Revista DO TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO

ARTIGOS ORIGINAIS

Desafios regulatórios e éticos relativos ao uso da inteligência artificial na prevenção e repressão à lavagem de dinheiro

Artificial intelligence in the prevention and repression of money laundering

El uso de la inteligencia artificial en la prevención y represión del blanqueo de capitales

João Paulo Orsini Martinelli[1]

Universidade de Pernambuco (PE - Brasil)
Lattes: http://lattes.cnpq.br/0279190483460977
Orcid: https://orcid.org/0000-0002-3168-2492

DOI: https://doi.org/10.65674/rev-trf3.v37i163.755

[1] Pós-doutorado em andamento na Universidade de Pernambuco (PE - Brasil). Pós-doutor em Direitos Humanos pela Universidade de Coimbra (Portugal). Doutor e Mestre em Direito Penal pela Universidade de São Paulo (SP - Brasil). Professor convidado do Mestrado Profissional do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (DF - Brasil). Advogado criminalista e consultor jurídico.

RESUMO: A lavagem de dinheiro representa uma ameaça global substancial, com trilhões de dólares movimentados anualmente. Diante da crescente sofisticação dos criminosos e da "hiper-globalização", denota-se que os métodos tradicionais de prevenção e repressão mostram-se cada vez mais ineficazes. Nesse contexto, o uso da inteligência artificial (IA) surge como uma ferramenta promissora, capaz de processar vastos volumes de dados e identificar padrões complexos de forma inatingível para humanos, otimizando o monitoramento de transações, a análise de redes e o suporte a investigações em setores vulneráveis, especialmente em ambientes de criptomoedas. Contudo, a implementação da IA enfrenta desafios éticos, legais e regulatórios significativos, como vieses algorítmicos que podem gerar discriminação, opacidade dos sistemas ("caixa-preta"), complexa atribuição de responsabilidade jurídica, preocupações com privacidade e risco de a própria IA ser usada para fins ilícitos. Diante disso, o presente artigo tem como objetivo analisar o uso da IA na prevenção e repressão à lavagem de dinheiro, explorando seu potencial, as principais aplicações e os desafios que precisam ser superados para que essa tecnologia seja empregada de forma eficaz e ética. Para tanto, adota o método de abordagem dedutivo, com base em uma revisão bibliográfica e documental de caráter qualitativo. Conclui-se que o pleno potencial da IA exige um arcabouço regulatório e ético robusto, pautado no desenvolvimento de IA explicável (XAI), na colaboração público-privada e na capacitação humana. Tais elementos garantem que a tecnologia sirva à justiça financeira de forma transparente, ética e responsável, otimizando mecanismos de prevenção e repressão à lavagem de dinheiro.

PALAVRAS-CHAVE: inteligência artificial; lavagem de dinheiro; prevenção; repressão; compliance; risco algorítmico; criptomoedas.

ABSTRACT: Money laundering represents a substantial global threat, with trillions of dollars moved annually. Given the increasing sophistication of criminals and 'hyper-globalization,' traditional methods of prevention and enforcement are proving increasingly ineffective. In this context, the use of artificial intelligence (AI) emerges as a promising tool, capable of processing vast volumes of data and identifying complex patterns in a way unattainable for humans, optimizing transaction monitoring, network analysis, and investigative support in vulnerable sectors, especially in cryptocurrency environments. However, the implementation of AI faces significant ethical, legal, and regulatory challenges, such as algorithmic biases that can lead to discrimination, system opacity ('black box'), complex attribution of legal liability, privacy concerns, and the risk of AI itself being used for illicit purposes. Therefore, this article aims to analyze the use of AI in the prevention and suppression of money laundering, exploring its potential, key applications, and the challenges that must be overcome for this technology to be employed effectively and ethically. To this end, it adopts a deductive approach, based on a qualitative bibliographic and documentary review. It concludes that the full potential of AI requires a robust regulatory and ethical framework, based on the development of explainable AI (XAI), public-private collaboration, and human capacity building. These elements ensure that technology serves financial justice in a transparent, ethical, and responsible manner, optimizing mechanisms for the prevention and suppression of money laundering.

