaron cada minuto 6,3 millones de búsquedas en Google y 6944 solicitudes a ChatGPT, mientras que 4 millones de personas publicaron contenidos en Facebook.

¹³ Véase Mantelero, *Informe sobre inteligencia artificial. Inteligencia Artificial y Protección de Datos: Retos y posibles soluciones*, Comisión Consultiva del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, 25 de enero de 2019.

¹⁴ The Economist, “The world’s most valuable resource is no longer oil, but data”, *The Economist*, publicado el 6 de mayo de 2017.

¹⁵ Véase Ricciuto, “La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno”, *Diritto dell’informazione e dell’informatica* (2018): 689-726.

datos personales, reconocido por el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

La actuación de la Unión Europea tiene por objeto impulsar un nuevo mercado, el mercado único digital europeo. A ello contribuyen el Reglamento (UE) 2016/679, 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”¹⁶ (en lo sucesivo, “el

¹⁶ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), publicado en DOUE. L 119/1, de 4 de mayo de 2016. En general, sobre el reglamento, véase Alpa, “L’identità digitale e la tutela della persona. Spunti di riflessione”, *Contratto e Impresa* (2017): 723-733; Bassini, “La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali”, *Quaderni costituzionali* 36, no. 3 (2016): 587-590; Busia, Liguori y Pollicino eds., *Le nuove frontiere della privacy nelle tecnologie digitali* (Aracne, 2016); Califano, “Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali”, en *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, eds. Califano y Colapietro (Editoriale Scientific, 2017); Califano, *Privacidad: afirmación y práctica de un derecho fundamental* (Collana Crispel, 2016); Cuffaro, “El derecho europeo a la protección de datos personales”, *Contratto e Impresa* (2018): 1098-1119; D’orazio, Finocchiaro, Pollicino y Resta, *Codice della privacy...*; Finocchiaro, “Introduzione al Regolamento Europeo sulla protezione dei dati”, *Le Nuove Leggi Civili Commentate* no. 1 (2017): 1-18; Finocchiaro ed., *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (Zanichelli, 2017); Piraino, “Il regolamento generale sulla protezione dei dati personali e i diritti dell’interessato”, *Le Nuove Leggi Civili Commentate* 40, no. 2 (2017): 369-409; Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679* (Giappichelli, 2016); Riccio, Scorza y Belisario, *GDPR e normativa privacy...*; Sica, D’Antonio y Riccio eds., *La nuova disciplina europea della privacy* (CEDAM, 2016); Stanzione, “Il Regolamento europeo sulla privacy: origini e ambito di applicazione”, *Europa e diritto privato* no. 4 (2016): 1249-1264.

reglamento” para abreviar), y el Reglamento (UE) 2014/910 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, “relativo a la identificación electrónica y los servicios de confianza para 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”¹⁷.

Los dos reglamentos, considerados en una perspectiva unitaria, indican claramente la intención del legislador europeo de diseñar un mercado digital único eliminando los obstáculos jurídicos constituidos por la falta de uniformidad de las normas aplicables. Se trata, y es ciertamente superfluo insistir en este punto, de reglamentos y no de directivas: por tanto, directamente aplicables y destinados a establecer un sistema jurídico de referencia uniforme y homogéneo.

A ello se añade la voluntad del legislador europeo de consolidar la posición europea en el marco mundial afirmando un enfoque unificado, que declina los principios fundamentales establecidos en la Carta de los Derechos Fundamentales de la Unión Europea.

Al igual que muchos otros actos legislativos europeos en este ámbito, su objetivo es reforzar la confianza en las transacciones electrónicas en el mercado interior, de forma que se garantice la protección de los datos personales y aumente así la eficacia de los servicios en línea públicos y privados en la Unión Europea. Desde

¹⁷ Publicado en el DOUE. L 257 de 28 de agosto de 2014. El reglamento se conoce comúnmente como “eIDAS”, donde “e” significa “electrónico”, “ID” significa “identificación”, “A” significa “autenticación” y “S” significa “firma”. Para un comentario, véase mi “Una prima lettura del reg. UE 910/2014 (c.d. eIDAS): identificazione on line, firme elettroniche e servizi fiduciari” *Le Nuove Leggi Civili Commentate* 3 (2015): 419 y ss, así como el volumen que edité con Delfini, *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno: commentario al Regolamento UE n. 910/2014* (Giappichelli, 2017). Como ya se ha señalado en este volumen, el reglamento ha sido modificado recientemente por el Reglamento (UE) 2024/1183. Véase, sobre este punto, lo que sigue en el capítulo 5.

los primeros estudios de la Comisión Europea sobre el comercio electrónico en los años 90¹⁸, el objetivo ha sido reforzar la confianza, en primer lugar, del consumidor, para favorecer el desarrollo del mercado.

3. MERCADO DIGITAL Y PROTECCIÓN DE DATOS

Así, el legislador europeo se mueve entre dos exigencias diferentes: la de favorecer el desarrollo del mercado digital europeo, cuyo activo de intercambio es la información y los datos personales, y la de proteger al individuo en sus derechos fundamentales.

De esta doble necesidad, surge el Reglamento Europeo 2016/679, que ya desde su título deja clara su doble finalidad: la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de datos.

¹⁸ Véase la Comunicación de la Comisión de las Comunidades Europeas al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, *Iniciativa europea de comercio electrónico*, COM(97) 157, 15 de abril de 1997, donde la creación de confianza es uno de los primeros objetivos en el desarrollo del comercio electrónico: “Para que el comercio electrónico se desarrolle, los consumidores y las empresas deben tener la certeza de que sus transacciones no son interceptadas ni alteradas, de que el vendedor y comprador están realmente en condiciones de efectuar una compra, y de que el comprador y el vendedor no realmente quienes dicen ser y que los mecanismos para realizar transacciones legales y seguras son accesibles. La creación de esta confianza es el requisito previo para que las empresas y los consumidores adopten el comercio electrónico” (p. 22). Del mismo modo, en la Comunicación de la Comisión de las Comunidades Europeas al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, *Garantizar la seguridad y la confianza en las comunicaciones electrónicas. Hacia la definición de un marco europeo para la firma digital y el cifrado*, COM(97) 503, 8 de octubre de 1997, se afirma que “la presente comunicación tiene por objeto desarrollar dicho marco político con vistas a [...] estimular y permitir a los usuarios de todos los sectores económicos beneficiarse de las oportunidades de la sociedad global de la información, que sólo pueden aprovecharse plenamente si se basan en un marco de confianza y seguridad”, 2.

En esta tensión, se desarrolla la disciplina dictada por el reglamento europeo, que gira en torno al principio de la necesaria ponderación de derechos e intereses.

En los numerosos actos de las instituciones europeas relativos a la inteligencia artificial se puede leer este equilibrio. De hecho, el intercambio y disponibilidad de datos se cuentan entre las acciones estratégicas para promover el desarrollo de sistemas de inteligencia artificial, siempre que estos objetivos se persigan respetando los derechos de las personas y los valores europeos. El citado COM(2018) 795 de la Comisión Europea hizo hincapié en la necesidad de hacer realidad un “espacio europeo de datos”¹⁹, afirmando expresamente que “para la IA siga desarrollándose, se necesita un ecosistema de datos viable basado en la confianza, la disponibilidad de datos y la infraestructura” y que el acceso a los datos “es un elemento clave de un panorama competitivo de la IA”²⁰. Se especificaba, no obstante, que la Unión Europea debería facilitar dicho acceso a los datos “respetando plenamente las normas sobre protección de datos”. Conceptos similares se expresaban también en el anexo de la citada Comunicación: “La actual difusión de la IA se ve impulsada por la disponibilidad de grandes conjuntos de datos, combinada potencia de cálculo y una conectividad cada vez mayores. Poner datos seguros, sólidos y de calidad a disposición de una amplia gama de usuarios a través de las fronteras es una de las piedras angulares de la política europea. Se seguirá garantizando la apertura a los flujos internacionales de datos, respetando plenamente la legislación de la UE para la protección de los datos personales”²¹. Finalmente, en

¹⁹ La expresión ya figuraba en la anterior Comunicación de la Comisión Europea, *Inteligencia artificial europa*, COM(2018) 237, 25 de abril de 2018, 11.

²⁰ Comisión Europea, *Inteligencia artificial...*, 6 y 7.

²¹ Véase el anexo de la Comunicación de la Comisión Europea, *Plan coordinado para el desarrollo y el uso de la inteligencia artificial “Made in Europe”*, COM(2018)

este, la citada Resolución del Parlamento Europeo de 12 de febrero de 2019 reconocía, por un lado, que el desarrollo de productos y servicios basados en la inteligencia artificial requiere libre circulación de datos y la accesibilidad a los mismos dentro de la Unión Europea, y que debe garantizarse un alto nivel de seguridad, protección y confidencialidad de los datos utilizados para la comunicación entre las personas, los robots y la inteligencia artificial, invitando “a la Comisión a velar por que todo futuro marco reglamentario de la UE sobre inteligencia artificial garantice la privacidad y confidencialidad de las comunicaciones, la protección de los datos personales, incluidos los principios de legalidad, equidad y transparencia, la protección de datos desde el diseño y por defecto, la limitación de la finalidad, la conservación, la exactitud y la minimización de datos, en pleno cumplimiento de la legislación de la UE sobre protección de datos”²².

Un intento de resolver la tensión entre la necesidad de utilizar datos para el desarrollo de nuevas actividades y la protección de las personas en lo que respecta a sus datos personales consiste en formular un nuevo enfoque del problema, basado en la ética²³. La citada Comunicación de la Comisión Europea de 25 de abril de

795 final, 14. Como ya se ha destacado en este volumen, el objetivo de la valorización de los datos ha sido perseguido por el legislador europeo con iniciativas legislativas como el Reglamento de datos, la Ley de datos, la Ley de gobernanza de datos y el reglamento sobre el espacio europeo de datos sanitarios. Véanse los capítulos 1 y 3 sobre este punto.

²² Véase la Resolución del Parlamento Europeo, de 12 de febrero de 2019, sobre una política industrial europea global sobre robótica e inteligencia artificial, apartados P, 125 y 128.

²³ Un ejemplo lo ofrece La Carta Ética Europea sobre el Uso la Inteligencia en los Sistemas de Justicia y Áreas Relacionadas, adoptada por la Comisión Europea para la Eficiencia de la Justicia (órgano del Consejo Europa) los días 3 y 4 de diciembre de 2018. Se trata del primer documento en el que se expresan determinados principios éticos a los que debe subordinarse desarrollo y la adopción de sistemas de inteligencia artificial. Estos principios incluyen, en particular, el respeto de los

2018 destacó la necesidad de promover iniciativas de inteligencia artificial respetando un “marco ético basado en los valores de la Unión y coherente con la Carta de los Derechos Fundamentales de la Unión Europea”. En particular, como parte de la estrategia europea destinada a hacer que Europa sea competitiva en términos de desarrollo y adopción de sistemas de inteligencia artificial, debía elaborarse un “proyecto de directrices éticas para la inteligencia artificial” en cooperación con el Grupo Europeo de Ética en Ciencia y Nuevas Tecnologías²⁴.

4. LOS PRINCIPIOS FUNDAMENTALES

Ahora, parece útil revisar los principios básicos de la normativa europea para ver qué cuestiones críticas de interpretación existen, si las hay, en relación con las aplicaciones de la inteligencia artificial.

4.1. Datos personales y anónimos

Partiendo de la definición de datos personales²⁵, puede verse que la mayor parte de la información son datos personales.

Por el contrario, es muy difícil identificar información que no sean datos personales. Aunque el objeto del derecho a la protección

derechos humanos fundamentales, la no discriminación y el control de los usuarios sobre los datos. Sobre este punto, véase el capítulo 8 de este volumen.

²⁴ “El proyecto abordará cuestiones como el futuro del trabajo, la equidad, la seguridad, la inclusión social y la transparencia de los algoritmos. En términos más generales, examinará el impacto sobre los derechos fundamentales, como la privacidad, la dignidad, la protección de los consumidores y la no discriminación [...]. Se invitará a empresas, instituciones académicas y otras organizaciones de la sociedad civil a contribuir. Paralelamente, la Comisión proseguirá su labor de promoción de la ética escala”, 16.

²⁵ Según el artículo 4, apartado 1, del reglamento, por datos personales se entiende “cualquier información sobre una persona física identificada o identificable (‘interesado’)”.

de datos personales es la información o los datos, datos e información no son el mismo término. Más concretamente, los datos son la fuente de información, en la que está contenida la información, y de datos individuales o del conjunto datos puede extraerse o inferirse la información. Pero la información, en sentido estricto, no coincide con los datos en sí. La información es el tratamiento de los datos.

Los datos anónimos son únicamente aquellos que, originariamente o como resultado de su tratamiento, no pueden vincularse a una persona física. En la sociedad de la información, en la que la recolección de datos o la catalogación de información, estableciendo conexiones que no pueden ser previstas por los interesados, convertido en una actividad cada vez más extendida, la clasificación de los datos anónimos adquiere una importancia creciente. El elemento clave, que marca la distinción entre datos personales y datos anónimos, es la enlazabilidad. La vinculabilidad depende de numerosos factores: el sujeto que establece el vínculo, el contexto en el que actúa y el dominio de conocimientos de que dispone. Por tanto, el anonimato es relativo: se configura en relación a determinados sujetos o circunstancias específicas, caso por caso²⁶.

²⁶ Se hace referencia al volumen que he editado, *Diritto all'anonimato. Anonimato, nome, identità personale*, en *Trattato di diritto commerciale e di diritto pubblico dell'economia*, dir. Giusella Finocchiaro (CEM, 2008). También conviene recordar la orientación expresada recientemente por el Tribunal de Justicia en el asunto T-557/20. El Tribunal de Primera Instancia de las Comunidades Europeas hizo hincapié en la necesidad de que la evaluación de la reidentificabilidad se lleve a cabo con referencia a la parte concreta que trata los datos, verificando si la posibilidad de que esa parte combine la información de que dispone con información adicional en posesión de un tercero constituye un medio que puede aplicarse razonablemente para identificar a los interesados. En efecto, no es condición suficiente para considerar que un dato no es anónimo que la información para la reidentificación esté a disposición del tercero. La sentencia, de 26 de abril de 2023, está disponible en <https://curia.europa.eu/juris/document/>

La definición de datos anónimos no figura en el reglamento europeo, sino en el Considerando N.º 26²⁷, mientras que, en el Decreto Legislativo N.º 196 de 30 de junio de 2003, la definición figuraba en el artículo 4, apartado 1, letra n)²⁸, posteriormente derogado por el Decreto Legislativo N.º 101, de 10 de agosto de 2018, que contiene las disposiciones para adaptación del sistema nacional al Reglamento (UE) N.º 2016/679²⁹. Por otra parte, la

document.js?text=&docid=272910&pageIndex=0&doclang=EN&- mode=ls-t&dir=&occ=first&part=1&cid=6608299 (consultado el 18 de junio de 2024). Posteriormente, el asunto también fue tratado por el Tribunal de Justicia, que, en su decisión de 7 de marzo de 2024 en el asunto C-604/22, sostuvo que un dato no podía considerarse anónimo si la reidentificación del interesado por la parte que lo trata podía hacerse solicitando la información necesaria a la parte contractualmente obligada a revelar la información. La decisión está disponible en CURIA - Documentos (europa.eu) (consultado el 22 de junio de 2024).

²⁷ El considerando 26 del reglamento establece lo siguiente: “Por consiguiente, los principios de la protección de datos no deben aplicarse a la información anónima, es decir, a la información que no se refiere a una persona física identificada o identificable, o a los datos personales convertidos en suficientemente anónimos para que el interesado no pueda o no deba ser identificado”. Hay que tener en cuenta que la definición de datos anónimos ni siquiera estaba presente en la antigua Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que fue derogada por el citado reglamento a partir del 25 de mayo de 2018.

²⁸ La definición de datos anónimos era la siguiente: “Datos que, en su origen o como resultado de su tratamiento, no pueden asociarse a un interesado identificado o identificable”.

²⁹ Decreto Legislativo N.º 101, de 10 de agosto de 2018: “Disposiciones para adaptación de la legislación nacional a las disposiciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)”, publicado en G.U. Serie General N.º 205, de 4 de septiembre de 2018.

definición de seudonimización³⁰, contenida en el reglamento europeo, no es relevante para identificar los principios fundamentales de la Ley Europea de Protección de Datos que se encuentra en la base del tratamiento. La seudonimización es una medida de seguridad, pero no afecta a la base jurídica del tratamiento.

Así, si las aplicaciones de inteligencia artificial utilizan datos no anónimos, se aplica el reglamento.

Si utilizan datos anónimos, el reglamento no se aplica, pero hay que recordar que la calificación de datos anónimos es dinámica y está sujeta a la verificación continua, derivada de la evolución de las tecnologías: depende en gran medida de los recursos, especialmente tecnológicos, disponibles.

4.2. Calidad de los datos

La IA se alimenta principalmente de grandes bases de datos. Por lo tanto, la calidad de los datos resulta esencial³¹. Unos datos cualitativamente incorrectos sólo pueden conducir a un tratamiento, según el conocido principio de “basura entrante, basura saliente”. La calidad de los datos es un principio consagrado en el reglamento³² y ya presente en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos per-

³⁰ Según el artículo 4, apartado 5, del reglamento, se entenderá por seudonimización “el tratamiento de datos personales de tal manera que datos personales ya no puedan atribuirse a un interesado concreto sin utilizar información suplementaria, siempre que dicha información suplementaria se conserve por separado y esté sujeta a medidas técnicas y organizativas que garanticen que los datos personales no se atribuyen a una persona física identificada o identificable”.

³¹ Cabe recordar que, como se explica en el capítulo 3, la calidad de los datos es uno de los requisitos de la Ley de IA para los sistemas de IA de alto riesgo.

³² Véase el artículo 5 del reglamento.

sonales y a la libre circulación de estos datos³³. Sobre la base de este principio, el responsable del tratamiento está obligado a garantizar que los datos tratados sean “adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se traten; exactos y, en caso necesario, actualizados”, y que “se tomen todas las medidas razonables para suprimir o rectificar a su debido tiempo los datos que sean inexactos en relación con los fines para los que se traten” y “se conserven en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que se traten”³⁴.

Surge un claro contraste, por una parte, entre la necesidad de disponer de una enorme cantidad de datos para desarrollar sistemas de inteligencia artificial y, por otra parte, la necesidad de respetar el principio de minimización establecido por el reglamento, según el cual el tratamiento sólo debe referirse a los datos estrictamente necesarios y pertinentes para los fines perseguidos. No obstante, esta tensión exige una ponderación de intereses, en la que se oponen el derecho a la protección de los datos personales y la necesidad de disponer de datos personales para desarrollar aplicaciones de inteligencia artificial.

³³ La directiva dedicó toda la sección VI a este principio, titulándola “Principios de calidad de los datos”.

³⁴ El marco de los principios aplicables al tratamiento se completa con los principios de licitud, lealtad y transparencia, según los cuales los datos deben tratarse de forma lícita, correcta y transparente respecto al interesado [art. 5(1)(letra a)]; de limitación de la finalidad, según el cual los datos deben recogerse para fines específicos, fines explícitos y legítimos, y posteriormente tratados de manera que no sea incompatible con dichos fines [art. 5(1)(letra b)]; integridad y confidencialidad, según las cuales los datos deben tratarse de manera que se garantice una seguridad adecuada mediante medidas técnicas y organizativas apropiadas [art. 5(1)(letra f)].

Se ha planteado la cuestión³⁵ de si el responsable del tratamiento puede ser la propia aplicación de inteligencia artificial o, si se prefiere, el robot. La definición de responsable del tratamiento³⁶ contenida en el reglamento indica claramente que el responsable del tratamiento debe ser una persona física o jurídica. Si la aplicación no tiene subjetividad jurídica, obviamente, no puede ser titular. Sin embargo, la atribución de subjetividad jurídica debe corresponder a una elección metodológica precisa y consciente y ser la base de un nuevo enfoque de la cuestión de la responsabilidad. Si no se atribuye a la aplicación una disponibilidad económica y si no se rediseña un régimen de responsabilidad para prescindir de elementos subjetivos, claramente no referibles a la aplicación, la atribución de subjetividad jurídica a las aplicaciones de inteligencia artificial y a los robots se convierte en un acto de complacencia romántica, un fin en sí mismo, cuando no perjudicial. El mismo argumento puede esgrimirse para la designación del robot como controlador³⁷. También en este caso la designación de la persona responsable requiere la subjetividad jurídica de esa persona, una subjetividad que, sin embargo, no puede ser un fin en sí misma, sino que debe formar parte de un nuevo modelo de responsabilidad.

4.3. Decisiones automatizadas y derecho de explicación

Se sobrevalora enormemente lo que el reglamento prevé en relación con las decisiones automatizadas.

³⁵ Véase Pizzetti, *Artificial intelligence*....

³⁶ El responsable del tratamiento es “la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o conjuntamente con otros, determine los fines y los medios del tratamiento de datos personales” (art. 4, apartado 7, del reglamento).

³⁷ Según el art. 4, apartado 8, del reglamento, el responsable del tratamiento es “persona física o jurídica, autoridad pública, agencia u otro organismo que trate datos personales por cuenta del responsable del tratamiento”.

El artículo 22 del reglamento establece que “el interesado tendrá derecho a no ser objeto de una decisión que se base únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, y que produzca efectos jurídicos en él o le afecte significativamente de modo similar” (apartado 1).

La norma no prohíbe las decisiones automatizadas, sino la toma de decisiones exclusivamente por sistemas automatizados³⁸.

Como ocurrió con el derecho al olvido, aunque en este caso en un círculo más restringido de comentaristas, se ha extendido una convicción errónea, tenida por cierta por la mayoría. En el caso del derecho al olvido, de hecho, la creencia y la expectativa social es que se trata de un derecho *ad nutum*, ejercitable por el interesado en cualquier circunstancia.

³⁸ Como se pone de relieve en Pellecchia, “Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell’algoritmo nella cornice della responsible research and innovation”, *Le nuove leggi civili commentate* 48, no. 5 (2018): 1224-1225, ha surgido un debate en torno al uso del adverbio “únicamente” utilizado para delimitar el ámbito del tratamiento prohibido por el reglamento. En efecto, la doctrina se encuentra dividida entre quienes ven un déficit en la protección de los interesados, argumentando que el uso de este adverbio llevaría a excluir de la prohibición todas aquellas decisiones en las que la intervención humana, aunque sea mínima, sea detectable; y quienes, por el contrario, consideran —a efectos de esta exención— que la intervención humana debe ser significativa. Parece que esta última es la postura compartida por el Consejo Europeo de Protección de Datos, que en sus *Directrices sobre la toma de decisiones individuales automatizadas y la elaboración de perfiles a efectos del Reglamento 2016/679* (aprobadas por última vez el 6 de febrero de 2018), excluye que el responsable del tratamiento pueda eludir la prohibición examinada “fabricando la intervención humana” (p. 21). Véanse, en sentido contrario, Wachter, Mittelstadt y Floridi, “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation”, *International Data Privacy Law* (2017): 76-99, y Malignieri y Comandé, “Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation”, *International Data Privacy Law* 7, no. 3 (2017): 243-265.

En el caso de las decisiones automatizadas, la creencia general es que el reglamento introduce una prohibición general. Esto, como en el caso del derecho al olvido, se basa en una lectura de la norma contenida en las versiones anteriores del reglamento³⁹ que no fueron aprobadas. La comunicación que tuvo lugar sobre las normas que aún estaban en proyecto generó la creencia de que el reglamento, entonces formulado de forma diferente, contiene disposiciones que no se aprobaron en su redacción original, sino que fueron objeto de estrechas negociaciones.

Del mismo modo, no existe un derecho pleno a una explicación en el artículo 15 del reglamento.

De hecho, no se trata de un derecho a una explicación, sino de un derecho a la información en el sentido del artículo 15, apartado 1, letra h, que limita el derecho del interesado a acceder a la información relativa a “la existencia de un proceso de toma de decisiones automatizado, incluida la elaboración de perfiles a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, [a obtener] información significativa sobre la lógica utilizada, así

³⁹ El Parlamento Europeo había modificado, en primera lectura, el texto del reglamento propuesto por la Comisión Europea, disponiendo en su artículo 20 (“Medidas basadas en la elaboración de perfiles”), que la elaboración de perfiles aptos para producir efectos jurídicos en la persona interesada o para afectar a sus intereses, derechos y libertades no podía basarse “exclusiva o predominantemente” en un tratamiento automatizado, sino que debía incluir obligatoriamente “una evaluación humana, incluida una explicación de la decisión adoptada tras dicha evaluación” (5º párrafo). Por lo tanto, está claro que, en la versión no definitiva del reglamento, no sólo se prohibía la decisión basada únicamente en el tratamiento automatizado (como se ve hoy en día), sino también aquella decisión en la que la intervención humana fuera menor que el uso de sistemas automatizados. Además, se concedía al interesado el “derecho a obtener una evaluación y una explicación humanas de la decisión”, derecho que —en el texto del reglamento entonces aprobado y hoy vigente— se limitaba al “derecho a obtener la intervención humana” (art. 22.4) y al derecho a acceder a “información significativa sobre la lógica utilizada” en la toma de decisiones automatizada (art. 15.1.h).

como sobre la importancia de dicho tratamiento para el interesado y las consecuencias previstas del mismo”.

Aquí puede leerse una falta de armonía entre el Considerando 71 y la disposición antes mencionada, ya que el primero prevé “el derecho a obtener la intervención de una persona, a expresar su opinión, a obtener una explicación de la decisión adoptada tras dicha evaluación y a impugnar la decisión”⁴⁰.

4.4. Finalidad del tratamiento

Otra cuestión relevante es la de la finalidad del tratamiento. Como es bien sabido, la legitimidad del tratamiento se mide no solo con respecto a los datos que se tratan, sino también con respecto a la finalidad del tratamiento de esos datos.

Ahora bien, aunque los datos que deben tratarse estén identificados, la finalidad del tratamiento puede no estarlo en el caso de los datos inferidos o, según una expresión más correcta, de la información inferida de los datos⁴¹. En este caso, la finalidad del

⁴⁰ El considerando parece tener eco en la Ley de IA y, en particular, en las disposiciones sobre la supervisión humana de los sistemas de alto riesgo (art. 14) y las que establecen el “derecho a presentar una reclamación ante una autoridad de vigilancia del mercado” y el “derecho a una explicación de los procesos individuales de toma de decisiones” (sección 4 “Recursos”, arts. 85 y 86).

⁴¹ El Consejo de Europa abordó esta cuestión en su Declaración de 13 de febrero de 2019 titulada *Declaración del Comité de Ministros sobre la capacidad de manipulación de los procesos algorítmicos*, en la que destacó la capacidad de los datos “derivados” para influir no solo en el comportamiento, sino también en los conocimientos, las elecciones, las opiniones y, en general, en la capacidad de autodeterminación de las personas: “Estos datos se utilizan para entrenar tecnologías de aprendizaje automático con el fin de priorizar los resultados de búsqueda, predecir y moldear las preferencias personales, alterar los flujos de información y, en ocasiones, someter a las personas a experimentación conductual” (párrafo 4). El Consejo Europa prosigue afirmando que “los medios informáticos permiten deducir información íntima y detallada sobre las personas

tratamiento no está clara desde el principio, sino que se define con el propio tratamiento y, por lo tanto, al no ser conocida, no comunicarse al interesado.

4.5. Responsabilidad

La cuestión de la protección de los datos personales en el caso de las aplicaciones de inteligencia artificial no puede separarse de la de la responsabilidad⁴².

La cuestión que se plantea con más frecuencia es quién es responsable en caso de daños causados por aplicaciones de inteligencia artificial. En particular, la atención se centra en los casos en que el resultado del tratamiento efectuado por la aplicación de inteligencia artificial no es totalmente controlable *a priori* y se caracteriza por un cierto grado de imprevisibilidad: es decir, no se trata de un proceso determinista, sino que se caracteriza por un cierto grado de autonomía de tratamiento.

Se discute si es el autor del programa, el productor, el vendedor o el usuario quien se beneficia de él. También se debate, como ya se ha dicho, si conviene introducir la subjetividad jurídica de la aplicación o, si se prefiere, del robot⁴³. Asimismo, se debate entre

a partir de datos fácilmente disponibles. Esto permite clasificar a los individuos en categorías, reforzando así diferentes formas de segregación y discriminación social, cultural, religiosa, jurídica y económica. También facilita la microdirigenciación de las personas en función de sus perfiles, en formas que pueden afectar profundamente a sus vidas”, párrafo 6.

⁴² Esta cuestión se trata con más detalle en el capítulo 6 de este volumen. Sobre el tema de la responsabilidad de las aplicaciones de inteligencia artificial, véanse Ruffolo, *Intelligenza artificiale e responsabilità*, Santosuosso, Boscarato y Caroleo, “Robot e diritto: una prima ricognizione”, *La nuova giurisprudenza civile commentata* 28, no.7-8 (2012): 494-516.

⁴³ Véase la Resolución del Parlamento Europeo, de 16 de febrero de 2017, sobre recomendaciones a la Comisión en relación con las normas de Derecho civil

la proclamada necesidad de introducir nuevas normas y la supuesta posibilidad de limitarse a aplicar, con una nueva perspectiva, las normas ya existentes.

Aun creyendo, como ya se ha ilustrado, que no todo nuevo fenómeno requiere una nueva norma, creo que la cuestión de la responsabilidad en las aplicaciones de la inteligencia artificial requiere un nuevo enfoque basado en un modelo conceptual diferente: por robar un término de la tecnología que nos ocupa, “disruptivo”. Es necesario superar el paradigma basado en el error y la culpa y, en su lugar, abordar el problema en términos de asignación de riesgos. En otras palabras, no importa quién comete el error y la búsqueda de este es una actividad costosa y prescindible que puede superarse. En su lugar, es necesario prever la imputación del coste del daño causado a las personas que abstractamente podrían ser responsables, por ejemplo, mediante la creación de un fondo al que se pueda recurrir, independientemente de la forma en que se haya producido el accidente o el error. Se ha previsto un mecanismo similar en el circuito de las tarjetas de crédito para el caso de clonación o robo.

Uno de los objetivos que se persiguen con este tipo de sistema de asignación de riesgos salta a la vista y es tranquilizar a los usuarios potenciales asegurándoles que, independientemente del resultado de una costosa investigación de errores, obtendrán una indemnización.

