

..ReCrim2026..

EL MACHINE LEARNING PARA LA PREVENCIÓN DEL BLANQUEO DE DINERO DESDE LA PERSPECTIVA DEL SECTOR FINANCIERO: BENEFICIOS OPERATIVOS Y DESAFÍOS ÉTICOS Y JURÍDICOS

Yago González Quinzán

Investigador predoctoral (FPU). Universidad de Santiago de Compostela

Automatización – Algoritmo – Explicabilidad – Chatbots - Sesgos
Automation – Algorithms – Explainability – Chatbots - Bias

Se analiza la aplicación del *Machine Learning* (en adelante, ML) para la adopción de modelos de prevención del blanqueo, especialmente relevantes desde la óptica de las instituciones financieras. El blanqueo de dinero se trata de un fenómeno en constante evolución, que se beneficia de los nuevos productos y servicios financieros, por lo que resulta necesario la búsqueda de sistemas preventivos que superen los esquemas basados en reglas, a los que se les atribuyen un elevado número de falsos positivos. En múltiples investigaciones se han propuesto alternativas predictivas basadas en el ML. Ello se enmarca en la contribución de la Inteligencia Artificial (en adelante, IA) para el diseño de medidas de conocimiento del cliente (en adelante, KYC), el monitoreo continuo de transacciones y la remisión de informes de operaciones sospechosas. El ML se determina como eficiente en la medida en que posibilita una tasa de éxito mayor en la detección del fraude. Con todo, el desarrollo de técnicas predictivas mediante algoritmos se enfrenta a problemas como la escasa calidad de los datos, la falta de explicabilidad de los resultados y la adecuación con la normativa de protección de datos.

This article examines the application of machine learning (hereinafter, ML) to the development of anti-money laundering systems, with particular emphasis on their relevance for financial institutions. Money laundering is a constantly evolving phenomenon that takes advantage of new financial products and services, making it necessary to develop preventive systems capable of overcoming traditional rule-based approaches, which are characterized by high false-positive rates. A growing body of research has proposed predictive models based on ML as an alternative to these conventional systems. In this context, Artificial Intelligence (hereinafter, AI) contributes to the design and implementation of know-your-customer (hereinafter, KYC) measures, continuous transaction monitoring, and the filing of suspicious transaction reports. ML is regarded as an effective tool insofar as it enables higher detection rates for fraudulent and potentially illicit transactions. Nevertheless, the development of algorithmic predictive techniques continues to face significant challenges, including poor data quality, the lack of model explainability, and compliance with data protection law.

Recibido: 27/07/26

Publicado: 30/08/2026

© 2026 Los derechos de la presente contribución corresponden a sus autores; los signos distintivos y la edición son propiedad del Instituto U. de Investigación en Criminología y CC.PP. La cita está permitida en los términos legalmente previstos, haciendo siempre expresa mención de autoría y de la disponibilidad en línea en <http://www.uv.es/recrim>

SUMARIO: I. Introducción II. La superación de los sistemas basados en reglas para la prevención del blanqueo de dinero III. La modernización y la optimización de los servicios financieros mediante la IA IV. El papel del sector financiero en la prevención del blanqueo de dinero en el marco de la digitalización actual V. La IA al servicio del sector financiero

para la prevención del blanqueo de dinero VI. El ML como herramienta para la detección de operaciones sospechosas VI.1 Aproximación y evaluación del ML para la prevención del blanqueo de dinero VI.2 Enfoques de ML para la prevención del blanqueo de dinero VII. Retos ante la aplicación de la IA en los sistemas de prevención del blanqueo de dinero VII.1 Planteamiento general VII.2 Explicabilidad y transparencia algorítmica VII.3 Sesgos algorítmicos y riesgo de discriminación VII.4 Disponibilidad de datos y desafíos derivados de la normativa de protección de datos VII.5 Aspectos organizativos, técnicos y económicos en la implantación del ML VIII. La escasa regulación en España para la aplicación del ML en el sector financiero IX. Conclusiones X. Bibliografía

I. Introducción

La Agenda 2030, aprobada por la Asamblea General de las Naciones Unidas en 2015, articula un conjunto de diecisiete Objetivos de Desarrollo Sostenible (en adelante, ODS) destinados a promover un crecimiento económico, social e institucional equilibrado¹. Entre ellos, el Objetivo n.º 16 adquiere una relevancia especial al incorporar metas orientadas al fortalecimiento del Estado de Derecho, la reducción de la criminalidad y la disminución de las distintas manifestaciones de violencia². Respecto a la presente investigación, partimos de que en la meta 16.4 se puede incluir el combate contra el blanqueo de dinero. A partir de la consideración de este último como amenaza para la seguridad global³, la prevención del blanqueo se concibe como clave para frenar la circulación de flujos financieros ilícitos. Este objetivo constituye un gran desafío que, debido a su complejidad, exige estudiar el uso de la capacidad predictiva y el análisis de patrones mediante técnicas de ML.

El blanqueo de dinero se define tradicionalmente desde una perspectiva criminológica como un proceso con tres fases sucesivas⁴, si bien precisa VIDALES RODRÍGUEZ⁵ que no todas ellas tienen que darse obligatoriamente en los esquemas delictivos. En una primera etapa, denominada colocación, los fondos de origen delictivo son incorporados al circuito financiero. Posteriormente, durante la fase de estratificación, se realizan numerosas transferencias para, a través de la circulación, dificultar la identificación de la procedencia de los activos. Finalmente, en la fase de integración, los recursos se reinvierten en la economía con una apariencia de legitimidad que dificulta su vinculación con la actividad criminal de origen. La referencia a las etapas clásicas asociadas al blanqueo es importante porque corrobora la idea de que las instituciones financieras soportan una exposición elevada frente al riesgo de ser instrumentalizadas para el delito⁶.

¹ CANHOTO, A. I. (2021): “*Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective*”, *Journal of Business Research*, n.º 131, p. 441.

² *Ibidem*.

³ MATA LLÍN EVANGELIO, Á. (2023): “La prueba del origen ilícito de los bienes y otros problemas interpretativos del blanqueo de capitales”, *Revista Penal México*, n.º 23, p. 48.

⁴ HOROBETS, N. et al. (2025): “*Artificial intelligence technologies in banking: challenges and opportunities for anti-money laundering in the context of EU regulatory initiatives*”, *Journal of Money Laundering Control*, vol. 28, n.º 4-5, p. 596.

⁵ VIDALES RODRÍGUEZ, C. (2012): “Blanqueo, ¿qué es blanqueo? Estudio del artículo 301.1 del Código Penal Español tras la reforma de la L.O. 5/2010”, *Revista General de Derecho Penal*, n.º 18, p. 3.

⁶ APRILIA, G. F. y MEIRYANI, M. (2024): “*Exploring detection and prevention of money laundering with information technology*”, *Journal of Money Laundering Control*, vol. 27, n.º 6, p. 998.

La prevención del blanqueo constituye un instrumento esencial para combatir la delincuencia organizada que, como indica LEÓN ALAPONT⁷, se considera en el seno de la Unión Europea (en adelante, UE) como un riesgo prioritario para el Estado de Derecho y la democracia. La lucha contra las actividades criminales de blanqueo se realiza tanto con la articulación de mecanismos preventivos, como con el diseño adecuado de medidas penales⁸. En punto a la primera opción, las entidades financieras deben cumplir con ciertas obligaciones de control, no solo a causa de la decisión de cada estado, sino en el marco de lo estipulado por las 40 Recomendaciones del Grupo de Acción Financiera Internacional (en adelante, GAFI)⁹. Dicho documento viene a imponer a las instituciones financieras -con remisión a la Sección D, sobre Medidas Preventivas, y, en particular, a las Recomendaciones n.º 10 a 21- el cumplimiento de diversos deberes referidos a la verificación de la identidad de los clientes, la evaluación de los riesgos asociados a cada relación de negocio, el seguimiento de las operaciones y la comunicación a las autoridades de las transacciones que presenten indicios de actividad ilícita¹⁰. Todo ello bajo la adopción de un enfoque basado en el riesgo¹¹.

Las 40 Recomendaciones del GAFI, recogidas en los distintos ordenamientos jurídicos, determinan que las instituciones financieras deban incorporar procedimientos destinados a impedir que los bienes delictivos accedan al sistema financiero. El GAFI, desde sus primeras actuaciones, ha impulsado la incorporación de soluciones tecnológicas en orden a incrementar la eficacia en la detección, incluido el ML¹². La digitalización de las operaciones financieras genera numerosos datos que pueden ser examinados mediante técnicas avanzadas en orden a reconstruir patrones de comportamiento, identificar vínculos entre sujetos y detectar estructuras de criminalidad organizada¹³. En consecuencia, el examen masivo de datos, las tecnologías de registro distribuido y las herramientas de IA han adquirido una importancia sin precedentes en los sistemas de prevención del blanqueo¹⁴, los cuales se benefician ahora de las mejoras en el procesamiento informático y en el almacenamiento de datos¹⁵.

Como ya he adelantado, por la posición que ocupan dentro del sistema económico, las entidades financieras desempeñan una función decisiva en la detección temprana de operaciones ilícitas¹⁶. Pero ello exige la implantación de mecanismos de control y de procedimientos internos avanzados para identificar con éxito y rapidez transacciones

⁷ LEÓN ALAPONT, J. (2026): "Líneas generales de la nueva política de la Unión Europea en materia de corrupción y recuperación de ganancias ilícitas", *ReCRIM: Revista de l'Institut Universitari d'Investigació en Criminologia i Ciències Penals de la UV*, n.º 36, p. 217.

⁸ Para comprender la reacción penal en España contra el crimen organizado, *vid.* VIDALES RODRÍGUEZ, C. y LARRIBA HINOJAR, B. (2015): "Estrategias legales frente a la criminalidad organizada en España", *Revista Penal México*, n.º 8, pp. 215-227.

⁹ HOROBETS, N. *et al.*: *op. cit.*, p. 594.

¹⁰ JENSEN, R. I. T. y IOSIFIDIS, A. (2023): "Fighting Money Laundering with Statistics and Machine Learning", *IEEE Access*, n.º 11, p. 2.

¹¹ *Vid.* FERRÉ OLIVÉ, J. C. (2024): *El delito de blanqueo de dinero*. Tirant lo Blanch, Valencia, p. 63 y ss.

¹² *Vid.* FATF (2021): *Opportunities and Challenges of New Technologies for AML/CFT*. Paris, France. En este documento se indica que el uso de la IA, y en concreto del ML, contribuye a una mejor identificación de riesgos de blanqueo, ya que la IA permite monitorear información en tiempo real. Con la implementación de las nuevas tecnologías comentadas, las instituciones financieras pueden mejorar las evaluaciones de riesgo y reducir costes operativos. Lo anterior se traduce en un mejor cumplimiento de las exigencias normativas.

¹³ CANHOTO, A. I.: *op. cit.*, p. 442.

¹⁴ *Ibidem*.

¹⁵ KUTE, D. V. *et al.* (2021): "Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering—A Critical Review," *IEEE Access*, n.º 9, p. 82307.

¹⁶ HOROBETS, N. *et al.*: *op. cit.*, p. 594.

potencialmente delictivas. A esta última precisión obedece que en lo que se refiere a la prevención del blanqueo se trate de automatizar una parte sustancial de las técnicas de supervisión y de verificación de identidades, con el fin de mejorar la eficiencia operativa¹⁷. En particular, las técnicas de ML han adquirido un papel destacado debido a su capacidad para procesar grandes volúmenes de datos, reconocer relaciones entre variables y detectar patrones de comportamiento que difícilmente podrían ser identificados mediante metodologías tradicionales¹⁸.

Los modelos de ML, de acuerdo con ABEL SOUTO¹⁹, desempeñan un papel cada vez más relevante en la identificación de comportamientos vinculados con actividades delictivas. Mediante algoritmos capaces de analizar automáticamente grandes cantidades de información, se generan alertas y se contribuye a anticipar riesgos de forma temprana²⁰. De hecho, la utilidad de las tecnologías disruptivas basadas en IA ha motivado la defensa de su incorporación por parte de varias organizaciones internacionales centradas en la lucha contra la delincuencia organizada²¹. Así, Interpol²² promueve el empleo de la IA para reforzar el análisis de redes criminales transnacionales y mejorar la detección de estructuras de criminalidad financiera²³. En la misma línea, Naciones Unidas ha destacado la importancia de promover el uso de tecnologías emergentes que incrementen la trazabilidad, la transparencia y la eficacia de los sistemas destinados a prevenir el blanqueo de dinero²⁴.

La incorporación de la IA supone un avance en el fortalecimiento de los mecanismos de prevención del blanqueo al posibilitar, como indica ÁLVARO PERIS²⁵, que las entidades financieras mejoren su capacidad para supervisar operaciones y detectar comportamientos sospechosos. La utilización de modelos algorítmicos permite identificar un mayor número de indicios de criminalidad económica, al tiempo que contribuye a reducir la elevada tasa de falsas alertas. Las técnicas de ML han demostrado una notable capacidad para extraer conocimiento relevante de amplios conjuntos de datos, identificando relaciones que difícilmente podrían apreciarse mediante métodos basados en reglas. Ampliamente, se indica que su aplicación resulta relevante en dos ámbitos concretos²⁶: los procedimientos KYC²⁷ y la monitorización de operaciones.

¹⁷ CHEN, Z. *et al.* (2018): “Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review”, *Knowledge and Information Systems*, n.º 57, p. 278.

¹⁸ GANDHAR, A. *et al.* (2024): “Fraud Detection Using Machine Learning and Deep Learning”, *SN Computer Science*, vol. 5, p. 1.

¹⁹ ABEL SOUTO, M. (2025): “Inteligencia artificial en la prevención y represión del blanqueo de dinero”. En GONZÁLEZ URIEL, D., ABADÍAS SELMA, A. y MORELL ALDANA, L. C. (coords.): *Ciberdelincuencia: Perspectiva penal, procesal y criminológica*. La Ley, Madrid, p. 178.

²⁰ *Ibidem*.

²¹ HOROBETS, N. *et al.*: *op. cit.*, p. 598.

²² Sobre una concreción del potencial de la IA, y en particular del ML, *vid.* INTERPOL (2024): *Responsible AI Innovation in Law Enforcement. AI Toolkit Technical Reference Book*.

²³ HOROBETS, N. *et al.*: *op. cit.*, p. 598.

²⁴ *Ibidem*.

²⁵ ÁLVARO PERIS, C. (2025): “Inteligencia artificial y blanqueo de capitales: prevención y comisión del delito”. En ABEL SOUTO, M., LORENZO SALGADO, J. M. y SÁNCHEZ STEWART, N. (coords.): *X Congreso Internacional sobre prevención y represión del blanqueo de dinero*. Tirant lo Blanch, Valencia, p. 557.