KEYWORDS: artificial intelligence; money laundering; prevention; repression; compliance; algorithmic risk; cryptocurrencies.

RESUMEN: El lavado de dinero representa una amenaza global sustancial, con billones de dólares movilizados anualmente. Ante la creciente sofisticación de los criminales y la 'hiperglobalización', se denota que los métodos tradicionales de prevención y represión se muestran cada vez más ineficaces. En este contexto, el uso de la inteligencia artificial (IA) surge como una herramienta prometisora, capaz de procesar vastos volúmenes de datos e identificar patrones complejos de forma inalcanzable para los humanos, optimizando el monitoreo de transacciones, el análisis de redes y el apoyo a investigaciones en sectores vulnerables, especialmente en entornos de criptomonedas. Sin embargo, la implementación de la IA enfrenta desafíos éticos, legales y regulatorios significativos, como sesgos algorítmicos que pueden generar discriminación, opacidad de los sistemas ('caja negra'), compleja atribución de responsabilidad jurídica, preocupaciones con la privacidad y el riesgo de que la propia IA sea utilizada para fines ilícitos. Ante esto, el presente artículo tiene como objetivo analizar el uso de la IA en la prevención y represión al lavado de dinero, explorando su potencial, las principales aplicaciones y los desafíos que necesitan ser superados para que esta tecnología sea empleada de forma eficaz y ética. Para ello, adopta el método de enfoque deductivo, con base en una revisión bibliográfica y documental de carácter cualitativo. Se concluye que el pleno potencial de la IA exige un marco regulatorio y ético robusto, pautado en el desarrollo de IA explicable (XAI), en la colaboración público-privada y en la capacitación humana. Tales elementos garantizan que la tecnología sirva a la justicia financiera de forma transparente, ética y responsable, optimizando los mecanismos de prevención y represión al lavado de dinero.

PALABRAS CLAVE: inteligencia artificial; blanqueo de capitales; prevención; represión; compliance; riesgo algorítmico; criptomonedas.

SUMÁRIO:

1 Introdução

A lavagem de dinheiro, a exemplo do que ocorre com outros crimes econômicos, representa uma das maiores ameaças à integridade dos sistemas financeiros globais e à estabilidade das economias nacionais. Ao longo das últimas décadas, a crescente sofisticação das organizações criminosas, aliada à globalização e ao avanço tecnológico, tem permitido que volumes massivos de recursos de origem ilícita sejam integrados ao fluxo econômico legítimo, dificultando a detecção e a persecução penal (Ruivo, 2025).

Estimativas de Christine Jojarth (2013) apontam que, anualmente, entre 2% e 5% (dois a cinco por cento) do produto interno bruto global, equivalente a US$ 1,3 a 3,2 trilhões em 2010, são lavados, evidenciando a magnitude avassaladora do problema. Peter Smith (2023) corrobora essa visão, ressaltando que a lavagem de dinheiro atingiu "proporções alarmantes" devido à "hiper-globalização", ao "rápido crescimento do comércio digital" e aos "sistemas bancários opacos".

Tradicionalmente, a prevenção e repressão à lavagem de dinheiro baseiam-se em abordagens regulatórias e fiscais, com instituições financeiras e outras entidades obrigadas a reportar transações suspeitas e a manter registros detalhados de seus clientes. No entanto, o relatório da Consultoria Z/Yen (2005), sediada em Londres, já destacava que, apesar dos altos custos e da rigorosa regulamentação, os requisitos antilavagem de dinheiro no Reino Unido, por exemplo, não eram percebidos como mais eficazes do que em outras jurisdições, sugerindo um ponto de inflexão em que os custos superam os benefícios.

Essa percepção de ineficácia e o ônus sobre as entidades reguladas impulsionaram a busca por soluções inovadoras. Nesse contexto, a inteligência artificial (IA) desponta como uma ferramenta promissora, capaz de processar e analisar volumes de dados em uma escala e complexidade inatingíveis para a análise humana, oferecendo novas perspectivas para a detecção, prevenção e repressão de atividades de lavagem de dinheiro.