Como es bien sabido, el reglamento introdujo un nuevo enfoque de la rendición de cuentas. Se trata del llamado *principio de rendición de cuentas*. El término “rendición de cuentas” puede traducirse como responsabilidad y, al mismo tiempo, prueba de res-

sobre robótica 2015/2103(INL), en la que, en particular, se invita a la Comisión Europea a estudiar determinadas posibles soluciones jurídicas en relación con el régimen de responsabilidad de los robots, incluido “el establecimiento de un estatuto jurídico específico para los robots a largo plazo [...] así como, posiblemente, el reconocimiento de la personalidad electrónica de los robots” (apartado 59, letra f).

ponsabilidad. El responsable del tratamiento debe poder demostrar que ha adoptado un proceso global de medidas jurídicas, organizativas y técnicas para la protección de datos personales, también mediante el desarrollo de modelos organizativos específicos, que, en aras de la brevedad, pueden considerarse análogos a los utilizados en Italia en la aplicación del Decreto Legislativo N.º 231 de 8 de junio de 2001. Las normas del reglamento sobre responsabilidad pretenden, por tanto, promover la adopción de medidas concretas y prácticas transformando los principios generales de la protección de datos en políticas y procedimientos concretos, de conformidad con las leyes y reglamentos aplicables. Asimismo, el responsable del tratamiento debe garantizar la eficacia de las medidas adoptadas y demostrar, cuando se le solicite, que ha tomado dichas medidas. Por lo tanto, hay que prever la responsabilidad y probar las medidas adoptadas para hacer frente a esta. En otras palabras, la responsabilidad es un mecanismo de dos niveles: por un lado, la aplicación de medidas y procedimientos y, por otro lado, la conservación de las pruebas pertinentes.

El *principio de responsabilidad* implica, por tanto, que es el responsable del tratamiento quien determina las medidas de seguridad adecuadas al tratamiento de datos personales que lleva a cabo, “teniendo en cuenta el estado de la técnica y los costes de aplicación, así como naturaleza, la finalidad, el contexto y fines del tratamiento, así como el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas”⁴⁴.

En este como en otros casos, el legislador hace recaer en el responsable del tratamiento la responsabilidad de determinar cómo cumplir los requisitos de la ley y adaptarlos al caso concreto, lo que lo responsabiliza no sólo de la aplicación, sino también de la evaluación. Así, para las disposiciones de seguridad, la aplicación del

⁴⁴ Así, el art. 32 del reglamento.

principio de responsabilidad consagrado en el reglamento europeo también implicó la derogación de las especificaciones técnicas en materia de medidas mínimas de seguridad establecidas en el Código de Protección de Datos Personales (Anexo B), declarado por el Decreto Legislativo N.º 101/2018. Por lo tanto, de nuevo, es necesario remitirse al principio de rendición de cuentas para una lectura más completa y plena de la base jurídica del interés legítimo⁴⁵, que exige que el responsable del tratamiento realice una valoración entre el interés legítimo en el tratamiento y los intereses, o los derechos y libertades fundamentales del interesado que requieren la protección de los datos personales.

En lo que respecta a las aplicaciones de la inteligencia artificial, el intento de formular un modelo de responsabilidad no puede prescindir de una combinación de, por una parte, la responsabilidad del propietario del tratamiento y, por otra parte, una formulación que prescinda de los elementos subjetivos, así como de la identificación del error⁴⁶.

5. CONCLUSIONES

Por último, no puede faltar una última consideración.

El Reglamento Europeo de Protección de Datos pretende ir más allá del planteamiento que se remonta al menos veinte años atrás con la llamada “directiva madre” en materia de tratamiento de datos

⁴⁵ Letra f) del apartado 1 del art. 6 del reglamento.

⁴⁶ Cabe destacar que, por el momento, las iniciativas legislativas europeas en el ámbito de la IA no abordan la cuestión de la responsabilidad: mientras que la Ley de IA sólo establece obligaciones para los proveedores, la propuesta de Directiva sobre responsabilidad por IA, que ya se ha mencionado en este volumen, sigue un planteamiento de armonización mínima; en otras palabras, se limita a armonizar las normas sobre responsabilidad por culpa que regulan la divulgación de pruebas y la carga de la prueba de quienes solicitan una indemnización por los daños causados por los sistemas de IA.

personales, la ya mencionada Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Había asumido un debate cultural y un pensamiento doctrinal que se habían desarrollado en décadas anteriores y esbozaba un modelo estático de tratamiento de datos personales, que ahora ha quedado obsoleto. La tecnología también era diferente en aquella época: era un mundo sin teléfonos inteligentes, redes sociales ni motores de búsqueda. El modelo normativo identificaba un único intercambio de datos: del interesado al responsable del tratamiento. En cambio, la realidad de las redes sociales y los motores de búsqueda, de un mundo cada vez más interconectado digitalmente, se basa en un modelo de intercambio y gestión de datos e información, destinado desde el principio a la circulación global.

El reglamento europeo se dicta como consecuencia de un cambio en el escenario tecnológico en el ámbito de las comunicaciones en particular y con consecuencias sociales inmediatas.

Sin embargo, el reglamento europeo no tiene en cuenta las aplicaciones de inteligencia artificial ni el Big Data, es decir, el tratamiento masivo de datos.

La lógica del reglamento se basa siempre en los datos personales, respecto de cuyo tratamiento la persona toma una determinación: el interesado controla y, en algunos casos, gestiona sus datos siguiendo su circulación. Otros fundamentos jurídicos contribuyen a legitimar el tratamiento de datos personales, pero el modelo cultural, incluso anterior al jurídico, en el que se basa la normativa es la autodeterminación. Esta lógica, aunque mitigada por la responsabilidad, no puede aplicarse a las grandes masas de datos, al Big Data. No es posible pensar en una gestión individualizada de los datos, y menos aún si se basa en el consentimiento. El

consentimiento, en abstracto el mejor modelo posible, a menudo se revela insuficiente para ofrecer una protección eficaz y eficiente. Más aún si nos enfrentamos a aplicaciones de inteligencia artificial basadas en Big Data, en las que la determinación *a priori* de los procesos de tratamiento no puede darse por sentada y en las que la finalidad del tratamiento a menudo no está clara.

Casi parece como si se intentara gobernar las olas del mar gota a gota⁴⁷, considerando individualmente la gota. Por tanto, parece necesario replantearse el modelo cultural de referencia.

⁴⁷ He traducido libremente la eficaz metáfora que cito: “Metafóricamente, es como si el Derecho del mar se basara en el principio de controlar cada gota de agua de los océanos según su origen”. Así, Bergé, Grumbach y Zeno Zencovich, “The ‘Datasphere’, Data Flows beyond Control, and the Challenges for Law and Governance”, *European Journal of Comparative Law and Governance* 5, no. 2 (2019): 162.

CAPÍTULO 5

EL CONTRATO EN LA ERA DE LA INTELIGENCIA ARTIFICIAL*

1. INTRODUCCIÓN

Las aplicaciones de la inteligencia artificial están ya muy extendidas en todos los contextos, empezando por la banca y los seguros.

Definir qué es la inteligencia artificial es una tarea difícil¹. Es más sencillo enumerar las aplicaciones más extendidas de la inteligencia artificial.

Según un análisis², las tecnologías que aplican la inteligencia artificial, consideradas de mayor importancia, son las siguientes: IA

* Este capítulo incorpora con algunas adaptaciones y actualizaciones, el artículo publicado en *Revista Trimestral de Derecho Civil y Procesal* (2018): 441 y ss.

¹ Se hace referencia sobre este punto en el capítulo 1 de este volumen.

² Investigación realizada por Forrester, *TechRadar: Artificial Intelligence Technologies, Q1 2017*, referido en el informe de Aspen Institute Italia, *Artificial Intelligence as a New Growth Factor*, julio de 2017, 7. Véase también el informe de Aspen Institute Italia, Observatorio Permanente sobre Adopción e Integración de Inteligencia Artificial, *Artificial Intelligence Report 2024*, disponible en https://www.aspeninstitute.it/wp-content/uploads/2024/06/aspen_rapporto_intelligenza_artificiale_2024_rev_27062024_r.pdf (consultado el 24 de junio de 2024),

Multimodal, IA Generativa de segunda ola, Procesamiento del Lenguaje Natural, Habla, Desinformación, Plataformas de Aprendizaje Automático, Hardware optimizado para IA, Gestión de Decisiones, Plataformas de Aprendizaje Profundo, Biometría, Robótica Multitarea, Análisis de Texto, Adaptación del Lenguaje. Sin entrar en las especificaciones técnicas de cada una de las aplicaciones, no se mencionan sus diferentes nombres.

Las denominaciones sugieren la finalidad de las nuevas aplicaciones, que es la optimización de los mecanismos de razonamiento utilizados para la resolución de problemas y la mejora de la relación entre máquinas y personas.

Las aplicaciones basadas en el estudio y la comprensión del lenguaje humano, por ejemplo, son capaces de traducir a lenguaje natural información codificada originalmente en lenguaje binario y viceversa, lo que permite la interacción entre personas y sistemas. Esta tecnología se utiliza desde servicios básicos automatizados de atención al cliente hasta sistemas, como los chatbots, capaces de comprender las necesidades del cliente y ofrecerle respuestas personalizadas. Permaneciendo en el ámbito de las relaciones máquina-usuario, las tecnologías biométricas asociadas a la inteligencia artificial establecen interacciones que parecen más naturales entre las personas y los sistemas informáticos, de forma que explotan capacidades de reconocimiento basadas no sólo en el lenguaje y la voz, sino también en la imagen, el tacto y el lenguaje corporal.

Además, las plataformas *de machine learning* y *deep learning* permiten implementar sistemas de toma de decisiones y realizar

así como Bergmann, “The most important AI trends in 2024”, IBM, febrero de 2024, disponible en <https://www.ibm.com/blog/artificial-intelligence-trends/> (consultado el 24 de junio de 2024); University Of Stanford, *The AI index report. Measuring trends in AI*, 2024, disponible en <https://aiindex.stanford.edu/report/> (consultado el 24 de junio de 2024).

predicciones de forma autónoma, más allá de las instrucciones dadas inicialmente. Pensemos, por ejemplo, en los sistemas de inteligencia artificial que utilizan las grandes plataformas de comercio electrónico para predecir las compras de los clientes basándose en el análisis de cantidades relevantes de datos relativos a preferencias, hábitos de consumo y características personales.

El uso de estas tecnologías basadas en la inteligencia artificial aporta beneficios considerables, pues disminuye los costes operativos, pero también mejora la eficacia de las actividades y la calidad del trabajo humano.

2. MÉTODO

Una vez más, un fenómeno nuevo obliga al jurista a conocerlo, a examinar sus características esenciales, a comprenderlo, a valorar si se puede remontar a las categorías existentes en el ordenamiento jurídico, en definitiva, a realizar la actividad que le es más querida, a saber, la actividad de calificación.

Esta actividad debería llevarse a cabo, de nuevo en relación con las aplicaciones de inteligencia artificial en el contexto de los contratos y, en particular, en relación con los *contratos inteligentes*³.

Los *contratos inteligentes* pueden definirse como “protocolos de información que facilitan, verifican o hacen cumplir la negociación

³ Allen y Widdison, “Can computers make contracts?”, *Harvard Journal of Law and Technology* 9, no. 1 (1996): 26 y ss.; Di Giovanni, “Sui contratti delle macchine intelligenti”, en *Intelligenza artificiale. Il diritto, i diritti l'etica*, ed. Ruffolo (Giuffrè, 2020), 251 y ss.; Di Sabato, “Gli smart contracts: robot che gestiscono il rischio contrattuale”, *Contratto e Impresa* 33, no. 2 (2017): 378-402 y Cuccuru, “Blockchain e automazione contrattuale. Riflessioni sugli smart contract”, *La nuova giurisprudenza civile commentata* 33, no. 1 (2017): 107-119; Jaccard, “Los contratos inteligentes y el papel del Derecho”, *Jusletter* (2017): 23 y ss.; Parola, Merati y Gavotti, Blockchain e smart contract: questioni giuridiche aperte, *Contratti* (2018): 681 y ss.; Werbach y Cornell, “Contracts ex machina”, *Duke Law Journal* (2017): 152 y ss.

o ejecución de un contrato, permitiendo a veces la exclusión parcial o total de una cláusula contractual”⁴.

Su encuadramiento desde el punto de vista jurídico exige responder a una pregunta previa sobre la reconstrucción exacta del fenómeno: ¿los *contratos inteligentes* son contratos o son actos de ejecución de un contrato? En otras palabras, ¿se expresa la voluntad contractual en los *contratos inteligentes* o se ejecuta con ellos una voluntad declarada en otro lugar?

Un problema conceptual no disímil se plantea en relación con los contratos bancarios y las transferencias electrónicas de fondos, que no son contratos, sino actos de ejecución de un contrato, por ejemplo, el contrato de cuenta corriente.

En el caso de los *contratos inteligentes*, la cuestión es aún más compleja. En efecto, los denominados *contratos inteligentes* pueden adoptar la forma de contratos o de actos de ejecución de un contrato. Sin embargo, a efectos de este debate, sólo interesan los que son auténticos contratos.

Así pues, se examinará el curso normal de la celebración de un contrato para verificar si, en caso se trate de un *contrato inteligente* (en sentido estricto), presenta aspectos tan novedosos que deben revisarse las categorías jurídicas establecidas.

En primer lugar, hay que señalar que el tema de la aplicación de la inteligencia artificial al derecho es sumamente sugerente y, además, tiene una fascinación literaria que también impresionó al Parlamento europeo, que se refirió expresamente a las Tres Leyes de la Robótica de Asimov en su Resolución de 16 de febrero de 2017⁵.

⁴ Véase Wikipedia, https://it.wikipedia.org/wiki/Smart_contract (consultado el 24 de junio de 2024).

⁵ Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión en relación con las normas de Derecho civil sobre robótica, 2015/2103(INL).

En ocasiones, el tema no está exento de cierta retórica que, sin duda, hace menos fácil la calificación jurídica del fenómeno, al menos en un primer momento. Se tiende a antropomorfizar el fenómeno y a narrarlo como si las inteligencias artificiales implicadas fueran emanaciones de sujetos humanos. Esto ha llevado también, siguiendo la sugerencia de la narración, a referirse al programa de ordenador como “representante” y, para alcanzar este resultado, a prever la necesidad de configurar una subjetividad jurídica para el programa de ordenador⁶.

Sin embargo, esto parece innecesario. De hecho, aunque el *software* se configurara como representante lo relevante en términos de responsabilidad sería, en última instancia, el patrimonio del representante a efectos de la indemnización por daños y perjuicios. Por lo tanto, seguiría siendo necesario atribuir activos a los *programas informáticos*. De hecho, esta opción fue contemplada por el Parlamento Europeo⁷.

La Comisión Europea respondió a las observaciones del Parlamento en un documento titulado “Seguimiento de la Resolución del Parlamento Europeo de 16 de febrero de 2017 sobre las normas de Derecho civil relativas a la robótica”, adoptado el 16 de mayo de 2017, en el que reconoce las recomendaciones del Parlamento y confirma su disposición y cooperación sobre el tema. Con este fin, la Comisión Europea anunció el 9 de marzo de 2018 la creación de un grupo de expertos sobre inteligencia artificial para asesorar y apoyar a la Comisión en las decisiones e iniciativas sobre el tema.

⁶ En ese sentido, la Resolución del Parlamento Europeo de 16 de febrero de 2017 brinda recomendaciones destinadas a la Comisión en relación con las normas de Derecho civil sobre robótica, 17.

Véase también mi artículo “La conclusione del contratto...”, 500-509 y, en el mismo volumen, Sartor, “Gli agenti software...”, 57-91.

⁷ Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión en relación con las normas de Derecho civil sobre robótica, 16.

El resultado de la construcción jurídica resumida no parece, en definitiva, especialmente significativo, ya que la responsabilidad puede en todo caso configurarse en manos del usuario del programa, que es el mismo resultado al que conduce la operación de configuración del programa como representante.

El hecho de que los sistemas automatizados sean un instrumento sin subjetividad jurídica propia y que deban rechazarse las soluciones basadas en la subjetividad de la máquina ha sido confirmado recientemente en la Ley Modelo sobre los contratos celebrados y ejecutados por medio de “sistemas automatizados” adoptada el 11 de julio de 2024 por la CNUDMI, la *Comisión de las Naciones Unidas para el Derecho Mercantil Internacional*. La *Ley Modelo*, que naturalmente también se aplica a la contratación mediante sistemas de IA, cuadra los principios ya existentes de los contratos en el nuevo contexto tecnológico y comunicativo, y da seguridad a los operadores a nivel mundial, poniendo de relieve que no es necesaria una ley especial que regule los contratos de IA.

3. LA IDENTIFICACIÓN DE LAS PARTES

Un primer problema que debe examinarse es el de la identificación de las partes⁸.

Para celebrar un contrato puede ser importante conocer con certeza la identidad de la otra parte contratante. Esto no siempre es fácil en Internet, donde de hecho es habitual que se oculte la identidad, con mecanismos de seudonimización o anonimización.

⁸ Como se observó en el capítulo 4 de este volumen, la identificación de las partes parece convertirse en un requisito del contrato en el artículo 8-ter del Decreto-Ley N.º 135, de 14 de diciembre de 2018, modificado por la Ley de Conversión N.º 12, de 11 de febrero de 2019, que, después de definir la tecnología *blockchain* y las aplicaciones de los *contratos inteligentes*, atribuye estos últimos a la forma escrita sólo si las partes se identifican de acuerdo con un proceso disciplinado por AgID. Sobre este punto, remítase a lo observado en el capítulo 4.

La seudonimización se define en el Reglamento (UE) 2016/679⁹ (Reglamento general de protección de datos) como “el tratamiento de datos personales de tal manera que los datos personales ya no puedan atribuirse a un interesado específico sin el uso de información, siempre que dicha información adicional se almacene por separado y esté sujeta a medidas técnicas y organizativas para garantizar que dichos datos personales no se atribuyan a una persona física identificada o identificable”¹⁰. Los datos seudonimizados siguen siendo datos. De hecho, la seudonimización no excluye la posibilidad de reidentificación del interesado. Se trata, más bien, de una medida de seguridad que no altera los requisitos de licitud del tratamiento de datos. En confirmación de esto, el reglamento sitúa la seudonimización, junto con el cifrado entre las medidas que deben tener en cuenta los responsables y encargados del tratamiento para proteger los datos personales que tratan.

En cambio, los datos anónimos, a los que no se aplica la legislación sobre protección de datos personales, son datos que no

⁹ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Para una revisión en profundidad de las principales novedades introducidas por la nueva disciplina de privacidad, véase Alpa, “L’identità digitale...”, 2017, 723-733; Bassini, “La svolta della privacy...”, 587-590; Busia, Liguori y Pollicino, *Le nuove frontiere della privacy...*; Califano, “Il Regolamento UE 2016/679...”; Califano, *Privacidad: afirmación y práctica...*; Cuffaro, “El derecho europeo...”, 1098-1119; D’orazio, Finocchiaro, Pollicino y Resta, *Codice della privacy...*; Finocchiaro, “Introduzione al Regolamento Europeo...”, 1-18; Finocchiaro, *Il nuovo regolamento europeo...*; Piraino, “Il Regolamento generale...”, 369-409; Pizzetti, *Privacy e il diritto europeo...*; Riccio, Scorza y Belisario, *GDPR e normativa privacy...*; Sica, D’Antonio y Riccio, *La nuova disciplina europea...*; Stanzione, “Il Regolamento europeo...”, 1249-1264.

¹⁰ Así, art. 4, apartado 5, del Reglamento (UE) 2016/679.

pueden asociarse a un interesado identificado o identificable ni originalmente ni después del tratamiento¹¹. Si se asume la definición en sentido absoluto, como datos que ya no pueden identificarse, independientemente de los costes y el tiempo necesarios para la reidentificación, es muy difícil hablar de datos anónimos en línea. Por el contrario, si el anonimato debe interpretarse según el criterio de lo razonable, debe hacerse referencia al grado en que la información puede referirse a un sujeto determinado¹². Como se subraya en el Dictamen 4/2007 del Grupo de Trabajo del artículo 29¹³, la verificación de la identificabilidad es un concepto dinámico y debe considerar el estado de la técnica en el momento del tratamiento de los datos. Los datos anónimos, de hecho, no sólo se definen en relación un sujeto, sino más generalmente con respecto a los costes, esfuerzos, tiempo, recursos y tecnología que permiten la reidentificación. Por lo tanto, también es variable con el tiempo, en relación con el desarrollo de la tecnología.

¹¹ Esta definición estaba prevista en el art. 4, letra n), del Decreto Legislativo N.º 196, de 30 de junio de 2003, “Código de Protección de Datos de Carácter Personal”, derogado por el Decreto Legislativo de adaptación del ordenamiento interno al Reglamento (UE) 2016/679, Decreto Legislativo N.º 101, de 10 de agosto de 2018. El reglamento, por otra parte, no contiene una definición expresa sobre el tema. En todo caso, la definición ya prevista por el Código es la misma que puede deducirse, según un razonamiento *inverso*, a partir de la definición de los datos personales. Además, planteamiento *inverso* es también el adoptado por el legislador europeo, primero, en el Reglamento (UE) 2018/1807, de 14 de noviembre de 2018, “por el que se establece un marco aplicable a la libre circulación de datos de carácter no personal en la Unión Europea”, donde se definen los datos como “datos distintos de los datos personales definidos en el art. punto 1, del Reglamento (UE) 2016/679”, y después en el Reglamento (UE) 2022/868 “relativo a la gobernanza europea de datos”, la Ley de Gobernanza de Datos, y el Reglamento (UE) 2023/2854 “relativo a normas armonizadas sobre el acceso equitativo a los datos y su uso”, la Ley de Datos.

¹² A este respecto, véase también el capítulo 4 de este volumen.

¹³ Art. 29 del Grupo De Trabajo Sobre Protección De Datos Personales, *Dictamen 4/2007 sobre el concepto de datos personales*, adoptada el 20 de junio de 2007

Existe una famosa y ahora manida viñeta publicada en el *New Yorker*, el 5 de julio de 1993, que reza: “En Internet, nadie sabe que eres un perro”. Esta frase resume una situación que sigue siendo actual. La viñeta muestra a dos perros: uno sentado en una silla frente a un ordenador; el otro, a quien iba dirigida esta frase, sentado en el suelo. Desde entonces, Internet ha cambiado, pero el problema de la identidad se ha mantenido y hoy la identidad digital es un tema de crucial interés. Se han eliminado obstáculos jurídicos a la plena digitalización de los procesos, las normas sobre documentos informatizados y firmas electrónicas permiten realizar por medios digitales esencialmente todos los actos jurídicos que pueden por medios de papel, pero la identificación en línea es un tema crucial hoy más que nunca, especialmente para el desarrollo de determinados servicios que requieren la verificación de la identidad.

Para responder a la creciente necesidad de certidumbre, el legislador europeo ha tratado de promover mecanismos de identificación de partes, considerando útil la identificación, aunque no sea obligatoria por ley, para aumentar la confianza y favorecer así la celebración de contratos en línea y, en consecuencia, el desarrollo del comercio electrónico. Esta dirección se ha tomado desde 1997, en los primeros estudios en profundidad sobre el tema realizados por la Comisión Europea. De hecho, siempre se ha supuesto que una de las causas más importantes del retraso en el desarrollo del comercio electrónico era la falta de confianza de los compradores potenciales, consumidores y otros, en el medio. Se han publicado numerosas directivas, entre ellas la del comercio electrónico, para fomentar la confianza de los internautas. La directiva sobre la firma electrónica¹⁴ también perseguía el mismo objetivo y pretendía

¹⁴ Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

eliminar los obstáculos jurídicos al desarrollo del comercio. Desde esta perspectiva, la firma electrónica, al permitir alcanzar una certeza razonable sobre la identidad de la parte contratante, contribuye a reforzar la confianza de los usuarios en el uso de las tecnologías de la información. En el ámbito del comercio privado, y por tanto sin perjuicio de las razones que impulsaron la promulgación de la normativa que nos ocupa en el ámbito de las Administraciones públicas, la regulación de la firma electrónica no nace únicamente para cumplir requisitos técnico-jurídicos de forma o prueba, sino, sobre todo, para crear confianza en el comercio electrónico.

Un paso importante para resolver el problema de la identificación *en línea* fue la promulgación del Reglamento (UE) 2014/910¹⁵. El reglamento se conoce comúnmente como “eIDAS”, donde “e” significa “electrónico”, “ID” “identificación”, “A” “autenticación” y “S” “firma”¹⁶. De hecho, además de la identificación en línea, el Reglamento abarca también la firma electrónica y los llamados “servicios de confianza”.

En primer lugar, el reglamento distingue entre identificación y autenticación electrónicas. La identificación electrónica se define como el proceso de utilización de datos de identificación personal en forma electrónica para presentar de manera única a una persona física o jurídica, o a la persona física que representa a una persona jurídica¹⁷; por otro lado, la autenticación se define como el proceso electrónico que permite confirmar la identificación electrónica de

¹⁵ Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

¹⁶ Para un estudio en profundidad sobre el Reglamento e-IDAS, véase el libro del que soy coautor con Delfini, *Identificazione elettronica....*

¹⁷ Apartado 1 del art. 3 del Reglamento e-IDAS.

una persona física o jurídica, o el origen y la integridad de los datos en forma electrónica¹⁸.

Este reglamento fue modificado por el Reglamento (UE) 2024/1183 del Parlamento europeo y del Consejo de 11 de abril de 2024, “por el que se modifica el Reglamento (UE) 910/2014 con respecto al establecimiento del marco europeo para una identidad digital”.

Las definiciones anteriores se mantienen esencialmente sin cambios¹⁹, y el nuevo reglamento innova principalmente los sistemas de identificación electrónica, con la introducción de los monederos europeos de identidad digital²⁰, y el de los servicios de confianza, ampliado con la prestación de nuevos servicios²¹.

¹⁸ Apartado 5 del art. 3 del Reglamento e-IDAS.

¹⁹ Cabe destacar la modificación parcial de la definición de “identificación electrónica”, enriquecida con la referencia a la persona física que representa a otra persona física y ya no sólo a la persona jurídica. De hecho, el art. 3, apartado 1, del Reglamento e-IDAS, modificado por el Reglamento (UE) 2024/1183, reza así: “‘Identificación electrónica’: el proceso mediante el cual se utilizan datos de identificación personal en forma electrónica que representan a una única persona física o jurídica, o a una única persona física que representa a otra persona física o jurídica”.

²⁰ Tal como se establece en el art. 3, apartado 42, del Reglamento e-IDAS revisado, el monedero europeo de identidad digital consiste en “un medio de identificación electrónica que permite al usuario almacenar, gestionar y validar de forma segura datos de identidad personal y certificados electrónicos de atributos para facilitarlos a las partes usuarias y a otros usuarios de los monederos europeos de identidad digital, así como firmar mediante firmas electrónicas cualificadas o estampar sellos mediante sellos electrónicos cualificados”. Cada Estado miembro tendrá que proporcionar una solución de monedero europeo en un plazo de 24 meses a partir de la entrada en vigor de los actos de ejecución del reglamento que adopte la Comisión Europea. Estas podrán ser proporcionadas directamente por el Estado, en nombre del Estado o independientemente del Estado, pero deberán ser reconocidas por el Estado. Así, art. 5-*bis*, apartados 1 y 2.

²¹ Entre los nuevos servicios de confianza, recordamos, en particular, la atestación electrónica de atributos, la gestión de dispositivos cualificados para la creación

Las definiciones señaladas también se mencionan en el ordenamiento jurídico italiano y, en particular, en el Decreto Legislativo N.º 82 de 7 de marzo de 2005, Código de la Administración Digital (en lo sucesivo, más brevemente, “DAC” por sus siglas en italiano). Tras las modificaciones introducidas por el Decreto Legislativo N.º 179, de 26 de agosto de 2016, que pretendían armonizar las disposiciones nacionales con el marco normativo europeo modificado, el DAC hace una referencia directa a las definiciones contenidas en el reglamento, derogando las anteriormente previstas²².

En el ámbito de la identidad, el objetivo del Reglamento e-IDAS era hacer interoperables las herramientas de identificación en línea utilizadas en los Estados miembros, de forma que se refuerza la seguridad de las transacciones y el comercio en el mercado interior.

de una firma electrónica (o de un sello electrónico) a distancia, archivo y registros electrónicos. También, está el certificado de autenticación de sitios web, ya previsto en el primer Reglamento e-IDAS y que ahora es objeto de una modernización de las normas.

²² En la anterior DAC, de hecho, la identificación informática se definía como la validación del conjunto de datos atribuidos de forma única e inequívoca a un sujeto, que permite su identificación en los sistemas de información, realizada mediante tecnologías apropiadas también con el fin de garantizar la seguridad acceso [artículo 1.1. *u-ter*]. La autenticación, por su parte, no se refería a la persona que accedía al sistema informático, sino al documento informático. Se definía como “la validación del documento informático mediante la asociación de datos informáticos relativos al autor o a las circunstancias, incluidas las temporales, de su elaboración” [art. 1(1)(b)].

Una definición más general de autenticación informática figuraba en el Código de Protección de Datos Personales [artículo 4(3)(c)], donde la autenticación se define como el conjunto de herramientas y procedimientos electrónicos para verificar la identidad, incluso indirectamente. Como ya se ha mencionado, el Código fue modificado por el Decreto Legislativo por el que se adapta el Derecho interno al Reglamento (UE) 2016/679, Decreto Legislativo N.º 101/2018, derogándose también la disposición que se acaba de examinar.

De acuerdo con el principio de neutralidad tecnológica, no se impone un único sistema de identificación a escala europea, pero se prevé que los Estados miembros puedan notificar a la Comisión el sistema de identificación en línea utilizado a nivel nacional, siempre que cumpla una serie de condiciones en términos de garantía y seguridad. Si el sistema es aprobado por la Comisión, también deberá ser reconocido por los demás Estados miembros, al igual que los procedimientos de identificación que se lleven a cabo a través de él. De acuerdo con el principio de reconocimiento mutuo, por tanto, los ciudadanos europeos pueden utilizar sus propias identidades digitales, emitidas por los sistemas nacionales de identificación notificados, para acceder a servicios o celebrar contratos telemáticos en los distintos Estados miembros, en todos los casos en que se requiera una identificación digital segura del usuario.

En el ordenamiento jurídico italiano, el sistema de identificación electrónica es ante todo el Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese (SPID), regulado por el artículo 64 de la DAC²³. Los cambios introducidos en el DAC por la citada coordinación con el Reglamento e-IDAS han dado centralidad al sistema de identificación, dando un nuevo impulso a su rápida implantación. Así, SPID fue notificado a la Comisión Europea y publicado en el *Diario Oficial de la Unión Europea*²⁴. A SPID se sumaron posteriormente el Documento de Identidad

²³ El SPID también se rige por el decreto del presidente del Gobierno de 24 de octubre de 2014, "Definición de las características del sistema público de gestión de la identidad digital de ciudadanos y empresas (SPID), así como de los plazos y procedimientos para la adopción del sistema SPID por las Administraciones Públicas y las empresas", publicado en la G.U. no. 285, de 9 de diciembre de 2014, y por una serie de reglamentos y determinaciones de desarrollo, publicados por Agid y disponibles en <https://www.agid.gov.it/it/piattaforme/spid> (consultado el 24 de junio de 2024).

²⁴ Más concretamente, C318 de 10 de septiembre de 2018.

Electrónico (CIE), también notificado a la Comisión Europea y posteriormente publicado en el *Diario Oficial*²⁵.

Con la introducción de los monederos europeos de identidad digital, el legislador europeo pretendía seguir desarrollando este sistema.