²⁶ ALKHALILI, M. *et al.* (2021): “Investigation of Applying Machine Learning for Watch-List Filtering in Anti-Money Laundering”, *IEEE Access*, n.º 9, p. 18483.

²⁷ NIE, C. *et al.* (2026): “AI Application in Anti-Money Laundering for Sustainable and Transparent Financial Systems”. En AA. VV.: *Proceedings of the 2025 International Conference on Artificial Intelligence and Sustainable Development. Association for Computing Machinery, New York*, p. 241. Los avances en IA permiten desarrollar modelos dinámicos de evaluación del riesgo que actualizan

Una característica relevante de los algoritmos del ML consiste en su capacidad de mejora continua²⁸. Los modelos pueden incorporar la experiencia obtenida tras cada evaluación, corrigiendo errores y ajustando sus parámetros conforme a la nueva información. Este aprendizaje incrementa la precisión de las predicciones y permite adaptar los mecanismos de detección a la evolución de las amenazas²⁹. Por tanto, a diferencia de los sistemas estáticos, los algoritmos de ML pueden perfeccionar sus mecanismos de detección mediante procesos de entrenamiento, permitiendo en el caso de las entidades financieras anticiparse a las amenazas emergentes. En particular, los modelos de ML muestran una elevada capacidad para descubrir esquemas complejos de blanqueo que frecuentemente permanecen ocultos cuando se emplean mecanismos basados en reglas predefinidas.

No obstante, la incorporación de algoritmos de ML en los sistemas de prevención del blanqueo plantea importantes retos que requieren un desarrollo normativo y una reflexión técnica para garantizar una utilización compatible con los principios básicos de cada ordenamiento jurídico³⁰; en este sentido, como precisa MATA LLÍN EVANGELIO³¹, la percepción del blanqueo como amenaza global vinculada al crimen organizado no puede significar una expansión desmesurada de los mecanismos de reacción que atente contra valores fundamentales. En particular, los desafíos comentados pueden agruparse en dos categorías³². La primera responde a la dimensión normativa. La IA exige, como señala LEAL RUÍZ³³, la configuración de un marco jurídico que permita aprovechar sus capacidades sin menoscabar derechos fundamentales, en equiparación a lo que se predica en punto al diseño de estrategias de seguridad, las cuales se deben interpretar desde la perspectiva de las libertades públicas³⁴. La segunda engloba las limitaciones inherentes a los propios modelos de ML: aunque estas técnicas suelen ofrecer un rendimiento predictivo superior al de los enfoques econométricos convencionales, presentan ciertas dificultades³⁵, como las relacionadas con la explicabilidad de los resultados, la estabilidad de las predicciones y el riesgo de reproducir sesgos presentes en los datos de entrenamiento³⁶.

continuamente el perfil del cliente conforme incorporan nueva información procedente de su actividad financiera y de las relaciones que mantiene dentro del sistema.

²⁸ GIMENO, R. y MARQUÉS, J. M. (2022): “Tradición e inteligencia artificial: oportunidades y retos del *machine learning* para los servicios financieros”, *ICE: Revista de economía*, n.º 926, p. 110.

²⁹ OYEDOKUN, O. et al. (2024): “A Comprehensive Review of Machine Learning Applications in AML Transaction Monitoring”, *International Journal of Engineering Research and Development*, vol. 20, n.º 11, p. 734.

³⁰ GIMENO, R. y MARQUÉS, J. M.: *op. cit.*, p. 116.

³¹ MATA LLÍN EVANGELIO, Á. (2018): “Blanqueo de capitales y principios penales”, *Teoría y derecho: Revista de Pensamiento Jurídico*, n.º 24, (ejemplar dedicado a: Garantías constitucionales, prensa y Derecho penal), p. 274.

³² GIMENO, R. y MARQUÉS, J. M.: *op. cit.*, p. 116.

³³ LEAL RUÍZ, R. (2024): “Entre la eficiencia y la opacidad: inteligencia artificial en la prevención del blanqueo de capitales”. En ABADÍAS SELMA, A. y GONZÁLEZ URIEL, D. (coords.): *El impacto de la IA en el aprendizaje y en la práctica del derecho*. Aranzadi La Ley, Madrid, p. 401.

³⁴ GONZÁLEZ CUSSAC, J. L. y FLORES GIMÉNEZ, F. (2017): “Una metodología para el análisis de las amenazas a la seguridad, la evaluación de las respuestas y su impacto sobre los derechos fundamentales”, *Cuadernos de estrategia*, n.º 188 (ejemplar dedicado a Seguridad global y derechos fundamentales), p. 29.

³⁵ GIMENO, R. y MARQUÉS, J. M.: *op. cit.*, p. 117.

³⁶ Estos aspectos adquieren una especial relevancia en un ámbito fuertemente regulado como el financiero, donde la adopción de decisiones automatizadas debe satisfacer elevados estándares de transparencia, fiabilidad y rendición de cuentas.

Añadimos que la expansión de la IA ha abierto un amplio debate acerca de los límites que deben regir su diseño, desarrollo e implementación³⁷. Antes de establecer un régimen normativo, resulta imprescindible identificar los principios éticos que deben orientar su empleo, pues solo a partir de ello es posible definir los contornos legales que garanticen una utilización responsable, proporcionada y compatible con los derechos fundamentales³⁸. Ahora bien, la evaluación de los riesgos asociados a la IA no puede realizarse de forma uniforme, ya que su impacto varía según el contexto de aplicación³⁹. Aspectos como la proliferación de sesgos o las dificultades para interpretar el razonamiento algorítmico presentan distinta intensidad dependiendo de la finalidad y de las consecuencias de la decisión automatizada⁴⁰.

II. La superación de los sistemas basados en reglas para la prevención del blanqueo de dinero

Los sistemas de detección fundamentados en reglas constituyen el modelo predominante para la identificación de operaciones fraudulentas en el ámbito financiero⁴¹. Estos mecanismos tratan de lograr el objetivo preventivo mediante la definición de umbrales que permitan señalar que ciertas transacciones están asociadas a finalidades ilícitas⁴². En el ámbito de la prevención del blanqueo, esta aproximación continúa siendo utilizada por las instituciones financieras para dar cumplimiento a las exigencias preventivas estipuladas esencialmente en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Este texto normativo recoge de forma elemental el contenido de actuaciones supranacionales, tales como las 40 Recomendaciones del GAFI o las directivas europeas sobre prevención del blanqueo⁴³.

Es cierto que una de las ventajas de los sistemas basados en reglas reside en la transparencia de sus criterios de decisión, ya que cada alerta puede vincularse con una regla previamente definida. Además, la relativa simplicidad de implementación favorece la expansión de este enfoque⁴⁴. No obstante, la metodología presenta ahora problemas: las alertas generadas requieren posteriormente una evaluación individualizada para determinar si los indicios corresponden a operaciones sospechosas o si, por el contrario, constituyen falsos positivos⁴⁵. Además, conforme a la evolución de las tipologías de

³⁷ HERNÁNDEZ OSORIO, J. A. (2024): “Inteligencia artificial: implicaciones éticas fundamentales para su regulación en el marco constitucional del siglo XXI”. En ABADÍAS SELMA, A. y GONZÁLEZ URIEL, D. (coords.): *El impacto de la IA en el aprendizaje y en la práctica del derecho*. Aranzadi La Ley, Madrid, p. 83.

³⁸ *Ibidem*.

³⁹ FERNÁNDEZ, A. (2019): “Inteligencia artificial en los servicios financieros”, *Boletín económico - Banco de España*, n.º 2, p. 7.

⁴⁰ LEAL RUÍZ, R.: *op. cit.*, p. 401.

⁴¹ MANAVADARIA, M. S. *et al.* (2025): “*Machine Learning for Fraud Detection and Financial Crimes*”. En AA. VV. (eds.): *Forensic Intelligence and Deep Learning Solutions in Crime Investigation*. IGI Global Scientific Publishing, Pennsylvania, p. 186.

⁴² *Ibidem*.

⁴³ EDDIN, A. N. *et al.* (2021): “*Anti-money laundering alert optimization using machine learning with graphs*”, *Computer Sciences*, n.º 12, p. 2.

⁴⁴ *Ibidem*.

⁴⁵ CHEN, Z. *et al.*: *op. cit.*, p. 246.

blanqueo, resulta necesario incorporar continuamente nuevas reglas, incrementándose la complejidad de un sistema caracterizado inicialmente por su sencillez⁴⁶.

Más concretamente, los modelos basados en reglas afrontan diversos problemas estructurales: la dificultad para mantener actualizadas las reglas, la imposibilidad práctica de asignar una ponderación adecuada a un gran número de criterios y la elevada tasa de falsos positivos derivada de la aplicación de umbrales rígidos sobre comportamientos financieros cada vez más heterogéneos⁴⁷. A los tres aspectos mencionados se suma la limitada capacidad para integrar y analizar información procedente de fuentes de diversa naturaleza, incluyendo datos estructurados y no estructurados⁴⁸. Estas limitaciones descritas adquieren especial relevancia en el caso de las entidades financieras, donde el volumen de información supera ampliamente a los modelos tradicionales⁴⁹.

La falta de detección de operaciones de blanqueo expone a las entidades financieras a múltiples consecuencias⁵⁰. Además de las sanciones administrativas que pueden imponerse por incumplimientos en materia de prevención⁵¹, la pérdida de confianza por parte de clientes e inversores puede comprometer la estabilidad de las instituciones. Ello convierte a las soluciones automatizadas de prevención en un elemento indispensable⁵². La creciente digitalización de los servicios financieros, el incremento de los pagos electrónicos y la expansión de nuevos medios de transferencia de valor han puesto de manifiesto la necesidad de desarrollar mecanismos de detección más avanzados⁵³. A ello se añade la evolución mediante criptoactivos del cibercrimen que, con una incidencia clara mismamente en los planteamientos más básicos del derecho penal⁵⁴, ha permitido a las organizaciones criminales diseñar actividades de blanqueo más sofisticadas⁵⁵.

Pese a su implantación, los sistemas basados en reglas tienen una naturaleza estática que impide responder con suficiente eficacia en la actualidad ante la realidad del blanqueo de dinero. Ello se debe a que cualquier modificación exige una intervención previa para incorporar nuevas reglas⁵⁶. Esta circunstancia facilita que las organizaciones criminales adapten sus métodos con mayor rapidez que los propios mecanismos de control y aprovechen las lagunas de los sistemas de detección⁵⁷. Por ello, los modelos tradicionales basados en reglas predefinidas se definen en la actualidad como sistemas

⁴⁶ Esta acumulación de criterios dificulta la coherencia del conjunto, reduce la capacidad de adaptación frente a patrones delictivos cambiantes y complica la evaluación objetiva del rendimiento alcanzado con cada una de las reglas.

⁴⁷ KUTE, D. V. *et al.*: *op. cit.*, p. 82304.

⁴⁸ HAN, J. *et al.* (2020): “*Artificial intelligence for anti-money laundering: a review and extension*”, *Digital Finance*, n.º 2, p. 8.

⁴⁹ Al depender exclusivamente de reglas previamente configuradas, los sistemas comentados carecen de mecanismos que les permitan aprender automáticamente de nuevos comportamientos o generalizar el conocimiento adquirido ante modalidades de blanqueo de dinero.

⁵⁰ EDDIN, A. N. *et al.*: *op. cit.*, p. 2.

⁵¹ En el caso español llamamos a confrontar el Capítulo VIII de la Ley 10/2010, de 28 de abril.

⁵² EDDIN, A. N. *et al.*: *op. cit.*, p. 2.

⁵³ HOROBETS, N. *et al.*: *op. cit.*, p. 594.

⁵⁴ Señala González Cussac que la aparición de nuevas tecnologías obliga al derecho penal a actualizarse en dos sentidos determinados: la definición de qué conducta constituye un delito (aspectos propios de tipificación) y la atribución del debido castigo (cumplimiento de la proporcionalidad); *vid.* GONZÁLEZ CUSSAC, J. L. (2011): “Estrategias legales frente a las ciberamenazas”, *Cuadernos de estrategia*, n.º 149 (ejemplar dedicado a: Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio), p. 110 y ss.

⁵⁵ HOROBETS, N. *et al.*: *op. cit.*, p. 594.

⁵⁶ MANAVADARIA, M. S. *et al.*: *op. cit.*, p. 187.

⁵⁷ *Ibidem*.

limitados en punto a la identificación de esquemas complejos de fraude, derivando muchas reacciones en alertas incorrectas, con el consiguiente coste operativo que supone la revisión de operaciones realmente legítimas⁵⁸.

III. La modernización y la optimización de los servicios financieros mediante la IA

Apunta ESCAJEDO SAN EPIFANIO⁵⁹ que desde los primeros desarrollos de la IA en la década de 1950, el reconocimiento de patrones y las redes neuronales han constituido el núcleo de la investigación, sentando las bases de las actuales técnicas de ML y de aplicaciones como el reconocimiento de imágenes, voz y datos biométricos. Esta precisión inicial nos da pie para exponer igualmente que la expresión “*Artificial Intelligence*” fue introducida durante la Conferencia de *Dartmouth* celebrada en 1956⁶⁰, para describir, como indica SERRANO ACITORES⁶¹, la disciplina orientada a desarrollar sistemas capaces de reproducir procesos propios de la inteligencia humana. En tal punto se cifra el inicio de la IA como rama de la informática dedicada a simular capacidades cognitivas mediante máquinas; con todo, durante un largo período su evolución quedó condicionada por las limitaciones computacionales y de almacenamiento de datos⁶².

La IA se consolida ahora como uno de los ejes estratégicos de transformación, “cuyo potencial es inmenso”⁶³, especialmente en el sector financiero, debido a su capacidad para modificar los procesos organizativos. Su presencia continúa expandiéndose hacia ámbitos diversos, impulsando cambios tanto en la prestación de los servicios, la toma de decisiones, como en el tratamiento de la información. La incorporación de la IA permite desarrollar productos financieros más eficientes, seguros e innovadores, acelerando los procesos del sector. PARAMESHA *et al.*⁶⁴ ponen de relieve que la IA constituye un importante motor de innovación en los mercados financieros. Con todo, su incorporación no debe entenderse como un mecanismo destinado a sustituir la intervención humana⁶⁵, sino como una herramienta orientada a reforzar la calidad de los

⁵⁸ GANDHAR, A. *et al.*: *op. cit.*, p. 2.