No entanto, a implementação da IA não está isenta de desafios. Questões éticas, legais, regulatórias e técnicas, como vieses algorítmicos, "opacidade" das decisões de IA e atribuição de responsabilidade, demandam atenção cuidadosa e uma abordagem multidisciplinar.

Diante desse quadro, o presente artigo tem como objetivo analisar o uso da IA na prevenção e repressão à lavagem de dinheiro, explorando seu potencial, as principais aplicações e os desafios que precisam ser superados para que essa tecnologia seja empregada de forma eficaz e ética.

Para tanto, a presente pesquisa adota o método de abordagem dedutivo, com base em uma revisão bibliográfica e documental de caráter qualitativo.

O texto está dividido em seções que abordam a contextualização da lavagem de dinheiro, os fundamentos da IA, suas aplicações práticas na prevenção e repressão da lavagem de dinheiro, as complexidades éticas e legais, bem como as perspectivas futuras e recomendações.

Conclui-se que o pleno potencial da IA exige um arcabouço regulatório e ético robusto, pautado no desenvolvimento de IA explicável (XAI), na colaboração público-privada e na capacitação humana. Tais elementos garantem que a

tecnologia sirva à justiça financeira de forma transparente, ética e responsável, otimizando mecanismos de prevenção e ampliando a eficácia da repressão à lavagem de dinheiro.

2 A lavagem de dinheiro: contexto, magnitude e métodos tradicionais

A lavagem de dinheiro é um processo intrinsecamente ligado à criminalidade organizada e à corrupção, que busca legitimar fundos provenientes de atividades ilícitas. Sua definição clássica, conforme Christine Jojarth (2013), envolve a criação de uma falsa aparência legítima para fundos maculados por sua origem ilegal.

Esse processo é tradicionalmente dividido em três fases, apesar de que a consumação do crime não exige necessariamente a ocorrência de todas elas[2]: a colocação (*placement*), que consiste na inserção dos fundos ilícitos no sistema financeiro; a ocultação (*layering*), que visa distanciar os fundos de sua origem mediante uma série complexa de transações; e a integração (*integration*), na qual os fundos são reintroduzidos na economia legítima com aparência de licitude. Essas fases, embora didáticas, muitas vezes se sobrepõem e ocorrem de forma contínua e complexa, o que aumenta a dificuldade de detecção.

A colocação representa a fase inicial e mais crítica do processo de lavagem de dinheiro, caracterizada pela introdução dos recursos de origem ilícita no sistema financeiro formal (Fabián Caparrós, 1998). Neste estágio, o criminoso busca inserir grandes volumes de dinheiro em espécie no circuito econômico legítimo, enfrentando os controles regulatórios e de *compliance* das instituições financeiras. Como exemplo prático, considere um esquema de tráfico internacional de drogas que gera milhões em dinheiro em espécie. Os traficantes utilizam interpostas pessoas (laranjas) para realizar múltiplos depósitos fracionados em contas bancárias de diferentes instituições, mantendo valores abaixo dos limites de comunicação obrigatória ao COAF, ou ainda adquirem bens de alto valor, como imóveis e veículos, pagando em dinheiro vivo através de terceiros que figuram como compradores aparentes.

A ocultação, segunda fase do ciclo, consiste em criar múltiplas camadas de complexidade nas transações financeiras para distanciar os recursos de sua origem criminosa. O objetivo é dificultar ou impedir o rastreamento pelos órgãos de inteligência financeira e autoridades policiais. No caso prático em análise, após os depósitos iniciais, os recursos são transferidos entre diversas contas bancárias de empresas de fachada, sediadas em diferentes paraísos fiscais, realizando operações simuladas de comércio exterior através de importações fictícias com superfaturamento. As empresas de fachada, sem atividade econômica real,