Las carteras, basadas en los sistemas nacionales existentes, amplían las funcionalidades, en particular incluyendo, además de los datos de identificación, otros datos, como los relativos a certificados médicos o títulos de estudios²⁶, y también amplían el ámbito de apli-

²⁵ Más concretamente, C309 de 13 de septiembre de 2019.

²⁶ Se trata de los denominados “certificados electrónicos de atributos”. El art. 5 *bis*, no. 4 del Reglamento e-IDAS modificado describe las funcionalidades del monedero del siguiente modo: “Los monederos europeos de identidad digital permiten, de forma intuitiva, transparente y rastreable a) solicitar, obtener, seleccionar, combinar, almacenar, suprimir, compartir y presentar de forma segura, bajo el control exclusivo del usuario, datos de identificación personal y, en su caso, en combinación con certificados electrónicos de atributos, necesarios para la autenticación de las partes que confían en la certificación en línea y, en su caso, fuera de línea, con el fin de acceder a servicios públicos y privados, de forma que garantizan al mismo tiempo que sea posible la divulgación selectiva de los datos b) generar seudónimos y almacenarlos forma cifrada y local dentro del Billetera Europea de Identidad Digital; c) autenticar de forma segura la Billetera Europea de Identidad Digital de otra persona, y recibir y compartir datos de identificación personal y declaraciones electrónicas de atributos de forma segura entre las dos Billeteras Europeas de Identidad Digital; d) acceder a un registro de todas las transacciones realizadas a través de la Billetera Europea de Identidad Digital mediante un panel de gestión común que permita al usuario (i) consultar una lista actualizada de las partes certificadoras fiables con las que el usuario ha establecido una conexión y, en su caso, todos los datos intercambiados; (ii) solicitar fácilmente que una parte certificadora fiable suprima datos personales de conformidad con el art. 17 del Reglamento (UE) 2016/679; (iii) denunciar fácilmente a la parte certificadora que confía a la autoridad nacional de protección de datos competente si se recibe una solicitud de datos personales presuntamente ilícita o sospechosa; e) firmar mediante firmas electrónicas cualificadas o estampar sellos mediante sellos electrónicos cualificados; f) descargar, en la medida en que sea técnicamente factible, datos de usuario, declaraciones

cación, ya que la obligación de hacer utilizables sus servicios a través de las carteras no sólo afecta a las entidades públicas, sino también a las entidades privadas que están obligadas a usar la autenticación fuerte del usuario por obligación reglamentaria o contractual²⁷.

Así pues, los dos sistemas, el de las herramientas de identificación electrónica imperantes y el de los monederos, se complementan. Al mismo tiempo, siguen siendo distintos y se complementan: “El uso de monederos europeos de identidad digital es opcional. El acceso a los servicios públicos y privados y al mercado laboral, así como la libertad de empresa, no se ven limitados ni perjudicados en modo alguno para las personas físicas o jurídicas que no utilicen los monederos europeos de identidad digital. El acceso a los servicios públicos y privados sigue siendo posible con otros medios de identificación y autenticación existentes”²⁸.

En el panorama mundial, sin embargo, la situación sigue siendo incierta. Actualmente no existen sistemas de identificación compartidos ni normas comunes que garanticen la interoperabilidad de los sistemas existentes.

El Grupo de Trabajo IV sobre comercio electrónico de la CNUDMI (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) viene trabajando en esta cuestión, cuyo objetivo es crear un sistema internacional unificado de identificación en las transacciones de comercio electrónico para garantizar un desarrollo seguro del mercado mundial en línea. A falta de normas internacionales compartidas, la digitalización del comercio ha obligado a numerosos actores del comercio electrónico a dotarse de sus propios sistemas de identificación, lo que ha dado lugar a la

electrónicas de atributos y configuraciones; g) ejercer el derecho del usuario a la portabilidad de los datos”.

²⁷ Así, el art. 5-septies, apartado 2, del Reglamento e-IDAS modificado.

²⁸ Así, el artículo 5 bis, apartado 15, del Reglamento e-IDAS modificado.

proliferación de multitud de credenciales y modos de acceso. Por ello, en julio de 2022, se adoptó la Ley Modelo sobre la Utilización y el Reconocimiento Transfronterizo de los Servicios de Gestión de la Identidad y de Confianza, que define unos requisitos mínimos y compartidos para la autenticación internacional de los usuarios, respetando las diferentes realidades nacionales²⁹.

4. LA IMPUTACIÓN DE LA VOLUNTAD

Las técnicas de imputación de voluntades en los contratos en línea están ya bien establecidas.

Con las llamadas “firmas” electrónicas o digitales, se ha pasado de un modelo basado en la autoría a otro basado en la responsabilidad. Así lo expresó también el Consejo de Estado en su dictamen de 7 de febrero de 2005³⁰. Sobre el tema de la desautorización, se afirma que “parece acertado superar los antiguos conceptos de falsificación, estrechamente vinculados al principio de ‘autoría’ de la firma y no al de ‘responsabilidad’ por la firma; por otra parte, es necesario hacer absoluta claridad sobre las hipótesis en las que se permite demostrar la ausencia de responsabilidad”. En efecto, la escritura informática es impersonal y carente de grafía, y la estampación de la firma digital no es, por su propia naturaleza, un gesto personal de la mano del firmante. Puede decirse, por tanto, que la particular naturaleza tecnológica de la firma digital y del documento informático han conducido a la elaboración de un

²⁹ La Ley Modelo está disponible en https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mlit_en.pdf (consultado el 24 de junio de 2024).

³⁰ Consejo de Estado, Dictamen de 7 de febrero de 2005, N.º 11995 sobre el proyecto de decreto legislativo que lleva por título “Código administración digital, por el que se aplica la delegación contenida en el artículo 10 de la Ley N.º 229 de 29 de julio de 2003, ‘Intervenciones en materia de calidad de la regulación, reorganización normativa y codificación-Ley de simplificación de 2001’”.

nuevo tipo de desautorización, que no tiene por objeto ni la firma ni la escritura, características externas del documento informático, sino exclusivamente el uso del dispositivo de firma³¹.

El término “firma” también debe considerarse metafórico y evocador de un sistema de conocimiento³². Aunque el término utilizado es “firma” en ambos casos, el adjetivo (digital, electrónica, electrónica cualificada, electrónica avanzada) que acompaña a la firma informática designa su distinta naturaleza. La firma informática se basa en la tecnología; la firma manuscrita, en la escritura. La firma informática es el resultado de un procedimiento tecnológico, mientras que la firma es el resultado de un gesto humano.

El uso del mismo término presagia consecuencias relevantes en términos de representación del conocimiento. Lleva a asociar de forma natural, casi instintiva, los dos objetos y a considerarlos realidades comparables y, por tanto, en este caso, sujetas al mismo régimen jurídico.

Y, en este caso, se trata de una operación de asunción de la firma como modelo. Uno tiene una aprehensión intuitiva del modelo y extrae libremente inferencias a partir de él. El modelo es un tipo de metáfora más general. “Una metáfora eficaz tiene el poder de poner en relación cognitiva y emocional dos dominios utilizando el lenguaje apropiado uno como lente para ver el otro”³³. La metáfora permite relacionar dos dominios del conocimiento.

³¹ Véase mi contribución, *Tecniche di imputazione della volontà negoziale: le firme elettroniche e la firma digitale* (Utet, 2007), 228.

³² Sobre este tema, véase mi contribución, *La firma digitale. Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici*. Art. 2699-2720 *Supplemento*, en *Commentario del codice civile Scialoja-Branca*, dirigido por Galgano, libro VI (Zanichelli, 2000) y la más reciente “La metáfora e il diritto...”, 1-16.

³³ Black, *Modelli, archetipi, metafore*, trad. Almansi y Paradisi (Pratiche, 1983), 87.

Se trata de una aplicación particular del uso de la metáfora con fines cognitivos³⁴.

Como escribe Galgano³⁵, ilustrando el uso de las metáforas en el derecho, constituyen “útiles síntesis verbales”, y la utilidad de la síntesis lingüística también en el caso de las firmas informáticas es evidente.

El enfoque seguido por el legislador italiano en la regulación de las firmas informatizadas se ha basado en el instrumento cognitivo del modelo y la metáfora. El legislador italiano ha vinculado las firmas manuscritas y las firmas informatizadas. La relación no es de identidad, pero los dos términos están asociados cognitivamente. Es una relación basada en el “como si”, que utilizando el instrumento de la metáfora se omite, y no en el “igual”³⁶.

Nuestro ordenamiento jurídico regula cuatro tipos diferentes de firma: electrónica, electrónica avanzada, electrónica cualificada y digital. La firma electrónica, no cualificada, se define como “los datos en forma electrónica, adjuntos o asociados lógicamente a otros datos electrónicos y utilizados por el firmante para firmar”. La definición, que remite a la del artículo 3 del Reglamento e-IDAS, difiere sustancialmente de la anteriormente prevista por la DAC, que la definía como “el conjunto de datos en forma electrónica unidos o conectados por asociación lógica con otros datos electrónicos, utilizados como método de identificación informática”. Con el Reglamento e-IDAS, se refuerza la función declarativa de la firma electrónica, en la que se presupone la función de identificación. En

³⁴ Sobre la función cognitiva de la metáfora, véase Eco, *Semiótica y filosofía del lenguaje* (Indiana University Press, 1984), 161 y ss.

³⁵ Galgano con su habitual riqueza cultural y profundidad de análisis ilustró el tema de la metáfora en el derecho en *Le insidie del linguaggio giuridico...*, en particular los v. 22-23.

³⁶ Véase mi contribución “La metafora e il diritto...”, 1-16.

el reglamento europeo, la firma electrónica es una herramienta de firma, que debe utilizarse para expresar el consentimiento.

Una firma electrónica avanzada se define como una firma electrónica que cumple los requisitos enumerados en el artículo 26 del Reglamento e-IDAS, es decir, “a) está vinculada de manera única al firmante; b) es capaz de identificar al firmante; c) ha sido creada mediante datos de creación de firma electrónica que el firmante puede, con un alto nivel de seguridad, utilizar bajo su exclusivo control; y d) está vinculada a los datos suscritos de tal manera que puede identificarse cualquier cambio posterior de dichos datos”³⁷. La firma electrónica reconocida, por su parte, es “una firma electrónica avanzada creada por un dispositivo reconocido de creación de firmas electrónicas y basada en un certificado reconocido de firma electrónica”³⁸. Por último, la firma digital, que no encuentra cabida en el Reglamento e-IDAS, es definida por el DAC como “un tipo particular de firma reconocida basada en un sistema de claves criptográficas, una pública y otra privada, correlacionadas entre sí, que permite al titular de la firma electrónica mediante la clave privada y a un tercero mediante la clave pública, respectivamente, poner de manifiesto y verificar procedencia e integridad de un documento informático o de un conjunto de documentos informáticos”³⁹.

³⁷ Con la revisión del Reglamento e-IDAS, se previó que, a más tardar el 21 de mayo de 2026, la Comisión Europea evaluará la necesidad de establecer una lista de normas de referencia y, en su caso, especificaciones y procedimientos aplicables a las firmas electrónicas avanzadas. Si la Comisión decide proceder, se entenderá que se cumplen los requisitos de firma electrónica avanzada cuando esta se ajuste a dichas normas, especificaciones y procedimientos. Así, el nuevo segundo párrafo del art. 26.

³⁸ Así, el artículo 3, apartado 12, del Reglamento e-IDAS.

³⁹ Así, el art. 1(1)(s) de la DAC.

Desde el punto de vista probatorio, el documento informático al que se adjunta una firma electrónica se valorará de forma diferente ante un tribunal en función del tipo de firma utilizada.

De conformidad con la letra a) del apartado 1 del artículo 20 de la DAC, en todos los casos en que el documento no lleve firma o lleve una firma electrónica no cualificada, la idoneidad del documento para satisfacer el requisito de forma escrita y su valor probatorio son libremente apreciables por el juez, en relación con las características de seguridad, integridad e inalterabilidad del documento. Por lo tanto, corresponde al juez determinar el valor que puede asumir la firma, caso por caso, en función de las circunstancias concretas examinadas por él.

Por el contrario, el mismo art. 20, párr. 1-*bis* establece que el documento informático en el que se estampa una firma digital, reconocida o avanzada tiene la eficacia prevista en el artículo 2702 del Código Civil para los contratos privados. La utilización del dispositivo de firma electrónica reconocida o digital se presume imputable al titular de la firma electrónica, salvo prueba en contrario por su parte⁴⁰. A este tipo de firmas, las modificaciones al DAC realizadas por el Decreto Legislativo N.º 217⁴¹, de 13 de diciembre de 2017, afianzaron entonces un nuevo sistema de firma, que se realiza en los casos en que un documento es “conformado, previa identificación informática de su autor, mediante un proceso que cuente con los requisitos establecidos por la AgID de conformidad

⁴⁰ Así, el apartado 1*b* del art. 20 de la DAC

⁴¹ Decreto Legislativo N.º 217, de 13 de diciembre de 2017, “Disposiciones complementarias y correctivas del Decreto Legislativo N.º 179, de 26 de agosto de 2016, relativo a las modificaciones y adiciones al Código Administración Digital, contemplado en el Decreto Legislativo N.º 82, de 7 de marzo de 2005, art. 1 de la Ley N.º 124, de 7 de agosto de 2015, de reorganización de las Administraciones Públicas” (Gaceta Oficial Serie General N.º 9, de 12 de enero de 2018).

con el artículo 71”. A efectos de valor probatorio, este nuevo sistema se equipara a una firma electrónica avanzada.

En materia contractual, una cuestión de gran interés es la de la aplicación de cláusulas abusivas mediante un sistema de señalar y hacer clic. Mediante esta técnica, la parte contratante contra la que se prevén cláusulas expresa su voluntad contractual seleccionando un ícono o una casilla de verificación. La manifestación del consentimiento puede tener lugar de cualquier forma, salvo que se exija la forma escrita y, por tanto, también con un clic. Pero se ha discutido si este sistema puede utilizarse también para la aprobación de cláusulas abusivas. de conformidad con el apartado 2 del artículo 1341 del Código Civil.

No cabe duda de que, en este caso, debe haber al menos dos manifestaciones de voluntad, una para la aprobación de las normas nupciales y otra para la aprobación específica de las cláusulas abusivas, como reiteran la decisión del Tribunal de Catanzaro⁴² y el Juez de Paz de Partanna⁴³, pero la cuestión es qué forma debe

⁴² Trib. Catanzaro, ord. 30 abril 2012. En el marco de un asunto relativo a la desactivación de una cuenta profesional en el sitio web de eBay, el tribunal tiene la oportunidad de pronunciarse sobre la firma por parte de un comerciante de cláusula abusiva (que otorgaba a eBay el derecho de rescisión) contenida en el contrato de alojamiento. En el presente caso, el comerciante había firmado el contrato que se le había presentado con una sola selección de la “clave de negociación”. Por lo tanto, el juez, observando la falta de aprobación específica de la cláusula abusiva, la anula.

Sólo como *obiter dictum* en el auto se menciona la circunstancia de que la suscripción de cláusulas abusivas debe hacerse mediante firma digital.

⁴³ G.d.P. Partanna, sentencia de 1 de febrero de 2002, N.º 15. El asunto en cuestión se refería a la validez de una cláusula de excepción a la competencia territorial, insertada en la regulación contractual de un contrato B2B, celebrado por vía telemática. El juez, destacando el carácter vejatorio de la cláusula de derogación contractual del foro, concluyó por considerar necesaria la recogida de un “doble asentimiento, presionando sobre el estatuto apropiado: uno de adhesión y otro

adoptar la aprobación escrita: si es suficiente la firma electrónica o si debe utilizarse un tipo particular de firma electrónica (es decir, la firma electrónica avanzada o la firma digital).

Según la sentencia del Tribunal de Justicia de la Unión Europea de 21 de mayo de 2015 en el asunto C-322/14⁴⁴, el “procedimiento de aceptación por un clic en las condiciones generales de un contrato de compraventa celebrado por vía electrónica, que contenga una cláusula de competencia, constituye una comunicación electrónica que permite el registro permanente de dicha cláusula, en el sentido de dicha disposición, cuando permite imprimir y guardar el texto de dichas condiciones antes de la celebración del contrato”.

de aprobación de las llamadas cláusulas vejatorias, entre las que debe incluirse la relativa a la derogación sobre la jurisdicción territorial”.

⁴⁴ El asunto sometido al Tribunal se refería a la compra de un coche eléctrico por un vendedor de coches en el sitio web de la empresa vendedora. Esta última, demandada ante el tribunal competente, se opuso a la renuncia a la competencia en favor de un tribunal distinto sobre la base de una cláusula contenida en las condiciones generales de venta. El comprador, por su parte, impugnó la inserción válida de dicha cláusula, alegando que debía constar por escrito, tal como exige el art. 23, apartado 2, del Reglamento Bruselas I.

Los tribunales, basándose en las conclusiones sobre el fondo, señalaron, en primer lugar, que el comprador debía aceptar expresamente, marcando la casilla correspondiente, las condiciones generales de venta del vendedor antes de efectuar la compra. Sin embargo, la transacción no implicaba automáticamente la apertura del documento que contenía las condiciones generales del vendedor, en las que se incluía la cláusula de jurisdicción. En segundo lugar, el Tribunal analizó la exigencia de forma escrita prevista en el art. 23.2 del Reglamento Bruselas I, señalando que esta disposición tiene por objeto equiparar determinadas formas de comunicación electrónica a la forma escrita con el fin de simplificar la celebración de contratos por vía electrónica. Para que la comunicación electrónica ofrezca las mismas garantías, en particular en materia de prueba, basta con que sea posible guardar e imprimir la información antes de la celebración del contrato.

En vista de ello, los tribunales europeos concluyeron que la aceptación mediante un clic de una cláusula de jurisdicción contenida en un contrato celebrado electrónicamente era válida y suficiente.

5. EL OBJETO DEL CONTRATO

Sin embargo, en el caso de los contratos inteligentes, se plantea otro problema y es el conocimiento real del contenido del contrato. Este problema es uno de los más fascinantes, entre otras cosas, porque conduce a una representación antropomórfica de los programas informáticos⁴⁵.

En efecto, dado que el contrato se perfecciona automáticamente si se cumplen determinadas condiciones, la parte contratante puede desconocer las condiciones reales en las que finalmente se perfecciona el contrato, especialmente si se trata de un mecanismo de decisión complejo en el que intervienen muchas variables. Ahora bien, mientras que es bastante sencillo imaginar, por ejemplo, que el contrato se celebrará si el precio de la compraventa de un bien se encuentra dentro de un rango entre 1 y 10, la representación del contenido del contrato resulta más difícil si las variables que lo determinan son muchas y si los mecanismos de combinación son a su vez numerosos. Esto se complica aún más si el programa utiliza un sistema de autoaprendizaje y, por tanto, “aprende”, por así decirlo, de las circunstancias. Hace algunos años, se habría dicho que la voluntad era en cualquier caso imputable al autor del programa⁴⁶. Hoy en día, no puede decirse que la voluntad esté predeterminada o predeterminada con certeza, dado que existen algoritmos capaces de aprender de forma autónoma y de tomar decisiones sin que las relaciones causa-efecto sean necesariamente comprendidas por el

⁴⁵ Problemas similares se analizaron a principios de siglo en relación con los contratos celebrados mediante distribuidores automáticos de bienes y servicios, y la doctrina más experimentada se basó en el supuesto de que con uso del autómatas se creaba un negocio. Cf. Cicu, “Gli automi nel diritto privato”, extracto de *Il Filangieri* no. 8 (1901) y Scialoja, *L'offerta a persona indeterminata ed il contratto concluso mediante automatico* (S. Lapi, 1902).

⁴⁶ Esta fue la tesis que defendí en mi *I contratti*....

ser humano. Esa frontera constituida por la difusión efectiva de los programas de inteligencia artificial ha sido traspasada.

En este caso, el objeto del contrato no está determinado. Es determinable, pero no siempre previsible, sobre la base de criterios y parámetros que, en algunos casos, no permiten una representación previa. En este caso, la parte contratante puede no estar en condiciones de conocer plenamente de antemano el contenido del contrato a celebrar. Pero, no obstante, habrá expresado respecto a la celebración del contrato su declaración positiva de voluntad. El contenido del contrato es, pues, determinable, pero de una manera que no siempre permite la comprensión previa. Por tanto, cabe preguntarse si se trata de una voluntad en sentido estricto, declarada de antemano, respecto de formación efectiva de las condiciones contractuales y, por tanto, del contenido negociado, al menos en parte, o si, en cambio, no es más apropiado representar todo ello en términos de un sistema de asunción de riesgos. En otras palabras, la narración jurídica puede declinarse afirmando que la parte contratante ha aceptado el riesgo de celebrar el contrato mediante un determinado sistema informático que utiliza un programa de inteligencia artificial, o afirmando que la misma parte contratante ha celebrado un contrato con un objeto que puede determinarse mediante un sistema de inteligencia artificial.

6. LA FORMA DEL CONTRATO

El requisito de forma, cuando la ley lo exige, no plantea problemas particulares. El legislador italiano y europeo pone a su disposición un rico instrumental jurídico.

Desde 1997, el legislador italiano ha considerado necesario introducir una definición de documento informático en nuestro ordenamiento jurídico. Esto se consideró necesario no tanto por razones técnico-jurídicas, sino más bien para romper un condicionamiento

cultural que lleva a pensar que el documento es necesariamente de papel, cuando nada obliga a ello.

Carnelutti hizo hincapié en la irrelevancia de la materia, afirmando que “cualquier materia, capaz de formar una cosa representativa, puede entrar en el documento: tela, cera, metal, piedra, etc.”⁴⁷. Por lo tanto, incluso un documento compuesto únicamente de *bytes* sería un documento, siendo la materia irrelevante también en este caso. En rigor, ni siquiera habría sido necesaria una regulación específica sobre la materia para configurar el documento informático como documento, desde el punto de vista de la materia que lo forma.

Como es sabido, la legislación italiana no preveía una definición de documento o, mejor dicho, no la preveía hasta la revisión del Decreto Legislativo N.º 82, de 7 de marzo de 2005, dictada por el Decreto Legislativo N.º 235, de 30 de diciembre de 2010, que conllevó la definición de documento analógico. Sólo con la difusión del documento informático se hizo necesario definirlo y, en consecuencia, definir el documento análogo.

Ahora, el art. 1(1) de la DAC, armonizado como se recordaba con la disciplina europea del Reglamento e-IDAS, prevé las siguientes definiciones de documento: “p) documento electrónico: el documento electrónico que contiene la representación electrónica de actos, hechos o datos jurídicamente relevantes” y “*p-bis*) documento análogo: la representación no informatizada de actos, hechos o datos jurídicamente relevantes”.

Por lo tanto, el DAC ha reformulado la definición de documento de información de manera insatisfactoria. De hecho, la definición actual se refiere dos veces al documento como contenedor: dice que el documento informatizado es el documento electrónico que contiene la representación. Además de esto, la referencia a

⁴⁷ Carnelutti, “Documento de entrada (Teoría moderna)”, en *Novissimo Digesto Italiano*, vol. VI (Utet, 1964), 86.

electrónico parece desafortunada porque podría entenderse como si se quisiera circunscribir la propia definición de documento electrónico al uso de aquellos soportes que hacen uso de tecnología exclusivamente electrónica (como las memorias USB), no considerando otros soportes que hacen uso de tecnología no electrónica (por ejemplo, *wi-fi*, *cd-rom*). En realidad, la tecnología empleada y el soporte utilizado deberían ser irrelevantes a efectos de definición. Lamentablemente, nuestro legislador ha tenido que ceñirse a la definición prevista en el reglamento europeo.

Con respecto a la idoneidad del documento para complementar la forma escrita, el artículo 21, párrafo 2-*bis* del DAC, estipula que un documento electrónico en el que se estampe una firma electrónica cualificada o una firma digital es capaz de satisfacer el requisito de forma escrita *ad substantiam*, que se ha estipulado para las escrituras privadas de conformidad con el artículo 1350, párrafo 1, números 1 a 12 del Código Civil. Las escrituras a las que se refiere el artículo 1350, apartado 1, número 13 del Código Civil, por otra parte, pueden firmarse bajo pena de nulidad no sólo con una firma electrónica o digital cualificada, sino también con una firma electrónica avanzada o se conforman de la forma adicional a la que se refiere el artículo 20, apartado 1, letra a) anterior.

En todos los demás casos, el art. 20 (*Ibis*) establece que la idoneidad del documento para complementar la forma escrita es libremente apreciable en juicio, teniendo en cuenta las características de seguridad, integridad e inmodificabilidad.

7. LIMITACIÓN DE AUTONOMÍA DEL INCUMPLIMIENTO

Otro tema de interés, según los primeros comentaristas, es el de la imposibilidad de incumplimiento⁴⁸. En otras palabras, el contrato

⁴⁸ Sobre el tema véase, entre otros, Di Sabato, “Gli smart contracts...” y Cuccuru, “Blockchain ed automazione...”.

se cumpliría automáticamente y, por tanto, la parte contratante no tendría ninguna posibilidad material de incumplimiento. Sin embargo, si se examina más de cerca, el cumplimiento, es decir, el pago, es un acto debido hasta el punto de que puede ser cumplida también por el deudor incapacitado. La cuestión se plantea más adecuadamente si se plantea en términos de una elección en cuanto, por ejemplo, la obligación que debe cumplirse, existiendo una alternativa entre dos obligaciones que en el caso no pueden cumplirse ambas. En este caso, la elección del cumplimiento podría ser automática y escapar así a la voluntad del deudor. Una vez más, la revocación de la declaración contractual podría no ser técnicamente factible debido al momento concreto de la transacción, es decir, ni siquiera habría tiempo para revocarla.

8. CONCLUSIONES SOBRE LOS *CONTRATOS INTELIGENTES*

Se ha revisado el camino normal hacia la celebración del contrato y sus requisitos, que son relevantes en este caso. Como resultado de este breve examen, no parece que, en el caso de un *contrato inteligente*, el jurista tenga que ir más allá de las categorías conocidas o inventar otras nuevas. Ciertamente, es necesario comprender plenamente el fenómeno, no sólo desde un punto de vista tecnológico, sino también sociológico, lo que ha provocado nuevos comportamientos sociales, pero no es necesario buscar nuevas reglas.

Sin embargo, no todo fenómeno requiere una nueva regla, como lamentablemente se suele afirmar: de hecho, a menudo se requiere una nueva ley para cada nuevo fenómeno. Pero, el jurista es un intérprete y no un mero contable de la ley y debe reivindicar con orgullo su papel.

Una reciente sentencia canadiense, *Moffatt contra Air Canada*, de 14 de febrero de 2024⁴⁹, confirma este planteamiento. Y la

⁴⁹ Se trata del pronunciamiento 2024 BCCRT 149.

respuesta desarrollada por el tribunal canadiense podría resumirse citando simplemente el conocido refrán: “Cuius commoda, eius et incommoda” (quien se beneficia de una situación, también debe soportar sus inconvenientes).

Un brocardo latino, por tanto, resuelve un problema creado por la inteligencia artificial.

Se trata de una sentencia sobre un asunto de escasa relevancia económica, como suele ocurrir con los *leading cases*, pero que ofrece muchas luces. En el centro, el error aparentemente cometido por un chatbot, es decir, como se mencionó al principio de esta contribución, por un *software* que, usando la inteligencia artificial, formula respuestas a las preguntas formuladas, simulando que se está conversando con un ser humano. En este caso, el chatbot de Air Canada fue interrogado por un usuario del sitio, que era el comprador de un billete de avión, el Sr. Moffatt⁵⁰.

El juez, con un razonamiento muy directo, afirma que, aunque el chatbot sea interactivo, sigue formando parte del sitio de Air Canada y que, obviamente, Air Canada es responsable de toda la información que aparece en su sitio, ya sea estática o interactiva. No hay ninguna razón por la que, como había argumentado la empresa, el cliente deba *volver a comprobar* la información facilitada a través del sitio o del chatbot.

La cuestión de la subjetividad de la aplicación de la inteligencia artificial no entra en juego en absoluto. El tribunal considera

⁵⁰ La historia es muy sencilla. El Sr. Moffatt, debido a la pérdida de su abuela, tiene que comprar un billete de avión. Air Canada ofrece tarifas con descuento en caso de viaje por duelo. El Sr. Moffatt consulta el chatbot de Air Canada, que le informa que el descuento también puede solicitarse después del viaje en un plazo de 90 días. Esto es lo que hace el Sr. Moffatt; sin embargo, descubre más tarde, tras cierta interacción con los empleados (humanos) de Air Canada, que el descuento debería haberse solicitado antes y que no puede aplicarse con carácter retroactivo. Moffatt emprende acciones legales y exige una indemnización. Air Canada se defiende argumentando que la responsabilidad es del chatbot.

simple y pragmáticamente que el *chatbot* forma parte del sitio de la empresa y, por tanto, la empresa que ha decidido hacer uso de él es responsable de este. Y corta así el nudo gordiano. Cabe preguntarse quién habría indemnizado al Sr. Moffatt por los daños, incluso si se hubiera admitido la subjetividad del chatbot, como Air Canada intentó argumentar. La respuesta sólo puede ser la misma: la empresa que decidió incluir el chatbot en su sitio web.

Esta decisión, también por ser de las primeras, fue un importante punto de partida.

Aunque circunscrito, el caso sirve para extraer algunas consideraciones. No se sabe de qué tipo de chatbot se trataba, si era un chatbot de los más utilizados hoy en día, que responde a preguntas básicas y automatizadas, o en cambio un chatbot capaz de aprender y personalizar sus respuestas en función de necesidades del usuario. La cuestión es que quienes lo utilizan son responsables, en este caso, al ponerlos a disposición de los clientes, y que la cuestión de la subjetividad no es relevante. Se habría llegado a una conclusión diferente si un empleado de la empresa hubiera dado respuestas igualmente incorrectas, con la diferencia de que el empresario habría podido tomar represalias contra el empleado, pero la respuesta al cliente no habría cambiado. Sin embargo, incluso en este caso, no puede excluirse la responsabilidad de la persona que formó al *chatbot* o lo programó. De esta puede extraerse otra consideración. No sólo el juez decidió, obviamente, sobre la base de la ley aplicable, sino que la decisión parece ser absolutamente adecuada. Por lo tanto, no siempre y en todos los casos son necesarias nuevas normas para regular nuevos fenómenos. Por el contrario, es necesario evaluar sector por sector cuándo son necesarias nuevas normas. En este caso, queda un amplio margen para la regulación contractual que puede circunscribir de diversas maneras e intentar limitar la responsabilidad por uso de sistemas de inteligencia artificial.

CAPÍTULO 6

INTELIGENCIA ARTIFICIAL Y RESPONSABILIDAD*

1. SOBRE EL MÉTODO: VERIFICACIÓN DE LA NECESIDAD DE UNA INTERVENCIÓN LEGISLATIVA

La inteligencia artificial es un tema que también suscita hoy la atención de los juristas¹. Existe una sucesión de conferencias y

* Este capítulo incorpora, con algunas adaptaciones y actualizaciones, el artículo publicado en *Contract and Enterprise* (2020), 713 y ss.