⁵⁹ ESCAJEDO SAN EPIFANIO, L. (2025): “Vigilancia biométrica masiva mediante IA y derechos fundamentales: Retos jurídico-constitucionales”. En BALAGUER CALLEJÓN, F. y ESCAJEDO SAN EPIFANIO, L. (dirs.): *Vigilancia biométrica masiva, Inteligencia Artificial y Derechos Fundamentales*. Dykinson, Madrid, p. 31.

⁶⁰ GIMENO, R. y MARQUÉS, J. M.: *op. cit.*, p. 109.

⁶¹ SERRANO ACITORES, A. (2023): “Consideraciones éticas y legales en el uso de la inteligencia artificial: el enfoque de la Unión Europea”, *Revista de fiscalidad internacional y negocios transnacionales*, n.º 24, p. 6.

⁶² *Ibidem*.

⁶³ LEÓN ALAPONT, J. (2024): “La inteligencia artificial al servicio de la desinformación: un nuevo reto para el derecho penal”. En JIMÉNEZ GARCÍA, F. (dir.): *Seguridad y responsabilidad penal e internacional en el uso de las TIC y la inteligencia artificial*. Iustel, Madrid, p. 95.

⁶⁴ PARAMESHA, M. *et al.* (2024): “*Artificial Intelligence, Machine Learning, Deep Learning, and Blockchain in Financial and Banking Services: A Comprehensive Review*”, *Partners Universal Multidisciplinary Research Journal*, vol. 1, n.º 2, p. 73.

⁶⁵ LAKHCHINI, W. *et al.* (2022): “*Artificial Intelligence & Machine Learning in Finance. A literature review*”, *International Journal of Accounting, Finance, Auditing, Management and Economics*, vol. 3, n.º 6, p. 438.

procesos de análisis y de toma de decisiones mediante la combinación entre conocimiento experto y sistemas algorítmicos⁶⁶.

La automatización de tareas repetitivas y la mejora de las capacidades analíticas contribuyen a incrementar la eficiencia operativa de las entidades financieras, a reducir los costes, a elevar la calidad de los servicios prestados y a favorecer una mayor inclusión financiera mediante soluciones personalizadas⁶⁷. Ante un conocimiento más preciso sobre el comportamiento de sus clientes, las entidades financieras pueden de este modo adoptar decisiones mejor fundamentadas y ofrecer una experiencia más satisfactoria⁶⁸. Por ello, la IA se ha extendido hasta el punto de abarcar todas las fases de la cadena de valor del negocio financiero⁶⁹: desde actividades internas de procesamiento y gestión administrativa (*back-office*), pasando por las funciones de supervisión y control de riesgos (*middle-office*), hasta los servicios de atención al cliente, comercialización y participación en los mercados financieros (*front-office*)⁷⁰.

La IA se define como una de las tecnologías con mayor capacidad transformadora en la economía actual y, de manera particular, en el sector financiero⁷¹. Proporciona ventajas para las entidades financieras al mejorar la rapidez, la precisión y la consistencia de numerosos procesos, tales como la gestión de riesgos, los mecanismos de ciberseguridad⁷² y el análisis de información financiera⁷³. Sin perjuicio de lo ya comentado hasta el momento, resulta conveniente enunciar a continuación las manifestaciones concretas más destacables:

- Las soluciones de conversación basadas en IA⁷⁴, como los asistentes virtuales y los *chatbots*⁷⁵, se han convertido en instrumentos esenciales destinados a automatizar la atención al cliente⁷⁶, garantizando de tal modo una mayor disponibilidad del servicio y reduciendo los tiempos de respuesta⁷⁷.

⁶⁶ Desde esta perspectiva, la interacción entre el saber humano y la IA constituye un modelo de cooperación que permite incrementar la eficiencia de los servicios financieros.

⁶⁷ FERNÁNDEZ, A.: *op. cit.*, p. 2.

⁶⁸ ESPINOZA VILLAVICENCIO, H. M. (2026): “Modelos predictivos de IA y su relación con la protección contra amenazas persistentes avanzadas del sistema bancario”, *Revista de Investigaciones Científicas y Tecnológicas Industriales*, n.º 1, p. 40.

⁶⁹ FERNÁNDEZ, A.: *op. cit.*, p. 3.

⁷⁰ *Ibidem*.

⁷¹ Reflejo de ello es el impulso al Proyecto *GalaxIA* de CaixaBank, que da continuidad a *GenIAI*, y que se trata de una iniciativa que aborda los usos posibles de la IA generativa para la innovación y la optimización de procesos internos. El proyecto se relaciona especialmente con la dotación de herramientas de asistencia, apoyo a la atención al cliente, mejora de la comunicación con clientes y mayor eficiencia en la gestión de reclamaciones mediante clasificación y tratamiento automatizado.

⁷² Diversas entidades financieras han empleado los servicios de *SEON*, que es una plataforma de ciberseguridad avanzada especializada en la prevención de fraude digital y el cumplimiento normativo. Utiliza IA para analizar en tiempo real la huella digital, el dispositivo y el comportamiento de los usuarios. En el sector financiero, los bancos la contratan para bloquear transacciones ilícitas y prevenir el robo de cuentas. Además, automatiza la verificación de identidad para evitar la creación de perfiles falsos y combatir el blanqueo de dinero.

⁷³ PARAMESHA, M. *et al.*: *op. cit.*, p. 69.

⁷⁴ GIMENO, R. y MARQUÉS, J. M.: *op. cit.*, p. 111.

⁷⁵ HOROBETS, N. *et al.*: *op. cit.*, p. 596.

⁷⁶ La utilización de asistentes virtuales y sistemas de conversación inteligentes ha transformado la relación entre las entidades financieras y sus clientes. Estas soluciones no solo agilizan la gestión de consultas y solicitudes, sino que comienzan a incorporar funcionalidades de apoyo al asesoramiento financiero, mejorando la accesibilidad y disponibilidad de los servicios. Todo ello repercute favorablemente en la satisfacción de los usuarios, quienes reciben respuestas más rápidas y, potencialmente, una reducción de los costes asociados a determinadas operaciones.

⁷⁷ FERNÁNDEZ, A.: *op. cit.*, p. 2.

- La IA ha favorecido la implantación de mecanismos avanzados de autenticación de la identidad, entre los que destacan los sistemas de verificación biométrica y las soluciones basadas en el análisis del comportamiento de los usuarios⁷⁸.
- El análisis masivo de datos mediante algoritmos de ML permite comprender las preferencias y los comportamientos de los usuarios, favoreciendo una oferta más personalizada⁷⁹.
- La automatización robotizada de procesos (en adelante, RPA) permite ejecutar de forma automática tareas repetitivas⁸⁰, altamente estandarizadas⁸¹.
- Las soluciones basadas en IA permiten monitorizar la actividad financiera con el fin de detectar comportamientos susceptibles de constituir operaciones de fraude o de blanqueo⁸². Especial relevancia adquieren los modelos de ML, cuya ventaja radica en que, mientras los sistemas basados en reglas permanecen invariables, los algoritmos pueden ser entrenados con información actualizada⁸³.
- Las entidades financieras incorporan cada vez con mayor frecuencia⁸⁴ modelos de ML para apoyar procesos como la clasificación de riesgo de los clientes⁸⁵, lo cual se realiza en función del examen de múltiples datos⁸⁶. En particular, los esquemas de calificación crediticia basados en IA⁸⁷ analizan simultáneamente varias fuentes de información⁸⁸ con el objetivo de estimar la probabilidad de incumplimiento⁸⁹.

En definitiva, la incorporación de soluciones de IA está modificando el funcionamiento del sector financiero al introducir mejoras en diversos ámbitos de la actividad, con incidencia en el cumplimiento, la optimización de la gestión de riesgos, la atención al cliente, los sistemas de evaluación crediticia y los mecanismos destinados a prevenir el fraude. Todo ello deriva en el acuerdo de que las entidades financieras deben aprovechar el potencial que ofrecen las tecnologías basadas en IA, sin comprometer en todo caso los principios éticos⁹⁰ que deben regir su actividad⁹¹. Esta última precisión exige desarrollar estructuras capaces de supervisar el diseño, la implantación y la utilización de los sistemas algorítmicos, garantizando la innovación tecnológica, pero también sobre todo el máximo respeto a los derechos fundamentales.

⁷⁸ PARAMESHA, M. *et al.*: *op. cit.*, p. 72.

⁷⁹ *Ibidem*.

⁸⁰ La RPA desempeña un papel relevante al asumir tareas repetitivas, como la introducción de datos o la elaboración de informes. Ello contribuye a reducir costes de funcionamiento, minimizar errores derivados de la intervención humana y liberar recursos para actividades de carácter estratégico.

⁸¹ HOROBETS, N. *et al.*: *op. cit.*, p. 596.

⁸² OYEDOKUN, O. *et al.*: *op. cit.*, p. 734.

⁸³ *Ibidem*.

⁸⁴ ALONSO, A. y CARBÓ MARTÍNEZ, J. M. (2021): “*Understanding the performance of machine learning models to predict credit default: A novel approach for supervisory evaluation*”, *Documentos de trabajo - Banco de España*, n.º 5, p. 7.

⁸⁵ Los sistemas de IA permiten construir evaluaciones más precisas del perfil de riesgo mediante el análisis conjunto de grandes volúmenes de información y variables de naturaleza diversa.

⁸⁶ HOROBETS, N. *et al.*: *op. cit.*, p. 596.

⁸⁷ GIMENO, R. y MARQUÉS, J. M.: *op. cit.*, p. 112.

⁸⁸ PARAMESHA, M. *et al.*: *op. cit.*, p. 73.

⁸⁹ Como consecuencia, estas herramientas mejoran tanto la calidad de las decisiones relativas a la concesión de financiación como la asignación eficiente de capital y la determinación de las provisiones necesarias en función del riesgo asumido por la entidad.

⁹⁰ HAN, J. *et al.*: *op. cit.*, p. 8.

⁹¹ GIMENO, R. y MARQUÉS, J. M.: *op. cit.*, p. 117.

IV. El papel del sector financiero en la prevención del blanqueo de dinero en el marco de la digitalización actual

El sistema financiero constituye uno de los principales canales para introducir en la economía legal recursos procedentes de actividades delictivas⁹²; por tanto, como apunta FERRÉ OLIVÉ⁹³, la regulación administrativa de prevención dibuja a dicho sector “como el generador de mayores riesgos, sin ser lógicamente el único”. Lo señalado se traduce en que las entidades financieras ocupan una posición central en las políticas de prevención del blanqueo⁹⁴. El incumplimiento de las obligaciones en materia de prevención no solo da lugar a consecuencias sancionadoras para las entidades financieras, sino que también compromete su reputación y la confianza de los clientes, inversores y autoridades supervisoras⁹⁵. En un entorno caracterizado por un volumen creciente de operaciones, resulta imprescindible para las entidades reducir los tiempos de análisis de las alertas y agilizar el ciclo de investigación de las transacciones potencialmente sospechosas⁹⁶. Recordamos que, una vez que los fondos de origen ilícito logran incorporarse al circuito económico, las opciones de reconstruir su trazabilidad disminuyen considerablemente.

Los ordenamientos jurídicos imponen a las entidades financieras un conjunto de obligaciones preventivas⁹⁷; entre ellas, la obtención y la conservación de información sobre los clientes, el análisis del riesgo asociado a cada relación de negocio, la supervisión continuada de las operaciones y la comunicación de las actividades que puedan presentar indicios de ilicitud⁹⁸. Estas se destinan a impedir que el sistema financiero sea utilizado como vehículo para el blanqueo⁹⁹. La identificación de operaciones sospechosas puede realizarse mediante la intervención directa de los empleados de una entidad financiera cuando, en el desarrollo de su actividad, detectan comportamientos inusuales por parte de un cliente¹⁰⁰. Sin embargo, la expansión de los servicios financieros, con el dominio actual de la despersonalización de las operaciones, ha reducido la viabilidad de este modelo¹⁰¹.

La generalización de la banca electrónica y el crecimiento del comercio digital han provocado un incremento exponencial del número de transacciones procesadas diariamente, circunstancia que ha ampliado simultáneamente las oportunidades para la comisión del blanqueo y otras formas de delincuencia económica¹⁰². En este escenario, el aumento de la capacidad para identificar de forma temprana acciones sospechosas se ha

⁹² HOROBETS, N. *et al.*: *op. cit.*, p. 596.

⁹³ FERRÉ OLIVÉ, J. C.: *El delito de...*, *cit.*, p. 63.

⁹⁴ Como ejemplo, piénsese en el hecho de que todas las directivas comunitarias contienen una referencia en su título a la prevención de la utilización del sistema financiero para el blanqueo.

⁹⁵ HAN, J. *et al.*: *op. cit.*, p. 4.

⁹⁶ ALKHALILI, M. *et al.*: *op. cit.*, p. 18495.

⁹⁷ Acerca de la consagración de un *compliance* obligatorio en el que distintos sujetos, especialmente del sector bancario, deben cumplir con múltiples medidas de prevención del blanqueo, *vid.* FERRÉ OLIVÉ, J. C. (2025): “Reflexiones en torno al *compliance* penal y a la ética en la empresa”, *Revista Penal*, n.º 44, p. 73.

⁹⁸ HOROBETS, N. *et al.*: *op. cit.*, p. 596.

⁹⁹ Sobre las instituciones financieras recae la carga de un modelo de vigilancia permanente cuyo objetivo consiste en identificar, investigar y reportar las operaciones susceptibles de estar relacionadas con actividades delictivas.

¹⁰⁰ ZHANG, Y. y TRUBEY, P. (2019): “*Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection*”, *Computational Economics*, n.º 54, p. 1044.

¹⁰¹ *Ibidem*.

¹⁰² PARAMESHA, M. *et al.*: *op. cit.*, p. 73.

convertido en una prioridad estratégica para todas las entidades financieras¹⁰³, que deben disponer de mecanismos avanzados para responder a modalidades delictivas cada vez más complejas¹⁰⁴. De este modo, puede decirse que ha sido la propia actividad financiera actual la que ha impulsado a las instituciones a automatizar procesos mediante la incorporación de tecnologías basadas en la IA¹⁰⁵.

El interés suscitado por los algoritmos de ML se explica, fundamentalmente, debido a su capacidad para identificar patrones de comportamiento complejos a partir del análisis de grandes volúmenes de datos. A diferencia de los sistemas tradicionales sustentados en reglas, cuya eficacia disminuye conforme evolucionan las estrategias de las organizaciones criminales, los modelos algorítmicos pueden adaptarse a nuevos riesgos mediante el aprendizaje obtenido de los datos de entrada. Esta capacidad permite reducir la probabilidad de que operaciones sospechosas permanezcan sin detectar, al tiempo que mejora la precisión de los sistemas de supervisión. Los algoritmos son capaces de descubrir correlaciones y estructuras de comportamiento que difícilmente resultarían identificables mediante el análisis tradicional, reforzando la eficacia de los programas de prevención del blanqueo de las entidades financieras¹⁰⁶.