[2] Nesse sentido: "Imperioso destacar, que, para fins de consumação do delito, não há a necessidade da ocorrência de todas as fases anteriormente declinadas, dispensando-se a comprovação de que os valores que foram ocultados, por exemplo, retornaram ao seu real proprietário (ainda que tal contexto possa ocorrer no mundo fenomênico) - sinteticamente, cada uma das etapas declinadas, isoladamente consideradas, tem o condão de configurar o crime de lavagem de dinheiro. Portanto, sob o aspecto jurídico não há a necessidade da ocorrência de todas as fases da lavagem para a sua configuração". (Tribunal Regional Federal da 3ª Região, Apelação Criminal 5000329-51.2021.4.03.6181, Relator Desembargador Federal Fausto de Sanctis, j. 07/08/2025, DJe 14/08/2025)

emitem notas fiscais por serviços jamais prestados, criando uma cadeia de transações que mascara a origem do dinheiro. Os recursos circulam por jurisdições com legislações opacas e baixa cooperação internacional, utilizando ainda o sistema paralelo de remessas conhecido como dólar-cabo para movimentações transfronteiriças sem registro oficial (Souza; Coelho, 2020).

A integração constitui a fase final, quando os recursos já "lavados" retornam à economia formal com aparência de legitimidade, sendo utilizados pelo criminoso sem despertar suspeitas. Neste momento, o dinheiro ilícito transforma-se em patrimônio aparentemente lícito, pronto para ser usufruído ou reinvestido (Oliveira, 1998). No exemplo do tráfico de drogas, após a complexa rede de ocultação, os recursos retornam ao país através de investimentos em negócios legítimos: aquisição de imóveis de alto padrão, participação societária em empresas consolidadas, aplicações em fundos de investimento imobiliário, ou ainda compra de títulos de capitalização e cotas de consórcio. O traficante passa a figurar como empresário de sucesso, com renda justificada por atividades econômicas formais, gozando livremente do patrimônio construído com recursos criminosos. A integração completa do ciclo torna extremamente difícil a identificação da origem ilícita sem investigações aprofundadas e cooperação internacional entre unidades de inteligência financeira.

A magnitude global desse problema é estarrecedora. Conforme apontado por Christine Jojarth (2013), a lavagem de dinheiro movimenta trilhões de dólares anualmente, volumes que corroem economias, enfraquecem governos e distorcem o desenvolvimento econômico ao direcionar investimentos para projetos de menor risco de detecção, em vez dos mais lucrativos.

Peter Smith (2023) enfatiza que esse capital ilícito tem um impacto devastador, especialmente em regiões em desenvolvimento, pois a dificuldade de recuperação desses valores prejudica iniciativas cruciais como os Objetivos de Desenvolvimento Sustentável (ODS). Ademais, a perda de bilhões de dólares em fluxos financeiros ilícitos em regiões como África, América Latina e Caribe reforça a gravidade da situação.

Outra questão relevante a ser considerada envolve o fato de que os métodos de lavagem de dinheiro evoluem constantemente, tornando as abordagens de combate um desafio contínuo, mormente em setores como o mercado imobiliário e o mercado de luxo, que são particularmente vulneráveis.

No que tange ao setor imobiliário, Luís Rodolfo Cruz E. Creuz (2011) destaca que a lavagem de dinheiro é muito frequente nesse setor, facilitada pela compra e venda de imóveis com recursos em espécie ou de origens diversas, e por falsas especulações. Para combater isso, o autor menciona a Lei nº 9.613/1998 e a Resolução COFECI nº 1.168/2010, substituída posteriormente pela Resolução COFECI nº 1.336/2014).

Tais resoluções impõem obrigações de identificação de clientes, registro de transações e comunicação de operações suspeitas ao Conselho de Controle de Atividades Financeiras (COAF). No entanto, essas regulamentações dependem da capacidade humana de identificar padrões complexos.

Similarmente, o mercado de luxo é um setor sensível para a prática de lavagem de dinheiro devido à subjetividade valorativa de seus bens e à facilidade de movimentação de itens como joias, metais preciosos e objetos de arte.

Sobre esse aspecto, José Paulo Micheletto Naves (2021) detalha que pessoas físicas e jurídicas que comercializam bens de luxo acima de R$ 10.000,00 (dez mil reais) são consideradas "sujeitos obrigados", com a responsabilidade de identificar clientes e comunicar operações suspeitas ao COAF (artigo 9º, XII, da Lei nº 9.613/1998; artigo 1º da Resolução nº 25/2013 do COAF[3]).