¹ El tema es también de gran interés en la banca hasta el punto de que se mencionó en informe del presidente de la ABI al Día del Ahorro 2019. Véase Grupo de expertos sobre obstáculos regulatorios a la innovación financiera (ROFIEG), *30 Recommendations on Regulation, Innovation and Finance-Final Report to the European Commission*, diciembre de 2019, disponible en https://finance.ec.europa.eu/publications/final-report-expert-group-regulatory-obstacles-financial-innovation-30-recommendations-regulation_en (consultado el 24 de junio de 2024).

Véase también el informe CEPS, *Artificial Intelligence...*, disponible en <https://www.ceps.eu/ceps-publications/artificial-intelligen-ce-ethics-governance-and-policy-challenges/> (consultado el 24 de junio de 2024) y presentado en Assonime el 25 de marzo de 2019, así como el informe del AI Now Institute At New York University, *AI Now Report 2019*, diciembre de 2019, disponible en https://ainowinstitute.org/AI_Now_2019_Report.pdf (consultado el 24 de junio de 2024).

artículos sobre el tema que pretenden describir y encuadrar el fenómeno que se discute cotidianamente hoy en día, así como examinar las implicaciones jurídicas de las nuevas aplicaciones tecnológicas. La conclusión de estos estudios en profundidad suele ser pedir la intervención del legislador.

Sin embargo, este resultado, aceptable en algunos casos, sólo puede representar la conclusión de una investigación sobre si las normas existentes permiten una solución interpretativa, que sería claramente, en todo o en parte, una alternativa ante la intervención legislativa y haría esta última superflua.

Ante todo, se plantea un problema metodológico, que a menudo se pasa por alto y sobre el que es importante renovar la conciencia del jurista: en primer lugar, es necesario comprender si las intervenciones reguladoras son realmente necesarias y cuáles son².

Sin embargo, el planteamiento de reclamar nuevas normas ha caracterizado la actitud de una parte de la doctrina jurídica hacia la informática a lo largo de los años, quizá por una especie de temor reverencial o quizá de reticencia hacia las nuevas tecnologías. Ya en los años sesenta, se plantearon cuestiones sobre la necesidad de nuevas leyes en relación con los nuevos casos. Puede remontarse al debate sobre la protección del *software*³, a la solicitud de dispo-

2024), pero también en Stanford University Human-Centered Artificial Intelligence, *Artificial Intelligence...*, disponible en <https://aiindex.stanford.edu/report/> (consultado el 26 de junio de 2024).

² También Alpa, “Fintech: un laboratorio per i giuristi”, *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, eds. Finocchiaro y Falce (Bologna, 2019), XIII-XXII.

³ Se hace referencia a Santini, “La tutela giuridica della programmazione elettronica”, *Giurisprudenza Italiana* (1968): 225-232, quien, señalando que algunos autores han negado “de plano que el programa, y por tanto el programador, gocen de protección alguna en el ordenamiento jurídico italiano”, sostiene que “la conclusión simplista de que no existe ningún medio de *iure condito* para

siciones de protección de la vida privada⁴ y más tarde a la génesis de las normas sobre documentos informatizados⁵ y comercio electrónico⁶. Sin embargo, ya podemos anticipar que sólo en un caso,

proteger la actividad original de los programadores de cálculos electrónicos debe rechazarse en nuestro ordenamiento jurídico”; a Luzzato, “Una norma di legge francese da non imitare (a proposito della brevettabilità o meno dei programmi o serie di istruzioni per lo svolgimento to le operazioni dei calcolatori elettronici)”, *Rivista Di Diritto Industriale* (1968): 297-306, que reconoce que “ciertas formas de programas informáticos merecen indudablemente una protección por patente, otras no merecen ninguna protección, y para otras, en fin, puede encontrarse una forma de protección diferente en el marco de las leyes existentes, interpretadas teniendo en cuenta la nueva realidad técnica, o en el marco de nuevas normas jurídicas” y concluye considerando que lo que “se necesita en este ámbito, si acaso, es una elaboración técnica profunda del problema y no la redacción de normas precipitadas, drásticas e injustificadas”. Por último, cuestionando la protección de los programas informáticos, véase Borruso, *Computer e diritto. Problemi giuridici dell'informatica*, vol. II (Giuffrè, 1988,) 389 y ss., busca una regulación adecuada teniendo en cuenta que los programas informáticos no pueden ser protegidos ni por el derecho civil y penal ni por el derecho de autor.

⁴ Cf. Frosini, “La protezione della riservatezza nella società informatica”, *Informatica e diritto* (1981): 5-14, quien consideraba ineludible la necesidad de colmar con nuevas disposiciones legales la laguna existente entonces en nuestro ordenamiento jurídico en materia de protección de datos; Losano, “Un progetto di legge sulla protezione dei dati personali”, *Diritto dell'informazione e dell'informatica* (1987): 465-485.

⁵ Cuestionando la conveniencia de retrotraer la forma electrónica a la forma oral o escrita, o de considerar la forma electrónica como una nueva forma, Montesano, “Sul documento informatico come rappresentazione meccanica della prova civile”, *Diritto dell'informazione e dell'informatica* (1987): 23-31; Parisi, *Il contratto concluso tramite computer* (Cedam, 1987); Stallone, “La forma dell'atto giuridico elettronico”, *Contratto e Impresa* (1990): 756-778.

⁶ Véase *ex multis* Mirabelli, “I contratti di informatica: modelli, tipicità, collegamento”, en *I contratti di informatica. Profili civilistici, tributari e di bilancio*, eds. Alpa y Zeno Zencovich (Giuffrè, 1987), 9-19, quien afirma muy claramente que “el legislador puede y debe intervenir sólo cuando se ha constatado que la nueva situación presenta elementos que no pueden insertarse de ningún modo

el de la legislación sobre protección de datos, fue promulgar un cuerpo legislativo totalmente nuevo, mientras que, en los demás casos, el legislador resolvió introducir modificaciones y adiciones en las leyes existentes.

Se podría, con un toque de ironía, hablar de apocalípticos e integracionistas, de conservadores e intervencionistas, y establecer así una distinción entre los que creen que las normas existentes son suficientes y los que, por el contrario, creen que la intervención legislativa es necesaria y, a menudo, urgente e inaplazable.

Aunque tal vez se corra el riesgo de afirmar lo obvio, hay que reiterar que los sistemas jurídicos se caracterizan por una elasticidad que les permite absorber las tensiones de los cambios en todos los sectores: desde los cambios en las costumbres hasta los cambios sociales, pasando por los cambios tecnológicos, por citar sólo algunos. La interpretación, principal herramienta de trabajo del jurista, permite renovar la norma desde dentro, dejando a menudo inalterado su aspecto formal. La evolución del artículo 2043 del Código Civil, por ejemplo, deja claro cuáles son las potencialidades interpretativas y cuáles las “fronteras móviles”⁷.

A veces, sin embargo, la caja de herramientas del jurista, que se basa principalmente en la interpretación, resulta insuficiente y

en el ordenamiento jurídico existente, es decir, cuando la realidad ha demostrado que los intereses que emergen de una nueva situación no pueden satisfacerse de ningún modo encuadrando esta situación en esquemas conocidos”. Véase también Zeno Zencovich, “Sul rilievo pratico e sistematico della categoria dei c.d. contratti informatica”, en *I contratti di informatica: profili civilistici, tributari e di bilancio*, eds. Alpa y Zeno Zencovich (Giuffrè: 1987): 31-41, quien advierte de la “peligrosa ambigüedad de los términos ‘contratos informáticos’ o ‘contratos de tecnología de la información’ si, yendo más allá de simples exigencias descriptivas, se les quisiera atribuir autonomía conceptual y sistemática respecto de contratos de otro tipo o que tuvieran un ‘objeto’ diferente”.

⁷ Según la célebre expresión de Galgano, “Le mobili frontiere del danno in giusto”, *Contratto e Impresa* (1985): 1 y ss.

es necesaria la intervención del regulador: bien para aclarar, lo que elimina así la inseguridad jurídica, o bien para colmar lagunas. Pero esta conclusión sólo puede surgir como resultado de un proceso de cuidadosa verificación de las vías interpretativas que pueden seguirse y de la legislación aplicable, y no de forma apodíctica, siguiendo sugerencias de innovación.

Si se examinan los sectores afectados por la tecnología y citados como ejemplo al principio de este trabajo, se observa que sólo en un caso se consideró necesario realizar intervenciones normativas radicales y precisas en materia de disposiciones de protección de datos personales, a partir de impulsos de organizaciones internacionales e instituciones europeas. Basta pensar en el Convenio 108 del Consejo de Europa⁸ y en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos⁹. En otros casos, sin embargo, se trataba de integrar normas ya existentes. Así, en el caso de la protección de los programas informáticos, cuando se modificó y completó la disciplina del derecho de autor¹⁰; así en el caso del documento informático, cuando se dictaron disposicio-

⁸ “Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal”, firmado en Estrasburgo el 28 de enero de 1981. El 5 de marzo de 2019, Italia adoptó el Protocolo por el que se modifica el Convenio 108, ahora también denominado “Convenio 108+”, que concluye el proceso de modernización del Convenio

⁹ Como es sabido, la Directiva fue derogada por el Reglamento (UE) 2016/679, que, desde el 25 de mayo de 2018, es de aplicación directa en todos los Estados miembros y ha dictado las nuevas normas de datos. Para aprobar Fundamentos, véase el volumen que he editado, *La protezione dei dati personali...*; y D’orazio, Finocchiaro, Pollicino y Resta, *Codice della privacy...*

¹⁰ La referencia es, obviamente, al Decreto Legislativo N.º 518 del 29 de diciembre de 1992, “Aplicación de la Directiva 91/250/CEE sobre la protección jurídica de programas de ordenador”, que modificó y completó la Ley N.º 633 del 22 de

nes de conexión al Código Civil que desarrollaron paralelamente al código la disciplina de la firma electrónica¹¹; así en materia de comercio electrónico, cuando se decidió no modificar la disciplina dictada por el Código Civil y el Código de Consumo en materia de contratos¹².

Así, a veces las intervenciones reguladoras no son necesarias, a veces son apropiadas para aclarar y resolver incertidumbres, y a veces son necesarias verdaderas innovaciones.

Lo que sin duda hay que rechazar es el recurso apriorístico a una legislación de emergencia que a menudo no respeta los principios internacionales establecidos.

2. EL PAPEL DEL LEGISLADOR EUROPEO

El campo de la inteligencia artificial se caracteriza por la pluralidad de niveles de normalización y la complejidad de las reglas abstractamente aplicables o deseables.

abril de 1941, “Protección de los derechos de autor y otros derechos relacionados con su ejercicio”.

¹¹ Una piensa en el Decreto Legislativo N.º 82, de 7 de marzo de 2005, “Código de Administración Digital”, modificado en varias ocasiones, la última por el Decreto Legislativo N.º 217 del 13 de diciembre de 2017, “Disposiciones complementarias y correctivas del Decreto Legislativo N.º 179, de 26 de agosto de 2016, relativo a las modificaciones y adiciones al Código de Administración Digital”.

¹² La regulación del comercio electrónico está contenida en el Decreto Legislativo N.º 70, de 9 de abril de 2003, por el que se aplica la Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información en el mercado interior, con especial referencia al comercio electrónico. El art. 68 del mismo Decreto Legislativo N.º 206 de 6 de septiembre de 2005 “Código de Consumo” remite al citado Decreto Legislativo N.º 70/2003 para la regulación de las ofertas de servicios de la sociedad de la información, realizadas a los consumidores por vía electrónica, en aquellos aspectos no regulados por el Código de Consumo.

Desde las normas deontológicas cuya contribución se invoca cada vez más¹³, pasando por las normas dictadas por la propia tecnología¹⁴ hasta las normas contractuales dictadas por los proveedores y pasando por *el soft law*. Si nos referimos a normas, es decir, *hard law*, el nivel en el que deben dictarse las normas es, como mínimo, el europeo, ya que los intereses que se enfrentan son globales, políticos y económicos debido al tamaño del mercado y de los actores.

Basta pensar en los grandes actores del ámbito de las redes sociales y los motores de búsqueda, que son estadounidenses o chinos, como Facebook, Google, Baidu y Ali Baba, por citar sólo algunos. No es casualidad que se haya adoptado el reglamento europeo que establece normas armonizadas de inteligencia artificial, la llamada Ley de IA, mientras que la propuesta de directiva del Parlamento Europeo y del Consejo “relativa a la adaptación de las normas sobre responsabilidad civil extracontractual a la inteligencia artificial”, la *AI Liability Directive*¹⁵, avanza en el camino de la armonización de las normas sobre responsabilidad extracontractual.

La acción del legislador nacional está naturalmente limitada porque el fenómeno es mundial y, de hecho, paradigmático de la era de la globalización, al igual que las normas contractuales, dictadas por los actores que lo rigen. Las disposiciones administrativas y

¹³ Se hace referencia, en particular, al intento de la Comisión Europea de esbozar un nuevo enfoque del problema ética, de conformidad con un “marco ético basado en los valores de UE y coherente con la Carta de los Derechos Fundamentales de la Unión Europea”. Un ejemplo lo ofrece *The European Ethical Charter on the Use of Artificial Intelligence in Justice Systems and Related Fields*, adoptada por la Comisión Europea para la Eficiencia de la Justicia (un órgano del Consejo de Europa) los días 3 y 4 de diciembre de 2018, ya mencionada en este volumen y objeto de un debate en profundidad en el capítulo 8.

¹⁴ Véase para todos Lessig, *Code and other laws of cyberspace* (Basic Books, 1999).

¹⁵ Para un análisis en profundidad del modelo europeo de regulación de la IA y una lectura geopolítica, véanse los capítulos 1, 2 y 3 de este volumen.

reglamentarias siguen siendo de los Estados nacionales, mientras que la acción judicial, así como la de las autoridades supervisoras y administrativas independientes, es ciertamente nacional¹⁶.

Es evidente que el legislador europeo está construyendo, también a través de la acción reguladora, el mercado digital europeo¹⁷.

En este sentido, deben leerse también el Reglamento (UE) 2016/679, 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”¹⁸ (en lo sucesivo, “el reglamento” para abreviar) y el

¹⁶ Cabe señalar que, mientras se tramitaba la aprobación de la Ley de AI, algunos legisladores nacionales adoptaron algunas iniciativas legislativas, anticipándose a menudo a las disposiciones del reglamento. Recordemos, en particular, el caso de España, que, en 2023, creó la “Agencia Española de Supervisión de la Inteligencia Artificial - AESIA”. También, es digno de mención el caso de Italia, donde los proyectos de ley sobre IA son numerosos. Entre ellos, figura, en particular, una iniciativa gubernamental: el denominado “ddl IA”, aprobado por el Consejo de Ministros el 23 de abril de 2024 y presentado al Senado el 20 de mayo de 2024.

¹⁷ A este respecto, remítase a lo expuesto en el capítulo 1 de este volumen sobre la articulación de la estructura reguladora del mercado único digital europeo.

¹⁸ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), publicado en DOUE. L 119/1, de 4 de mayo de 2016. En general, sobre el Reglamento, véase Alpa, “L'identità digitale...”, 723-733; Busia, Liguori y Pollicino, *Le nuove frontiere della privacy...*; Califano y Colapietro, *Innovazione tecnologica...*; Cuffaro, D'orazio y Ricciuto, *I dati personali nel diritto europeo* (Giappichelli, 2019); D'orazio, Finocchiaro, Pollicino y Resta, *Codice della privacy...*; Finocchiaro, *La protezione dei dati personali...*; Panetta (ed.), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018* (Giuffrè, 2019); Pizzetti, *Privacy e il diritto europeo...*; Riccio, Corza y Belisario, *GDPR e normativa privacy...*; Sica, D'Antonio y Riccio (eds.), *La nuova disciplina*

Reglamento (UE) 2014/910 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, “relativa a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE”, modificada recientemente por el Reglamento (UE) 2024/1183¹⁹.

La primera, como es bien sabido, se refiere tanto a la protección de datos personales como a la libre circulación de datos, aunque en Italia esta última suele quedar relegada a un segundo plano. La segunda trata del reconocimiento mutuo de sistemas de identificación en línea, la autenticación y los servicios de confianza.

Hoy en día, la fuente normativa es europea, y el legislador europeo ha reescrito la legislación italiana sobre firma electrónica y documentos de información, así como la relativa a la protección de datos personales.

Como es bien sabido, Italia había regulado la firma digital, un tipo particular de firma electrónica, ya en 1997, con la Ley 59/97 y el posterior Decreto Presidencial 513/1997. Esta disciplina fue luego reescrita para hacerla compatible con la europea, que es de signo contrario, hasta llegar al actual marco jurídico dictado conjuntamente por el Reglamento e-IDAS y el Código de la Administración Digital.

El legislador europeo también reescribió las normas sobre protección de datos personales con el Reglamento (UE) 2016/679. Lo

europea...; Tosi (ed.), *Privacy Digitale...*; Zorzi ed., *Persona e mercato dei dati. Riflessioni sul GDPR* (CEDAM, 2019).

¹⁹ Publicado en el DOUE. L 257 de 28 de agosto de 2014. El reglamento se conoce comúnmente como “eIDAS”, donde “e” significa “electrónico”, “ID” significa “identificación”, “A” significa “autenticación” y “S” significa “firma”. Para un comentario, puede consultarse mi “Una prima lettura...”, 419 y ss., así como el volumen que he editado con Delfini, *Identificazione elettronica...* Permítanme referirme, también en relación con la reciente modificación del reglamento, al capítulo 5 de este volumen.

que queda del Código de Protección de Datos Personales, que ahora carece de organización, estructura y orden de un código, debería haberse derogado, también para promover la mayor claridad posible en el sistema de construcción de la protección de datos personales, como se ha ilustrado en varias ocasiones²⁰.

Por tanto, el papel del legislador europeo es construir el mercado europeo y hacer valer un modelo europeo también desde el punto de vista normativo.

Sin embargo, el legislador europeo se encuentra en una posición nada fácil: la de compatibilizar impulsos que parecen, al menos a primera vista, divergentes. Se trata, por una parte, de la valorización, también económica, de los datos personales y, más en general, de la información y, por otra parte, de la protección de los derechos fundamentales.

Así pues, el planteamiento es inevitablemente ambivalente: por un lado, se fomenta el mercado y, por otro lado, se restringe el mercado para proteger los derechos fundamentales. Sin embargo, ambos intereses parecen conciliables y, de hecho, deben conciliarse construyendo un modelo europeo de circulación segura de datos e información, sin que prevalezca a priori y necesariamente uno u otro requisito.

La protección de la persona y la construcción del mercado digital europeo²¹ constituyen el doble objetivo que debe alcanzar el legislador europeo también en relación con el tema de mayor actualidad, el del desarrollo de la inteligencia artificial. Se trata del “espacio europeo de datos” ya mencionado en la Comunicación

²⁰ Consúltese el volumen que he editado, *La protezione dei dati personali*....

²¹ Véase, Zorzi, *Persona e mercato dei dati*.... Sobre el mismo tema, véase también Ricciuto, “La patrimonializzazione dei dati personali...”, 689-726.

de la Comisión Europea “Inteligencia Artificial para Europa”²² en el que la necesidad de disponer de datos personales se contrapone a la necesidad de garantizar el pleno respeto de la ley sobre la protección de estos²³.

En efecto, como es bien sabido, la inteligencia artificial se basa en los datos.

²² Comunicación de la Comisión Europea, *Inteligencia Artificial para Europa*, COM(2018) 237 final, 25 de abril de 2018, 11.

²³ Así también COM(2018) 795 y anexo, titulado *Plan coordinado para el desarrollo y el uso de la inteligencia artificial “Made in Europe”*, 14. En el mismo sentido, la Resolución del Parlamento Europeo de 12 de febrero de 2019, en la que se pide “a la Comisión que vele porque todo futuro marco reglamentario de la UE sobre inteligencia artificial garantice la privacidad y la confidencialidad de las comunicaciones, la protección de los datos personales, incluidos los principios de legalidad, equidad y transparencia, la protección de datos y por defecto, la limitación de la finalidad, la limitación del almacenamiento, la precisión y la minimización de los datos, respetando plenamente el Derecho de la Unión en materia de protección de datos”. A este respecto, cabe mencionar también la Resolución del 21 de enero de 2020 por la Comisión de Mercado Interior y Protección del Consumidor del Parlamento Europeo, que reitera la importancia de que los sistemas de inteligencia artificial utilicen conjuntos de datos imparciales y de alta calidad y “algoritmos explicables e imparciales” para confianza y la aceptación de los consumidores, 5. Por último, el Comité Económico y Social Europeo también se ha pronunciado sobre esta cuestión en su dictamen *Creación de confianza en la inteligencia artificial creada por el hombre*, publicado en el DOUE de 11 de febrero de 2020, donde recomienda “anticipar, prevenir e impedir el uso malintencionado la IA y el aprendizaje automático” y “desarrollar un enfoque de la IA que sitúe al ser humano (“antropocéntrico”) en el centro y esté en consonancia con los valores en los que se fundamenta la Unión como, por ejemplo, el respeto de la dignidad humana, la libertad, la democracia, la igualdad y la no discriminación, el Estado de Derecho, y el respeto de los derechos humanos”.

3. LA INTELIGENCIA ARTIFICIAL Y SUS IMPLICACIONES JURÍDICAS

“La inteligencia artificial no es ciencia ficción: ya forma parte de nuestras vidas”²⁴. Como ya se ha mencionado, la Comisión ha dedicado numerosos estudios y profundizaciones al tema, empezando por la conocida Resolución del Parlamento Europeo de 16 de febrero de 2017 con recomendaciones a la Comisión sobre las disposiciones de Derecho civil en materia de robótica, que también se recuerda por su cita de las leyes de Asimov²⁵.

Las aplicaciones de inteligencia artificial pueden tener un gran impacto en determinadas instituciones jurídicas.

Se ha planteado, por ejemplo, la cuestión de si los *contratos inteligentes* son realmente jurídicamente vinculantes²⁶ y en qué sentido podrían modificar la institución de referencia. O si no son más bien modos de la ejecución de contratos celebrados de otro modo. De hecho, pueden una cosa u otra en función de las aplicaciones de que se trate.

Si se repasan los requisitos del contrato, según el código civil y en derecho viviente, no parece necesario ir más allá de las categorías establecidas, ni inventar otras nuevas. La identificación de las partes, las técnicas de imputación de la voluntad, el conocimiento del contenido del contrato celebrado “por ministerio de

²⁴ Así, la Comisión Europea en su Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Inteligencia Artificial para Europa*, COM(2018) 237, de 25 de abril de 2018, 1.

²⁵ Como se ha señalado anteriormente en este volumen, en la resolución, el punto (t) dice lo siguiente: “Las leyes de Asimov deben considerarse dirigidas a los diseñadores, fabricantes y usuarios de robots, incluidos los robots con autonomía incorporada y capacidad de autoaprendizaje, ya que estas leyes no pueden convertirse en código máquina”.

²⁶ Véase Di Giovanni, “Attività contrattuale...”, 1677-1686.

la ley”²⁷, la forma digital son temas ya explorados en profundidad por la doctrina y la jurisprudencia, y en algunos casos ya objeto de intervención normativa²⁸.

En otras palabras, con respecto a los *contratos inteligentes*, que, como se suele decir hoy en día, ni son inteligentes ni son contratos, hay que hacer un esfuerzo por comprender y matizar el fenómeno, pero no se necesitan nuevas normas.

Otra cuestión de gran relevancia es la de verificar el rigor de la copiosa normativa de protección de datos frente a las aplicaciones de inteligencia artificial. Como es bien sabido, la normativa europea, aunque bastante reciente, fue concebida antes de que el tema que nos ocupa tuviera la prevalencia actual y, sobre todo, no fue diseñada para grandes flujos de datos. Aplicar la base jurídica del consentimiento también al tratamiento de datos personales en aplicaciones de Big Data es una solución ineficaz tanto para el responsable del tratamiento, que se encuentra solicitando miles de consentimientos, como para el interesado, que da su consentimiento a un tratamiento cuyas finalidades sólo pueden formularse con un difícil ejercicio de equilibrio acrobático entre la generalidad, ya que no puede conocer todas las implicaciones de las aplicaciones de inteligencia artificial, y la especificidad exigida por la ley. El modelo parece inadecuado al fenómeno que debe regularse: se centra en los datos individuales en lugar de en el flujo de datos que debe gestionarse y gobernarse²⁹.

Una vez más, sin duda, también habrá que comprobar si el sistema de responsabilidad es adecuado para los nuevos casos de

²⁷ Se hace referencia aquí al famoso artículo de Cicu, “Gli automi...”.

²⁸ Me remito a mi “Il contratto...”, en el capítulo 5 de este volumen.

²⁹ Para una ilustración más amplia de esta tesis, véase mi trabajo “Intelligenza Artificiale e protezione dei dati personali”, *Giurisprudenza Italiana* (2019): 1670-1677, en el capítulo 4 de este volumen.

responsabilidad de los robots. De hecho, este es uno de los pocos ámbitos en los que es deseable una intervención reguladora. De hecho, si bien la Ley Modelo sobre Comercio Electrónico y la Ley Modelo de la CNUDMI sobre Contratación Automatizada de julio de 2024, la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, son aplicables a los *contratos inteligentes* además de las normas generales sobre contratos, los Principios de los Contratos Comerciales Internacionales del UNIDROIT y numerosas directivas europeas y, por tanto, sólo sería necesario un esfuerzo interpretativo y comunicativo, y, eventualmente, un ajuste del lenguaje³⁰. En cambio, por lo que respecta a las cuestiones relativas a la responsabilidad, se considera necesaria una intervención normativa sustancial³¹.

³⁰ Por ejemplo, el art. 12 de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales se refiere a los “sistemas automatizados de mensajes”, mientras que, hoy en día, en lo que respecta a los sistemas de inteligencia artificial, convendría referirse no sólo a “automáticos”, sino también a “autónomos”.

³¹ Ya en su Resolución de 16 de febrero de 2017, el Parlamento Europeo pidió a la Comisión “que proponga un marco jurídico coherente para el desarrollo de la robótica, incluidos los sistemas autónomos y los robots autónomos inteligentes”. Sobre la base de esta invitación, la Comisión Europea creó un grupo de expertos sobre inteligencia artificial. En su Resolución de 12 de febrero de 2019, el Parlamento Europeo reiteró entonces que “las normas y procedimientos existentes deben revisarse y, en su caso, modificarse para tener en cuenta la inteligencia artificial y la robótica (y que) el marco europeo para la IA debe desarrollarse respetando plenamente los derechos consagrados en la Carta de los Derechos Fundamentales y, en particular, los principios de protección de datos, privacidad y seguridad” (véanse los puntos (k) y (l) de la Resolución del Parlamento Europeo, de 12 de febrero de 2019, sobre una política industrial europea global sobre robótica e artificial). Como ya se adelantó en el capítulo 1 de este volumen, la formulación de un nuevo modelo de responsabilidad queda sustancialmente aplazada por el momento, ya que la Ley de IA se limita a estipular que el proveedor de un sistema de IA de alto riesgo debe garantizar

4. RETÓRICA

Existe una implicación en el discurso, incluido el discurso jurídico, sobre la inteligencia artificial. Esto es que la inteligencia artificial implica una entidad que expresa inteligencia. Si hay inteligencia, entonces, hay una entidad inteligente. Como siguiente paso en la narrativa o el razonamiento, a esta entidad se le atribuye subjetividad.

En otras palabras, se supone implícitamente que si hay una inteligencia (aunque sea artificial), debe haber un sujeto inteligente (aunque sea artificial) del que emane esa inteligencia.

Bien, incluso el uso del término “inteligencia” es condicionante. De hecho, la inteligencia se atribuye a los seres humanos o a los animales.

Por tanto, utilizar este término ya induce a desarrollar la narración en términos antropomórficos.

Se cree que, si las aplicaciones de la inteligencia artificial son inteligentes, entonces, hay un ser humano o animal al que debe atribuirse la inteligencia.

Las palabras utilizadas, como siempre, condicionan el discurso y el razonamiento. En su lugar, hay que despejar el campo de prejuicios, encontrar la página en blanco y, a continuación, cuestionar la subjetividad.

La perspectiva es diferente si, por el contrario, se asume con Turing que, más que definir lo que es la inteligencia, hay que comparar los resultados de un proceso. Si el proceso se califica

que el sistema cumple los requisitos del reglamento, mientras que la mencionada propuesta de “Directiva sobre la adaptación de las normas de derecho de daños a la inteligencia artificial” adopta un enfoque de armonización mínima, centrándose en las normas de responsabilidad basadas en la culpa que rigen la carga de la prueba de quienes solicitan una indemnización por los daños causados por los sistemas de IA.

de inteligente cuando lo realiza un ser humano, entonces, puede calificarse de inteligente si lo realiza una máquina³². Así pues, la inteligencia artificial puede definirse como la ciencia de hacer que los ordenadores hagan cosas que requieren inteligencia cuando las hacen los humanos.

Parece un enfoque metodológico menos engañoso y condicionante, en comparación con otros métodos adoptados a menudo sin plena conciencia metodológica, y que no conduce a suposiciones implícitas de subjetividad al comparar los resultados de dos procesos: si el primero se califica de inteligente, también se dará la misma calificación al segundo.

Es útil y de hecho necesario depurar el discurso de la retórica que inevitablemente lo puebla. De este modo, el caso puede esbozarse con neutralidad y sin “prejuicios”.

Una cosa es decir que un robot inteligente ha funcionado de una determinada manera, y otra muy distinta es decir que una aplicación de inteligencia artificial basada en *software* ha producido un determinado resultado. Las palabras utilizadas y la narrativa elegida pueden conllevar un condicionamiento. Basta pensar en los casos en que el cine y la literatura han humanizado robots y programas que, sin duda, no habrían tenido el mismo atractivo sin nombres, rostros y voces sensuales.

³² Se hace referencia método del Juego de Imitación, desarrollado por Alan Turing, al que el autor dedica el primer párrafo de su “Computing Machinery...”, 433-460. Como ya se ha ilustrado en este volumen, la prueba fue ideada por Turing para determinar si una máquina es capaz de pensar, es decir, de establecer conexiones, concatenar ideas y expresarlas. Como ya se ha ilustrado en este volumen, la *prueba* fue ideada por Turing para determinar si una máquina es capaz de pensar, es decir, capaz de establecer conexiones, concatenar ideas y expresarlas. La *prueba* se basa en la evaluación de la capacidad de un ordenador para imitar el comportamiento de un ser humano: en caso de resultado positivo, la máquina debe considerarse capaz de pensar de forma equivalente o, en cualquier caso, indistinguible de un ser humano.

El término “inteligencia” o “listo” conduce inevitablemente a la antropomorfización del discurso.

5. NUEVAS CUESTIONES RELATIVAS A LA RESPONSABILIDAD

Ahora, despejando la retórica, se trata de programas informáticos que realizan determinadas actividades para las que han sido programados. Hasta aquí, nada nuevo con respecto a lo conocido. La responsabilidad por el mal funcionamiento del programa o por los daños causados por el mismo debe atribuirse, según las reglas conocidas, al autor del programa o al productor, de acuerdo con las normas sobre responsabilidad civil y responsabilidad por productos defectuosos³³. No está de más recordar que también en relación con el tema de los daños causados por programas informáticos tuvo lugar hace algunos años una investigación doctrinal similar³⁴, en la que, en su momento como ahora, se estaba investigando quién debía responder de los daños causados por el *software*³⁵.