En resumen, la necesidad de identificar las operaciones sospechosas en el mismo momento en que se producen convierte la capacidad de respuesta en un elemento esencial para limitar el impacto económico del fraude¹⁰⁷. El ML ha modificado sustancialmente las posibilidades de análisis disponibles para las instituciones financieras. La utilización de modelos algorítmicos permite descubrir relaciones complejas, identificar anomalías y reconocer patrones de comportamiento que permanecerían ocultos mediante el seguimiento de procedimientos convencionales. Estas capacidades explican el interés de las entidades financieras por incorporar la IA a la prevención del blanqueo¹⁰⁸, partiendo como he indicado del aumento del volumen de transacciones, la rápida evolución de las tipologías delictivas y la intensificación de las exigencias legales¹⁰⁹.

V. La IA al servicio del sector financiero para la prevención del blanqueo de dinero

La evolución de la delincuencia económica ha ido acompañada del desarrollo de mecanismos de detección más sofisticados¹¹⁰ impulsados, de acuerdo con ÁLVAREZ

¹⁰³ KUTE, D. V. *et al.*: *op. cit.*, p. 82301.

¹⁰⁴ GANDHAR, A. *et al.*: *op. cit.*, p. 9.

¹⁰⁵ KUTE, D. V. *et al.*: *op. cit.*, p. 82301.

¹⁰⁶ HAN, J. *et al.*: *op. cit.*, p. 4.

¹⁰⁷ Destacamos en este punto que *Sopra Steria* e *Iberpay* han desarrollado un proyecto basado en IA y ML para reforzar la detección del fraude y la prevención del blanqueo en el sistema nacional de pagos. La solución identifica patrones anómalos en las transferencias bancarias mediante el análisis avanzado de datos y el entrenamiento continuo de modelos predictivos. La iniciativa contribuye a una detección más temprana de operaciones potencialmente fraudulentas, reforzando la seguridad del sistema financiero.

¹⁰⁸ Por ejemplo, la tecnología avanzada de *Siopelia-GEB*, para la prevención del blanqueo, desarrollada por el *Grupo AIA*, y que incorpora modelos de ML e IA para el análisis automatizado de grandes volúmenes de datos, identificando patrones de comportamiento y anomalías, ha sido implantada por entidades como CaixaBank, Banco Sabadell, Kutxabank, Banco Santander, BBVA y Unicaja Banco.

¹⁰⁹ MANZOOR, M. F. y ASLAM, M. F. (2025): “*Enhancing Banking Fraud Detection: Role of Machine Learning and Deep Learning Methods*”, *Premier Journal of Artificial Intelligence*, n.º 3, p. 1.

¹¹⁰ Hasta la misma AEAT ha desarrollado una herramienta llamada *Nidel*, que combina *Big Data*, IA y algoritmos de análisis para detectar redes de blanqueo mediante el cruce masivo de información. El sistema analiza simultáneamente múltiples bases de datos para identificar incrementos patrimoniales injustificados

JAREÑO¹¹¹, por los avances tecnológicos y por la disponibilidad de nuevas herramientas de análisis de datos. La IA ha adquirido un papel central como instrumento de apoyo a la toma de decisiones, al proporcionar modelos capaces de analizar información compleja con un elevado grado de precisión. Su utilización permite disminuir la generación de alertas innecesarias que tradicionalmente caracterizaban a los sistemas convencionales¹¹². Frente a los modelos basados en reglas predefinidas, cuya eficacia disminuye cuando los delincuentes modifican sus estrategias, los algoritmos de ML poseen la capacidad de aprender a partir de grandes volúmenes de información y descubrir relaciones que no resultan comprensibles mediante la utilización de técnicas basadas en reglas¹¹³.

El sector financiero constituye uno de los ámbitos donde la aplicación de la IA ha demostrado un mayor potencial para mejorar la detección del fraude económico¹¹⁴. La enorme cantidad de operaciones que procesan diariamente las entidades hace imprescindible disponer de herramientas capaces de identificar de forma rápida comportamientos contrarios a la legalidad¹¹⁵. Los algoritmos de ML ofrecen una solución especialmente adecuada al permitir automatizar el análisis de grandes volúmenes de datos y reforzar los mecanismos de prevención frente a nuevas modalidades de fraude¹¹⁶. Una de las principales fortalezas de estas tecnologías reside en su capacidad para procesar datos de naturaleza diversa, incluyendo no solo aquellos estructurados, sino también contenidos no estructurados, como imágenes o grabaciones de voz¹¹⁷.

El análisis de grupos de datos permite identificar tendencias y estimar la evolución de determinadas modalidades delictivas. Esta capacidad facilita una asignación más eficiente de los recursos destinados a la supervisión, permitiendo intensificar las actuaciones de control en los ámbitos donde el riesgo resulta más elevado. La IA favorece un proceso continuo de mejora de los mecanismos de reacción frente a la criminalidad económica¹¹⁸. Téngase en cuenta que los modelos algorítmicos pueden adaptarse a nuevas estrategias utilizadas por las organizaciones criminales, lo que incrementa la capacidad de respuesta conforme evolucionan las técnicas empleadas para ocultar el origen ilícito de los bienes¹¹⁹. La eficacia de estas tecnologías ha impulsado, como destaca LEAL

y vínculos con actividades delictivas. Además, integra información sobre personas, sociedades, productos bancarios y propiedades para generar perfiles de riesgo. Su finalidad es reforzar la detección de operaciones de blanqueo y optimizar las investigaciones patrimoniales y financieras.

¹¹¹ ÁLVAREZ JAREÑO, J. A. *et al.* (2019): “Aplicación de métodos estadísticos, económicos y de aprendizaje automático para la detección de la corrupción”, *Revista internacional de transparencia e integridad*, n.º 9, p. 2.

¹¹² HAN, J. *et al.*: *op. cit.*, p. 4.

¹¹³ OYEDOKUN, O. *et al.*: *op. cit.*, p. 734.

¹¹⁴ PARAMESHA, M. *et al.*: *op. cit.*, p. 73.

¹¹⁵ Podemos destacar en este sentido los servicios ofrecidos por *Scalian Spain*, que diseña modelos de IA para la prevención del fraude. La empresa utiliza técnicas de análisis avanzado de datos y *Big Data* para mejorar el rendimiento operativo y proteger los activos de las instituciones. Igualmente, diseña e implementa modelos analíticos basados en IA para la detección temprana de fraude, así como optimiza sistemas automatizados para la prevención del blanqueo.

¹¹⁶ HERNÁNDEZ AROS, L. *et al.* (2024): “Financial fraud detection through the application of machine learning techniques: a literature review”, *Humanities and Social Sciences Communications*, n.º 11, p. 2.

¹¹⁷ CANHOTO, A. I.: *op. cit.*, p. 443.

¹¹⁸ ESPINOZA VILLAVICENCIO, H. M.: *op. cit.*, p. 48.

¹¹⁹ Esta actualización permanente contribuye a desarrollar sistemas de protección cada vez más sofisticados y alineados con un entorno de amenazas en constante transformación.

RUÍZ¹²⁰, la participación del sector privado en el desarrollo de soluciones avanzadas para la prevención del blanqueo de dinero¹²¹.

La combinación entre IA y *RegTech*¹²² facilita la automatización de numerosas funciones relacionadas con la supervisión, permitiendo gestionar de forma más eficiente tanto las obligaciones de cumplimiento como la adaptación a las modificaciones normativas que se producen de manera constante¹²³. Con ello se contribuye a fortalecer la resiliencia organizativa de las entidades financieras, mejorar la confianza de los usuarios y favorecer un funcionamiento más sostenible del ecosistema¹²⁴. Entre las aplicaciones de la IA destacan la elaboración automatizada de informes, la monitorización de las operaciones financieras, la evaluación de riesgos y la actualización de los procedimientos internos conforme evolucionan los marcos normativos. En este sentido, las soluciones *RegTech* impulsadas por IA se han convertido en un instrumento esencial para incrementar la eficiencia del cumplimiento¹²⁵.

La IA ofrece un marco adecuado para desarrollar sistemas avanzados capaces de identificar con mayor precisión comportamientos de blanqueo y disminuir la generación de falsas alertas, si bien aún con el reto pendiente de proporcionar explicaciones sobre los criterios utilizados por los modelos de ML en aras de confirmar la transparencia y la confianza en las decisiones automatizadas. La utilización de algoritmos puede derivar en que se considere sospechosa una transacción completamente legítima si esta comparte determinadas características con operaciones previamente identificadas como ilícitas, lo que pone de manifiesto la necesidad de diseñar sistemas con la máxima precisión. Desde esta perspectiva, el desarrollo de soluciones basadas en IA debe incorporar criterios que garanticen la fiabilidad de los resultados, puesto que, de acuerdo con ABEL SOUTO¹²⁶, los modelos algorítmicos no son en todo caso “infalibles”¹²⁷, al igual que LEÓN ALAPONT¹²⁸ advierte que “la IA no es una *bala de plata*” y que “las tecnologías automatizadas son limitadas en su precisión”.

¹²⁰ LEAL RUÍZ, R.: *op. cit.*, p. 399.

¹²¹ La IA ya se usa por empresas para reforzar la monitorización financiera. Podemos ejemplificar esta afirmación con el sistema *Anti-Money Laundering AI* desarrollado por Google, cuyas pretensiones son una mejor elaboración de perfiles de riesgo y la detección temprana de patrones de blanqueo mediante técnicas de ML. Se trata de una alternativa al sistema basado en reglas y se usan los datos en manos de las instituciones financieras para entrenar modelos avanzados de ML. La implementación de prueba de la aplicación se realizó con la entidad HSBC y se determinó un mayor éxito en el número de alertas, reduciendo a su vez hasta en un 60% el número de falsos positivos.

¹²² GÓMEZ JIMÉNEZ, M. L. (2021): “*Regtech*, inteligencia artificial y transformación digital en el mercado financiero: el caso de la atención al cliente usando *chatbots* y las obligaciones de información en la resolución extrajudicial de conflictos”, *Revista de Derecho del Sistema Financiero: mercados, operadores y contratos*, n.º 2, p. 200, que indica que el concepto de *RegTech* consiste en la aplicación de soluciones tecnológicas al cumplimiento normativo, con el objetivo de automatizar, optimizar y reforzar la observancia de las obligaciones regulatorias por parte de las organizaciones. En este sentido destacamos a la empresa británica *Napier AI*, fundada en 2015 y con sede en Londres, que desarrolla soluciones basadas en IA para prevenir el blanqueo y otros delitos financieros; su plataforma *Napier AI Continuum* integra monitoreo de transacciones, filtrado de clientes y optimización de la gestión de riesgos.

¹²³ HOROBETS, N. *et al.*: *op. cit.*, p. 598.

¹²⁴ NIE, C. *et al.*: *op. cit.*, p. 239.

¹²⁵ OYEDOKUN, O. *et al.*: *op. cit.*, p. 742.

¹²⁶ ABEL SOUTO, M.: *op. cit.*, p. 174.

¹²⁷ *Ibidem*. Su funcionamiento depende de la calidad de los datos utilizados para su entrenamiento, de las decisiones adoptadas durante su programación y de un proceso continuo de revisión y ajuste. En consecuencia, la IA no excluye la posibilidad de errores ni elimina la necesidad de una intervención humana constante en su validación y perfeccionamiento.

¹²⁸ LEÓN ALAPONT, J.: “La inteligencia artificial...”, *cit.*, p. 106.

Asimismo, la integración de tecnologías disruptivas basadas en IA exige una planificación estratégica que contemple tanto las inversiones necesarias en infraestructuras tecnológicas como la adaptación de los procedimientos internos. La implantación de soluciones de IA no constituye una mera sustitución tecnológica, sino un proceso de transformación que requiere supervisión. Esto exige la colaboración entre IA y experiencia humana con el fin de desarrollar sistemas más transparentes y adaptables a las tipologías de blanqueo. La IA no reemplaza el saber humano, sino que la primera actúa como una herramienta de apoyo¹²⁹. De hecho, como subraya ALBERRUCHE DÍAZ-FLORES¹³⁰, el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio, por el que se establecen normas armonizadas en materia de IA y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (en adelante, RIA)¹³¹, apoya en su Considerando 27 una supervisión humana durante todo el ciclo de vida de los sistemas de IA, garantizando una intervención real que permita revisar o corregir decisiones automatizadas con efectos perjudiciales.

VI. El ML como herramienta para la detección de operaciones sospechosas

VI.1 Aproximación y evaluación del ML para la prevención del blanqueo de dinero

En la actualidad debemos destacar el hecho de que se haya aprobado el RIA, pues ello contribuye a establecer, como pondera ÁLVARO PERIS¹³², algunas certezas sobre el mismo concepto de IA y el desarrollo que se debe hacer de la misma. Antes de ello, resulta conveniente indicar que el modelo de regulación de la IA trae causa de la Estrategia Europea sobre la Inteligencia Artificial, que impulsó el desarrollo tecnológico mediante la inversión, acompañándose ello de un marco ético y jurídico. El posterior “Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza”, publicado por la Comisión Europea el 19 de febrero de 2020, consolidó un enfoque basado en el riesgo de los usos de la IA, anticipando la arquitectura normativa que encierra ahora el texto de 2024¹³³.

Atendemos tras lo señalado al artículo 3 del RIA, que define los sistemas de IA, si bien advertimos ante todo que establece una definición amplia y tecnológicamente neutra, delimitando el ámbito de aplicación con criterios adaptables a la evolución tecnológica. Esta noción comprende, siguiendo a ALBERRUCHE DÍAZ-FLORES¹³⁴, sistemas con distintos niveles de autonomía y capacidad de inferencia, sin restringirse exclusivamente a técnicas de ML. En particular, en la norma se indica que los sistemas de IA son aquellos basados en máquinas capaces de operar con distintos niveles de

¹²⁹ FATF: *op. cit.*, p. 39, Nota 113, que subraya que la IA es una herramienta de apoyo para procesar grandes volúmenes de información, identificar patrones complejos y facilitar el cumplimiento normativo.

¹³⁰ ALBERRUCHE DÍAZ-FLORES, M. M. (2025): “Europa ante el reto de la inteligencia artificial: una regulación pionera para un futuro responsable”, *Revista de fiscalidad internacional y negocios transnacionales*, n.º 30, p. 9.