Contudo, a efetividade dessas medidas é questionável, visto que transações em espécie, pagamentos por terceiros sem justificativa ou valores incompatíveis com a capacidade financeira das partes, apesar de poderem configurar indício de lavagem de dinheiro, costumam ser subnotificadas pelos lojistas. Portanto, a dificuldade de fiscalização representa um grande desafio.

Outro método de lavagem cada vez mais comum e insidioso envolve a utilização de "money mules" (mulas de dinheiro), indivíduos recrutados sem o seu conhecimento para transferir fundos ilícitos. A maioria dessas transações está ligada ao cibercrime, como *phishing* e fraudes *online*, e as vítimas são frequentemente pessoas em situações de vulnerabilidade, como desempregados, estudantes ou idosos (Esoimeme, 2020).

A detecção desses esquemas requer que os bancos fiquem atentos a padrões como a idade e situação de vida dos clientes, países de origem e destino dos fundos, depósitos frequentes e grandes em dinheiro, seguidos de transferências eletrônicas, e o uso de serviços de gestão de patrimônio.

Também deve-se atentar para o crescimento das empresas financeiras na internet. Embora as *fintechs* e as novas tecnologias possam oferecer ferramentas para o *compliance*, o desenvolvimento tecnológico também introduz riscos significativos que dificultam a prevenção da lavagem de dinheiro.

Principalmente no que tange aos ativos virtuais, como as criptomoedas, o problema reside em características intrínsecas e na falta inicial de regulamentação clara. A possibilidade de anonimato nas transações, a dificuldade em identificar e verificar os participantes do mercado, a ausência de um órgão supervisor centralizado e a complexidade no rastreamento dos fluxos de troca tornam as criptomoedas particularmente atraentes para criminosos.

Essas tecnologias facilitam as fases de ocultação (com a abertura de contas anônimas e conversão rápida de recursos ilícitos), dissimulação (pela facilidade de movimentação transfronteiriça sem barreiras) e integração (devido à crescente aceitação para aquisição de bens), permitindo que os ativos ilegais sejam mascarados e reinseridos na economia formal com maior agilidade e menor risco de detecção.

Além disso, a lavagem de dinheiro baseada no comércio (*trade-based money laundering* - TBML) é uma das formas mais sofisticadas e difíceis de detectar, uma vez que envolve a manipulação de preços de bens e serviços – subfaturação e

[3] Na página institucional do COAF está disponível um "conjunto de regras e diretrizes estabelecidas por entidades reguladoras setoriais com o objetivo de prevenir e combater a lavagem de dinheiro, o financiamento do terrorismo e a proliferação de armas de destruição em massa nos respectivos setores econômicos sob sua supervisão. Essas normas impõem obrigações específicas aos regulados, como a implementação de políticas internas de prevenção, a avaliação de riscos, o conhecimento do cliente (KYC), o monitoramento e a análise de operações, a comunicação de operações suspeitas ao Coaf, além de exigências de capacitação de colaboradores e governança compatível com o porte e complexidade da instituição". (Brasil, COAF, 2024)

superfaturação – para movimentar lucros ilícitos por meio de transações comerciais internacionais.

Trata-se de um método complexo de movimentar dinheiro ilícito ou esconder sua origem mediante transações comerciais internacionais. O objetivo é disfarçar a transferência de fundos e integrá-los ao sistema financeiro legítimo. A escala desse fenômeno é astronômica, com discrepâncias nos dados comerciais globais que somam trilhões de dólares, conforme pesquisas da *Global Financial Integrity* (GFI).

Diante desse cenário, as abordagens tradicionais de combate à lavagem de dinheiro, embora essenciais, enfrentam sérias limitações. O relatório da Z/Yen (2005), desde aquela época, já apontava para custos elevados e uma percepção de baixa eficácia dos programas de prevenção à lavagem, com a conformidade muitas vezes motivada mais pelo temor de sanções do que pela convicção na efetividade das medidas.

