08/01/2026

La IA y el análisis de redes revolucionan el modo de perseguir el fraude y el blanqueo de capitales

En 2017, la fundadora de la criptomoneda OneCoin subió a un avión en Sofía (Bulgaria) y desapareció. Se esfumó con una fortuna estimada en más de 4 000 millones de dólares, estafados a millones de personas en todo el mundo en uno de los mayores esquemas piramidales de la historia. Desde entonces, el objetivo del FBI no es solo encontrar a la fundadora (incluida en su lista de los diez delincuentes más buscados), sino responder a la pregunta: ¿dónde está el dinero?.

Casos como el de OneCoin, popularizados por pódcasts como Scam Inc. de The Economist (2024), revelan dos crímenes. El primero es la estafa. El segundo, más silencioso y complejo, es el blanqueo de capitales: el proceso de hacer que ese dinero robado parezca legítimo.

El gato y el ratón

El fraude de OneCoin no es un hecho aislado. Cada año se blanquea en el sistema financiero global entre el 2 % y el 5 % del PIB mundial, o hasta 2 billones de dólares. Ese dinero es el combustible del terrorismo, la trata de personas y la corrupción.

Durante décadas, la lucha contra el blanqueo de capitales (Anti-Money Laundering o AML) ha sido un juego del gato y el ratón. Los reguladores creaban una norma y los delincuentes encontraban cómo saltársela.

Tras analizar la vanguardia de esta lucha, hemos comprobado que el tablero de juego ha cambiado. La era de las hojas de cálculo va llegando a su fin y está comenzando la era de la inteligencia artificial.

Capacidad de adaptación

Hasta hace poco, las administraciones públicas obligaban a los bancos y a otras entidades a usar sistemas basados en reglas. Eran simples: si una transacción superaba los 10 000 euros, se marcaba. Si una cuenta recibía de repente 50 transferencias pequeñas, se marcaba.

El problema es que los delincuentes se adaptan. Para evitar ser detectados, comenzaron a dividir el dinero en cientos de transacciones diminutas, logrando así pasar por debajo de los umbrales de alerta.

Los blanqueadores de OneCoin, por ejemplo, usaron redes de empresas fantasma y transferencias opacas para mover el dinero por todo el mundo. El resultado era un caos para las entidades, que se ahogaban en miles de falsos positivos mientras el dinero de origen realmente ilegítimo se colaba por las grietas del sistema.

Nuestro estudio identifica un cambio de paradigma desde la estadística hacia el aprendizaje automático (machine learning). En lugar de seguir reglas rígidas, estos sistemas de IA aprenden patrones de comportamiento. La inteligencia artificial antiblanqueo aprende qué es normal para una cuenta y detecta anomalías: transferencias a paraísos fiscales, operaciones nocturnas o redes de cuentas que parecen diseñadas solo para mover dinero.

Análisis de redes: una herramienta revolucionaria

Las administraciones se han dado cuenta de que el blanqueo de capitales no se realiza en un acto aislado, sino en una red de transacciones. En lugar de mirar cada transacción como un punto individual, el análisis de redes (network analysis) dibuja un mapa

que conecta las cuentas.

Imagine: una transferencia de 5 000 euros de la cuenta A a la cuenta B no es sospechosa. Pero el análisis de redes puede mostrar que esos 5 000 euros van de A a B, de B a C, de C a D y, finalmente, de D vuelven a A. Este patrón circular se utiliza para disimular el origen ilícito mediante múltiples capas de transacciones. El análisis de redes detecta el mapa completo.

Nadie tiene la imagen completa

En nuestro estudio identificamos un problema crítico que llamamos “ceguera de red” (network blindness). Esto ocurre cuando cada banco ve solo su parte de las transacciones, sin acceso a la foto completa del flujo ilícito. Si el dinero de la trama salta del banco A al banco B, la primera entidad solo registra la salida y la segunda solo la entrada, perdiendo así el rastro global.

Aquí, la acción de la administración pública es crucial. Para encontrar a los blanqueadores las autoridades financieras deben convertirse en tecnólogos. Nuestro análisis de las investigaciones sobre el tema apunta a un nuevo kit de herramientas para estos organismos:

- **Marcos para compartir datos y homogenización:** la ceguera de red solo se cura si las entidades pueden compartir información de forma segura y colaborativa. La nueva Autoridad Europea contra el Blanqueo (AMLA) es un paso en esta dirección.
- **Sandboxes regulatorios:** se deben crear entornos de prueba seguros para que los entidades obligadas puedan experimentar de forma controlada con nuevas IA antiblanqueo.
- **Medir lo que importa:** abandonar los indicadores simples de cumplimiento (como el número de informes de sospecha rellenados) o las lista de comprobación, y empezar a medir la efectividad real, con métricas orientadas a resultados.
- **Afrontar la privacidad:** el equilibrio entre vigilancia y privacidad es el gran reto. La solución pasa por nuevas tecnologías, como el aprendizaje federado (federated learning), que permite a las IA de varias entidades aprender de patrones comunes sin compartir nunca los datos personales de los clientes.

La lucha contra el blanqueo de capitales ha dejado de ser un asunto de contables para convertirse en una batalla del big data. La mejor forma para encontrar los miles de millones de OneCoin y frenar a las próximas redes de delincuencia es usar redes de inteligencia para desmantelarlas.The Conversation

María Dolores Lagoa Varela, Profesora del departamento de Empresa (Área: Economía Financiera) , Universidade da Coruña; José Castelao López, Economía financiera y contabilidad, Universidade da Coruña y María Teresa Corzo Santamaría, Profesora de Finanzas de la Facultad de Ciencias Económicas y Empresariales de la Universidad Pontificia Comillas (Comillas ICADE), Universidad Pontificia Comillas.

Fuente: https://elobrero.es

LINK DE LA NOTICIA