¹³¹ Para una visión de las disposiciones más relevantes del RIA, *vid.* LEÓN ALAPONT, J.: “La inteligencia artificial...”, *cit.*, pp. 108 a 111.

¹³² ÁLVARO PERIS, C.: *op. cit.*, p. 556.

¹³³ ALBERRUCHE DÍAZ-FLORES, M. M.: *op. cit.*, p. 3.

¹³⁴ ALBERRUCHE DÍAZ-FLORES, M. M.: *op. cit.*, p. 11.

autonomía y, en su caso, de adaptarse, en orden a inferir, a partir de la información de entrada, resultados tales como predicciones, recomendaciones, contenidos o decisiones, susceptibles de producir efectos sobre entornos físicos o digitales¹³⁵.

El ML y la IA no son conceptos equivalentes. Acogiendo las palabras de ESCOLÁ PÉREZ¹³⁶, preciso que mientras que la IA engloba un conjunto de tecnologías destinadas a reproducir capacidades cognitivas mediante sistemas computacionales, el ML representa una de sus ramas específicas, centrada en el desarrollo de algoritmos capaces de aprender automáticamente a partir de conjuntos de datos y mejorar su comportamiento con el fin de utilizar ese conocimiento para predecir el comportamiento de una o varias variables, sin necesidad de que todas las reglas de decisión sean programadas explícitamente¹³⁷. Para la prevención del blanqueo, esta aproximación presenta ventajas respecto a los modelos basados en reglas. La capacidad de inferir patrones a partir de la información disponible permite superar las limitaciones de los enfoques basados en reglas¹³⁸, cuya adaptación a nuevas modalidades delictivas resulta más lenta al depender de una intervención previa necesaria¹³⁹.

La utilidad del ML radica en la capacidad para identificar patrones de comportamiento, detectar anomalías y estimar niveles de riesgo mediante el tratamiento automatizado de grandes conjuntos de datos, proporcionando a las entidades financieras herramientas de análisis predictivo que favorecen una gestión más avanzada de riesgos asociados a la delincuencia económica¹⁴⁰. Los modelos de ML analizan de manera continua información procedente de múltiples fuentes, permitiendo identificar comportamientos que pueden revelar la existencia de operaciones de blanqueo¹⁴¹. La rapidez con la que estos algoritmos procesan la información incrementa la capacidad de reacción de las entidades financieras y contribuye a reforzar la seguridad de las operaciones.

La incorporación del ML supone una transformación en los sistemas de detección del fraude utilizados por las entidades financieras¹⁴². A diferencia de los enfoques tradicionales, las técnicas algorítmicas automatizan los procesos de decisión mediante modelos capaces de extraer conocimiento a partir de volúmenes de información¹⁴³. Sobre la base de los datos de transacciones realizadas, los algoritmos identifican desviaciones respecto de los patrones habituales y reconocen comportamientos compatibles con actividades fraudulentas¹⁴⁴. Una de las ventajas de estos modelos reside en su capacidad para disminuir la generación de falsos positivos, es decir, aquellas operaciones legítimas clasificadas erróneamente como sospechosas¹⁴⁵. La reducción de estas alertas resulta

¹³⁵ Vid. artículo 3 del RIA.

¹³⁶ ESCOLÁ PÉREZ, M. C. (2021): «Aplicaciones del “*machine learning*” en el sector legal y nuevas profesiones jurídico-tecnológicas», *Revista Aranzadi de derecho y nuevas tecnologías*, n.º 55, p. 13.

¹³⁷ MONTESDEOCA RODRÍGUEZ, D. (2025): “Aportaciones de la inteligencia artificial al desarrollo del *compliance* penal”. En ESTUPIÑÁN CÁCERES, R. y FONTICIELLA HERNÁNDEZ, B. (dirs.): *Una mirada jurídica poliédrica a la normativa europea sobre inteligencia artificial*. Dykinson, Madrid, p. 475.

¹³⁸ GANDHAR, A. et al.: *op. cit.*, p. 9.

¹³⁹ HERNÁNDEZ AROS, L. et al.: *op. cit.*, p. 2.

¹⁴⁰ CHEN, Z. et al.: *op. cit.*, p. 251.

¹⁴¹ COMPAGNINO, A. A. et al. (2025): “An Introduction to Machine Learning Methods for Fraud Detection”, *Applied Sciences*, vol. 15, n.º 21, p. 2.

¹⁴² MANZOOR, M. F. y ASLAM, M. F.: *op. cit.*, p. 3.

¹⁴³ *Ibidem*.

¹⁴⁴ ZHANG, Y. y TRUBEY, P.: *op. cit.*, p. 1044.

¹⁴⁵ OYEDOKUN, O. et al.: *op. cit.*, p. 734.

relevante para las entidades financieras, ya que evita investigaciones innecesarias y concentra los recursos en los casos que presentan un mayor nivel de riesgo¹⁴⁶.

Las técnicas de ML aplicables a la detección del fraude presentan distintos niveles de complejidad, interpretabilidad y exigencia computacional, lo que implica seleccionar la metodología más adecuada en función de las características del problema¹⁴⁷. A partir de lo anterior, la técnica algorítmica incrementa la precisión en la identificación de operaciones fraudulentas, circunstancia que reduce las pérdidas económicas y mejora la protección de los clientes¹⁴⁸. Del mismo modo, estos modelos avanzados ofrecen una capacidad relevante para el análisis prácticamente inmediato de las transacciones. Frente a los sistemas tradicionales, que suelen presentar retrasos entre la ejecución de una operación y su posterior revisión, los algoritmos de ML permiten procesar grandes volúmenes de datos, facilitando una respuesta temprana ante comportamientos ilícitos¹⁴⁹. El desarrollo de infraestructuras de computación de alto rendimiento ha reforzado estas capacidades, permitiendo procesar cantidad de datos en tiempo muy reducido.

En definitiva, los modelos de ML contribuyen a descubrir tipologías de fraude desconocidas, incrementando la capacidad preventiva de las entidades financieras¹⁵⁰. Ello no solo permite reducir las pérdidas derivadas de la actividad fraudulenta, sino que mejora la eficiencia de los procesos internos y disminuye el impacto que las medidas de control pueden generar sobre la experiencia de los clientes. El ML se consolida como una de las principales herramientas para afrontar los nuevos retos en la prevención del blanqueo. Con todo, la eficacia de cualquier solución tecnológica destinada a la detección de operaciones sospechosas depende de diversos factores. Entre ellos destacan: la disponibilidad de datos fiables, la precisión de los modelos, la capacidad para procesar grandes volúmenes de información y la rapidez con la que el sistema genera respuestas frente a operaciones potencialmente ilícitas¹⁵¹.

VI.2 Enfoques de ML para la prevención del blanqueo de dinero

La diversidad de técnicas desarrolladas dentro del ML ha dado lugar a numerosas clasificaciones. Tomando como base el trabajo de CHEN *et al.*¹⁵², se distinguen tres grandes categorías de modelos algorítmicos aplicables a la prevención del blanqueo: los métodos supervisados, los sistemas no supervisados y los enfoques híbridos o semisupervisados. Aunque cada uno de ellos presenta ventajas específicas, una revisión de los estudios publicados hasta la actualidad nos permite señalar que la mayor parte de las investigaciones se ha centrado en la aplicación de algoritmos supervisados, debido a que, cuando se dispone de datos etiquetados, suelen proporcionar mayor precisión en la detección de operaciones de fraude¹⁵³. A continuación exponemos las notas que corresponden a cada modelo:

¹⁴⁶ *Ibidem*.

¹⁴⁷ MANZOOR, M. F. y ASLAM, M. F.: *op. cit.*, p. 4.

¹⁴⁸ GANDHAR, A. *et al.*: *op. cit.*, p. 9.

¹⁴⁹ OYEDOKUN, O. *et al.*: *op. cit.*, p. 734.

¹⁵⁰ HOROBETS, N. *et al.*: *op. cit.*, p. 598.

¹⁵¹ APRILIA, G. F. y MEIRYANI, M.: *op. cit.*, p. 1000.

¹⁵² CHEN, Z. *et al.*: *op. cit.*, p. 251.

¹⁵³ HERNÁNDEZ AROS, L. *et al.*: *op. cit.*, p. 2.

– El aprendizaje no supervisado agrupa las técnicas que permiten extraer conocimiento de conjuntos de datos sin etiquetar¹⁵⁴. En estos modelos únicamente se dispone de las variables de las observaciones, correspondiendo al algoritmo descubrir de manera autónoma las relaciones entre ellas y organizar la información atendiendo a criterios de proximidad estadística¹⁵⁵. Esta metodología ha adquirido una importancia creciente en los sistemas de prevención del blanqueo, especialmente en los supuestos en los que resulta difícil disponer de ejemplos previamente identificados como fraudulentos. Mediante el agrupamiento (*clustering*), las entidades financieras¹⁵⁶ pueden localizar operaciones que se apartan del comportamiento transaccional habitual, sin necesidad de contar con etiquetas que indiquen cuáles son las operaciones ilícitas¹⁵⁷.

La principal fortaleza del enfoque de ML no supervisado reside en su independencia respecto de datos etiquetados, cuya obtención suele resultar compleja¹⁵⁸. Precisamente en este sentido destacan FRITZ-MORGENTHAL *et al.*¹⁵⁹ que las técnicas de aprendizaje no supervisado permiten identificar patrones y relaciones en grandes conjuntos de datos sin necesidad de etiquetado previo, apoyándose en herramientas de visualización y redes gráficas para facilitar su análisis a gran escala. No obstante, también hemos de indicar que esta metodología presenta limitaciones, como la necesidad de establecer los parámetros de funcionamiento o la concreción del número de clústeres¹⁶⁰.

– El aprendizaje supervisado se basa en la utilización de datos etiquetados¹⁶¹, en los que cada observación incorpora tanto la información de la operación como el resultado que el algoritmo debe aprender a predecir. A partir de este entrenamiento, el modelo identifica las relaciones entre las variables de entrada y la clasificación correspondiente, generando reglas de decisión aplicables a nuevos casos¹⁶². Este enfoque constituye la metodología predominante en la investigación sobre detección del fraude financiero, debido a que ofrece resultados satisfactorios cuando existe un volumen suficiente de datos etiquetados¹⁶³. La disponibilidad de estos últimos permite entrenar modelos con un elevado nivel de precisión y mejorar progresivamente su rendimiento mediante la incorporación de nueva información¹⁶⁴.

El ML supervisado permite que un sistema mejore progresivamente su rendimiento mediante el entrenamiento con grandes volúmenes de datos previamente etiquetados y la retroalimentación sobre los resultados obtenidos. Corresponde al analista seleccionar y preparar los datos de entrenamiento. A partir de estos ejemplos, el algoritmo desarrolla la capacidad de generalizar patrones y aplicarlos a situaciones nuevas¹⁶⁵.

¹⁵⁴ HOROBETS, N. *et al.*: *op. cit.*, p. 598.

¹⁵⁵ CHEN, Z. *et al.*: *op. cit.*, p. 251.

¹⁵⁶ OYEDOKUN, O. *et al.*: *op. cit.*, p. 734.

¹⁵⁷ Estos algoritmos generan observaciones que comparten características comunes, diferenciándolos de otros conjuntos con propiedades distintas. El análisis posterior de dichos grupos permite identificar comportamientos que requieren una investigación más detallada.

¹⁵⁸ GANDHAR, A. *et al.*: *op. cit.*, p. 9.

¹⁵⁹ FRITZ-MORGENTHAL, S. *et al.* (2022): “Financial Risk Management and Explainable, Trustworthy, Responsible AI”, *Frontiers in Artificial Intelligence*, n.º 5, p. 8.

¹⁶⁰ GANDHAR, A. *et al.*: *op. cit.*, p. 9.

¹⁶¹ HOROBETS, N. *et al.*: *op. cit.*, p. 598.

¹⁶² CANHOTO, A. I.: *op. cit.*, p. 443.

¹⁶³ COMPAGNINO, A. A. *et al.*: *op. cit.*, p. 5.

¹⁶⁴ El aprendizaje supervisado resulta adecuado en aquellos problemas donde las categorías de interés son conocidas de antemano y pueden utilizarse como referencia para el entrenamiento del algoritmo.

¹⁶⁵ SERRANO ACITORES, A.: *op. cit.*, p. 5.

Entre las técnicas algorítmicas de ML supervisado atendemos a las cuatro siguientes¹⁶⁶:

- Los árboles de decisión (en adelante, AD) representan el proceso de clasificación mediante una estructura jerárquica interpretable¹⁶⁷. Estos modelos organizan la información a través de una sucesión de decisiones condicionadas por los valores que adoptan las distintas variables, permitiendo clasificar cada observación mediante un recorrido lógico desde el punto inicial hasta el resultado final¹⁶⁸.

Una de las principales ventajas de esta técnica radica en la transparencia del proceso de decisión. A diferencia de otros modelos algorítmicos cuya lógica interna resulta difícil de interpretar, los AD permiten reconstruir el razonamiento seguido para alcanzar una conclusión¹⁶⁹. No obstante, esta simplicidad¹⁷⁰ presenta limitaciones; cuando los datos contienen relaciones complejas, los AD pueden ajustarse excesivamente a la información de entrenamiento, reduciendo su capacidad para generalizar frente a nuevos datos.

- La regresión logística (en adelante, RL) constituye otro de los modelos ampliamente empleados¹⁷¹, especialmente por su equilibrio entre capacidad predictiva, simplicidad e interpretabilidad. Su funcionamiento se basa en la estimación de la probabilidad de que una determinada operación pertenezca a una categoría a partir del análisis de las características de la transacción¹⁷².
- Las redes neuronales artificiales son modelos computacionales integrados por unidades de procesamiento interconectadas (“neuronas”), que colaboran en el tratamiento de la información¹⁷³. Se tratan de sistemas con capacidad adaptativa, que modifican su configuración interna mediante el ajuste de lo asignado a las variables de entrada. Cada dato de entrada es ponderado y, tras sumar los valores junto con un sesgo, se obtiene la salida¹⁷⁴.
- Las máquinas de vectores de soporte (en adelante, SVM) constituyen una herramienta de interés para los sistemas de prevención del blanqueo¹⁷⁵. Su funcionamiento se basa en transformar un problema no lineal en otro lineal dentro de un espacio de mayor dimensión, lo que facilita su resolución¹⁷⁶. En ámbitos con un elevado número de variables, las SVM favorecen la generalización¹⁷⁷.