Segundo o documento, a sobrecarga dos sistemas de relatórios de atividades suspeitas (*suspicious activity reports* - SARs) e a falta de *feedback* das agências de inteligência financeira para as instituições financeiras minavam a motivação e a eficácia.

Nesse sentido, Tatiana Tropina (2017) salienta que as ferramentas tradicionais não conseguem lidar com o volume crescente de dados não estruturados que caracterizam a era digital.

Adicionalmente, Barbara Kowalczyk-Hoyer *et al* (2017) criticam a falta de transparência nos dados sobre os esforços de combate à lavagem de dinheiro, ressaltando que, em muitos países com grandes centros financeiros, esses dados são tratados como "top secret", impedindo o escrutínio público e a avaliação independente da eficácia das medidas.

Por sua vez, Max Heywood e Jessica Ebrard (2017) também sublinham a "limitada e inconsistente" implementação dos padrões internacionais de PLD/FTP[4], especialmente no setor de luxo e para empresas e profissões não financeiras designadas (EPNFDs), que sofrem com "baixos níveis de supervisão e fiscalização eficazes".

Todas essas lacunas e desafios apontam para a necessidade de soluções mais avançadas e eficientes, que a IA pode oferecer, consoante será apresentado neste estudo.

3 Fundamentos da inteligência artificial e seu potencial

A IA representa a automação do comportamento inteligente, replicando habilidades mentais humanas como reconhecimento de padrões, compreensão da

[4] O COAF é a "unidade de inteligência financeira (UIF) brasileira e coordena a participação brasileira junto aos principais organismos multilaterais relacionados à *prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação de armas de destruição em massa (PLD/FTP)*. O Brasil integra desde 1999 o Grupo de Ação Financeira (Gafi/FATF) e o Grupo de Egmont de Unidades de Inteligência Financeira. Desde 2000, também faz parte do Grupo de Ação Financeira da América Latina (Gafilat)". (Brasil, COAF, 2026)

linguagem natural e aprendizado adaptativo a partir da experiência (De Spiegeleire *et al*, 2017). Longe de ser uma tecnologia singular, a IA é uma coleção de campos distintos que trabalham em diferentes tecnologias.

Predominantemente, a IA opera em nível de inteligência artificial estreita (ANI), superando a inteligência humana em tarefas específicas, como reconhecimento de imagem, transcrição de fala, tradução, algoritmos de negociação de alta frequência e filtros de *spam*.

No âmbito desse trabalho, é importante compreender a definição de Anirban Chakraborty e Shilpa Sharma (2020) sobre aprendizado de máquina (*machine learning* - ML), entendido como uma categoria da IA que capacita algoritmos a melhorar a precisão na previsão de desempenho sem programação explícita, aprendendo com os dados e aprimorando-se ao longo do tempo. Essa capacidade é fundamental para lidar com a complexidade e a mutabilidade dos métodos de lavagem de dinheiro.

Além disso, é imprescindível considerar que a atual "revolução da IA", iniciada por volta de 2011, é impulsionada por avanços conceituais, por um aumento exponencial do poder computacional e, crucialmente, pela disponibilidade massiva de *big data*[5].

O *big data*, como aponta Tatiana Tropina (2017), é uma poderosa arma de escolha no combate a fluxos financeiros ilícitos, pois permite processar e analisar conjuntos de dados não lineares e conectar dados aparentemente desconectados, superando as limitações das ferramentas tradicionais.

Para funcionar, a IA geralmente passa por um processo de treinamento, em que é exposta a uma vasta quantidade de dados rotulados ou não rotulados. Por meio de técnicas como aprendizado de máquina (*machine learning*) e aprendizado profundo (*deep learning*), os modelos de IA ajustam seus parâmetros internos para otimizar seu desempenho em uma tarefa específica. Por exemplo, em um cenário de reconhecimento de imagens, o modelo aprende a identificar objetos após analisar milhares de fotos de diferentes objetos, aprimorando sua capacidade de generalização e precisão ao longo do tempo.

Sendo assim, na análise de dados, a IA é uma ferramenta poderosa que automatiza e aprimora a descoberta de *insights* complexos. Ela pode ser usada para identificar tendências, anomalias, segmentar clientes, prever comportamentos futuros e otimizar processos.