³³ Sobre las normas de responsabilidad aplicables a la inteligencia artificial, Ruffolo, *Intelligenza artificiale e responsabilità*.

³⁴ Véase Alpa, “Responsabilità extracontrattuale ed elaboratore elettronico”, *Diritto dell'informazione e dell'informatica* (1986): 387-393; Rossello, “La responsabilità da inadeguato funzionamento di programmi per elaboratore elettronico: aspetti e problemi dell'esperienza nord-americana”, *Computers e responsabilità civile*, ed. Alpa (Giuffrè, 1985), 87-142; Trialles, “L'applicazione della direttiva comunitaria sulla responsabilità del produttore nel campo del software”, *Diritto dell'Informazione e dell'Informatica* no. 2 (1990): 724-735.

³⁵ En un contexto, ya en los años noventa, la CNUDMI, a propósito de la celebración automática de contratos y de los llamados “agentes”, afirmó que el principio de imputación de responsabilidad bien puede aplicarse a los “agentes electrónicos”, incluso en el caso en que actúen no sólo de forma automática, sino también autónoma, de modo que se demostraría preferir una operación de clarificación e interpretación más que de innovación normativa. Véase Naciones Unidas, Asamblea General, *Aspectos jurídicos del comercio electrónico*, A/CN.9/WG.IV/WP.95, párrs. 71-73.

Lo novedoso hoy en día, es el caso en el que existe cierta autonomía decisoria en el programa, o incluso cuando existe imprevisibilidad en los resultados, es decir, cuando el método utilizado para alcanzar el resultado no es determinista. Es el caso, por ejemplo, de las aplicaciones de inteligencia artificial consistentes en modelos de aprendizaje automático que utilizan redes neuronales y algoritmos de aprendizaje profundo³⁶, a veces denominados algoritmos de “caja negra”, que también constituyen un nuevo tipo de riesgo en el mundo financiero³⁷. Sin embargo, los riesgos de caja negra pueden limitarse, según el mencionado informe del Grupo de Expertos sobre Obstáculos Normativos a la Innovación Financiera, con un enfoque que implique contextualmente la representación del

³⁶ Los distintos tipos de aprendizaje automático se ilustran mediante el Grupo de Expertos en Obstáculos Reglamentarios a La Innovación Financiera (RO-FIEG), *30 Recommendations...*, 28, que define el *deep learning* como un tipo de *machine learning* que utiliza redes neuronales. Incluso la Comisión Europea, en la citada Comunicación “Inteligencia Artificial Europa”, habla del aprendizaje profundo como “un elemento revolucionario la inteligencia artificial, que ha dado lugar a una increíble mejora del rendimiento en tareas específicas como el reconocimiento de imágenes o del habla o la traducción automática”. Entrenar un algoritmo de aprendizaje profundo para clasificar objetos significa proporcionarle un gran número de ejemplos etiquetados (por ejemplo, imágenes) que estén correctamente categorizados (por ejemplo, imágenes de aviones). Una vez entrenados, los algoritmos pueden clasificar correctamente objetos que nunca han visto, en algunos casos con una precisión que supera la humana. El uso de grandes conjuntos de datos y una capacidad de procesamiento sin precedentes han permitido avances significativos en estas tecnologías”, 11. Por otro lado, “el aprendizaje automático, un tipo de IA, funciona identificando patrones a partir de los datos disponibles y aplicando después este conocimiento a nuevos datos. Cuanto mayor sea el conjunto de datos, más precisa será la identificación de relaciones, incluso imperceptibles, entre los datos. Cuando se trata de utilizar la inteligencia artificial, los entornos con gran cantidad de datos también ofrecen las mayores oportunidades, porque los datos son el medio a través del cual el algoritmo aprende e interactúa con su entorno”, 10.

³⁷ Cfr. el *Informe...*, 11 y 39.

conocimiento, el aprendizaje profundo, el aprendizaje automático y el procesamiento del lenguaje natural³⁸.

La complejidad puede depender del número de datos que haya que procesar y analizar, y de la forma en que se establezcan las conexiones, a través de las llamadas redes neuronales.

En este caso, el autor, el productor, el vendedor, el usuario del programa y, en general, las partes que se benefician de la aplicación no pueden prever *a priori* el resultado.

Se plantea, pues, el problema de la atribución de la responsabilidad jurídica en caso de daños causados por la aplicación. Si la cuestión se plantea con la legislación vigente, se aplicarán, con un necesario esfuerzo interpretativo, las normas sobre responsabilidad civil y responsabilidad del productor³⁹.

³⁸ Cfr. el citado *Informe...*, 31. Se utiliza la expresión “computación perceptiva”, que implica el uso de sofisticados sistemas de reconocimiento para el análisis predictivo: “En el paradigma de la computación perceptiva, los modelos/algoritmos intentan emparejar las entradas digitales entrantes (y comprometer la cognición asociada) con categorías digitales previamente etiquetadas. A continuación, pueden emplearse modelos predictivos en forma de “si A, entonces B”. Un caso de uso podría ser el reconocimiento facial o los modelos biométricos (por ejemplo, que llevan a cabo evaluaciones de riesgo con fines de seguros” (también en el *Informe...*, 28-29).

³⁹ La relación entre responsabilidad civil e inteligencia artificial se examina adecuadamente en Ruffolo y Gabrielli, “Artificial Intelligence...”. En particular, véanse las contribuciones de Costanza, “L’intelligenza artificiale...”, 1686-1689, que identifica la responsabilidad en cabeza de la parte más próxima al hecho dañoso causado por la aplicación de la inteligencia artificial, tocando un tema también ampliamente explorado por Franzoni, “La ‘vicinanza della prova’...”, 360 y ss.; por Ruffolo, “Intelligenza artificiale, machine learning...”, 1689-1704, que examina las posibilidades de identificar y calificar la responsabilidad de la inteligencia artificial a la luz del Código, examinando también las hipótesis de reconocimiento de personalidad; por Gambini, “Algoritmi e sicurezza...”, 1726-1740, que aborda la seguridad en el sector de la inteligencia artificial examinando las soluciones ya existentes y adoptadas en el ámbito de los servicios de la sociedad de la información y del tratamiento automatizado de datos personales.

Si, por el contrario, la investigación se lleva a cabo en un intento de definir nuevas normas y modelos, hay que tener en cuenta, en primer lugar, que hay quienes proponen reconocer una subjetividad jurídica al programa y, en consecuencia, atribuirle responsabilidad⁴⁰. Esta posibilidad también se menciona en la Resolución del Parlamento Europeo de 16 de febrero de 2017, en la que se invita a la Comisión Europea a considerar “el establecimiento de un estatuto

Con especial referencia al tema de la responsabilidad civil de los denominados *coches autónomos*, véase Al Mureden, “Autonomous cars...”, 895-924.

El libro editado por Pizzetti, *Artificial intelligence...*, y, en particular, la contribución de Bassini, Liguori y Pollicino, *Sistemi di Intelligenza Artificiale...*, profundiza también en la cuestión de la responsabilidad derivada de las aplicaciones de los sistemas de inteligencia artificial. *Verso nuovi paradigmi?*, 333-371, en el que los autores ofrecen una panorámica de las diferentes orientaciones expresadas por la doctrina y la jurisprudencia en relación con la cuestión de la responsabilidad civil y penal derivada de los posibles daños causados por los sistemas de inteligencia artificial; Massolo, “Responsabilità civile...”, 373-382, en cambio, valora la idoneidad del marco jurídico nacional y europeo para regular las relaciones civiles en la era de la inteligencia artificial.

Para una revisión de las cuestiones planteadas, véase también el volumen editado por De Franceschi y Schulze, *Digital Revolution...*, y, en particular, las contribuciones de Mazzini, “A System of Governance...”, 245-298; y de Mezzanotte, “Risk Allocation...”, 169-189; Rachum-Twaig, “Whose Robot Is It Anyway? Liability for Artificial-Intelligence-Based Robots”, *University of Illinois Law Review* (2020); Weber-Staiger, “New Liability Patterns...”, 197-214.

⁴⁰ Sobre el reconocimiento de la personalidad jurídica, Pagallo, *The Laws of Robots...*; Sartor, “Cognitive automata...”, 253-290; Teubner, “Rights of Non-Humans...”, 497-521. Teubner profundiza en el tema en el volumen *Soggetti giuridici digitali...*? En sentido contrario, sin embargo, Bertolini y Aiello, “Robot companions...”, 130-140; Bertolini, “Robots as Products...”, 214-247; Coppini, “Robotica e intelligenza artificiale...”, 713-739; Toffoletto, *IoT e intelligenza artificiale: le nuove frontiere della responsabilità civile (e del risarcimento)*, notas al margen de la conferencia “Artificial Intelligence and Early Application Profiles: Justicia, IoT y trabajadores” (Aula Magna del Palacio de Justicia de Milán), 17 de abril de 2018. Véase también mi contribución, “La conclusione del contratto...”, 500-509.

jurídico específico para los robots a largo plazo, de modo que al menos los robots autónomos más sofisticados puedan ser considerados personas electrónicas responsables de indemnizar por cualquier daño causado por ellos, así como posiblemente el reconocimiento de la personalidad electrónica de los robots toman decisiones autónomas o interactúan de forma independiente con terceros”⁴¹.

Sin embargo, esta solución no es más que una solución aparente que sucumbe al encanto retórico de la subjetividad de las aplicaciones de inteligencia artificial, sin llegar en realidad a una solución completa del problema. En efecto, aunque se reconociera la subjetividad jurídica de la aplicación, si se la considerara responsable, quedaría por resolver el problema de la indemnización por los daños causados. En efecto, el programa de inteligencia artificial no dispondría de ningún bien con el que indemnizar el daño. Por lo tanto, el problema de la indemnización quedaría sin resolver.

Se objeta que podría construirse un patrimonio reservado a la aplicación de la inteligencia artificial, precisamente con el fin de permitir la indemnización de los daños⁴². Sin embargo, si se quiere preservar un patrimonio para este fin, no es necesario construir el complejo edificio de la subjetividad del programa. Se puede, sin embargo, construir un patrimonio reservado a la indemnización de este tipo de daños.

Al término del seminario UNIDROIT-UNCITRAL, antes mencionado, se acordó que debía desarrollarse un nuevo modelo de responsabilidad. El nuevo modelo de responsabilidad debería estar completamente libre de condicionamientos subjetivos⁴³.

⁴¹ Véase el apartado 59, letra (f), de la Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho relativas a la robótica 2015/2103(INL).

⁴² Véase Pagallo, “Robotrust...”, 367-379; Sartor, “Gli agenti software...”, 465-499.

⁴³ También presente en la Resolución del Parlamento Europeo de febrero de 2017. Como se observa en Ruffolo, “Per i fondamenti di un diritto...”, 11-12: “No

Resulta engañoso e ineficaz intentar aplicar categorías y criterios de naturaleza subjetiva, como la malicia o la culpabilidad, a la aplicación informática a la que se atribuye subjetividad.

Si, por el contrario, se trata de atribuir una responsabilidad objetiva, sin después y sin culpa, entonces, la subjetividad de la aplicación de la inteligencia artificial es inútil. Alguien responderá independientemente de la subjetividad del programa. Una vez más, hay que detenerse en la ilusión de la solución fácil del problema.

Si se quiere construir un nuevo modelo normativo, la búsqueda del error, desde un punto de vista jurídico, parece igualmente poco útil. La búsqueda del error *a posteriori*, sin duda útil para quienes desarrollan programas informáticos, es muy costosa y no siempre tiene éxito cuando se trata de aplicaciones que funcionan de forma no determinista. Por lo tanto, el nuevo modelo de responsabilidad debería caracterizarse por ser una responsabilidad objetiva y colectiva, repartida entre varios sujetos, independientemente de la búsqueda infructuosa y lenta del error. Debería ser un modelo de asignación de riesgos.

Un principio que puede resultar de gran utilidad es el basado en la rendición de cuentas⁴⁴, es decir, la habilitación del sujeto en la responsabilidad del sujeto que se beneficia de la aplicación de la inteligencia artificial. Según este criterio, la parte más beneficiada responde adoptando las medidas necesarias para evitar el riesgo. Por lo tanto, la carga de adoptar medidas para evitarlo recae en la persona más cercana al riesgo y debe demostrar cómo ha tomado medidas para evitarlo.

parece estar completamente exento de cierta centralidad del elemento subjetivo de la negligencia como criterio de atribución de responsabilidad por lesiones causadas por robots *autodidactas*".

⁴⁴ Véase Costanza, "L'intelligenza artificiale...", 1689; Comandé, "Intelligenza artificiale...", 169-188. Sobre este punto véase también mi contribución, "L'accountability nel Regolamento ...". Véase también el capítulo 4 de este volumen.

Si se plantean nuevos modelos de regulación, conviene avanzar hacia un modelo de responsabilidad que sea un sistema puro de asignación de riesgos, prescindiendo de la búsqueda del error⁴⁵, y repartiendo los costes colectivamente entre las partes implicadas en la transacción económica⁴⁶, contemplando eventualmente la creación de un fondo o la formulación de mecanismos de seguro para las partes que puedan ser llamadas a indemnizar los daños.

⁴⁵ A favor de un régimen de responsabilidad objetiva está Vladeck, “Machines without principals...”, 117-150, quien, no obstante, aboga por la creación de la subjetividad pura de las aplicaciones autónomas.

⁴⁶ Para más detalles sobre la responsabilidad de la organización en su conjunto con respecto a la realización de actos, véase mi libro, *I contratti informatici...*, en particular 187 y ss. Calabresi ya habló de “responsabilidad de la empresa” en su obra “Some Thoughts...”, 449-553.

CAPÍTULO 7

INTELIGENCIA ARTIFICIAL Y DERECHOS DE AUTOR. SUGERENCIAS

La inteligencia artificial también plantea muchas cuestiones en relación con la aplicación de la legislación sobre derechos de autor, que se menciona aquí.

Si nos fijamos sólo en algunas de las cuestiones problemáticas y, en particular, en la protección jurídica de las obras generadas por inteligencia artificial, hay al menos dos cuestiones que abordar:

1. ¿Quién puede ser reconocido como autor?
2. ¿Cuál es el contenido creativo mínimo necesario para que la obra esté protegida?

A la primera pregunta, la jurisprudencia actual responde que es la persona física que, en este caso concreto, ha utilizado un programa de IA, siempre que tenga suficiente contenido creativo, en respuesta a la segunda pregunta.

Según el Tribunal de Internet de Pekín, que falló en una decisión de noviembre de 2023, una imagen generada por la inteligencia artificial puede ser protegida por derechos de autor y la contribución humana de dirigir el programa de IA es suficientemente creativa.

Merece la pena ilustrar dicha historia.

El actor Li había utilizado el programa de inteligencia artificial “Stable Diffusion” para crear una imagen de una mujer y la había publicado en una plataforma en línea, Xiaohongshu, como Instagram. El demandado, Liu, la utilizó sin permiso de Li en otra plataforma de contenidos, Baijiahao, propiedad de Baidu.

El Tribunal de Internet de Pekín consideró que la imagen generada por un sistema de IA estaba protegida por derechos de autor y condenó a Liu a pagar una indemnización de 500 yuanes (70,43 dólares), así como a disculparse públicamente.

El tribunal sostuvo que la imagen, producida por un sistema de IA, debía protegerse habida cuenta de la originalidad y la contribución creativa del autor, una persona física. En otras palabras, consideró que había un nivel suficiente de creatividad.

Según se informa, la aportación creativa consiste en la elección de los textos propuestos, la fijación de los parámetros y el diseño de la presentación. Hubo, dice, un esfuerzo continuo de ajuste y puesta a punto para crear una imagen que correspondiera a los gustos estéticos del creador y, si la obra refleja inversión humana del autor, debe estar protegida por los derechos de autor.

EE. UU. decidió lo contrario en el caso *Zarya of the Dawn* de febrero de 2023. La Oficina de Derechos de Autor sostuvo que, debido al funcionamiento del sistema de IA, el resultado de su actividad era impredecible y, por tanto, el supuesto autor nunca tuvo suficiente control sobre las imágenes así generadas como para ser considerado “el autor intelectual”.

También, en Estados Unidos, con sentencia de 18 de agosto de 2023, el Tribunal de Distrito de Columbia denegó la atribución de derechos de autor a una imagen generada de forma autónoma por una aplicación de IA según las instrucciones proporcionadas por

un usuario: el caso¹ se originó a partir de la solicitud de Stephen Thaler de registrar una obra creada por un sistema informático de su propiedad (“Creativity Machine”) indicando como autor al sistema informático. El juez estadounidense, sin embargo, confirmó la opinión de la Oficina de Derechos de Autor de Estados Unidos, según la cual no puede reconocerse la protección de los derechos de autor en ausencia de cualquier “orientación” por parte de un ser humano y, por tanto, el requisito, considerado fundamental, de la autoría humana.

En Australia, ha habido varias sentencias que niegan que un programa pueda ser considerado autor desde el punto de vista jurídico. En relación con las obras de compilación realizadas de forma independiente por programas informáticos, se ha afirmado que “la autoría es un elemento fundamental para determinar si existen o no derechos de autor” y que “no se puede conceder protección a la obra generada automáticamente como consecuencia del funcionamiento del programa informático que cartografía los datos”².

Los tribunales australianos también se enfrentaron al caso de Stephen Thaler, los que tuvieron que decidir si el sistema de IA de su diseño “DABUS” podía calificarse de “inventor” en virtud de la Ley de Patentes australiana. Sorprendentemente, tras la denegación por parte de la Oficina Australiana de Patentes, la solicitud de Thaler fue estimada por el juez Beach del Tribunal Federal Australiano, según el cual una solución interpretativa que reconociera al sistema de IA como “inventor”, al tiempo que lo excluyera de ser el solicitante de

¹ Caso 22-1564, Stephen Thaler contra el Registro Derechos de Autor y Directo de la Oficina de Derechos de Autor de los Estados Unidos.

² Cabe destacar los casos Telstra c. Phone Directories, resuelto por el Tribunal Federal de Australia en noviembre de 2015, y IceTV Pty Ltd. c. Nine Network Australia Pty Ltd, resuelto por el Tribunal Superior de Australia en abril de 2009.

la patente o el beneficiario de los ingresos resultantes, sería acorde no sólo con la ley, sino también con la realidad tecnológica y el fomento de la innovación. El Tribunal Federal está compuesto por cinco jueces; sin embargo, el llamado Tribunal Plenario desvirtuó posteriormente el fallo del juez: “La ley relativa al derecho de una persona a la concesión de una patente se basa en la premisa de que, a efectos de la Ley de Patentes, una invención surge de la mente de una persona o personas físicas. Tienen derecho a la concesión quienes contribuyen al concepto inventivo o lo aportan. La concesión de una patente de invención recompensa su ingenio”. Así reza la decisión³. Se estableció así una orientación acorde con la de Estados Unidos y Thaler no ha sido el único que ha presentado su solicitud en muchas partes del mundo, incluso en la Unión Europea, viendo siempre reafirmado que el inventor es una persona humana⁴.

En Italia, la cuestión fue abordada sólo incidentalmente por el Tribunal de Casación, Auto N.º 1107 de 16 de enero de 2023, relativo a un caso de explotación ilícita de una obra de arte que había sido creada con un sistema IA. Aunque el Tribunal no se pronunció sobre el fondo del asunto en cuanto a si se trataba o no de una obra protegida por derechos de autor, afirmó que la obra era una obra de arte.

Se ha sostenido que la utilización de un programa informático en el proceso creativo de una imagen no basta para negar el carácter creativo de una obra de arte y que dicha utilización sólo requiere un examen más riguroso del índice de creatividad, encaminado a

³ Así pues, apartado 105 de la sentencia, con fecha de 13 de abril de 2022 y disponible en <https://www.wipo.int/wipolex/en/text/588126> (consultado el 24 de junio de 2024).

⁴ En este sentido, entre otros, las autoridades del Reino Unido y la Oficina Europea de Patentes, con una resolución confirmada por la Sala de Recursos de la Oficina Europea de Patentes el 21 de diciembre de 2021.

“comprobar si, y en qué medida, la utilización del instrumento ha absorbido la elaboración creativa del artista que se sirvió de él”. En otras palabras, si, al término de esta evaluación fáctica, se considera que la contribución humana prevalece sobre la de la máquina, podría concederse la protección autoral a la persona que hizo uso del instrumento.

La legislación británica sobre derechos de autor, aunque no se refiere explícitamente a las denominadas “obras generadas por IA”, regula las obras generadas por ordenador, y se las define como “obras que se generan en circunstancias tales que no hay un autor humano de la obra”⁵.

Respecto a la titularidad de los derechos de autor derivados de la producción de estas obras, los tribunales británicos han tenido ocasión de pronunciarse, estableciendo cómo debe entenderse que esta protección debe otorgarse al creador del sistema identificado como “la persona por la que se llevan a cabo las disposiciones necesarias para creación de la obra”⁶. En otras palabras, según la jurisprudencia británica, el autor es la persona que ha proporcionado las instrucciones y los datos necesarios para controlar, así como acondicionar la máquina con el fin de producir un determinado resultado, mientras que la titularidad de derechos de autor se niega al simple usuario de la propia máquina que se limita a proporcionar datos no creativos⁷.

⁵ Así, la Ley de Derechos de Autor, Diseños y Patentes del Reino Unido, sección 178 “Definiciones menores”.

⁶ Así, Ley de Propiedad Intelectual, Diseños y Patentes, art. 9(3).

⁷ Conviene recordar, en particular, la sentencia *Nova Productions Ltd. v. Mazooma Games Ltd.*, en la parte en la que el Tribunal británico se expresa en relación con la identificación del autor de las imágenes que componen la parte visual de un videojuego: “En la medida en que cada fotograma compuesto es una obra generada por ordenador, los preparativos necesarios para la creación de la obra fueron llevados a cabo por el Sr. Jones, porque él ideó la apariencia de los diversos

El índice de creatividad sólo puede evaluarse caso por caso, incluso cuando la obra es generada por un sistema de inteligencia artificial.

En el ámbito de la UE, la Comisión Europea, en su informe *Trends and Developments in Artificial Intelligence* de 2020, había identificado una serie de criterios para el reconocimiento de la protección de los derechos de autor para una obra creada con la ayuda de la IA, incluida la necesidad de un esfuerzo intelectual humano y una elección libre y creativa por parte del autor⁸. Esta orientación se reiteró en febrero de 2022, cuando el *Estudio sobre derechos de autor y nuevas tecnologías* señaló que, a la luz de las investigaciones llevadas a cabo, “debería mantenerse la actual solución de compromiso dentro de la legislación sobre derechos de autor, según la cual no existen derechos de autor en ausencia de elecciones creativas humanas”⁹. En su resolución de 20 de octubre de 2020 sobre los

elementos del juego y las reglas y la lógica por las que se genera cada fotograma y escribió el programa pertinente. En estas circunstancias, estoy convencido de que el Sr. Jones es la persona que llevó a cabo los preparativos necesarios para la creación de las obras y, por lo tanto, se le considera autor en virtud del artículo 9, apartado 3” (apartado 105). Al mismo tiempo, el Tribunal excluye a los jugadores del *videojuego* de la calificación de autores, aunque las imágenes de la pantalla también dependen en cierta medida de la aportación del jugador. El Tribunal señaló a este respecto: “Su aportación no es de naturaleza artística y no ha aportado ninguna habilidad o trabajo de tipo artístico. Tampoco ha llevado a cabo ninguno de los preparativos necesarios para la creación de los fotogramas. Lo único que ha hecho es jugar” (apartado 106).

⁸ Comisión Europea, *Trends and Developments in Artificial Intelligence. Challenges to the Intellectual Property Rights Framework*, septiembre de 2020, 77-84, disponible en <https://op.europa.eu/en/publication-detail/-/publication/394345a1-2ecf-11eb-b27b-01aa75ed71a1/language-es> (consultado el 24 de junio de 2024).

⁹ Comisión Europea, *Study on copyright and new technologies: copyright data management and artificial intelligence*, febrero de 2022, 273, disponible en <https://op.europa.eu/en/publication-detail/-/publication/cc293085-a-4da-11ec-83e1-01aa75ed71a1/language-es> (consultado el 24 de junio de 2024).

derechos de propiedad intelectual para el desarrollo de tecnologías de inteligencia, el Parlamento Europeo declaró que los resultados generados por la IA deberían protegerse dentro del marco jurídico de los derechos de propiedad intelectual.

Más allá de las respuestas aportadas por los distintos ordenamientos jurídicos actuales, debemos preguntarnos si la idea de autor, incluso antes de las normas sobre protección de los autores, es adecuada para dar cabida a nuevas formas creativas, como las generadas por o con inteligencia artificial.

En Occidente, y sobre todo en Europa, hemos introyectado en cambio una idea romántica del autor. El autor es una persona física, a la que debe dirigirse el reconocimiento de la actividad creadora.

La legislación continental sobre derechos de autor, que se originó en el siglo XIX, establece implícita o explícitamente que el autor es un ser humano, al que se conceden derechos morales y patrimoniales. El concepto de creatividad también se entiende implícitamente estrechamente vinculado a la persona física.

Pero nada excluye que la autoría pueda ser sentida y luego formulada de manera diferente, incluso jurídicamente. Así ocurrió en otros momentos de la historia en los que ni siquiera la figura del autor era valorada, ni por la cultura de la época, ni, en consecuencia, por el derecho. Así que puede que, en el futuro, nos encontremos formulando paradigmas autorales y normativos diferentes más adecuados a los tiempos que vivimos.

Es una reflexión cultural, antes que jurídica, sobre el paradigma farisaico, el cual, luego, la ley podrá transponer.

Al hablar de IA surge con insistencia otra cuestión: la de los derechos sobre las obras que procesan las aplicaciones de inteligencia artificial.

En general, las aplicaciones de IA procesan datos. Lo hemos visto antes al tratar de datos personales y no personales. Por supuesto,

los datos y, por tanto, la información utilizada también pueden ser imágenes, fotografías, vídeo, audio. En todos los casos, puede tratarse de información legalmente protegida, que a veces está cubierta por más de un cuerpo de legislación protectora: por ejemplo, obras de arte, protegidas por derechos de autor; fotografías, protegidas por derechos de autor y también, en el caso de fotografías de personas, por el derecho a la protección de datos personales; información organizada, protegida por el derecho *sui generis* sobre bases de datos y archivos; bienes, protegidos por legislación específica; por no mencionar la información protegida para la seguridad nacional. Todos los tratamientos efectuados por las aplicaciones de IA están, como los efectuados por cualquier persona, sujetos a la legislación vigente, que debe identificarse cada cierto tiempo.

Por lo tanto, hay que preguntarse si las actividades realizadas por un sistema de IA cumplen la ley: por ejemplo, si las fotografías que alimenta son de libre uso. Dicho sea de paso, es irrelevante que estén disponibles en la web, ya que la disponibilidad *de facto* no coincide con la disponibilidad legal. Hay que comprobar si no existen derechos sobre las obras que hagan su utilización contraria a la legislación aplicable o si el titular de los derechos pertinentes, que en el ejemplo de las fotografías puede ser tanto el fotógrafo como la persona retratada, cada titular de derechos diferentes, ha manifestado su consentimiento al uso de la fotografía, incluso mediante contrato o licencia específica.

En este aspecto concreto, destacan las cada vez más populares licencias de la comunidad creativa. Permiten comunicar, de forma concisa y también mediante un lenguaje icónico, cuál es la estructura de derechos sobre una obra protegida por derechos de autor, favoreciendo así su circulación más rápida y, al mismo tiempo, conforme a la ley.

Por poner otro ejemplo, la polémica en la que el *New York Times* se opuso recientemente a OpenAI dejó claro que la información,

en este caso los artículos de prensa disponible en línea, no podía utilizarse para entrenar el sistema de IA.

La Ley de IA, en el reglamento europeo, que establece normas armonizadas sobre inteligencia artificial¹⁰, aborda esta cuestión estipulando que los proveedores de modelos de IA de uso general deben aplicar políticas para cumplir la legislación de la UE sobre derechos de autor, y elaborar y poner a disposición del público un resumen “suficientemente detallado” de los contenidos utilizados para el entrenamiento de los modelos¹¹.

La normativa europea actúa entonces sobre lo reconocible de los contenidos generados o manipulados por IA, una cuestión que se cruza naturalmente con la legislación sobre derechos de autor, ya que podría argumentarse que lo reconocible actúa como salvaguarda para proteger la creatividad humana.

En particular, la Ley de IA exige que los proveedores de sistemas de IA que generen contenidos sintéticos garanticen que dichos contenidos estén marcados en un formato legible por máquina y detectable como generado o manipulado artificialmente¹². Además, se espera que los usuarios de un sistema de IA que genere o manipule imágenes, contenidos de audio o vídeo que constituyan una “falsificación profunda” revelen que el contenido ha sido generado o manipulado artificialmente¹³. Además, se espera que los usuarios de sistemas que generen o manipulen textos publicados con el fin de informar al público sobre asuntos de interés público revelen que el texto ha sido generado o manipulado artificialmente, a menos que

¹⁰ Reg. (UE) 2024/1689, citado varias veces en este volumen.

¹¹ Art. 53 de la Ley de IA. Para la definición de “modelo de IA para fines generales” y el concepto de proveedor, véase el capítulo 3 de este volumen.

¹² Así, art. 50(2) de la Ley de AI. Para un análisis más detallado, véase el capítulo 3 de este volumen.

¹³ Así, art. 50(4) de la Ley de AI. Véase de nuevo el capítulo 3 de este volumen.

el contenido generado por IA haya sido sometido a un proceso de revisión humana o control editorial, y una persona física o jurídica ostente la responsabilidad editorial de la publicación del contenido¹⁴.

También el “AI bill”, el proyecto de ley gubernamental “sobre el tema de la inteligencia artificial”, aprobado en el Consejo de Ministros N.º 78 de 23 de abril de 2024 y actualmente en el Parlamento, aborda la identificación de los contenidos generados o modificados mediante sistemas de IA, previendo, a raíz de la Ley de AI, obligaciones de transparencia¹⁵.

Sin embargo, el proyecto de ley también aborda otra cuestión, la de la protección de las obras generadas con ayuda de la inteligencia artificial. Mientras que la Ley de IA no aborda esta cuestión, el proyecto de ley italiano, al modificar la ley de derechos de autor de 1941, por un lado, precisa el ámbito de protección, indicando que las obras protegidas son las obras de inteligencia “humana”, y, por otro lado, lo amplía expresamente a las obras “creadas con ayuda de herramientas de inteligencia artificial, siempre que sean fruto del trabajo intelectual del autor”¹⁶.

¹⁴ Así art. 50(4)(2).

¹⁵ Así, en particular, el art. 23 del proyecto de ley, bajo el epígrafe “Identificación de contenidos textuales, fotográficos, audiovisuales y radiofónicos producidos por sistemas de inteligencia artificial”.