¹⁶⁶ SEGURA PEÑA, L. *et al.* (2024): “*Machine Learning Models for Money Laundering Detection in Financial Institutions. A Systematic Literature Review*”, 22nd LACCEI International Multi-Conference for Engineering, Education, and Technology: Sustainable Engineering for a Diverse, Equitable, and Inclusive Future at the Service of Education, Research, and Industry for a Society 5.0, p. 2.

¹⁶⁷ COMPAGNINO, A. A. *et al.*: *op. cit.*, p. 6.

¹⁶⁸ ALKHALILI, M. *et al.*: *op. cit.*, p. 18485.

¹⁶⁹ CHEN, Z. *et al.*: *op. cit.* p. 264.

¹⁷⁰ GANDHAR, A. *et al.*: *op. cit.*, p. 4.

¹⁷¹ Este modelo resulta apropiado para problemas de clasificación binaria, ampliamente presentes en los sistemas de prevención del blanqueo, donde el objetivo consiste en determinar si una operación debe ser considerada normal o potencialmente fraudulenta (COMPAGNINO, A. A. *et al.*: *op. cit.*, p. 6).

¹⁷² GANDHAR, A. *et al.*: *op. cit.*, p. 4.

¹⁷³ COMPAGNINO, A. A. *et al.*: *op. cit.*, p. 7.

¹⁷⁴ *Ibidem*.

¹⁷⁵ GANDHAR, A. *et al.*: *op. cit.*, p. 4.

¹⁷⁶ CHEN, Z. *et al.*: *op. cit.*, p. 256.

¹⁷⁷ El rendimiento de las SVM depende bastante de la calidad y tamaño del conjunto de entrenamiento, por lo que ofrece mejores resultados cuando se trabaja con conjuntos de datos pequeños o medianos.

– El ML semisupervisado constituye una metodología que integra características tanto del aprendizaje supervisado como del aprendizaje no supervisado. Los modelos semisupervisados combinan ambas técnicas para aprovechar la información contenida en un conjunto limitado de datos etiquetados y en otro mucho más amplio de datos no etiquetados¹⁷⁸. Los primeros, en particular, orientan el proceso de aprendizaje y permiten incrementar la precisión en la identificación de operaciones sospechosas¹⁷⁹. La evolución de estos sistemas pone de manifiesto la relevancia de desarrollar metodologías híbridas¹⁸⁰.

En definitiva, las entidades financieras desempeñan un papel esencial en la identificación de transacciones vinculadas con actividades de blanqueo¹⁸¹. El elevado volumen de movimientos susceptibles de ser utilizados para el delito hace imprescindible, como señala SEGURA PEÑA¹⁸², automatizar los procesos de generación de alertas y de comunicación de operaciones sospechosas. En este contexto, las técnicas de ML permiten analizar los patrones de comportamiento de los clientes e identificar conductas que se apartan de la legalidad¹⁸³. Gracias a algoritmos, capaces de actualizarse, las entidades financieras pueden detectar la evolución de las técnicas empleadas por las organizaciones criminales para ocultar el origen ilícito de los fondos¹⁸⁴, siendo una de las principales aportaciones del ML la disminución del número de falsos positivos¹⁸⁵.

VII. Retos ante la aplicación de la IA en los sistemas de prevención del blanqueo de dinero

VII.1 Planteamiento general

La incorporación de la IA en los sistemas de prevención del blanqueo se enfrenta a diversos obstáculos como la formulación de resultados sesgados, las deficiencias en la calidad de los datos y la aparición continua de nuevas tipologías de blanqueo¹⁸⁶. Aunque determinadas organizaciones financieras han iniciado proyectos basados en IA y ML¹⁸⁷, una parte considerable de las instituciones continúa apoyándose en sistemas fundamentados en reglas¹⁸⁸. Y ello obedece, acogiendo las palabras de LUNA ÁLVAREZ¹⁸⁹, al hecho de que la IA no constituye una tecnología neutral, ya que su funcionamiento puede amplificar sesgos presentes en los datos de los que se nutre.

¹⁷⁸ GANDHAR, A. *et al.*: *op. cit.*, p. 5.

¹⁷⁹ OYEDOKUN, O. *et al.*: *op. cit.*, p. 735.

¹⁸⁰ COMPAGNINO, A. A. *et al.*: *op. cit.*, p. 20.

¹⁸¹ HOROBETS, N. *et al.*: *op. cit.*, p. 598.

¹⁸² SEGURA PEÑA, L. *et al.*: *op. cit.*, p. 2.

¹⁸³ *Ibidem*.

¹⁸⁴ OYEDOKUN, O. *et al.*: *op. cit.*, p. 732.

¹⁸⁵ La incorporación de modelos de ML contribuye a reducir estas alertas innecesarias, optimizando los recursos disponibles y permitiendo que los especialistas concentren sus esfuerzos en las operaciones que realmente presentan un mayor nivel de riesgo.

¹⁸⁶ HOROBETS, N. *et al.*: *op. cit.*, p. 599.

¹⁸⁷ KUTE, D. V. *et al.*: *op. cit.*, p. 82313.

¹⁸⁸ PETTERSSON RUIZ, E. y ANGELIS, J. (2022): “Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges”, *Journal of Money Laundering Control*, vol. 25, n.º 4, p. 768.

¹⁸⁹ LUNA ÁLVAREZ, E. R. (2025): “Anatomía jurídica del sesgo algorítmico en el uso de la IA”, *Revista de derecho y proceso penal*, n.º 79, p. 3.

Además, la opacidad de determinados modelos de ML dificulta su explicabilidad, supervisión y control desde una perspectiva jurídica¹⁹⁰.

La implantación de tecnologías basadas en IA avanza de forma lenta debido a tres factores¹⁹¹. En primer lugar, la reducida explicabilidad¹⁹², ya que los modelos de ML suelen presentar una estructura compleja que dificulta comprender el razonamiento que sustenta sus decisiones; se emplea el concepto de “caja negra” para indicar que la capacidad predictiva de los modelos de ML contrasta con la imposibilidad de comprender el proceso interno mediante el cual se adoptan decisiones, lo cual plantea desafíos en materia de transparencia y rendición de cuentas¹⁹³. En segundo término, la confianza, puesto que los sistemas de “caja negra” carecen de la transparencia e interpretabilidad para generar seguridad en su utilización¹⁹⁴. Finalmente, el respeto a la privacidad, dado que los algoritmos de ML requieren procesar información relativa a identidad de los clientes, las cuentas bancarias y las operaciones, lo que únicamente es posible cuando sea acorde con la normativa de protección de datos.

VII.2 Explicabilidad y transparencia algorítmica

Uno de los inconvenientes asociados a los algoritmos de ML es el mencionado carácter de “caja negra”¹⁹⁵ al que se asocian, como apunta FERRÉ OLIVÉ¹⁹⁶, aspectos negativos tales como procedimientos internos opacos, falta de justificación y dificultad de comprensión de decisiones. Cuando además de obtener predicciones se pretende discernir los criterios que fundamentan los resultados alcanzados, es imprescindible que el modelo sea interpretable. Sin embargo, a medida que los algoritmos incorporan un mayor volumen de datos y un número creciente de variables, la lógica que sustenta las decisiones adquiere un grado de complejidad que dificulta su entendimiento¹⁹⁷. Los sistemas de IA funcionan mediante el tratamiento automatizado de datos conforme a un conjunto de instrucciones implementadas a través de algoritmos, entendidos como secuencias de código informático destinadas a ejecutar operaciones específicas. No obstante, las reglas de decisión generadas por determinados modelos presentan relaciones complejas entre las variables de entrada y el resultado obtenido, impidiendo identificar de manera clara la contribución de cada factor en la decisión final¹⁹⁸.

La transparencia debe presidir en todo caso la utilización de la IA, si bien representa uno de los principales desafíos desde una perspectiva ética y jurídica¹⁹⁹. La complejidad interna de los modelos algorítmicos impide, en muchas ocasiones, que los interesados comprendan de qué manera se generan las decisiones automatizadas²⁰⁰. Esta

¹⁹⁰ *Ibidem*.

¹⁹¹ KUTE, D. V. *et al.*: *op. cit.*, p. 82312.

¹⁹² CANHOTO, A. I.: *op. cit.*, p. 448.

¹⁹³ SERRANO ACITORES, A.: *op. cit.*, p. 9.

¹⁹⁴ OYEDOKUN, O. *et al.*: *op. cit.*, p. 738.

¹⁹⁵ GIMENO, R. y MARQUÉS, J. M.: *op. cit.*, p. 114.

¹⁹⁶ FERRÉ OLIVÉ, J. C. (2026): “Superinteligencia artificial penal: ¿justicia algorítmica o Lombroso 4.0?”, *Revista Penal México*, n.º 29, p. 53.

¹⁹⁷ LEAL RUÍZ, R.: *op. cit.*, p. 394.

¹⁹⁸ GALEANO, P. y PEÑA, D. (2019): “Las nuevas oportunidades del *Big Data* para las instituciones financieras”, *Papeles de economía española*, n.º 162, p. 83.

¹⁹⁹ MONTESDEOCA RODRÍGUEZ, D.: *op. cit.*, p. 481.

²⁰⁰ *Ibidem*.

problemática mantiene una estrecha relación con la calificación de “caja negra”, aunque trasciende dicho concepto al proyectarse sobre el deber general, también para el caso de las entidades financieras, de garantizar la claridad y trazabilidad de los procedimientos²⁰¹. Si bien el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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 (en adelante, RGPD), refuerza las exigencias de transparencia, los modelos avanzados de ML se caracterizan por elevados niveles de opacidad²⁰²; estos pueden alcanzar un considerable rendimiento predictivo, pero ofrecen una capacidad limitada para explicar los fundamentos de las decisiones que producen²⁰³.

VII.3 Sesgos algorítmicos y riesgo de discriminación

Los sistemas de ML pueden incorporar sesgos derivados tanto de los conjuntos de datos empleados para su entrenamiento como de las estructuras sobre las que se construyen²⁰⁴. Al basarse en relaciones de correlación extraídas de los datos, estos sistemas pueden reproducir e intensificar patrones discriminatorios, lo que repercute en el comportamiento del algoritmo²⁰⁵. Particularmente, cuando los datos de entrenamiento dibujan una representación insuficiente de determinados aspectos, las evaluaciones automatizadas del riesgo pueden resultar injustificadas, generando consecuencias jurídicas y reputacionales verdaderamente trascendentes en el caso de las entidades financieras. Si los datos contienen sesgos, los modelos de ML tenderán no solo a reproducirlos, sino también a amplificarlos, provocando que determinados clientes experimenten una mayor probabilidad de rechazo de operaciones financieras o incluso el bloqueo de sus cuentas²⁰⁶.

Las decisiones sesgadas pueden comprometer la eficacia de los sistemas de prevención del blanqueo, al igual que, como apunta ABEL SOUTO²⁰⁷, producir un menoscabo en derechos fundamentales, como la igualdad y la no discriminación²⁰⁸, dando lugar a responsabilidades legales para las instituciones financieras²⁰⁹. Los algoritmos de ML orientan su funcionamiento a la identificación de correlaciones que optimicen la capacidad predictiva del modelo, circunstancia que, en determinadas ocasiones, puede conducir a establecer asociaciones sin relación causal. Los sesgos pueden originarse tanto en la calidad y la composición de los datos utilizados durante el entrenamiento²¹⁰, como en la metodología empleada para desarrollar el algoritmo²¹¹. Además, la opacidad de los sistemas de “caja negra” dificulta la corrección de patrones no deseados, favoreciendo que los sesgos se reproduzcan e incluso se acentúen durante la toma de decisiones²¹².

²⁰¹ OYEDOKUN, O. *et al.*: *op. cit.*, p. 738.

²⁰² *Ibidem*.

²⁰³ KUTE, D. V. *et al.*: *op. cit.*, p. 82301.

²⁰⁴ MONTESDEOCA RODRÍGUEZ, D.: *op. cit.*, p. 472.

²⁰⁵ *Ibidem*.

²⁰⁶ COMPAGNINO, A. A. *et al.*: *op. cit.*, p. 24.

²⁰⁷ ABEL SOUTO, M.: *op. cit.*, p. 175.

²⁰⁸ HERNÁNDEZ OSORIO, J. A.: *op. cit.*, p. 95.

²⁰⁹ OYEDOKUN, O. *et al.*: *op. cit.*, p. 738.

²¹⁰ FRITZ-MORGENTHAL, S. *et al.*: *op. cit.*, p. 3.

²¹¹ FERNÁNDEZ, A.: *op. cit.*, p. 4.

²¹² GIMENO, R. y MARQUÉS, J. M.: *op. cit.*, p. 114.

VII.4 Disponibilidad de datos y desafíos derivados de la normativa de protección de datos

Otra de las limitaciones para el desarrollo de modelos eficaces de detección de operaciones sospechosas de blanqueo a través del ML reside en la escasa disponibilidad de datos²¹³. La aplicación del ML en la prevención del blanqueo requiere, por regla general, grandes volúmenes de datos que permitan reconocer con precisión los patrones asociados a actividades ilícitas²¹⁴. Esta exigencia constituye un importante obstáculo, ya que la recopilación, etiquetado y almacenamiento de datos exige una inversión considerable de recursos técnicos, económicos y humanos²¹⁵. Asimismo, la calidad de los datos condiciona directamente el rendimiento de los modelos predictivos, puesto que la precisión en la detección depende de la existencia de información fiable y estructurada²¹⁶.

Las exigencias derivadas de la protección de datos personales añaden un nivel adicional de complejidad a la aplicación de modelos de ML²¹⁷. La información relativa a clientes y transacciones financieras se encuentra sometida a estrictos regímenes, como el establecido por el RGPD²¹⁸, lo que limita las posibilidades de compartir datos entre entidades para el entrenamiento de los modelos. De hecho, indica ALBERRUCHE DÍAZ-FLORES²¹⁹ que el RIA mantiene una relación de complementariedad con el RGPD, sin ser incompatibles las disposiciones de ambos, dado que numerosos sistemas de IA, especialmente aquellos basados en el ML supervisado, tratan datos personales durante su funcionamiento. Por tanto, el RIA no altera las obligaciones impuestas por el RGPD, cuyo cumplimiento resulta exigible a lo largo de la vida del sistema de IA²²⁰.

El RGPD reconoce como exigencias básicas el adecuado manejo de los datos, la existencia de mecanismos que garanticen la explicabilidad, así como el respeto de los principios éticos que rigen el tratamiento automatizado de información²²¹. En especial, atendemos al “derecho a la explicación”²²², que en el RGPD se deriva de la lectura combinada del “derecho a obtener información transparente” previsto en los artículos 13, 14 y 15, del “derecho a no ser objeto de decisiones basadas en el tratamiento automatizado” reconocido en el artículo 22, así como del Considerando 71. Ello contrasta con la consagración explícita de aquel en el artículo 86 del RIA sobre sistemas de IA de alto riesgo. En todo caso, ambos cuerpos normativos vienen a indicar la obligación de justificar las decisiones adoptadas mediante procesos automatizados²²³.