Ao lidar com volumes massivos de informações, que seriam impossíveis de analisar manualmente, a IA permite que empresas e pesquisadores extraiam valor estratégico dos dados, transformando-os em conhecimento acionável para a tomada de decisões mais eficazes e eficientes.

Essa capacidade de processamento de volumes gigantescos de informações é a essência do potencial da IA em PLD/FTP, como será demonstrado nos próximos tópicos.

---

[5] *Big data* refere-se ao conjunto massivo de dados – estruturados e não estruturados – gerados continuamente por sistemas, dispositivos, transações e interações digitais, em volume, velocidade e variedade tão grandes que ferramentas tradicionais de processamento não conseguem analisar eficientemente.

4 A inteligência artificial na prevenção à lavagem de dinheiro: aplicações e vantagens

A capacidade da IA em processar grandes volumes de dados e identificar padrões complexos a torna uma ferramenta inestimável para a prevenção à lavagem de dinheiro, superando muitas das limitações das abordagens tradicionais. De fato, suas aplicações na PLD/FTP são vastas e abrangem diversas áreas.

Uma das aplicações mais diretas é o monitoramento de transações e a detecção de anomalias. Como explicam Anirban Chakraborty e Shilpa Sharma (2020), o *machine learning* permite que algoritmos melhorem continuamente sua precisão na previsão de desempenho, sem serem explicitamente programados. Isso é crucial em um cenário em que os métodos criminosos estão sempre mudando.

Nessas circunstâncias, a IA pode analisar fluxos financeiros em tempo real, identificar transações que fogem do perfil usual do cliente ou da média do mercado, e sinalizar atividades suspeitas que sistemas baseados em regras fixas não conseguiriam captar. Essa capacidade de reconhecimento de padrões e aprendizado adaptativo é a essência da eficácia da IA para a PLD/FTP.

Outra área de destaque para a IA se refere à análise de redes complexas e a identificação de beneficiários finais, pois a lavagem de dinheiro frequentemente envolve estruturas corporativas opacas, empresas de fachada e uma teia de transações entre múltiplos atores para ocultar a origem dos fundos.

Federico Paesano (2023) salienta que, mesmo em ambientes de criptomoedas, em que o anonimato aparente é um desafio, a IA pode auxiliar na atribuição, processo que permite vincular transações e endereços a pessoas reais por meio da análise de *clusters* de endereços e heurísticas.

Ademais, sistemas de IA são excepcionalmente capazes de realizar *graph analytics*[6] em grandes bases de dados, revelando as conexões ocultas entre indivíduos e entidades que compõem esquemas de lavagem, auxiliando na identificação dos verdadeiros proprietários beneficiários, superando um desafio significativo na implementação de padrões internacionais de prevenção na lavagem de dinheiro.

A IA também contribui significativamente para a otimização de programas de *compliance* e a mitigação de responsabilidade pela diminuição de riscos. José Rodolfo Juliano Bertolino (2023) elenca pilares de um programa de *compliance* eficaz, como avaliação de riscos, controles internos e vigilância, áreas em que a IA pode atuar de forma transformadora. Uma vez que pode processar e analisar dados em larga escala para identificar vulnerabilidades e *red flags*[7] de lavagem de

---

[6] *Graph analytics* é uma técnica de IA que analisa relacionamentos e conexões entre entidades representando-as como grafos (redes) – estruturas compostas por nós (pontos/entidades) e arestas (linhas/conexões entre eles).

[7] *Red flags* (bandeiras vermelhas) é expressão utilizada em análise financeira para indicar casos concretos em que, provavelmente, há prática de lavagem de dinheiro, considerando os elementos suspeitos, como, por exemplo, transações de valores sem origem explicada ou grandes volumes movimentados para "paraísos fiscais".

dinheiro com muito mais eficiência que métodos manuais, garantindo um monitoramento contínuo e a automação de alertas.