¹⁶ Así, el art. 24 del proyecto de ley, que también introduce una extensión expresa de la disciplina de minería de textos y datos a la reproducción, así como de la extracción “de obras u otros materiales mediante modelos y sistemas de inteligencia artificial, también de carácter genérico”.

CAPÍTULO 8

INTELIGENCIA ARTIFICIAL EN EL PODER JUDICIAL*

1. EL ESCENARIO

La inteligencia artificial (IA) ya ha entrado en el mundo judicial: los sistemas de IA ya se han utilizado para la redacción de documentos judiciales; las aplicaciones de IA pueden, en algunas jurisdicciones, decidir en lugar del juez, y las investigaciones también se llevan a cabo mediante sistemas de IA.

Este escenario, que hasta hace algún tiempo hubiera parecido ciencia ficción, es ahora actualidad.

A decir verdad, el debut de la inteligencia artificial en el proceso se ha producido de forma un tanto desordenada. Son conocidos los casos en los que ChatGPT, que no es más que una de las aplicaciones de la inteligencia artificial, pero de momento la más famosa, al menos para el gran público, se ha convertido recientemente en protagonista también en el ámbito judicial, creando sentencias

* Este capítulo reproduce, con algunas adaptaciones y actualizaciones, el artículo publicado en *Rivista Trimestrale di Diritto e Procedura Civile* (2024): 425 y ss.

inexistentes. La aplicación, de hecho, había sido utilizada para redactar un documento judicial por un bufete de abogados y, como apoyo al documento que redactó para los abogados que la habían utilizado, creó sentencias puramente ficticias. Posteriormente, los abogados fueron condenados a pagar una multa de 5000 dólares por ello, así como a enviar una carta a los jueces a los que habían atribuido falsamente las decisiones para informarles de lo sucedido¹.

Esto también ha llevado a algunos colegios de abogados a reflexionar sobre el tema y ofrecer algunas orientaciones a los profesionales. El Colegio de Abogados de Florida ha publicado un dictamen sobre el uso de la IA por los abogados y las obligaciones de información resultantes². Recomendando, entre otras cosas, que los

¹ Esta es la orden emitida el 22 de junio de 2023 por el juez Castel, quien condenó a los abogados que habían utilizado ChatGPT en los tribunales haciendo referencia a precedentes judiciales inexistentes. El juez impuso una sanción total de 5000 USD, y ordenó el envío “por correo de primera clase” de una “carta dirigida individualmente a cada juez falsamente identificado como autor de las falsas [...] opiniones”.

Según el juez, “las normas vigentes imponen a los abogados la función de velar por la exactitud de sus escritos. [...] Levidow & Oberman P.C. (el Bufete Levidow) (colectivamente, Demandados) abandonaron sus responsabilidades cuando presentaron opiniones judiciales inexistentes con citas y citas falsas creadas por la herramienta de inteligencia artificial ChatGPT, y, luego, continuaron manteniendo las opiniones falsas después de que las órdenes judiciales pusieran en duda su existencia”.

² Se trata de la *Propuesta de Opinión Consultiva 24-1 sobre el uso por los abogados de Inteligencia Artificial Generativa*, publicada por el Colegio de Abogados de Florida el 13 de noviembre. Según Reuters, “además del requisito de que los abogados obtengan el consentimiento de sus clientes antes de utilizar IA, el comité también considerará si dicha IA está sujeta a los mismos requisitos de supervisión por parte del abogado que los asistentes que no son abogados, y si los honorarios de los abogados deberían ser más bajos cuando se utiliza IA. También estudiará si se debe permitir a los bufetes de abogados anunciar su IA generativa como superior o única, y si los abogados pueden animar a los clientes a confiar en los informes de diligencia debida generados por la IA”.

abogados informen a los clientes si utilizan sistemas de IA, obtengan su consentimiento y revisen los honorarios en consecuencia.

También, se ha ocupado del tema el Comité de Responsabilidad y Conducta Profesional (COPRAC) del Colegio de Abogados de California, que elaboró una *Guía práctica para el uso de la inteligencia artificial generativa en el ejercicio de la abogacía*. La premisa es que, aunque las “reglas de conducta profesional existentes son sólidas, y las normas de conducta cubren el panorama de cuestiones que presenta la IA generativa en sus formas actuales. [...] La IA generativa es una tecnología en rápida evolución que presenta cuestiones novedosas que podrían requerir una nueva regulación y normas en el futuro”. Las orientaciones prácticas representan un primer paso en esta dirección y pretenden ayudar a los abogados en los nuevos deberes éticos en el ámbito de la IA generativa. También, en este caso, las disposiciones se centran en las obligaciones de información a los clientes y la remodelación de los honorarios. Un abogado debe revisar todos los resultados de la IA generativa, incluidos, entre otros, el análisis y las citas de autoridad para comprobar su exactitud antes de su presentación al tribunal, y corregir cualquier error o declaración engañosa realizada ante el tribunal”, reza la *Guía*³.

Así, Sloan, “Florida bar weighs whether lawyers using AI need client consent”, Reuters, 16 de octubre de 2023, <https://www.reuters.com/legal/transactional/florida-bar-weighs-whether-lawyers-using-ai-need-client-consent-2023-10-16/> (consultado el 26 de junio de 2024).

³ *Guidance for the Use of Generative Artificial Intelligence in the Practice of Law* en el ejercicio de la abogacía, acompañada de la exposición de motivos del COPRAC, disponible en <https://aboutblaw.com/bbpZ> (consultada el 26 de junio de 2024).

En Estados Unidos, las iniciativas aquí descritas han ido acompañadas de la creación de grupos de trabajo dedicados a cuestiones de IA en Colegios de Abogados de muchos Estados, así como por la American Bar Association. Para una visión de conjunto, véase la reconstrucción ofrecida por la American Bar Association, que lleva a cabo una actividad de seguimiento de las iniciativas

En Europa, la Comisión de Nuevas Tecnologías de la *Fédération des Barreaux d'Europe*, la Asociación de Colegios de Abogados Europeos, elaboró en junio de 2023 las “directrices para que los abogados aprovechen al máximo las oportunidades que ofrecen los modelos lingüísticos y la inteligencia artificial generativa”.

Con el objetivo de “garantizar que los abogados europeos estén preparados para las nuevas tecnologías, de modo que puedan utilizar las herramientas de IA de forma responsable y de acuerdo con los principios que rigen la profesión”, la Comisión ha identificado siete criterios, entre los que se incluyen: conocer la tecnología, tener en cuenta sus limitaciones inherentes, utilizarla como una mera herramienta de apoyo, sin que sustituya “en modo alguno” el juicio y la capacidad del profesional, mantener una comunicación transparente con los clientes, y asumir la responsabilidad de los resultados.

Algunos jueces federales estadounidenses ya han dictaminado que los abogados deben especificar expresamente que han utilizado sistemas de inteligencia artificial para los asuntos en cuestión si han recurrido a ellos⁴. En particular, el juez Vaden del Tribunal de Comercio Internacional de los Estados Unidos relacionó la orden de revelación y la protección de la información confidencial, destacando el riesgo de que “los programas de inteligencia artificial generativa pongan en entredicho la capacidad del tribunal para proteger la información confidencial y de propiedad empresarial

emprendidas por los Colegios de Abogados estatales, disponible en https://www.americanbar.org/groups/centers_commissions/center-for-innovation/state-ai-task-force-information/ (consultado el 26 de junio de 2024).

⁴ Así se informa Merken, “Another US judge says lawyers must disclose AI use”, Reuters, 9 de junio de 2023, <https://www.reuters.com/legal/transactional/another-us-judge-says-lawyers-must-disclose-ai-use-2023-06-08/> (consultado el 26 de junio de 2024).

frente al acceso de terceros no autorizados”⁵. Este último aspecto reviste especial interés y aún no ha sido examinado en profundidad. Se refiere, en efecto, al caso en que existe información confidencial en los documentos, protegida por derechos de autor o de propiedad intelectual, y es objeto de tratamiento por sistemas de inteligencia artificial. Además del riesgo de que esta información no esté adecuadamente protegida, existe ciertamente también el peligro real de que pueda constituir la base del entrenamiento del sistema de inteligencia artificial, que podrá entonces utilizar esa información en otros procedimientos. Esto es también lo que parece haber ocurrido con el uso, sin permiso de los titulares de los derechos, del archivo del *New York Times* y otros periódicos para el entrenamiento de ChatGPT, lo que dio lugar, como es bien sabido, a un litigio entre el NYT y OpenAI.

La guía elaborada por el Colegio de Abogados de California también aborda este punto cuando afirma que “el abogado no debe introducir ninguna información confidencial del cliente en ninguna solución de IA generativa que carezca de protecciones adecuadas de confidencialidad y seguridad. El abogado debe anonimizar la información del cliente y evitar introducir detalles que puedan utilizarse para identificarlo”.

La razón de ser de esta disposición radica en que “los productos de IA generativa son capaces de utilizar la información introducida, incluidos los avisos y los documentos o recursos cargados, para entrenar a la IA, y también podría compartir la consulta con terceros o utilizarla para otros fines. Aunque el producto no utilice ni comparta la información introducida, puede carecer de una seguridad razonable o adecuada”.

⁵ Tribunal de Comercio Internacional de los Estados Unidos, *Order on Artificial Intelligence*, 8 de junio de 2023, 2, disponible en <https://www.cit.uscourts.gov/sites/cit/files/Order%20on%20Artificial%20Intelligence.pdf> (consultado el 26 de junio de 2024).

Esto también se aborda en las directrices europeas, que advierten lo siguiente: “La inclusión directa o indirecta de datos de clientes como parte de una solicitud en sistemas GenAI [acrónimo de inteligencia artificial generativa] puede no estar permitida debido al posible tratamiento posterior de la información contenida en la solicitud”.

Otro conocido perfil problemático relacionado con el uso de ChatGPT en la judicatura lo constituyen los casos de difamación basados en hechos completamente inventados y apoyados en la presentación de pruebas documentales construidas *ad hoc*. Este es, por ejemplo, el caso de Jonatan Turley, profesor de Derecho de la Universidad de Georgetown, que fue incluido en una lista de profesores acusados de insinuaciones sexuales hacia sus alumnas debido a una pura invención de ChatGPT, que también proporcionó un artículo, inexistente, en el *Washington Post* en el que se denunciaban las insinuaciones sexuales del profesor hacia una alumna. De nuevo, el recién elegido alcalde del condado australiano de Hepburn Shire, Brian Hood, tuvo que defenderse de acusaciones infundadas de corrupción después de que ChatGPT, al preguntarle por la vida del alcalde, afirmara que era corrupto, aportando una condena (puramente ficticia) de 30 meses por aceptar sobornos de un banco local. En realidad, Brian Hood había trabajado en el banco y había descubierto los casos de corrupción y no había participado en ellos, sino que los había denunciado. Por último, Mark Walters, locutor de radio de la emisora Armed American Radio, fue acusado de apropiación indebida de dinero de la Second Amendment Foundation, basándose en una reconstrucción de ChatGPT: en este caso, que ocurrió realmente, el locutor no estaba implicado en modo alguno.

Obviamente, esto provocó que se emprendieran acciones legales contra OpenAI, la empresa que produce ChatGPT.

Para evitar los riesgos de presentar documentos falsos, algunos grandes bufetes de abogados han prohibido uso de ChatGPT. No cabe duda, de hecho, de que en estos casos la responsabilidad recae siempre en el abogado que hacía uso del sistema de IA cuyo trabajo debía supervisar, del mismo modo que se supervisa el trabajo de los becarios y empleados de un bufete de abogados.

Más recientemente, también se está debatiendo el uso de la inteligencia artificial, que obviamente no coincide con el uso de ChatGPT, para decidir la suerte de un juicio.

A este respecto, conviene subrayar que la utilización de la inteligencia artificial en la actividad judicial es una actividad que debe mantenerse bien diferenciada de su mera digitalización. Esta última no es, desde luego, un tema nuevo, pues los abogados y magistrados conocen bien a estas alturas las alegrías y las penas del proceso telemático. Los sistemas expertos aplicados a la justicia también han sido muy discutidos y lo son desde hace muchos años: baste mencionar el precursor POLIS, el gran proyecto de publicación de las decisiones, hace más veinte años, en el Tribunal de Bolonia. Es bien sabido que la digitalización de la actividad judicial ha exigido algunas innovaciones legislativas importantes que, como mínimo, han regulado el documento informático, la firma, las copias digitales de documentos en papel y las copias impresas de documentos digitales. Esto también ha exigido replantearse el concepto de documento original y ha transformado la actividad de archivo de documentos⁶.

⁶ Para una reflexión sobre el enfoque italiano del tema, véase Finocchiaro, *La firma digitale...*. Para un resumen de la normativa y reflexiones sobre los documentos informatizados y la firma electrónica, véase Delfini y Finocchiaro, *Identificazione elettronica...*

Específicamente sobre el proceso telemático, véase Carpi, "Processo civile e telematica: riflessioni di un profano", *Rivista trimestrale di diritto e procedura civile* no. 2 (2000): 467 y ss.; Liccardo, "Introduzione al processo civile telemático",

Por otra parte, el uso inteligencia artificial en los juicios implica la realización de una actividad parcialmente autónoma por parte del sistema: la posible sustitución del juez por aplicaciones de inteligencia artificial se debate cada vez con más frecuencia. Esto se ha discutido, en particular, en relación con una iniciativa de Estonia para gestionar los procedimientos judiciales con la ayuda de la inteligencia artificial para los casos civiles con un valor de hasta 7000 euros y, en cualquier caso, con la provisión de intervención humana.

Las ventajas de utilizar inteligencia artificial o sistemas automáticos de toma de decisiones en el proceso parecen, a primera vista, evidentes: mayor rapidez y también mayor uniformidad de las decisiones⁷. Pero también existen muchos riesgos, que se mencionarán a continuación. Y quizá precisamente por los riesgos, el legislador francés modificó en 2019 el *Code de l'organisation judiciaire* introduciendo la prohibición de reutilizar los datos de identificación de los magistrados en las resoluciones judiciales con el fin o efecto de evaluar, analizar, comparar o predecir sus prácticas

Rivista trimestrale di diritto e procedura civile (2000): 1165 y ss.; Caponi, “Il processo civile telematico tra scrittura e oralità”, *Rivista trimestrale di diritto e procedura civile* 54, no. 4 (2015): 305 ss.; Zucconi, Galli y Fonseca, “L’incontro tra informatica e processo”, *Rivista trimestrale di diritto e procedura civile* no. 4 (2015): 1185 y ss.; Ruffini ed., *Il processo telematico nel sistema del diritto procedurale civile* (Giuffrè, 2019); Teoldi, “Il processo civile telematico tra logos e techne”, *Rivista trimestrale di diritto e procedura civile* (2021): 843 y ss.; Punzi, Sul processo civile telematico, *Rivista di diritto processuale* 77, no. 1 (2022): 1 y ss.; Graziosi, “Giurisdizione civile e nuove tecnologie”, *Il giusto processo civile* (2024), de próxima publicación.

⁷ Ya en 1989, se hizo hincapié en el potencial de la IA “para contribuir a un sistema jurídico más justo y eficaz”. Así, Berman y Hafner, “The potential of Artificial Intelligence to help solve the crisis in our legal system”, *Social Aspects of Computing* 32, no. 8 (1989): 928 y ss. La referencia era, por supuesto, al sistema jurídico estadounidense, “ampliamente considerado en estado de crisis, plagado de costes excesivos, largos retrasos e incoherencias que conducen a una creciente falta de confianza pública”.

profesionales reales o presuntas. De este modo, se descartó que los datos contenidos en las sentencias pudieran utilizarse para el entrenamiento de sistemas de inteligencia artificial, al tiempo que se asistía a la prohibición con una sanción penal⁸.

Por último, para completar el escenario de referencia, en muchos casos, se contempla ya el uso la inteligencia artificial para llevar a cabo una actividad previa o de reconocimiento. Últimamente, en nuestro país también, por citar una norma reciente en la materia, la Ley N.º 111, de 9 de agosto de 2023, de “Delegación del Gobierno para la revisión del sistema tributario”, donde se prevé expresamente su utilización para prevenir, combatir y reducir el fraude y la evasión fiscal.

2. EL MARCO REGLAMENTARIO ACTUAL

Actualmente, se reclama en muchos ámbitos una regulación general de la inteligencia artificial. No es posible tratar el tema en

⁸ Se trata, más concretamente, del art. 33 de la Ley N.º 2019-222, de 23 de marzo de 2019, de programación 2018-2022 y de reforma de la justicia, que reza así: “Los datos de identidad de los magistrados y de los miembros del Consejo no podrán ser objeto de una utilización que tenga por objeto o por efecto evaluar, analizar, comparar o predecir sus prácticas profesionales reales o supuestas. La violación de esta prohibición se castiga con las penas previstas en los artículos 226-18, 226-24 y 226-31 del Código Penal, sin perjuicio de las medidas y sanciones previstas por la Ley N.º 78-17 del 6 de enero de 1978, relativos a la informática, a los archivos y a las libertades”. La decisión del legislador francés se produjo supuestamente a raíz de la divulgación de un estudio que había detectado tendencias en las decisiones de algunos jueces sobre las solicitudes de asilo. Ofrece una reconstrucción del caso Galgani, “Considerazioni sui ‘precedenti’ dell’imputato e del giudice al cospetto dell’IA nel processo penale”, *Sistema penale* 15, no. 4 (2020): 91 y ss. Hay que tener en cuenta que el ordenamiento jurídico francés, con la *Loi N.º 2016- 1321 du 7 octobre 2016 pour une République numérique*, introdujo el principio de gratuidad general de la publicación de todas las resoluciones judiciales.

su conjunto en este documento⁹, pero cabe mencionar que, en lo que respecta a la aplicación de la inteligencia artificial al proceso, ya pueden encontrarse algunas referencias normativas.

En primer lugar, cabe mencionar la *Carta ética europea sobre el uso de la inteligencia artificial en los sistemas judiciales y ámbitos relacionados*, publicada en 2018 por la Comisión Europea. En esta, se identifica cinco principios para el uso de la inteligencia artificial en los sistemas judiciales y contiene un “estudio en profundidad sobre el uso de la inteligencia en los sistemas judiciales, en particular las aplicaciones de la inteligencia artificial para el tratamiento de decisiones y datos judiciales”. Los cinco principios identificados por la carta son el principio de respeto de los derechos fundamentales; el principio de no discriminación; el principio de calidad y seguridad; el principio de transparencia, imparcialidad y equidad; y, por último, el principio de “control del usuario”.

La carta, por tanto, exige ante todo que el desarrollo y el uso de sistemas de IA sean compatibles con los derechos fundamentales. “Cuando se utilizan herramientas de inteligencia artificial para resolver un litigio, proporcionar apoyo en el proceso de toma de decisiones judiciales, o proporcionar orientación al público, es esencial asegurarse de que no socavan las garantías del derecho de acceso a un juez y el derecho a un juicio justo (igualdad de armas y respeto del proceso contradictorio)”, reitera la carta, haciendo hincapié en la conveniencia de un enfoque de “ética desde el proceso” o de “derechos humanos desde el proceso”¹⁰.

⁹ Para un tratamiento orgánico del tema, remito a Finocchiaro, *Intelligenza artificiale. Quali regole?* (Il Mulino, 2024).

¹⁰ “Esto significa que”, explica la Carta, “ya desde las fases de elaboración y aprendizaje, están plenamente previstas normas que prohíben la violación directa o indirecta de los valores fundamentales protegidos por los Convenios”. La referencia es, en particular, al Convenio Europeo de Humanos y al Convenio

El segundo principio, el de no discriminación, pretende “prevenir específicamente el desarrollo o la intensificación de cualquier discriminación entre personas o grupos de personas” y fomentar “el uso del aprendizaje automático y del análisis científico multidisciplinar para contrarrestar dicha discriminación”.

Además, el principio de calidad y seguridad, según el cual “en lo que respecta al tratamiento de las resoluciones y datos judiciales”, “las fuentes certificadas y los datos intangibles deben utilizarse con modelos multidisciplinarios y elaborados en un entorno tecnológico seguro”. En la carta, se espera que los desarrolladores de modelos de aprendizaje automático hagan un amplio uso de la experiencia de los profesionales del sistema judicial, jueces, fiscales, abogados e investigadores en los campos del derecho y las ciencias sociales, economistas, sociólogos y filósofos, ya que la multidisciplinariedad es esencial para una mayor calidad y seguridad de los sistemas.

Por último, el principio de transparencia, imparcialidad y equidad, según el cual es necesario “hacer accesibles y comprensibles las metodologías de tratamiento de datos”, “permitir auditorías” y lograr “un equilibrio entre la propiedad intelectual de determinadas metodologías de tratamiento y la necesidad de transparencia (acceso al proceso creativo), imparcialidad (ausencia de prejuicios), equidad e integridad intelectual (dar prioridad a los intereses de la justicia)”, así como el principio de “control del usuario”, según el cual “debe excluirse un enfoque prescriptivo y los usuarios deben ser agentes informados que controlen sus decisiones.

Entre otras cosas, la carta también aborda el uso de herramientas de justicia predictiva por parte de los abogados señalando las ventajas y los peligros que supone para los abogados la aplicación de dichas herramientas. Entre las ventajas, “en particular, la posibilidad

relativo a la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

de proporcionar a los clientes un asesoramiento más informado gracias a la evaluación empírica y sistemática de la probabilidad de éxito de un procedimiento”. En cuanto a los riesgos, se señala que, debido a la baja probabilidad de éxito en juicio que puede detectar el sistema de IA, las personas que necesiten asesoramiento jurídico pueden verse privadas de él.

En el marco de la legislación vigente, ya el artículo 22 del 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, ahora conocido como “RGPD”, regula las decisiones automatizadas. No se trata de una norma *ad hoc* para el juicio, sino de una norma que, relativa a las decisiones automatizadas, puede aplicarse también al juicio¹¹.

¹¹ Para un análisis de la disposición, véase Goodman y Flaxman, “European Union Regulations on Algorithmic Decision Making and a ‘Right to explanation’”, *AI Magazine* 38, no. 3 (2017): 38 y ss., disponible en <https://doi.org/10.1609/aimag.v38i3.2741> (consultado el 26 de junio de 2024); Malgieri y Comandé, “Why a right to legibility...”, *International Data Privacy Law* 7, no. 3 (2017): 7 y ss., disponible en <https://ssrn.com/abstract=3088976> (consultado el 26 de junio de 2024); Caia, “Processo decisionale automatizzato compresa la profilazione”, en *GDPR e normativa privacy*, eds. Riccio, Scorza y Belisario (Ipsos, 2018), 219 y ss.; Moretti, “Algoritmi e diritti fondamentali della persona. Il contributo del Regolamento (UE) 2016/679”, *Diritto informazione e informatica* no. 1 (2018): 799 y ss.; Patti y Sesso Sarti, “Commento all’art. 22”, en *Commentario del Codice Civile Utet. Modulo delle Persone*, vol. II, eds. Gabrielli, Barba y Pagliantini (Utet, 2019), 460 y ss.; Ricci, “I diritti dell’interessato”, en *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, ed. Finocchiaro (Zanichelli, 2019), 392 y ss.; Lagioia-Sartor-Simoncini, “Art. 22”, en *Codice della privacy e data protection*, eds. D’orazio, Finocchiaro, Pollicino y Resta (Giuffrè, 2021), 378 y ss. El Grupo de Trabajo del Artículo 29 sobre Protección de Datos (GT29) también se ha pronunciado al respecto, en “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, disponible en <https://edpb.europa.eu/>

La disposición establece que “el interesado tendrá derecho a no ser objeto de una decisión basada únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar”.

Esto significa que la persona física cuyos datos personales se tratan tiene derecho a que la decisión que le concierna no sea tomada únicamente por sistemas automatizados.

Como aclara el Considerando 71, se trata, por ejemplo, del “rechazo automático de una solicitud de crédito en línea o de prácticas de contratación electrónica sin intervención humana”. Dicho tratamiento incluye la “elaboración de perfiles”, que consiste en una forma de tratamiento automatizado de datos personales que evalúa aspectos personales relativos a una persona física, en particular con el fin de analizar o predecir aspectos de su rendimiento profesional, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, localización o sus movimientos, cuando ello produzca efectos jurídicos sobre ella o la afecte de manera significativa de forma similar”.

No obstante, la disposición y los considerandos que la ilustran no excluyen la admisibilidad de decisiones automatizadas con el consentimiento del interesado o cuando el tratamiento esté expresamente previsto por el Derecho de la Unión o de los Estados miembros, por ejemplo, como aclara el mismo, “con fines de control y prevención del fraude y la evasión fiscal de conformidad con la normativa, normas y recomendaciones de las instituciones de la Unión o de los organismos nacionales de control y para garantizar la seguridad y fiabilidad de un servicio prestado por el responsable del tratamiento, o si es necesario para la celebración o ejecución de un contrato entre el interesado y un responsable del tratamiento”.

[our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en](#) (consultado el 26 de junio de 2024).

No obstante, “en cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, que deben incluir información específica al interesado y el derecho a obtener intervención humana, a expresar su opinión, a obtener una explicación de la decisión adoptada tras dicha evaluación y a impugnar la decisión”. Y nuevamente, “con el fin de garantizar un tratamiento leal y transparente con respecto al interesado, teniendo en cuenta las circunstancias específicas y el contexto en el que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, se rectifiquen los factores que dan lugar a inexactitudes en los datos y se reduzca al mínimo el riesgo de errores, así como para garantizar la seguridad de los datos personales de forma que se tengan en cuenta los riesgos potenciales para los intereses y derechos del interesado y se evite, entre otras cosas, la discriminación de las personas físicas por motivos de origen racial o étnico, opiniones políticas, religión o convicciones, afiliación sindical, situación genética, salud u orientación sexual, o el tratamiento que implique medidas que tengan tales efectos. La toma de decisiones automatizadas y la elaboración de perfiles basados en categorías especiales de datos personales sólo deben permitirse en determinadas condiciones”.

Así pues, el artículo 22 del RGPD prevé la necesidad de una intervención humana en la toma de la decisión, que no puede dejarse enteramente en manos del “sistema automatizado”, salvo excepciones específicas¹².

¹² Cabe señalar que, en el ámbito específico de la prevención, investigación, detección y enjuiciamiento de delitos y la ejecución de sanciones penales, la norma de referencia en materia de procesos automatizados de toma de decisiones el art. 11 de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes

La inteligencia artificial en los procedimientos se aborda en el Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre la inteligencia artificial, la llamada Ley de IA. El reglamento clasifica como sistemas de alto

para la prevención, investigación, detección y enjuiciamiento de delitos o la ejecución de sanciones penales, así como a la libre circulación de estos datos. El art. 11 de la Directiva incorpora parcialmente las disposiciones del art. 22 del RGPD. En particular, el art. 22, apartado 1, exige a los Estados miembros que dispongan que “se prohíba toda decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca un efecto jurídico adverso o afecte de forma significativa al interesado, a menos que esté autorizada por el Derecho de la Unión o por el Derecho del Estado miembro al que esté sujeto el responsable del tratamiento y que ofrezca garantías adecuadas para los derechos y libertades del interesado, incluido al menos el derecho a obtener la intervención humana por parte del responsable del tratamiento”. Por lo tanto, en el ámbito penal, como también señaló el Grupo de Trabajo sobre Protección de Datos (GT29) del Artículo 29, en su *Parere su alcune questioni fondamentali della Direttiva UE 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia*. La prohibición de tomar una decisión basada únicamente en un tratamiento automatizado relativo a personas físicas se aplica a la toma de decisiones que produce no solo un “efecto jurídico”, sino un efecto jurídico “negativo” sobre el interesado. “Un efecto negativo típico derivado de decisiones automatizadas” —señala el dictamen del WP29— “podría ser el refuerzo de las medidas de seguridad o de vigilancia por parte de las autoridades”. Sin embargo, el mismo artículo considera que esta prohibición también es válida en relación con una decisión que “afecte significativamente” a la persona afectada, por ejemplo, en el caso de que no se permita embarcar a un pasajero por estar incluido en una lista negra, de forma que se amplía el ámbito del art. 11. El adverbio “de manera significativa” excluye que los efectos menores puedan considerarse suficientes para aplicar la prohibición: el efecto debe ser lo suficientemente significativo como para merecer atención y afectar al interesado”. Además, dada la naturaleza específica del tratamiento con fines policiales, el art. 11 de la Directiva no contiene ninguna referencia a las excepciones establecidas en el art. 22, apartado 2, del RGPD. En este contexto, de hecho, “el consentimiento nunca podría funcionar como base jurídica, ya que existe un claro desequilibrio de poderes entre el interesado y el responsable del tratamiento” (así, el citado Dictamen del WP29, 12).

riesgo los sistemas de inteligencia artificial “concebidos para ser utilizados por una autoridad judicial o en su nombre para asistir a las autoridades judiciales en la investigación e interpretación de los hechos y del derecho y en la aplicación del derecho a un conjunto concreto de hechos o para ser utilizados de manera similar en la resolución alternativa de litigios”¹³.

La clasificación de los sistemas de IA aplicados a la actividad judicial como sistemas de alto riesgo tiene ciertas consecuencias. Evidentemente, permite su utilización, pero exige que cumplan una serie de requisitos establecidos en el reglamento, que, como es sabido, se basa en un modelo de gestión de riesgos que parte de la clasificación de los sistemas de inteligencia artificial en función del riesgo que presentan: sistemas con un riesgo inaceptable, sistemas de alto riesgo y sistemas de bajo riesgo o mínimos.

Por estas razones, el Reglamento Europeo sobre Inteligencia Artificial clasifica los sistemas de inteligencia artificial destinados a ser utilizados por la judicatura como sistemas de alto riesgo, con la consecuencia de que deben cumplir requisitos específicos en términos de rendimiento, precisión y solidez y someterse a verificación para poder introducirse en el contexto europeo¹⁴.

Las decisiones también deben ser suficientemente transparentes, explicables y documentadas.

El principio general de prohibición de decisiones totalmente automáticas ya figuraba, como se ha señalado, en el reglamento europeo de protección de datos, en el que se exigía la intervención humana.

Las razones que llevaron al legislador europeo a clasificar los sistemas de IA utilizados en el trabajo judicial como sistemas de alto riesgo están bien explicadas en los considerandos.

¹³ Así, el Anexo III, N.º 8, letra a), del reglamento.

¹⁴ En el capítulo 3 de este volumen, se ofrece una visión general de los requisitos y obligaciones de los sistemas de alto riesgo.

Preocupa el impacto en los derechos fundamentales de las decisiones adoptadas por las autoridades policiales y judiciales para la prevención, investigación, detección o enjuiciamiento de delitos, en particular si el sistema no se entrena con datos de alta calidad, si no cumple los requisitos adecuados en términos de rendimiento, precisión o solidez, o si no se diseña y prueba adecuadamente antes de su comercialización. El peligro es que se produzca un trato discriminatorio y que el uso de herramientas de IA se convierta en un factor de desigualdad, brecha social o exclusión. De hecho, en el Considerando 59, se afirma que “no deben ignorarse las repercusiones del uso de las herramientas de IA en el derecho de defensa de los sospechosos, en particular la dificultad de obtener información significativa sobre su funcionamiento y la consiguiente dificultad para refutar sus resultados ante los tribunales, especialmente en el caso de las personas investigadas”. El Considerando 61 destaca el riesgo de que los sistemas de IA creen “distorsiones, errores y opacidad potenciales”¹⁵.