El artículo 22 del RGPD reconoce el derecho a no ser objeto de decisiones exclusivamente automatizadas, incluida la elaboración de perfiles, cuando tales

²¹³ CHEN, Z. *et al.*: *op. cit.*, p. 247.

²¹⁴ OYEDOKUN, O. *et al.*: *op. cit.*, p. 738.

²¹⁵ *Ibidem*.

²¹⁶ CHEN, Z. *et al.*: *op. cit.*, p. 248.

²¹⁷ NIE, C. *et al.*: *op. cit.*, p. 244.

²¹⁸ *Ibidem*.

²¹⁹ ALBERRUCHE DÍAZ-FLORES, M. M.: *op. cit.*, p. 6.

²²⁰ La protección de los datos personales constituye un derecho fundamental reconocido por el artículo 18.4 de la Constitución Española. En el ámbito comunitario, se prevé en el artículo 8 de la Carta de los Derechos Fundamentales de la UE y en el artículo 16 del Tratado de Funcionamiento de la UE.

²²¹ ALBERRUCHE DÍAZ-FLORES, M. M.: *op. cit.*, p. 6.

²²² COMPAGNINO, A. A. *et al.*: *op. cit.*, p. 23.

²²³ KUTE, D. V. *et al.*: *op. cit.*, p. 82307.

decisiones produzcan efectos jurídicos o afecten significativamente a la persona²²⁴; tras ello se garantiza la intervención humana, la posibilidad de formular alegaciones y de impugnar la decisión²²⁵. Ello supone que las entidades financieras que recurran a soluciones de IA deben asegurar el pleno ejercicio de este derecho²²⁶. En el caso de que sistemas de IA asistan en la toma de decisiones, aquellos deberán respetar de forma concurrente tanto el marco legal del RGPD como las exigencias del RIA en materia de transparencia²²⁷, trazabilidad²²⁸ y supervisión humana²²⁹, de modo que la falta de explicabilidad o de intervención humana efectiva implicaría el incumplimiento de ambas normativas²³⁰.

La explicabilidad se establece como un requisito esencial tanto desde la perspectiva del cumplimiento normativo como de la legitimidad de los sistemas de IA. En extensión a la prevención del blanqueo, ello supone que la identificación de patrones de actividad ilícita por las entidades financieras debe ir acompañada de elementos suficientes que permitan fundamentar la remisión de los informes de operaciones sospechosas a las autoridades competentes²³¹. Las alertas generadas por modelos algorítmicos no pueden constituir por sí solas una motivación para dar cumplimiento al deber de comunicación. Debe asegurarse en todo caso la comprensión de la lógica del algoritmo para poder motivar, supervisar y validar con criterio humano la decisión final.

VII.5 Aspectos organizativos, técnicos y económicos en la implantación del ML

La incorporación de soluciones de IA en el sector financiero requiere inversiones en infraestructura tecnológica, ingeniería de datos y formación del personal encargado de su desarrollo y supervisión²³². Asimismo, la integración de estas tecnologías suele exigir la adaptación de sistemas heredados, especialmente las bases de datos tradicionales, con el fin de garantizar su compatibilidad con las herramientas de ML²³³. Desde una perspectiva funcional, los modelos deben ser actualizados periódicamente, por más que su reentrenamiento constituya un desafío técnico y económico²³⁴. En consecuencia, las

²²⁴ Artículo 22.1 del RGPD: “Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar”.

²²⁵ LUNA ÁLVAREZ, E. R.: *op. cit.*, p. 7. Indica, no obstante, que la efectividad de estas garantías depende de un régimen de responsabilidad adecuado, persistiendo el debate entre modelos de responsabilidad objetiva y sistemas basados en la acreditación del defecto, el daño y el nexo causal, especialmente complejos en el contexto de sistemas algorítmicos opacos.

²²⁶ MONTESDEOCA RODRÍGUEZ, D.: *op. cit.*, p. 479.

²²⁷ Atendiendo a los artículos 13 y 50 del RIA, se exige informar al usuario del empleo de la IA y de facilitar instrucciones sobre el funcionamiento y límites de los sistemas de alto riesgo.

²²⁸ Los artículos 11 y 12 del RIA obligan a conservar la documentación técnica del sistema para permitir su posterior auditoría.

²²⁹ Los artículos 14 y 26 del RIA, relativos a la supervisión humana, imponen el diseño de controles para la vigilancia del algoritmo, pudiendo corregir, anular o detener sus decisiones. Con mención del primer precepto indicado, y acerca de la importancia de la transparencia algorítmica, *vid.* FERRÉ OLIVÉ, J. C.: “Superinteligencia artificial penal...”, *cit.*, p. 64.

²³⁰ ALBERRUCHE DÍAZ-FLORES, M. M.: *op. cit.*, p. 26.

²³¹ *Ibidem.*

²³² NIE, C. *et al.*: *op. cit.*, p. 244.

²³³ CANHOTO, A. I.: *op. cit.*, p. 442.

²³⁴ MANAVADARIA, M. S. *et al.*: *op. cit.*, p. 198.

entidades financieras deben dotarse de sistemas tecnológicos para gestionar el elevado volumen de información requerido por estos modelos.

Diversos estudios apuntan que los costes asociados a la implantación de sistemas de IA, sumado a los gastos de cumplimiento de la normativa de prevención del blanqueo, pueden llegar a superar los beneficios, incluso considerando las mejoras en la eficiencia de los procesos y en el conocimiento del cliente²³⁵. A ello se añaden costes indirectos, como la formación de profesional especializado²³⁶. Por ello, para las entidades puede ser preferible mantener modelos basados en reglas. Esto permite indicar que a pesar de los avances tecnológicos, todavía existe cautela en la implementación por las instituciones financieras de modelos de ML para la prevención del blanqueo, obedeciendo tanto a los costes aquí comentados, como a los riesgos de errores por los sistemas de IA y el consiguiente daño reputacional²³⁷.

VIII. La escasa regulación en España para la aplicación del ML en el sector financiero

En España, pese a iniciativas como la Estrategia Nacional de IA (en adelante, ENIA) y la aprobación de la Ley 7/2020, de 13 de noviembre, de transformación digital del sistema financiero, continúa apreciándose una ausencia de regulación específica que discipline de manera integral el empleo de la IA en el ámbito financiero²³⁸.

La ENIA²³⁹ apenas desarrolla el papel de la IA. Primero, se limita a incluir el “ámbito financiero” dentro de una enumeración de sectores, sin concretar los usos, los retos normativos o las implicaciones legales. Luego enuncia únicamente la existencia de empresas líderes en “servicios financieros”. Finalmente, destaca el *sandbox* como instrumento destinado a proporcionar un entorno jurídico seguro para el desarrollo de la innovación financiera. Estos últimos constituyen marcos de experimentación supervisada que permiten evaluar sistemas de IA en condiciones controladas, conciliando la innovación tecnológica con la transparencia, la no discriminación y la seguridad jurídica²⁴⁰. Los *sandboxes* se estiman como el medio para fomentar el desarrollo de sistemas de IA en línea con los derechos fundamentales²⁴¹.

La Ley 7/2020, de 13 de noviembre, no regula el uso del ML en las instituciones financieras; su enfoque es neutro y emplea la noción de “innovación de base tecnológica aplicable al sistema financiero”²⁴², lo que nos permite concluir que la norma se destina a constituir el marco básico para un posterior desarrollo de la innovación financiera

²³⁵ CANHOTO, A. I.: *op. cit.*, p. 443.

²³⁶ *Ibidem*.

²³⁷ TURKSEN, U. *et al.* (2024): “Legal implications of automated suspicious transaction monitoring: enhancing integrity of AI”, *Journal of Banking Regulation*, n.º 25, p. 360.

²³⁸ HOROBETS, N. *et al.*: *op. cit.*, p. 601.

²³⁹ *Vid.* MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL (2020): *ENIA: Estrategia Nacional de Inteligencia Artificial. Versión 1.0*, pp. 1-89.

²⁴⁰ LUNA ÁLVAREZ, E. R.: *op. cit.*, p. 6.

²⁴¹ ALBERRUCHE DÍAZ-FLORES, M. M.: *op. cit.*, p. 34.

²⁴² Artículo 3 letra e) de la Ley 7/2020, de 13 de noviembre: «A efectos de lo previsto en esta Ley se entenderá por: e) “Innovación de base tecnológica aplicable en el sistema financiero”: aquella actuación o conjunto de actuaciones que, mediante el uso de la tecnología, pueda dar lugar a nuevas aplicaciones, procesos, productos o modelos de negocio con incidencia sobre los mercados financieros, la prestación de servicios financieros y complementarios o el desempeño de las funciones públicas en el ámbito financiero».

mediante la IA. Ha ensayado GÓMEZ JIMÉNEZ²⁴³ que la Ley 7/2020, de 13 de noviembre, no define expresamente la IA y emplea una noción amplia de "innovación de base tecnológica". Tras ello, destaca el papel de los *sandboxes* como espacios para la prueba de nuevos productos y servicios bajo supervisión pública. Finalmente, subraya que la Ley articula mecanismos de coordinación entre las autoridades supervisoras mediante la creación de una Comisión de Coordinación encargada de impulsar la transformación digital, supervisar el funcionamiento de los *sandboxes* y aplicar el principio de proporcionalidad²⁴⁴.

IX. Conclusiones

El sector financiero constituye uno de los ámbitos en los que la IA y el ML están llamados a producir una transformación de mayor alcance. La capacidad de estas tecnologías para procesar grandes volúmenes de datos en tiempo real permite a las entidades financieras identificar patrones, detectar anomalías y responder con mayor rapidez a las amenazas relacionadas con la criminalidad económica. En particular, los modelos algorítmicos poseen la capacidad de aprender a partir de volúmenes considerables de datos y adaptarse continuamente a nuevas modalidades de fraude.

El impacto de la IA en el sector financiero trasciende, con todo, la prevención de delitos, extendiéndose a la modernización del conjunto de la actividad mediante la mejora de la eficiencia operativa, el refuerzo de la seguridad y el incremento de la calidad de los servicios ofrecidos a los clientes. Las técnicas de ML están sustituyendo los enfoques tradicionales al proporcionar herramientas más avanzadas para el análisis de datos, la evaluación del riesgo, el procesamiento de operaciones y la adopción de decisiones. Entre las aplicaciones destacamos en particular los sistemas de calificación crediticia; sobre ello, CaixaBank ha sido la primera entidad española en aplicar un esquema de computación híbrida para la clasificación de perfiles de riesgo crediticio.

El ML constituye una disciplina integrada dentro de la IA cuyo objetivo consiste en desarrollar algoritmos capaces de extraer conocimiento a partir de datos y utilizar aquel para realizar predicciones o adoptar decisiones de forma automatizada. En el ámbito financiero, estas técnicas se aplican de manera generalizada en tareas de predicción, entre las que destacan la estimación de la evolución de los mercados, la evaluación del riesgo de crédito y la identificación de oportunidades de inversión. Mediante el análisis de información y la detección de patrones en los datos, los modelos de ML permiten anticipar tendencias y adoptar decisiones con precisión.

Igualmente, otra de las principales ventajas de la aplicación de la IA en el sector financiero radica en la RPA, que contribuye a reducir los costes operativos, los tiempos de respuesta y ampliar el alcance de los servicios. A ello se añade un incremento significativo de la capacidad de procesamiento de información, lo cual se lleva a cabo de forma más rápida y precisa, así como la incorporación de nuevas fuentes de datos.

El presente estudio partió del propósito de analizar si el ML puede contribuir de manera efectiva a la detección del blanqueo de dinero y, con ello, favorecer el cumplimiento del ODS n.º 16 de la Agenda 2030 de las Naciones Unidas, relativo a la promoción de instituciones eficaces y a la lucha contra la delincuencia organizada. Existe

²⁴³ GÓMEZ JIMÉNEZ, M. L.: *op. cit.*, p. 203 y ss.

²⁴⁴ *Ibidem*.

un claro interés por las tecnologías de IA, si bien tampoco se puede negar que su utilización en los sistemas de prevención está condicionada por los procesos de diseño, entrenamiento e implementación de los algoritmos.

A lo largo de este trabajo se ha examinado el papel de la IA en los mecanismos de detección del fraude a través de las entidades financieras, cuya posición como intermediarias en el tráfico económico les atribuye una responsabilidad esencial en la prevención del blanqueo. Del análisis realizado sobre las características del ML se desprende que estas herramientas ofrecen importantes posibilidades para identificar patrones atípicos de comportamiento financiero y detectar operaciones sospechosas, las cuales podrían pasar inadvertidas mediante mecanismos tradicionales de supervisión.

La integración del conocimiento especializado en la prevención del blanqueo de dinero con soluciones de IA sustentadas en datos de calidad y sobre infraestructuras tecnológicas potentes constituye una vía para desarrollar sistemas de supervisión más eficientes. Este enfoque permite establecer mejores modelos de cumplimiento, así como mecanismos preventivos óptimos que refuerzan la integridad del sistema financiero. Al mismo tiempo, la reducción de ineficiencias operativas, el incremento de la transparencia y el fortalecimiento de la confianza en el ecosistema financiero contribuyen a un desarrollo sostenible de la economía.

El ML ha supuesto una evolución en la prevención de la criminalidad económica, especialmente el blanqueo, al proporcionar herramientas flexibles. El examen de grandes volúmenes de datos a través de algoritmos permite mejorar la capacidad de identificación de operaciones de fraude, disminuir el número de falsos positivos y responder con rapidez a las amenazas delictivas. Frente a la sofisticación de las técnicas de blanqueo, los modelos basados en reglas muestran limitaciones para gestionar la complejidad de los riesgos actuales. La incorporación de IA en los procedimientos KYC, la monitorización de transacciones y la elaboración de informes de operaciones sospechosas optimiza la respuesta preventiva.

Pese a lo anterior, la implantación de soluciones de ML continúa condicionada por diversos factores, como la disponibilidad de datos, las exigencias de explicabilidad de los modelos y la necesidad de generar confianza entre las autoridades supervisoras. Las entidades financieras deben reforzar tanto sus infraestructuras tecnológicas como sus mecanismos de gobernanza y gestión de datos para aprovechar las capacidades que ofrece la IA. El desarrollo de futuros sistemas de detección deberá combinar los avances tecnológicos propios del ML con sólidas garantías jurídicas que aseguren el respeto de los derechos fundamentales y la fiabilidad de las decisiones automatizadas.

X. Bibliografía

- ABEL SOUTO, M. (2025): “Inteligencia artificial en la prevención y represión del blanqueo de dinero”. En GONZÁLEZ URIEL, D., ABADÍAS SELMA, A. y MORELL ALDANA, L. C. (coords.): *Ciberdelincuencia: Perspectiva penal, procesal y criminológica*. La Ley, Madrid, pp. 171-182.
- ALBERRUCHE DÍAZ-FLORES, M. M. (2025): “Europa ante el reto de la inteligencia artificial: una regulación pionera para un futuro responsable”, *Revista de fiscalidad internacional y negocios transnacionales*, n.º 30, pp. 1-47 (versión digital).

- ALKHALILI, M. *et al.* (2021): “*Investigation of Applying Machine Learning for Watch-List Filtering in Anti-Money Laundering*”, *IEEE Access*, n.º 9, pp. 18481-18496. <https://doi.org/10.1109/access.2021.3052313>
- ALONSO, A. y CARBÓ MARTÍNEZ, J. M. (2021): “*Understanding the performance of machine learning models to predict credit default: A novel approach for supervisory evaluation*”, *Documentos de trabajo - Banco de España*, n.º 5, pp. 3-44.
- ÁLVAREZ JAREÑO, J. A. *et al.* (2019): “*Aplicación de métodos estadísticos, económicos y de aprendizaje automático para la detección de la corrupción*”, *Revista internacional de transparencia e integridad*, n.º 9, pp. 1-11.
- ÁLVARO PERIS, C. (2025): “*Inteligencia artificial y blanqueo de capitales: prevención y comisión del delito*”. En ABEL SOUTO, M., LORENZO SALGADO, J. M. y SÁNCHEZ STEWART, N. (coords.): *X Congreso Internacional sobre prevención y represión del blanqueo de dinero*. Tirant lo Blanch, Valencia, pp. 555-559.
- APRILIA, G. F. y MEIRYANI, M. (2024): “*Exploring detection and prevention of money laundering with information technology*”, *Journal of Money Laundering Control*, vol. 27, n.º 6, pp. 995–1004. <https://doi.org/10.1108/JMLC-08-2023-0138>
- CANHOTO, A. I. (2021): “*Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective*”, *Journal of Business Research*, n.º 131, pp. 441-452. <https://doi.org/10.1016/j.jbusres.2020.10.012>
- CHEN, Z. *et al.* (2018): “*Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review*”, *Knowledge and Information Systems*, n.º 57, pp. 245–285. <https://doi.org/10.1007/s10115-017-1144-z>
- COMPAGNINO, A. A. *et al.* (2025): “*An Introduction to Machine Learning Methods for Fraud Detection*”, *Applied Sciences*, vol. 15, n.º 21, pp. 1-32. <https://doi.org/10.3390/app152111787>
- EDDIN, A. N. *et al.* (2021): “*Anti-money laundering alert optimization using machine learning with graphs*”, *Computer Sciences*, n.º 12, pp. 1-8. <https://doi.org/10.48550/arXiv.2112.07508>
- ESCAJEDO SAN EPIFANIO, L. (2025): “*Vigilancia biométrica masiva mediante IA y derechos fundamentales: Retos jurídico-constitucionales*”. En BALAGUER CALLEJÓN, F. y ESCAJEDO SAN EPIFANIO, L. (dirs.): *Vigilancia biométrica masiva, Inteligencia Artificial y Derechos Fundamentales*. Dykinson, Madrid, pp. 21-37.
- ESCOLÁ PÉREZ, M. C. (2021): «*Aplicaciones del “machine learning” en el sector legal y nuevas profesiones jurídico-tecnológicas*», *Revista Aranzadi de derecho y nuevas tecnologías*, n.º 55, pp. 1-20 (versión digital).
- ESPINOZA VILLAVICENCIO, H. M. (2026): “*Modelos predictivos de IA y su relación con la protección contra amenazas persistentes avanzadas del sistema bancario*”, *Revista de Investigaciones Científicas y Tecnológicas Industriales*, n.º 1, pp. 38-50 <https://doi.org/10.47422/jstri.v7i1.74>

- FATF (2021): *Opportunities and Challenges of New Technologies for AML/CFT*. Paris, France.
- FERNÁNDEZ, A. (2019): “Inteligencia artificial en los servicios financieros”, *Boletín económico - Banco de España*, n.º 2, pp. 1-10.
- FERRÉ OLIVÉ, J. C. (2024): *El delito de blanqueo de dinero*. Tirant lo Blanch, Valencia.
- FERRÉ OLIVÉ, J. C. (2025): “Reflexiones en torno al *compliance* penal y a la ética en la empresa”, *Revista Penal*, n.º 44, pp. 61-80.
- FERRÉ OLIVÉ, J. C. (2026): “Superinteligencia artificial penal: ¿justicia algorítmica o Lombroso 4.0?”, *Revista Penal México*, n.º 29, pp. 41-72.
- FRITZ-MORGENTHAL, S. et al. (2022): “Financial Risk Management and Explainable, Trustworthy, Responsible AI”, *Frontiers in Artificial Intelligence*, n.º 5, pp. 1-14. <https://doi.org/10.3389/frai.2022.779799>
- GALEANO, P. y PEÑA, D. (2019): “Las nuevas oportunidades del *Big Data* para las instituciones financieras”, *Papeles de economía española*, n.º 162, pp. 78-97.
- GANDHAR, A. et al. (2024): “Fraud Detection Using Machine Learning and Deep Learning”, *SN Computer Science*, vol. 5, pp. 1-10. <https://doi.org/10.1007/s42979-024-03236-y>
- GIMENO, R. y MARQUÉS, J. M. (2022): “Tradición e inteligencia artificial: oportunidades y retos del *machine learning* para los servicios financieros”, *ICE: Revista de economía*, n.º 926, pp. 109-118. <https://doi.org/10.32796/ice.2022.926.7403>
- GÓMEZ JIMÉNEZ, M. L. (2021): “Regtech, inteligencia artificial y transformación digital en el mercado financiero: el caso de la atención al cliente usando *chatbots* y las obligaciones de información en la resolución extrajudicial de conflictos”, *Revista de Derecho del Sistema Financiero: mercados, operadores y contratos*, n.º 2, pp. 195-218.
- GONZÁLEZ CUSSAC, J. L. (2011): “Estrategias legales frente a las ciberamenazas”, *Cuadernos de estrategia*, n.º 149 (ejemplar dedicado a: Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio), pp. 83-127.
- GONZÁLEZ CUSSAC, J. L. y FLORES GIMÉNEZ, F. (2017): “Una metodología para el análisis de las amenazas a la seguridad, la evaluación de las respuestas y su impacto sobre los derechos fundamentales”, *Cuadernos de estrategia*, n.º 188 (ejemplar dedicado a: Seguridad global y derechos fundamentales), pp. 15-64.
- HAN, J. et al. (2020): “Artificial intelligence for anti-money laundering: a review and extension”, *Digital Finance*, n.º 2, pp. 211–239. <https://doi.org/10.1007/s42521-020-00023-1>
- HERNÁNDEZ AROS, L. et al. (2024): “Financial fraud detection through the application of machine learning techniques: a literature review”, *Humanities and Social Sciences Communications*, n.º 11, pp. 1-22. <https://doi.org/10.1057/s41599-024-03606-0>
- HERNÁNDEZ OSORIO, J. A. (2024): “Inteligencia artificial: implicaciones éticas fundamentales para su regulación en el marco constitucional del siglo XXI”. En ABADÍAS SELMA, A. y GONZÁLEZ URIEL, D. (coords.): *El impacto de la IA*

en el aprendizaje y en la práctica del derecho. Aranzadi La Ley, Madrid, pp. 83-104.

HOROBETS, N. *et al.* (2025): “Artificial intelligence technologies in banking: challenges and opportunities for anti-money laundering in the context of EU regulatory initiatives”, *Journal of Money Laundering Control*, vol. 28, n.º 4-5, pp. 593–608. <https://doi.org/10.1108/JMLC-03-2025-0041>

INTERPOL (2024): *Responsible AI Innovation in Law Enforcement. AI Toolkit Technical Reference Book*.

JENSEN, R. I. T. y IOSIFIDIS, A. (2023): “Fighting Money Laundering with Statistics and Machine Learning”, *IEEE Access*, n.º 11, pp. 8889-8903. <https://doi.org/10.1109/ACCESS.2023.3239549>

KUTE, D. V. *et al.* (2021): “Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering—A Critical Review”, *IEEE Access*, n.º 9, pp. 82300-82317. <https://doi.org/10.1109/ACCESS.2021.3086230>

LAKHCHINI, W. *et al.* (2022): “Artificial Intelligence & Machine Learning in Finance. A literature review”, *International Journal of Accounting, Finance, Auditing, Management and Economics*, vol. 3, n.º 6, pp. 437-455. <https://doi.org/10.5281/zenodo.7454232>

LEAL RUÍZ, R. (2024): “Entre la eficiencia y la opacidad: inteligencia artificial en la prevención del blanqueo de capitales”. En ABADÍAS SELMA, A. y GONZÁLEZ URIEL, D. (coords.): *El impacto de la IA en el aprendizaje y en la práctica del derecho*. Aranzadi La Ley, Madrid, pp. 385-406.

LEÓN ALAPONT, J. (2024): “La inteligencia artificial al servicio de la desinformación: un nuevo reto para el derecho penal”. En JIMÉNEZ GARCÍA, F. (dir.): *Seguridad y responsabilidad penal e internacional en el uso de las TIC y la inteligencia artificial*. Iustel, Madrid, pp. 95-127.

LEÓN ALAPONT, J. (2026): “Líneas generales de la nueva política de la Unión Europea en materia de corrupción y recuperación de ganancias ilícitas”, *ReCRIM: Revista de l'Institut Universitari d'Investigació en Criminologia i Ciències Penals de la UV*, n.º 36, pp. 216-230.

LUNA ÁLVAREZ, E. R. (2025): “Anatomía jurídica del sesgo algorítmico en el uso de la IA”, *Revista de derecho y proceso penal*, n.º 79, pp. 1-12 (versión digital).

MANAVADARIA, M. S. *et al.* (2025): “Machine Learning for Fraud Detection and Financial Crimes”. En AA. VV. (eds.): *Forensic Intelligence and Deep Learning Solutions in Crime Investigation*. IGI Global Scientific Publishing, Pennsylvania, pp. 183-206. <https://doi.org/10.4018/979-8-3693-9405-2.ch010>

MANZOOR, M. F. y ASLAM, M. F. (2025): “Enhancing Banking Fraud Detection: Role of Machine Learning and Deep Learning Methods”, *Premier Journal of Artificial Intelligence*, n.º 3, pp. 1-13. <https://doi.org/10.70389/PJAI.100014>

MATALLÍN EVANGELIO, Á. (2018): “Blanqueo de capitales y principios penales”, *Teoría y derecho: Revista de Pensamiento Jurídico*, n.º 24, (ejemplar dedicado a: Garantías constitucionales, prensa y Derecho penal), pp. 272-303.

MATALLÍN EVANGELIO, Á. (2023): “La prueba del origen ilícito de los bienes y otros problemas interpretativos del blanqueo de capitales”, *Revista Penal México*, n.º 23, pp. 47-69.

- MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL (2020): *ENIA: Estrategia Nacional de Inteligencia Artificial. Versión 1.0*.
- MONTESDEOCA RODRÍGUEZ, D. (2025): “Aportaciones de la inteligencia artificial al desarrollo del *compliance* penal”. En ESTUPIÑÁN CÁCERES, R. y FONTICIELLA HERNÁNDEZ, B. (dirs.): *Una mirada jurídica poliédrica a la normativa europea sobre inteligencia artificial*. Dykinson, Madrid, pp. 466-485.
- NIE, C. et al. (2026): “*AI Application in Anti-Money Laundering for Sustainable and Transparent Financial Systems*”. En AA. VV.: *Proceedings of the 2025 International Conference on Artificial Intelligence and Sustainable Development. Association for Computing Machinery, New York*, pp. 239–251. <https://doi.org/10.1145/3786484.3786522>
- OYEDOKUN, O. et al. (2024): “*A Comprehensive Review of Machine Learning Applications in AML Transaction Monitoring*”, *International Journal of Engineering Research and Development*, vol. 20, n.º 11, pp. 730-743.
- PARAMESHA, M. et al. (2024): “*Artificial Intelligence, Machine Learning, Deep Learning, and Blockchain in Financial and Banking Services: A Comprehensive Review*”, *Partners Universal Multidisciplinary Research Journal*, vol. 1, n.º 2, pp. 68-83. <http://dx.doi.org/10.2139/ssrn.4855893>
- PETTERSSON RUIZ, E. y ANGELIS, J. (2022): “*Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges*”, *Journal of Money Laundering Control*, vol. 25, n.º 4, pp. 766–778. <https://doi.org/10.1108/JMLC-09-2021-0106>
- SEGURA PEÑA, L. et al. (2024): “*Machine Learning Models for Money Laundering Detection in Financial Institutions. A Systematic Literature Review*”, *22nd LACCEI International Multi-Conference for Engineering, Education, and Technology: Sustainable Engineering for a Diverse, Equitable, and Inclusive Future at the Service of Education, Research, and Industry for a Society 5.0*, pp. 1-10. <https://doi.org/10.18687/LACCEI2024.1.1.1682>
- SERRANO ACITORES, A. (2023): “Consideraciones éticas y legales en el uso de la inteligencia artificial: el enfoque de la Unión Europea”, *Revista de fiscalidad internacional y negocios transnacionales*, n.º 24, pp. 1-24 (versión digital).
- TURKSEN, U. et al. (2024): “*Legal implications of automated suspicious transaction monitoring: enhancing integrity of AP*”, *Journal of Banking Regulation*, n.º 25, pp. 359-377. <https://doi.org/10.1057/s41261-024-00233-2>
- VIDALES RODRÍGUEZ, C. (2012): “Blanqueo, ¿qué es blanqueo? Estudio del artículo 301.1 del Código Penal Español tras la reforma de la L.O. 5/2010”, *Revista General de Derecho Penal*, n.º 18, pp. 1-29.
- VIDALES RODRÍGUEZ, C. y LARRIBA HINOJAR, B. (2015): “Estrategias legales frente a la criminalidad organizada en España”, *Revista Penal México*, n.º 8, pp. 215-227.
- ZHANG, Y. y TRUBEY, P. (2019): “*Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection*”, *Computational Economics*, n.º 54, pp. 1043–1063. <https://doi.org/10.1007/s10614-018-9864-z>