¹⁵ Más concretamente, el Considerando 59 y Considerando 61 del reglamento rezan como sigue: “(59) Habida cuenta de su función y responsabilidad, la actuación de las autoridades policiales y judiciales en relación con determinados usos de los sistemas de IA es se caracteriza por un nivel significativo de desequilibrio de poder y puede conducir vigilancia, detención o privación de libertad de una persona física, así como tener otras repercusiones negativas sobre los derechos fundamentales garantizados en la Carta. En particular, el sistema de IA, si no se entrena con datos de alta calidad, si no cumple los requisitos adecuados en términos de rendimiento, precisión o solidez, o si no se diseña y prueba adecuadamente antes de su comercialización o puesta en de otro modo, puede identificar a personas de forma discriminatoria o de otro modo incorrecto o injusto. También, puede verse obstaculizado el ejercicio de importantes derechos procesales fundamentales, como el derecho a la tutela judicial efectiva y a un juez imparcial, así como los derechos de defensa y la presunción de inocencia, en particular, si tales sistemas de IA no son suficientemente transparentes, explicables y documentados. Por consiguiente, procede clasificar de alto riesgo, en la medida en que su uso esté permitido en virtud del Derecho de la Unión

Por último, el uso de la IA en la actividad judicial es objeto de

y nacional pertinente, una serie de sistemas de IA destinados a ser utilizados en el contexto de la aplicación de la ley, en el que la exactitud, la fiabilidad y la transparencia son especialmente importantes para evitar repercusiones negativas, mantener la confianza del público y garantizar la rendición de cuentas y la eficacia de los recursos. Habida cuenta de la naturaleza de las actividades y de los riesgos asociados a ellas, dichos sistemas de IA de alto riesgo deben incluir, en particular, los sistemas de IA destinados a ser utilizados por las autoridades policiales o en su nombre, o por organismos o entidades de la Unión en apoyo de las autoridades policiales para evaluar el riesgo de que una persona física sea víctima de un delito, como los polígrafos y herramientas similares, para evaluar la fiabilidad de las pruebas en el curso de la detección y persecución de delitos y, en la medida en que no lo prohíba el presente reglamento, determinar el riesgo de delito o reincidencia en relación con una persona física no sólo sobre la base de la elaboración de perfiles de personas físicas, sino también sobre la base de la evaluación de rasgos y características de la personalidad o del comportamiento delictivo anterior de personas físicas o grupos, a efectos de la elaboración de perfiles en el curso de la investigación, detección y enjuiciamiento de delitos. Los sistemas de IA destinados específicamente a ser utilizados en procedimientos administrativos por las autoridades fiscales y aduaneras, así como por las unidades de inteligencia financiera que realizan tareas administrativas de análisis de la información de conformidad con la legislación de la Unión contra el blanqueo de capitales, no deben clasificarse como sistemas de IA de alto riesgo utilizados por las fuerzas y cuerpos de seguridad para la prevención, detección, investigación y enjuiciamiento de delitos. El uso de herramientas de IA por parte de las autoridades policiales y otras autoridades pertinentes no debe convertirse en un factor de desigualdad o exclusión. No deben ignorarse las repercusiones del uso de herramientas de IA en el derecho de defensa de los sospechosos, en particular la dificultad de obtener información significativa sobre el funcionamiento de dichos sistemas y la consiguiente dificultad para refutar sus resultados ante los tribunales, especialmente en el caso de las personas investigadas”. “(61) Algunos sistemas de IA destinados a la administración de justicia y los procesos democráticos deben clasificarse como sistemas de alto riesgo, habida cuenta de su impacto potencialmente significativo en la democracia, el Estado de Derecho, las libertades individuales y el derecho a un recurso efectivo y a un juicio justo. En particular, para hacer frente a los riesgos de posibles distorsiones, errores y opacidad, deben clasificarse como de alto riesgo los sistemas de IA destinados a ser utilizados por una autoridad judicial o en su nombre para ayudar a las autoridades judiciales investigar e interpretar los hechos y el Derecho y a aplicar

intervención por parte del legislador nacional. Se hace referencia al artículo 14 de la Ley de Inteligencia Artificial aprobado por el Consejo de Ministros el 23 de abril de 2024 y remitido al Senado el 20 de mayo de 2024, donde se dice lo siguiente: “Los sistemas de inteligencia artificial se utilizan exclusivamente para la organización y simplificación del trabajo judicial, así como para la investigación jurisprudencial y doctrinal. El Ministerio de Justicia regulará el uso de los sistemas de inteligencia artificial por las oficinas judiciales ordinarias. Para otras jurisdicciones, el uso se regulará de acuerdo con sus respectivos sistemas”. Apartado 2: “La decisión sobre la interpretación de la ley, la valoración de los hechos y las pruebas y la adopción de cualquier medida queda siempre reservada al magistrado”.

3. JURISPRUDENCIA

La jurisprudencia italiana ha tenido ocasión de pronunciarse sobre decisiones adoptadas mediante algoritmos, que conviene recordar, aunque no se refieran precisamente al funcionamiento de los sistemas de inteligencia artificial. Algunas decisiones se

el Derecho a un conjunto concreto de hechos. Los sistemas de IA destinados a ser utilizados por entidades de resolución alternativa de litigios para tales fines también deben considerarse de alto riesgo cuando los resultados de los procedimientos de resolución alternativa de litigios produzcan efectos jurídicos para las partes. El uso de herramientas de IA puede apoyar el poder decisorio de los jueces o la independencia del poder judicial, pero no debe sustituirlo: el proceso decisorio final debe seguir siendo una actividad dirigida por el ser humano. Sin embargo, no procede ampliar la clasificación de los sistemas de IA como de alto riesgo a los sistemas de IA destinados a actividades administrativas puramente auxiliares que no afectan a la administración efectiva de justicia en casos individuales, como la anonimización o seudonimización de resoluciones judiciales, documentos o datos, la comunicación entre el personal y las tareas administrativas”.

referían, por ejemplo, a sistemas que utilizaban mecanismos opacos o discriminatorios.

Se trata, en particular, de los sistemas algorítmicos utilizados en el marco de los procedimientos relativos al personal docente de los centros de enseñanza, que fueron objeto de numerosas sentencias del Tribunal Administrativo Regional del Lacio¹⁶, algunas de las cuales llegaron posteriormente al Consejo de Estado.

Cabe considerar, en primer lugar, la decisión dictada por el Consejo de Estado en 2019¹⁷, cuando reformó la sentencia con la que el Tribunal Administrativo Regional del Lacio, en 2016, había desestimado el recurso de algunos profesores contra los resultados del procedimiento iniciado en aplicación del plan extraordinario de contratación conocido como “Buena Escuela”, gestionado mediante un sistema algorítmico. Los profesores se quejaban, en particular, de que se desconocía el funcionamiento del sistema, lo que daba lugar a medidas carentes de motivación, así como a resultados poco razonables¹⁸.

En esa ocasión, el Consejo de Estado afirmó algunos principios cardinales. En primer lugar, que “el mecanismo a través del cual se realiza la decisión robotizada (es decir, el algoritmo) debe

¹⁶ Además de las sentencias que se mencionan a continuación, cabe mencionar también Tar Lazio, sección III, 21 de marzo de 2017, N.º 3742, en la que se ordenó al Ministerio de Universidad y “entregar al demandante una copia de los códigos fuente del *software* del algoritmo de gestión procedimiento”; Tar Lazio, sección *III-bis*, 13 de septiembre de 2019, N.º 10964. 10964, en línea con el enfoque ya adoptado en las anteriores sentencias N.º 9924/2018 y N.º 6606/2019, según el cual “un algoritmo, aunque preestablecido de tal manera que tenga en cuenta las posiciones, calificaciones y puntuaciones personales, nunca puede asegurar la salvaguardia de las garantías procesales que los artículos 2, 6, 7, 8, 9, 10 de la Ley 7.8.1990, N.º 241 han proporcionado”.

¹⁷ Cons. St., sec. VI, 8 de abril de 2019, N.º 2270.

¹⁸ Tar Lazio, sec. *III-bis*, 1 de diciembre de 2016, N.º 12026.

ser ‘conocible’, según una declinación reforzada del principio de transparencia, que implica también el del pleno conocimiento de una norma expresada en un lenguaje distinto del jurídico. [...] En otras palabras, la ‘caracterización multidisciplinar’ del algoritmo (construcción que ciertamente requiere no sólo conocimientos jurídicos, sino también técnicos, informáticos, estadísticos y administrativos) no exime de la necesidad de que la ‘fórmula técnica’, que de hecho representa el algoritmo, sea acompañada de explicaciones que traduzcan en la ‘norma jurídica’ subyacente y la hagan legible y comprensible, tanto para los ciudadanos como para el juez”.

En segundo lugar, que “la regla algorítmica debe ser no sólo conocida en sí misma, sino también sujeta al pleno conocimiento, y a la plena revisión, del juez administrativo. Dicha exigencia responde, en efecto, a la irrenunciable necesidad de poder revisar cómo se ha ejercido concretamente la potestad, planteándose en última instancia como una directa declinación del derecho de defensa del ciudadano, al que no puede impedírsele conocer las modalidades (aunque sean automatizadas) con las que se ha adoptado concretamente una decisión destinada a afectar a su esfera jurídica”.

Esta orientación fue confirmada e integrada posteriormente. En 2019, de hecho, el Consejo de Estado volvió a ocuparse de la cuestión¹⁹. En este caso, el TAR había estimado el recurso interpuesto por los profesores²⁰. Las quejas del Tribunal Administrativo

¹⁹ Cons. St., sec. VI, 13 de diciembre de 2019, N.º 8472. En los mismos términos, Cons. St., sec. VI, 13 diciembre 2019, N.º 8473 y 8474. Sobre el tema véase Dalfino, “Decisione amministrativa robotica ed effetto performativo. Un beffardo algoritmo per una ‘buona scuola’”, *Questione Giustizia* 13 de enero de 2020. También aborda este tema Resta, “Governare l’innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza”, *Politica del diritto* 50, no. 2 (2019): 233.

²⁰ Tar Lazio, sec. III, 10 de septiembre de 2018, N.º 9230. En los mismos, Tar Lazio, sec. III, 10 de septiembre de 2018, N.º 9225 y 9227.

se referían, en particular, a la vulneración del principio de igualdad, así como a la vulneración del “principio fundamental de la instrumentalidad del uso de las tecnologías de la información en los procedimientos administrativos”. El plan extraordinario en el que se insertaba el procedimiento de movilidad —observó el TAR— no había ido acompañado de actividad administrativa alguna, sino que se había delegado en un algoritmo, “aún desconocido”.

La decisión del Consejo de Estado, que confirmó la sentencia del TAR²¹, puso aún más de relieve los “elementos de garantía mínima para cada hipótesis de utilización de algoritmos en la toma de decisiones: a) conocimiento previo completo del módulo utilizado y de los criterios aplicados; b) la imputabilidad de la decisión al órgano que ostenta el poder, que debe poder llevar a cabo la necesaria verificación de la lógica y legitimidad de la elección y de los resultados confiados al algoritmo”²².

²¹ Más concretamente, el Consejo de Estado confirmó la sentencia del TAR, pero con un razonamiento diferente. En efecto, la sentencia reza así: “Toda la ley de procedimiento administrativo, concebida en un momento en que la administración del Estado estaba en condiciones de ejercer sus funciones, no puede por tanto considerarse aplicable indiscriminadamente a las actividades administrativas algorítmicas, como se considera en los fundamentos de la sentencia de primera instancia. El tema de los peligros asociados al instrumento no queda obviado por la aplicación rígida y mecánica de todas las minuciosas normas procesales de la Ley N° 241 de 1990 [...], ya que, por el contrario, debe considerarse que la necesidad fundamental de protección que plantea la utilización del denominado instrumento informático algorítmico es la transparencia en los términos antes destacados, que se remonta al principio de motivación y/o justificación de la decisión”.

²² Naturalmente, los principios afirmados por el Consejo de Estado se transmitieron después a decisiones relativas a ámbitos distintos del escolar. Por ejemplo, Tar Napoli, sección III, 14 de noviembre de 2022, N.° 7003, en la que, basándose en la jurisprudencia del Consejo de Estado, se aceptó la solicitud de anulación de dos disposiciones adoptadas por la Agencia de Desembolsos Agrícolas.

4. CONCLUSIONES: ¿SUSTITUIRÁ LA INTELIGENCIA ARTIFICIAL AL JUEZ Y AL ABOGADO?

Una pregunta cada vez más recurrente es si el sistema de inteligencia artificial puede sustituir al juez y al abogado.

Para responder a esta pregunta, primero es necesario examinar en qué consiste el trabajo en un bufete de abogados y en una sala de vistas. En un intento de clasificación, pueden identificarse al menos cuatro tipos de actividades: investigación, interpretación, redacción de documentos y toma de decisiones.

En primer lugar, hay una primera parte del trabajo que consiste en la búsqueda de la legislación y los precedentes judiciales pertinentes. Ciertamente, esta actividad no es nueva y siempre se ha llevado a cabo en los sistemas de *common law* y *civil law*. Para calificar un caso, es necesario buscar la legislación pertinente e interpretarla, también es necesario leerla a través de la lente de quienes la han leído antes, es decir, a la luz de los precedentes judiciales. Esto es de la función nomofiláctica que están llamados a ejercer los tribunales superiores²³.

Sin duda, una primera parte del trabajo del jurista consiste en la búsqueda de normas y decisiones pertinentes.

Esta actividad se ha llevado a cabo a lo largo del tiempo de diversas formas, a través de revistas, mediante el uso de bases de datos, en Internet. Se trata de una actividad que ciertamente puede confiarse a sistemas auto-mediados, una vez que el jurista haya definido el método y los criterios de la investigación, y cabe señalar de nuevo que, obviamente, no todos los sistemas digitales son de inteligencia artificial. Como sabemos, de hecho, la investigación jurídica en bases de datos se viene realizando desde hace tiempo.

²³ Sobre la nomofilia véanse las reflexiones de Galgano, "L'efficacia vincolante del precedente di Cassazione", *Contr. Impr.* (1999): 889 y ss.; y "Stare decisis e no nella giurisprudenza italiana", *Contr. Impr.* (2004): 2 y ss.

Pero la diferencia es que los sistemas de inteligencia artificial pueden ir más allá y no limitarse a una búsqueda sobre términos introducidos incluso con ayuda de operadores booleanos. Pueden, por ejemplo, deducir otros términos relevantes del contexto, aunque no se utilicen directamente, y buscar en ellos. También, pueden clasificar las decisiones encontradas a favor y en contra, a efectos del litigio en cuestión.

Así pues, en esta actividad “administrativa”, hay un amplio margen para los sistemas de inteligencia artificial que pueden sumarse a los digitales.

Sin embargo, a veces la actividad investigadora del jurista también se extiende más allá de los límites que puedan haberse predefinido. A menudo, se produce un salto creativo, una asociación imprevista, en la que se expresa la creatividad del jurista. Como ocurre en el desempeño de cualquier actividad investigadora, a veces se encuentra algo que no se buscaba: es la llamada “serendipia”, difícil de imaginar en este caso.

Una segunda fase de este intento de clasificación es la actividad de interpretación, que caracteriza y califica la labor del jurista. Las reversiones jurisprudenciales son el resultado de una nueva interpretación de las normas que refleja la evolución de la sociedad: desde la interpretación evolutiva que ha tenido lugar desde la entrada en vigor del código civil hasta nuestros días de las normas sobre responsabilidad civil, que es enteramente atribuible a la jurisprudencia, hasta las disposiciones relativas a la ética que reflejan necesariamente los cambios en las costumbres, desde el concepto de modestia hasta la idea de familia, por citar sólo algunos ejemplos.

La interpretación evolutiva, esencia del trabajo del jurista, no pertenece hoy a los sistemas de IA.

Los sistemas de *machine learning* aprenden a partir de la información de que disponen: en este caso, de juicios ya emitidos. Así,

aprenden de la experiencia o, si se prefiere, del pasado, como los seres humanos, pero con la diferencia de que reproducen e imitan el pasado.

El juez, en cambio, puede innovar y crear jurisprudencia en función de las particularidades del caso concreto, del contexto social cambiante y de las exigencias que se han desarrollado en la sociedad cada vez más interconectada económica y socialmente.

De hecho, con el paso del tiempo, el contenido de muchas normas ha cambiado sin que cambie la letra de la norma. Baste pensar en el artículo 2043 del Código, norma fundamental sobre la indemnización de daños y perjuicios: en las primeras decisiones jurisprudenciales, nada más entrar en vigor el código, sólo eran indemnizables los daños resultantes de la lesión de derechos absolutos como los derechos de la personalidad y los derechos reales. Hoy en día, el ámbito del daño indemnizable es mucho más amplio: es el daño causado por la lesión de intereses protegidos por el ordenamiento jurídico. Y este es un cambio enteramente jurisprudencial.

La interpretación es la esencia del trabajo del jurista y, al mismo tiempo, la gran fuerza del derecho: de hecho, nunca podrá haber normas tan analíticas como para prever cualquier caso. En la situación actual, esta capacidad no la tienen los sistemas de inteligencia artificial, que se basan en la utilización de datos que se toman y se procesan, y los datos que se procesan son los que ya están a disposición del sistema.

En resumen, puede decirse que, en la actualidad, los sistemas de IA son conservadores: basándose en la experiencia, emiten juicios acordes con ella. Así pues, actualmente no hay lugar para los sistemas de inteligencia artificial en las actividades innovadoras de interpretación²⁴.

²⁴ Así lo señala también Zaccaria, "Figure del giudicare: calcolabilità, precedenti, decisione robótica", *Riv. dir. civ.* (2020): 293, en el que leemos lo siguiente:

Otro riesgo es el de la consolidación de los prejuicios. El sistema de IA se basa en datos y en el conocido principio de “basura que entra, basura que sale”: si se introducen datos que, por ejemplo, son fruto de prejuicios sociales, se reproducen, como en los casos que penalizaban el acceso a la libertad condicional de las personas de raza negra en Estados Unidos, de forma que reproduce el sesgo. Por lo tanto, en la fase de interpretación, leemos tanto una limitación relacionada con los sistemas de IA, ya que no pueden ir más allá de la interpretación ya establecida, como un riesgo de cristalización de los sesgos.

Una tercera actividad propia del jurista es la redacción de actos, entendida en sentido amplio.

Los sistemas de inteligencia artificial que trabajan sobre el lenguaje son ciertamente capaces de redactar actos: ya sean del abogado o del juez. Los recursos, por ejemplo, o los alegatos, así como las sentencias. Luego, está la vasta tarea de redactar actas de reuniones y traducciones, que sin duda también pueden realizar los sistemas

“Aumentando el presente y considerando el futuro como ya presente, [la justicia predictiva] homogeneiza arbitrariamente futuro y pasado, que no son dimensiones homogéneas, y suprime la consistencia del tiempo, ya que hace que el futuro sea tan familiar como el pasado; y así, paradójicamente, devalúa el futuro en favor del pasado y del presente, cristalizados y sacralizados como inmutables en una repetición sin fin. Y no sólo los comportamientos humanos son cristalizados por la justicia predictiva, que no contempla correcciones ni transformaciones: también lo son las normas jurídicas, que, si se toman como datos inmutables y se petrifican en un programa informático, pierden por completo su plasticidad, su capacidad de seguir siendo estas, pero al mismo tiempo de cambiar y adaptarse elásticamente a los cambios del presente y del futuro”. Véase también Gabellini, “La ‘comodità nel giudicare’: la decisione robótica”, *Riv. trim. dir. proc. civ.* (2019): 1305 y ss.; Carratta, “Decisione robotica e valori del proceso”, *Riv. dir. proc.* (2020): 491 y ss.; Zaccaria, “Mutaciones del derecho: innovación tecnológica y aplicaciones predictivas”, *Ars interpretandi* (2021): 29 y ss.; Santuososso y Sartor, “Justicia predictiva: una visión realista”, *Giur. it.* (2022): 1781 y ss.

de IA y que tienen algunas funcionalidades más que los digitales utilizados hasta ahora.

Sin embargo, en esta fase de rodaje de los sistemas, es necesaria la intervención humana para la supervisión y el control con el fin de no tropezar con los problemas mencionados al principio del artículo y, tal vez, arriesgarse a que el abogado sea demandado por los daños causados por la IA. Así lo han manifestado expresamente algunos tribunales estadounidenses, que, naturalmente, responsabilizan al abogado en cualquier caso.

Sin embargo, es útil mencionar brevemente las razones por las que los sistemas de IA han inventado decisiones inexistentes o han cometido errores. Estos sistemas no funcionan con la lógica aristotélica, deductiva y matemática que caracteriza o debería caracterizar el razonamiento jurídico. La lógica que emplean se basa en asociaciones estadísticas y probabilísticas. Asocian una palabra o una secuencia de palabras con las que normalmente la preceden, sin un enfoque semántico. En otras palabras, no se trata de una estructura lógico-deductiva, sino de una asociación conceptual que prescinde del significado de las palabras. Evidentemente, es una forma diferente de representar el conocimiento: las lenguas extranjeras también pueden aprenderse de distintas maneras, empezando por la gramática o escuchando y memorizando muchas palabras²⁵.

Por tanto, no cabe duda de que hay margen para uso de sistemas de inteligencia artificial en la investigación y la redacción de documentos, con las limitaciones antes mencionadas.

Pero la verdadera pregunta es: ¿puede el sistema de IA decidir en lugar del acusado o el juez?

²⁵ Sobre el tema, véase Contucci, *Revolución de inteligencia artificial* (Bari, 2023) y Cristianini, *El atajo. Cómo las máquinas se hicieron inteligentes sin pensar de humana* (Bologna, 2023).

El abogado decide la estrategia que se utilizará y a menudo también desempeña un papel importante como asesor del cliente. El sistema de IA puede recopilar los pros y los contras de una determinada estrategia, acompañados de una indicación de las tasas de éxito y, luego, presentarlos al abogado, que también tendrá en cuenta otros elementos contextuales.

El sistema de IA también puede proponer la decisión judicial, en lugar o en ayuda del juez, según los patrones que haya identificado. Pero esto no significa que la decisión pueda ser tomada por el sistema de IA.

Una de las razones es que los juicios deben estar razonados y las decisiones deben ser explicables y, por tanto, recurribles. La llamada “explicación” (“explicabilidad”) es un requisito previo y no está presente en todos los sistemas de IA actuales.

La opacidad de la decisión es uno de los riesgos previstos en el reglamento europeo²⁶ y señalado por nuestra jurisprudencia al tratar de la transparencia de los algoritmos²⁷.

En el caso concreto de la toma de decisiones judiciales, como se afirma en los considerandos de la Ley de IA, “el uso de herramientas de inteligencia artificial puede servir de apoyo al poder de decisión de los jueces o a la independencia del poder judicial, pero no debe

²⁶ Como se ha anticipado, se hace referencia a ello, en particular, en el Considerando 61 del reglamento. Como señala la Comisión Europea en el memorando que acompaña a la propuesta de reglamento, en sus conclusiones de 21 de octubre de 2020, el Consejo Europeo “instó [...] a abordar la opacidad, la complejidad, la parcialidad, un cierto grado de imprevisibilidad y el comportamiento parcialmente autónomo de determinados sistemas de IA, con el fin de garantizar su compatibilidad con los derechos fundamentales y facilitar la aplicación de las normas jurídicas”.

²⁷ Como se ha ilustrado anteriormente, la jurisprudencia del Consejo de Estado ha afirmado ante todo una “declinación reforzada del principio de transparencia”. Así, en particular, la ya citada Cons. St. 2270/2019.

sustituirlo: el proceso final de toma de decisiones debe seguir siendo una actividad dirigida por el ser humano”.

¿Sustituirá por tanto la inteligencia artificial al juez y abogado? Por el momento, se puede concluir lo siguiente: algunas funciones, como la investigación y la redacción, pueden ser sustituidas. Pero, al menos a corto plazo, la mayoría de las funciones de toma de decisiones y actividad más creativa seguirán siendo de dominio humano.

Así pues, por el momento, los sistemas de inteligencia artificial pueden constituir sin duda una ayuda importante, especialmente en lo que respecta a las controversias en las que el mecanismo de decisión requiere la simple comprobación de determinadas circunstancias bien definidas, pero no es posible desvincularlos de la compleja actividad interpretativa que caracteriza toda actividad de abogados y jueces.

CAPÍTULO 9

RESPONSABILIDAD DE LAS PLATAFORMAS Y PROTECCIÓN DE LOS CONSUMIDORES*

1. DESDE LA DIRECTIVA 2000/31/CE...

El 23 de abril de 2022, cuando el Parlamento Europeo y el Consejo alcanzaron un acuerdo político sobre el texto del reglamento relativo a un mercado único de servicios digitales¹, la llamada Ley de Servicios Digitales (en lo sucesivo también “DSA”, por sus siglas en inglés.), la Presidenta de la Comisión Europea, Ursula von der Leyen, declaró lo siguiente: “El acuerdo de hoy sobre la Ley de Servicios Digitales es histórico [...] Cuanto mayor sea el tamaño,

* Este capítulo retoma, con algunas adaptaciones y actualizaciones, el artículo publicado en *Giornale di Diritto amministrativo* (2023): 730 y ss.

¹ Reglamento (UE) 2022/2065 Parlamento Europeo y del Consejo, de 19 de octubre de 2022, “relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento sobre servicios digitales)”, publicado en el *Diario Oficial de la Unión Europea* L 277 de 27 de octubre de 2022, disponible en el siguiente enlace: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2022.277.01.0001.01.ITA (consultado el 26 de junio de 2024).

mayores serán las responsabilidades de las plataformas en línea”². Las palabras de Von der Leyen revelan la urgencia que siente el legislador europeo por asignar responsabilidades a los gigantes de la red. “Es [...] oportuno establecer un conjunto específico de normas obligatorias uniformes, eficaces y proporcionadas a escala de la Unión para proteger y mejorar el funcionamiento del mercado interno”, reza el considerando 4 del citado reglamento, aprobado el 19 de octubre de 2022.

Así, se atestigua un cambio de ritmo.

Hace veinte años, de hecho, el legislador europeo había considerado necesario circunscribir la responsabilidad para fomentar el comercio electrónico³. Así, la Directiva 2000/31/CE⁴ sobre el comercio electrónico adoptó un modelo de responsabilidad limitada, cuando no incluso de exención de responsabilidad, en favor de los proveedores de servicios digitales. En lugar de prever un régimen general de responsabilidad para los intermediarios en línea, la Directiva, a través del denominado *principio de puerto seguro*, estableció normas específicas en virtud de las cuales estas entidades quedaban exentas de responsabilidad en determinadas condiciones, atribuibles esencialmente a la neutralidad y pasividad del proveedor⁵. Además

² Véase el comunicado de prensa publicado por la Comisión Europea, disponible en https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545 (consultado el 26 de junio de 2024).

³ He desarrollado estas reflexiones en mi “Transparencia de los proveedores digitales y brecha digital”, en *Privacy and Data Protection in Software Services*, eds. Senigaglia, Irti y Bernes (Milán, 2021), 3 y ss. y en mi “La sovranità digitale”, *Diritto pubblico* (2022): 809 y ss.

⁴ Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, “relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)”.

⁵ La referencia es, en particular, a los arts. 12, 13 y 14 de la Directiva, que, como es sabido, establecían un régimen de responsabilidad diferenciado en función

de este marco de exención condicional, la Directiva establecía la ausencia de una obligación general de supervisar los contenidos en línea de los usuarios: en otras palabras, los proveedores de servicios en línea no estaban obligados a buscar activamente hechos o circunstancias que indicaran una actividad o contenidos ilegales cargados o transmitidos a través de los servicios prestados⁶.

La propensión del legislador europeo a una regulación especialmente flexible y sin obligaciones rígidas se debió al momento histórico en que se promulgó la legislación. El desarrollo del mercado digital estaba en sus inicios y se consideró que imponer obligaciones y cargas, incluso económicas, a los proveedores de servicios habría corrido el riesgo de desincentivar el desarrollo de los servicios digitales y las transacciones en línea, en detrimento de los propios internautas, sobre los que estas cargas se habrían repercutido inevitablemente.

Por supuesto, esta es sólo una perspectiva de lectura —podrían añadirse muchas otras—, pero probablemente sea la más aceptada desde un punto de vista funcional y económico⁷.

Sin embargo, el modelo identificado por la Directiva sobre comercio electrónico se ha visto progresivamente erosionado por la jurisprudencia italiana y europea, que han identificado diversas

de que el servicio prestado por el prestador fuera calificable de “mero conducto” o “simple canalización”, “almacenamiento temporal” o “caching” o “hosting”.

⁶ El art. 15 coloca bajo el epígrafe “ausencia obligación general de supervisión” y establece en su primer párrafo: “En la prestación de los servicios contemplados en los arts. 12, 13 y 14, los Estados miembros no impondrán a los prestadores una obligación general de supervisión sobre la información que transmiten o almacenan, ni una obligación general de buscar activamente hechos o circunstancias que indiquen actividades ilegales”.

⁷ Para una reconstrucción de otras perspectivas, véase Facci, “La responsabilità dei providers”, en *Commercio elettronico*, eds. Rossello, Finocchiaro y Tosi (Turín, 2007), 233 y ss. y Mantelero, “Responsabilità aquiliana per uso della Rete e respon- sabilità del provider”, *Diritto dell'informatica* (2014): 785 y ss.

formas de responder a la necesidad cada vez más acuciante de que los proveedores rindan cuentas⁸.

2. ... A LA NECESIDAD DE LA UNIÓN EUROPEA DE RECUPERAR EL ESPACIO REGLAMENTARIO

El cambio en el planteamiento de la responsabilidad forma parte de un marco más amplio, que debe analizarse a la luz de

⁸ En Italia, es histórica la sentencia del Tribunal de Milán, de 12 de abril de 2010, N.º 1972, conocida como *Google contra Vivi Down*. Los jueces de primera, tras valorar calificación de Google como *hosting* o como proveedor de contenidos, habían negado la existencia de una obligación de la empresa de realizar controles preventivos sobre los contenidos que transmitía en Internet a petición de los usuarios y, en consecuencia, habían descartado la posibilidad de condenar al proveedor por complicidad de omisión en el delito cometido por el usuario que había subido el vídeo. Sin embargo, habían considerado penalmente responsable, en relación con el delito de tratamiento ilícito de datos, a la dirección de la división italiana de Google, definida como “responsable, al menos a los efectos de la ley de privacidad”. Más recientemente, Cass. civ., secc. I, 19 de marzo de 2019, núms. 7708 y 7709, donde los jueces, si bien reconocieron la inexistencia de una obligación general y constante de vigilancia y activación previa por parte del proveedor, señalaron la existencia de una obligación de eliminar los actos ilícitos de los que tuviera conocimiento. En cuanto a la jurisprudencia europea, basta recordar la jurisprudencia del Tribunal de Justicia que, si bien respeta la prohibición de imponer un mecanismo de control previo a los prestadores, por una , no excluye la posibilidad de que los jueces nacionales impongan obligaciones de filtrado de los contenidos cargados o transmitidos en línea y por otro lado, establece que, orden judicial, los proveedores de servicios de Internet están obligados a el acceso de sus usuarios a un sitio web que contenga material que infrinja los derechos de autor, así como a buscar y suprimir contenidos difamatorios. Cabe destacar que, en los considerandos de la Ley de Servicios Digitales, el legislador europeo se refirió expresamente a la jurisprudencia del TJUE en materia de responsabilidad, al considerar necesario “aclarar algunos elementos de este marco [“el marco horizontal de exenciones condicionales de responsabilidad para los prestadores de servicios intermediarios de la Directiva 2000/31/CE”] a la luz de la del Tribunal de Justicia de Europa”, tal y como recoge el considerando 16 del reglamento.

los profundos cambios que se han producido desde la década de 1990⁹.

El escenario ha cambiado al menos en tres aspectos, que son, si se examinan más de cerca, expresión de uno solo: la creciente relevancia, no sólo económica, sino también social y política de lo digital.

En primer lugar, desde finales de los años noventa hasta hoy, nuestras vidas se han ido desplazando cada vez más hacia lo digital. Para utilizar la afortunada expresión de Floridi, vivimos en la *onlife*¹⁰. Si hasta hace unos años podíamos distinguir entre lo “real” y lo “virtual”, hoy esta distinción ya no tiene sentido.

Las percepciones del individuo y la sociedad han cambiado, y lo digital se considera cada vez más integrado en nuestra propia existencia.

La información se ha “entificado” y “cosificado”. Se han convertido en “cosas”.

Los datos, personales y no personales, se han convertido en objeto de comunicación y también de explotación.

Son activos que pueden compartirse e intercambiarse. Como es bien sabido, el gran desarrollo reciente de la inteligencia artificial también tiene su origen en el acceso a los datos que ahora es posible.

Por último, el papel de los grandes actores digitales, que crean condiciones y la arquitectura de *onlife*, se ha ampliado. Se han convertido no sólo en actores, sino en directores. O, mejor dicho, productores de la *onlife*, dado el peso económico que ejercen, gracias al valor que adquieren los datos y la información.

En resumen, lo digital ha pasado de un público de nicho, el ámbito militar y, luego, de la academia, en los inicios del Internet, del comercio electrónico para, luego, impregnar toda la vida social.

⁹ También he profundizado en esta cuestión en mi artículo *Soberanía digital*, cit.

¹⁰ Floridi, *El Manifiesto Onlife. Ser humano en una era hiperconectada*, Cham, 2015.

Algunos signos de cambio y del cambio de actitud de la Unión Europea fueron la decisión Google España¹¹, los casos Schrems¹², las decisiones antimonopolio¹³ y, posteriormente, la promulgación del 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”, ahora más conocido como “GDPR” (acrónimo de General Data Protection Regulation).

El caso Trump fue entonces paradigmático del cambio¹⁴.

-
- ¹¹ Tribunal de Justicia de la Unión Europea, 13 de mayo de 2014, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos y Mario Costeja González* (la sentencia mencionada y las posteriormente citadas están disponibles en la URL: curia.europa.eu/jcms/jcms/j_6/en/). La decisión fue objeto de numerosos tributos. Para una recopilación de los principales temas, véase *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, eds. Resta y Zeno-Zencovich (Roma, 2015), disponible en <https://romatrepress.uniroma3.it/wp-content/uplo-ads/2020/02/Il-dir-all'oblio-su-Internet-dopo-la-sentenza-Google-Spain.pdf> (consultado el 26 de junio de 2024).
- ¹² Tribunal del 6 de octubre de 2015, C-362/14, *Maximillian Schrems c. Comisario de Protección de Datos*, y 16 de julio de 2020, C-311/18, *Comisario de Protección de Datos c. Facebook Ireland Ltd. y Maximillian Schrems*. Véase Zeno-Zencovich, “En torno a la decisión en el asunto Schrems: la soberanía digital y la gobernanza internacional las redes de telecomunicaciones”, *Dir. Inf.* (2015): 683 y ss.
- ¹³ Entre las numerosas acciones emprendidas por la Comisión Europea destacan, en particular, las multas impuestas a Google por infracción de las normas de competencia de la UE a partir de 2017, mediante la Decisión de 27 de junio de 2017, C(2017) 4444, confirmada posteriormente en la sentencia del Tribunal General de la Unión Europea T-612/17 de 10 de noviembre de 2021, la Decisión de 18 de julio de 2018, C(2018) 4761 y la resolución de 20 de marzo de 2019, C(2019) 2173.
- ¹⁴ Como es bien sabido, el 8 de enero de 2021, Twitter tachó el perfil del entonces presidente de los Estados Unidos por violación de la normativa contractual de Twitter, por el riesgo de incitación a la violencia. Declaración de Twitter: “Tras revisar detenidamente los últimos tuits de la cuenta @realDonaldTrump y el contexto que los rodea —específicamente cómo están siendo recibidos e interpretados dentro y fuera de Twitter— hemos suspendido permanentemente la

Tras la eliminación del perfil del entonces presidente de los Estados Unidos de Twitter, el problema se hizo evidente¹⁵. Se ha planteado la cuestión de si las normas contractuales y las disposiciones de Derecho privado son suficientes, o si las relaciones que son relevantes desde el punto de vista público deben regularse de forma diferente. En otras palabras, se ha planteado la cuestión de si, cuando el tema es de interés público (por ejemplo, comunicación, información, *fake news*), debe revisarse el modelo jurídico de regulación de los intereses.

La crisis de la globalización va acompañada de la crisis de los instrumentos jurídicos que permitieron que se produjera, que son de

cuenta debido al riesgo de que se siga incitando a la violencia. En el contexto de los terribles acontecimientos de esta semana, dejamos claro el miércoles que cualquier otra infracción de las normas de Twitter podría dar lugar a esta misma medida. Nuestro marco de interés público existe para permitir que el público escuche directamente a los funcionarios electos y a los líderes mundiales. Se basa en el principio de que el pueblo tiene derecho a pedir cuentas al poder en público. Sin embargo, hace años que dejamos claro que estas cuentas no están totalmente por encima de nuestras normas y no pueden utilizar Twitter para incitar a la violencia, entre otras cosas. Seguiremos siendo transparentes en cuanto a nuestras políticas y su aplicación”. Sobre este tema, puede consultarse la contribución de Bassini, “Lo statuto costituzionale dei social network: nuovi attori e servizi pubblici?”, en *Diritto costituzionale e nuove tecnologie*, eds Ferri (Nápoles, 2022), 47 y ss.

¹⁵ Según Stanzione, “Introducción”, en *I poteri privati delle piattaforme e le nuove frontiere della privacy*, ed. Stanzione (Turín, 2022), 1, en el caso Trump emergió de manera “deflagrante” el “papel central que asumen las plataformas en el sistema actual”. El caso Trump tuvo entonces una continuación, ya que Google no aprobó la distribución en su tienda de Truth Social, la *app* que permite conectarse a la red social creada por el expresidente de Estados Unidos. Según Google, la red social violaría las normas de moderación de contenidos, en particular en lo que se refiere a amenazas e incitación a la violencia. Véase <https://www.ilpost.it/2022/08/31/truth-social-not-available-google-android-donald-trump/> (consultado el 26 de junio de 2024).

naturaleza tecno-lógica y técnico-jurídica, como la *lex mercatoria*¹⁶ y la *lex informatica*¹⁷. La expresión “poderes privados”¹⁸ se tiñe de una connotación negativa, indicando a las grandes corporaciones que gestionan lo digital, que han ocupado todo el espacio que quedaba libre, dictando incluso las reglas, y que asumen cada vez más un papel político. Y el despliegue del discurso en términos de “soberanía”¹⁹, con una expresión que por su propia naturaleza está asociada al Estado-nación, revela la necesidad de que el poder público se reapropie de los “nuevos espacios”. También se contraponen

¹⁶ Algunos juristas han intentado reconstruir el proceso de formación de la ley aplicable en Internet en términos de analogía con la *lex mercatoria*, haciendo referencia en particular a la autorregulación: Johnson y Post, “Law and Borders - The Rise of Law in Cyberspace”, *Stanford L. Rev.* (1996): 1389 y ss.; Burnstein, “Conflicts on the Net: Choice of Law in Transnational Cyberspace”, *Vanderbilt J. of Transnational L.* (1996): 108 y ss. La *lex mercatoria* también es mencionada por Kessedjian, “Rapport de synthèse”, en *Internet. Which Court Decides? Which Law Applies?*, eds. Boele-Woelki Y Kessedjian (Londres-Boston, 1998), 148, quien afirma “une néo lex mercatoria est née: la Net lex”. He hecho algunas consideraciones al respecto en mi “Lex mercatoria e commercio elettronico”, *Contr. Impr.* (2001): 571 y ss.

¹⁷ La *lex informatica* consiste en la formulación de normas a través de la tecnología y se considera un sistema paralelo de normas. Sobre este tema, véase Reidenberg, “Lex Informatica: The Formulation of Information Policy Rules through Technology”, *Texas L. Rev.* (1998): 553 y ss. y Lessig, “The Constitution of Code: Limitations on Choice- based critiques of Cyber-space Regulation”, *CommLaw Conspectus* (1997): 185 y ss. Ferrarese, *Poteri nuovi* (Bologna, 2022), quien afirma que “las plataformas y los algoritmos tienen una sustancia normativa” (73) y que están “lejos de los criterios de transparencia democrática” (76).

¹⁸ Es obligado citar a Lombardi, *Poder privado y derechos fundamentales* (Turín, 1970), que investigó, obviamente, en un contexto completamente distinto, “las posiciones de la libertad con respecto al poder privado” y a Bianca, *Le autorità private* (Nápoles, 1977), sobre las “autoridades de hecho”. Los temas se retoman en el volumen *I poteri privati e il diritto della regolazione. Cuarenta años después de Le autorità private de C.M. Bianca*, eds. Sirena y Zoppini, Roma, 2018.

¹⁹ Retomando a C.M. Bianca, Stanzione, “Introducción”, 5, habla de “predominio contractual” en la base de las autoridades de facto (y del abuso de su poder).

los instrumentos jurídicos: la dimensión privada a la dimensión pública y el contrato a la ley. El legislador europeo adopta un nuevo enfoque normativo, basado en reglamentos más que en directivas y claramente decidido a construir el mercado digital europeo.

3. EL MODELO DE RESPONSABILIDAD ADOPTADO EN LA LEY DE SERVICIOS DIGITALES Y EL PARADIGMA USUARIO-CONSUMIDOR

Una vez abordada la evolución del contexto de referencia, se ilustran los resultados con respecto a la responsabilidad de los proveedores.

El Considerando 16 de la DSA afirma lo siguiente: “La seguridad jurídica que proporciona el marco horizontal de exenciones condicionales de responsabilidad para los prestadores de servicios intermediarios de la Directiva 2000/31/CE ha permitido la aparición y expansión de numerosos servicios nuevos en todo el mercado interior. Conviene, por tanto, preservar este marco”, y los artículos 4, 5, 6 y 8 de la DSA recogen lo ya previsto en la Directiva sobre comercio electrónico²⁰.

Así pues, se confirma la exención de responsabilidad sujeta al cumplimiento de condiciones basadas en la presunción de neutralidad y pasividad del proveedor. También, se confirma la regla de que no existe obligación general de controlar o averiguar activamente los hechos.

²⁰ En su lugar, una nueva disposición el art. 7 de la LSD, destinada a especificar que “no se considerará que los prestadores de servicios intermediarios no pueden acogerse a la exención de responsabilidad prevista en los arts. 4, 5 y 6 por el mero hecho de que lleven a cabo de buena fe y con la diligencia debida, investigaciones voluntarias por iniciativa propia o adopten otras medidas destinadas a detectar identificar y retirar contenidos ilícitos o a inhabilitar el acceso a los mismos, o a adoptar las medidas necesarias para cumplir los requisitos del Derecho de la UE y del Derecho nacional de conformidad con el Derecho de la UE, incluidos los requisitos establecidos en el presente reglamento.

Sin embargo, el marco normativo cambia. La exención de responsabilidad forma ahora parte de un espeso manto de normas —las 89 disposiciones adicionales de la DSA—, casi todas ellas destinadas a identificar obligaciones específicas para los proveedores de servicios digitales y a procedimentar sus actuaciones, distinguiendo según la naturaleza del servicio ofrecido y el tamaño del proveedor. Así pues, si se examina más de cerca, el modelo de responsabilidad también acaba cambiando: mientras que en la Directiva sobre comercio electrónico el prestador de servicios se encontraba en una posición privilegiada en la que, de hecho, disfrutaba de una responsabilidad limitada, ahora es el internauta el centro de la protección. El objetivo es reforzar la posición del usuario individual, de forma similar a lo que ocurre en la protección de datos personales y en la normativa de protección del consumidor. Así, el “usuario” goza de la protección de la posición subjetiva de “interesado”, según la ley de protección de datos, y de “consumidor”, según la ley de consumidores. Los consumidores, que viven en la *onlife*, son usuarios de servicios digitales. Por lo tanto, al contemplar el panorama de los usuarios de servicios digitales, el paradigma que emerge es el del usuario-consumidor y el del consumidor-usuario²¹.

A esto hay que añadir al menos dos elementos de complejidad.

La primera: el consumidor, en la red, no es sólo un usuario de servicios digitales, sino que es un prosumidor, es decir, un consumidor y un productor que, al utilizar servicios digitales, contribuye

²¹ Según la Comunicación de la Comisión Europea “Nueva Agenda del Consumidor. Reforzar la resistencia de los consumidores con vistas a una recuperación sostenible”, COM(2020) 696 final, entre 2014 y 2019, el porcentaje de usuarios de Internet en la UE que compraron o encargaron bienes o servicios *en línea* para uso privado aumentó del 63% al 71% y en algunos Estados miembros, como Dinamarca, Países Bajos, Suecia y Alemania, el 80%. La Comunicación está disponible en el siguiente enlace: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:-52020DC0696> (consultado el 14 de octubre de 2023).

a la producción de estos servicios. Los motores de búsqueda, el comercio electrónico, los blogs y las redes sociales también basan su funcionamiento en la colaboración del usuario-consumidor, que, mientras navega y vive su *onlife*, contribuye a determinar el precio de los anuncios o a construir la reputación de un vendedor o de un producto²².

El segundo es el conocido nivel de asimetría tecnológica y de información entre los usuarios y los operadores de la web. No se trata sólo de un desequilibrio económico, sino sobre todo de un desequilibrio provocado por la disparidad de conocimientos técnicos y de información. Esta asimetría puede afectar a la correcta formación de la voluntad del usuario, incluso contractual. Teniendo en cuenta que, en el momento de celebrar un contrato en línea, suele haber una diferencia considerable entre el conocimiento de las partes contratantes. Tal vacío de información puede generar expectativas erróneas o una confianza ilegítima en el prestador de servicios hasta el punto de viciar el momento de formación de la voluntad.

4. LAS OBLIGACIONES INTRODUCIDAS POR LA DSA

La DSA establece obligaciones generales aplicables a todos los prestadores de servicios intermediarios y obligaciones adicionales exclusivas para los prestadores de servicios de alojamiento²³ y, en

²² La definición es de Menduni, “Prosumer”, en *Enc. Ciencia y Tecnología* (Roma, 2008). Como es bien sabido, la expresión “prosumidor” se debe a Alvin Toffler, que en su *The third wave* (Nueva York, 1980) propuso el término como una crisis de los términos productor y consumidor. El concepto también es retomado por Alpa, “Sul potere contrattuale delle piattaforme digitali”, *Contr. Impr.* (2022): 721 y ss.

²³ En el Art. 3, letra g) DSA se define “hosting” como el “servicio almacenamiento de información [...] consistente en almacenar información suministrada por un destinatario del servicio a petición de este”. Se trata de la misma definición ya adoptada en la Directiva sobre comercio electrónico.

particular, para las plataformas en línea²⁴, para las que permiten a los consumidores celebrar contratos a distancia con comerciantes y para las grandes plataformas²⁵.

Se trata de obligaciones de diligencia, transparencia y lucha contra las conductas ilícitas y la protección de los usuarios.

Entre ellas figura, en primer lugar, la obligación de que todos los proveedores de servicios de almacenamiento de información establezcan un mecanismo de notificación y retirada²⁶.

Según la redacción de la legislación, las alertas recibidas en el ámbito de tales mecanismos dan lugar a la adquisición por parte

²⁴ En el art. 3, *lett.* (i) de la LSD se define una “plataforma en línea” como “un servicio de almacenamiento de información que, a petición de un destinatario del servicio, almacena y difunde información al , a menos que esta actividad sea una función menor y puramente accesoria de otro servicio o una funcionalidad menor del servicio principal y, por razones objetivas y técnicas, no pueda utilizarse sin ese otro servicio y siempre que la integración de esa función o funcionalidad en el otro servicio no sea un medio de eludir la aplicabilidad del presente reglamento”.

²⁵ Se trata de las plataformas en línea y los motores de búsqueda en línea que tienen un número medio mensual de destinatarios activos del servicio en la UE igual o superior a 45 millones y que son designados por decisión de la Comisión Europea. Así, el art. 33 de la DSA establece. Cabe señalar que el 25 de abril de 2023, la Comisión Europea adoptó las primeras decisiones identificando diecisiete plataformas en línea a gran escala y dos motores de búsqueda en línea a gran escala: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 (consultado el 14 de octubre de 2023).

²⁶ El art. 16 de la DSA. Ya mencionado en la Directiva sobre comercio electrónico, *el* mecanismo de notificación y retirada se define como un mecanismo que permite al cualquier persona o entidad a notificar a los prestadores la presencia de información específica que se considere ilícita. El concepto también es recogido por el legislador europeo en la Directiva (UE) 2019/790, de 17 de abril de 2019, sobre derechos de autor y derechos afines en el mercado único digital, que ha elevado el nivel de diligencia exigido a los prestadores de servicios por compartir contenidos en línea protegidos por derechos de autor u otras materias protegidas imponiendo una mayor responsabilidad.

de los prestadores de un conocimiento efectivo del contenido, lo que es pertinente a efectos de la definición de la responsabilidad del prestador, ya que cabe suponer que permitirían a un prestador diligente detectar la ilegalidad de la actividad o de la información sin necesidad de un examen exhaustivo. La cuestión, como es bien sabido, había sido muy debatida en relación con la Directiva 2000/31/CE. En otras palabras, ahora, una vez recibido un informe completo, surge una presunción relativa. Se considera que se cumple una de las condiciones para la inaplicabilidad de la exención de responsabilidad: ya no puede suponerse que el proveedor de servicios de almacenamiento de información no tenía conocimiento efectivo de actividad o el contenido ilícito.

La ASD establece que las decisiones sobre el contenido de los informes deben adoptarse “de manera oportuna, diligente, no arbitraria y objetiva” y que el denunciante debe recibir, sin demoras indebidas, primero un acuse de recibo del informe y, posteriormente, una notificación de la decisión adoptada al respecto, junto con indicaciones sobre la posibilidad de recurrir.

La lucha contra los contenidos ilícitos incluye también la introducción de obligaciones relativas a la suspensión del servicio a quienes “frecuentemente” proporcionen contenidos manifiestamente ilícitos²⁷.

Las políticas adoptadas por los proveedores de plataformas en línea en relación con la suspensión por abuso deben establecerse en las condiciones generales, de forma clara y detallada.

²⁷ La noción de “contenido ilícito” se recoge el Art. 3, letra h) de la LSD, en base al cual es “ilícito” el contenido “no conforme con el Derecho de la UE o de cualquier Estado miembro conforme con el Derecho de la Unión”. La obligación de suspender está consagrada en el artículo 23, que, para equilibrar los intereses contrapuestos en juego, establece una regulación muy detallada: la suspensión debe ir precedida de un preaviso y sólo puede tener lugar “durante un plazo razonable”; la valoración de la suspensión debe realizarse caso por caso y de forma diligente, oportuna y objetiva, teniendo en cuenta todos los hechos y circunstancias relevantes, algunos de los ya están identificados por la norma.

Las condiciones generales, a las que se dedica una disposición específica²⁸, también deben incluir información sobre las restricciones que los proveedores pretenden imponer al uso del servicio. Los proveedores deben especificar qué políticas y herramientas utilizan a efectos de la moderación de contenidos, incluidos los procesos algorítmicos de toma de decisiones y de “verificación humana”. Además, se impone un deber de justificación a los proveedores de alojamiento²⁹ y se establecen obligaciones relativas al diseño de las interfaces para los proveedores de plataformas en línea³⁰.

Predomina el tema de la transparencia, que el legislador impone también en el ámbito de la publicidad, previendo obligaciones específicas de divulgación en referencia a los contenidos publicitarios individuales³¹, así como a los sistemas publicitarios³².

²⁸ Se trata del art. 14 DSA.

²⁹ Así el art. 17 DSA. Más concretamente, el prestador está obligado a proporcionar a todos los destinatarios del servicio en cuestión una justificación clara y específica cuando imponga restricciones a un usuario que haya facilitado contenidos ilícitos o incompatibles con condiciones generales.

³⁰ Véase, en particular, el art. 25 DSA. En el caso que nos ocupa, se trata de la obligación de los proveedores mencionados de no diseñar y organizar sus interfaces de manera que engañen o manipulen a los destinatarios o menoscaben su capacidad de tomar decisiones libres e informadas.

³¹ Así, el art. 26 de la DSA. El art. 39 del reglamento también establece obligaciones adicionales para los proveedores de plataformas en línea y motores de búsqueda en línea muy grandes. En particular, se les exige que elaboren y pongan a disposición del público un registro con información sobre cualquier contenido público presentado en sus interfaces.

³² Así, el art. 27 de la DSA. En particular, se exige que los proveedores de plataformas en línea que hagan uso de sistemas de recomendación especifiquen en las condiciones generales, en un lenguaje claro e inteligible, los principales parámetros utilizados en dichos sistemas, así como las opciones de que disponen los destinatarios del servicio para modificar o influir en dichos parámetros. Se trata de dar a conocer al destinatario del servicio por qué se le sugiere determinada información.

También se pretende excluir la posibilidad de que los denominados “datos especiales”, que gozan de protección reforzada en virtud del RGPD, puedan tratarse con fines públicos, prohibiendo la presentación de anuncios a los destinatarios del servicio, basada en la elaboración de perfiles utilizando categorías especiales de datos personales³³.

Las disposiciones aplicables a los proveedores de plataformas en línea que permiten a los consumidores celebrar contratos a distancia con comerciantes completan el panorama³⁴.

Las obligaciones van desde la identificación completa y fiable de los comerciantes, pasando por el diseño y la organización de la intercara de forma que permita a los comerciantes cumplir sus obligaciones en materia de información precontractual y seguridad de los productos, hasta la advertencia a los consumidores si tienen conocimiento de que han ofrecido un producto o servicio ilegal sus servicios.

También, se prevé un régimen de responsabilidad diferenciado³⁵. La exención de responsabilidad prevista para los proveedores de alojamiento no se aplica en relación con los supuestos de responsabilidad previstos en la legislación de protección de los consumi-

³³ Como es sabido, según la definición dictada el art. 9 del Reglamento 2016/679, se trata de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como los datos genéticos, los datos biométricos destinados a identificar de manera unívoca a una persona, los datos la salud o a la vida sexual de una persona o a su orientación sexual.

³⁴ Se trata de los arts. 30, 31 y 32 DSA, y el art. 29 del reglamento. Estas disposiciones adicionales no se aplican a los proveedores de plataformas en línea que permiten a los consumidores celebrar contratos a distancia con comerciantes que reúnen las condiciones para ser considerados microempresas o pequeñas empresas.

³⁵ La referencia al art. 6(3) DSA.

dores para los proveedores de plataformas en línea que permiten a los consumidores celebrar contratos a distancia con comerciantes, si las plataformas inducen a un consumidor medio a creer que la información, el producto o el servicio objeto de la transacción es suministrado por la propia plataforma o por un destinatario del servicio que actúa bajo su autoridad o control.

5. PROTECCIÓN DEL CONSUMIDOR: UN SISTEMA COMPUUESTO

Llevará tiempo comprobar la eficacia del dispositivo de protección apreciada por las numerosas y específicas obligaciones impuestas por la DSA.

Según algunos, puede no ser suficiente. “En la sociedad digital, la vulnerabilidad es arquitectónica porque los archivos de elección digital por los que navegamos a diario están diseñados para inferir o incluso crear vulnerabilidades”³⁶. Así, se observa que la ASD parece insuficiente, porque no se ha tenido debidamente en cuenta la vulnerabilidad del consumidor³⁷. Ciertamente, hay que considerar que la protección de los consumidores-destinatarios de servicios digitales impregna también los demás ámbitos en los que se articula la estructura normativa sobre la que se asienta el mercado digital europeo. Esta estructura se compone básicamente de cuatro ámbitos, que ya han sido mencionados: el de la protección de los datos personales, con el RGPD, y el de la valorización de los datos

³⁶ Así Helberger, Lynskey, Micklitz, Rott, Sax y Strycharz, *Consumidor de la UE Protección 2.0. Asimetrías estructuradas en los mercados digitales de consumo. Informe conjunto de la investigación realizada en el marco del proyecto EUCP2.0* (Bruselas, 2021).

³⁷ En estos, Riefa, “Protecting Vulnerable Consumers in the Digital Single Market”, *European Business Law Review* (2022): 607 y ss., donde se observa lo siguiente: “La DSA apenas menciona a los consumidores vulnerables. Y cuando lo hace, la conceptualización de la vulnerabilidad sigue siendo muy limitada”.

previsto en la Ley de Datos³⁸, la Ley de Gobernanza de Datos³⁹ y el Reglamento sobre el Espacio Europeo de Datos de Salud⁴⁰; el del mercado digital y de los servicios digitales, con la Ley de Mercados Digitales⁴¹ y la Ley de Servicios Digitales⁴²; la identidad digital, con la revisión del Reglamento e-IDAS de 2014⁴³; y, por último,

³⁸ Se trata del Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, “relativo a normas armonizadas acceso y el uso equitativo de los datos y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de datos)”, disponible en <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R2854> (consultado el 10 de junio de 2024).

³⁹ Se trata del Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, “relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento sobre gobernanza de datos)”, disponible en <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022R0868> (consultado el 10 de junio de 2024).

⁴⁰ Se trata del Reglamento del Parlamento Europeo y del Consejo “sobre el Espacio Europeo de Datos Sanitarios”, aprobado por el Parlamento Europeo el 24 de abril de 2024. En el momento de redactar este documento, está pendiente la aprobación del texto por el Consejo. El texto aprobado por el Parlamento está disponible en https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_EN.pdf (consultado el 10 de junio de 2024).

⁴¹ Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, “sobre mercados justos y competitivos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento del mercado digital)”, disponible en <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022R1925> (consultado el 26 de junio de 2024).

⁴² Como se anticipó, Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, “relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento sobre servicios digitales)”, disponible en <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022R2065> (consultado el 10 de junio de 2024).

⁴³ Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, “por el que se modifica el Reglamento (UE) 910/2014 en lo que se refiere al establecimiento del marco europeo para una identidad”, disponible

el reglamento relativo a la inteligencia artificial⁴⁴, la llamada Ley de IA, que va acompañada de la propuesta de “Directiva sobre la adaptación de las normas sobre responsabilidad civil extracontractual a la inteligencia artificial (*Directiva sobre responsabilidad por IA*)⁴⁵.

También se pueden encontrar perfiles de protección del consumidor en la Ley de Mercados Digitales, que, al establecer normas para garantizar la contestabilidad y la equidad en los mercados del sector digital, afecta positivamente a la posición los usuarios finales⁴⁶.

Un refuerzo de la posición de los usuarios-consumidores puede venir también de la Ley de Datos: al establecer quién y en qué condiciones puede tener acceso a los datos personales y no personales generados por el uso de productos y servicios relacionados, la normativa conocida como “ley de datos” pretende garantizar un reparto equitativo del valor de los datos, en el que el usuario-consumidor también participe de ese valor. La consolidada protección que ofrece el RGPD también es relevante, dada la recurrente superposición de las posiciones subjetivas de consumidor y sujeto de quien ya se ha mencionado⁴⁷.

en https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L_202401183 (consultado el 26 de junio de 2024).

⁴⁴ Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, “por el que se establecen normas armonizadas sobre inteligencia artificial (Reglamento sobre inteligencia artificial)”.

⁴⁵ Propuesta de Directiva “relativa a la adaptación de las normas sobre responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad inteligencia artificial)”, disponible en <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496> (consultada el 10 de junio de 2024).

⁴⁶ Así lo señala también “Kanceljak, Interplay of Gatekeepers’ Obligations and Consumer Rights under the Digital Markets Act”, en *2023 46th MIPRO ICT and Electronics Convention (MIPRO)* (Opatija, 2023), 1484 y ss.

⁴⁷ Véase Colangelo y Maggiolino, “From fragile to smart consumers: shifting paradigm for the digital era”, *Comput Law Secur Rev.* (2019): 173 y ss., quienes

Este es el marco normativo de protección sobre el que descansa la Ley de IA, en la que se establece un marco normativo general para el acceso de la IA al mercado europeo, pero sin prever nuevas formas de protección para el individuo⁴⁸.

Queda, pues, el sistema de protección previsto por la disciplina de consumo que ha constituido, y constituye aún hoy, la base normativa de referencia⁴⁹.

incluyen el GDPR, con su regulación del derecho a la portabilidad, entre las normas europeas que están allanando el camino para el empoderamiento de los consumidores. Los autores mencionan también la Directiva (UE) 2015/2366 sobre servicios de pago en el mercado interior, la llamada “PSD2”, que introdujo la “regla de la banca abierta” y la Directiva (UE) 2019/770 “sobre determinados aspectos de los contratos de suministro de contenidos y servicios digitales”.

⁴⁸ Véanse los capítulos 1, 2 y 3 de este volumen.

⁴⁹ En este sentido, cabe hacer referencia a la Comunicación de la Comisión Europea “Un nuevo trato para los consumidores”, COM(2018) 183 final, en la que, en 2018, el entonces presidente de la Comisión Juncker destacó la necesidad de moderar las normas de protección de los consumidores. Entre las iniciativas legislativas que persiguen este objetivo figura, en particular, la Directiva (UE) 2019/2161 “para una mejor aplicación y modernización de las normas de la UE en materia de protección de los consumidores”. La modernización también continuó durante la presidencia de Von der Leyen, con la identificación, en la mencionada Comunicación 2020, de cinco áreas prioritarias clave: por supuesto, la “transformación digital”, pero también la transición verde; la reparación y la aplicación de los derechos de los consumidores; las necesidades específicas de determinados grupos de consumidores; y la cooperación internacional.

Se terminó de imprimir en los
talleres de iVerso Impresión,
en mayo de 2025, por encargo de
Palestra Jurídica S. L.