A capacidade de a IA registrar e analisar a efetividade das medidas de *compliance* pode, inclusive, fornecer evidências concretas da robustez de um programa, o que é crucial para a mitigação de responsabilidade (Tonin, 2022). A utilização de *big data* para prever e interromper fluxos financeiros ilícitos (FFI) é uma das maiores vantagens da IA.

Tatiana Tropina (2017) descreve como a análise de *big data* está substituindo as abordagens tradicionais baseadas em "bandeiras vermelhas" por modelos preditivos em tempo real, utilizando dados estruturados e não estruturados, incluindo informações de geolocalização, dispositivos móveis e mídias sociais. Isso permite a detecção do uso indevido de novos tipos de pagamentos e o rastreamento de transações para garantir sua legitimidade.

No caso da lavagem de dinheiro baseada no comércio (TBML), a IA pode combinar registros de comércio de diferentes países e instituições para descobrir padrões suspeitos, como incompatibilidades em documentos e discrepâncias entre descrições de mercadorias.

Por fim, a possibilidade de adaptação da IA a novas tipologias criminosas demonstra a magnitude de seu potencial, especialmente nesse cenário em que criminosos buscam constante inovação, e os métodos de lavagem de dinheiro evoluem rapidamente.

Decerto, a capacidade de aprendizado da IA (*machine learning*) é vital para se adaptar a essas novas tipologias, identificando padrões emergentes de lavagem de dinheiro que um sistema baseado em regras predefinidas não conseguiria captar. Em ambientes de criptomoedas, a IA pode analisar vastos dados para identificar padrões e anomalias que o "olho humano" dificilmente perceberia, transformando a complexidade em inteligência acionável.

Por outro lado, torna-se imprescindível a adoção da IA explicável (XAI), visando assegurar a transparência e os mecanismos *feedback* necessários. Sobre essa temática, Jennifer L. Bauer (2018) destaca a XAI como uma forma de permitir que as máquinas "não apenas expliquem, mas também racionalizem e prevejam seu padrão de comportamento futuro para uma melhor compreensão humana".

No contexto da lavagem de dinheiro, um sistema XAI poderia não apenas sinalizar uma transação como suspeita, mas também explicar os fatores e padrões que levaram a essa conclusão, tornando a decisão compreensível e auditável. Isso é crucial para que os analistas humanos possam validar as detecções, reduzir falsos positivos e garantir a conformidade legal e ética.

5 A inteligência artificial na repressão à lavagem de dinheiro: aprimorando as investigações

Além de sua aplicação preventiva, a IA também pode desempenhar um papel fundamental no aprimoramento das investigações e na repressão à lavagem de dinheiro, fornecendo aos órgãos de aplicação da lei e ao Poder Judiciário ferramentas poderosas para desvendar esquemas criminosos e recuperar ativos.

Nesse aspecto, o exemplo das criptomoedas corrobora como a IA é essencial para a análise forense digital e para a atribuição, como já mencionado acima. Pois, embora as criptomoedas e a tecnologia *blockchain* tenham sido inicialmente vistas como ferramentas para criminosos anônimos, a IA tem demonstrado a capacidade de penetrar no aparente anonimato.

De fato, algoritmos de aprendizado de máquina podem analisar padrões de transações na *blockchain*, identificar *clusters* de endereços que pertencem à mesma entidade e usar técnicas de análise de rede para vincular pseudônimos a entidades do mundo real (Paesano, 2023).

Essa capacidade de atribuição é vital para as investigações, permitindo que as autoridades sigam a trilha de dinheiro digital e identifiquem os agentes por trás das atividades ilícitas.

Conforme ilustrado por Topo Santoso *et al* (2011), a IA também é crucial na identificação de padrões de corrupção e lavagem em setores específicos, como o setor florestal. Os autores detalham como essas práticas ilícitas podem ocorrer em todas as fases da exploração ilegal de madeira, desde a emissão de licenças até a venda.

Nesses casos, é possível mapear as mais diversas movimentações, por exemplo, envolvendo depósitos de propinas em contas de funcionários, compra de seguros com lucros ilícitos e transferências internacionais complexas, a fim de acompanhar a capilaridade dos delitos. A partir disso, a IA pode analisar e cruzar dados financeiros com informações setoriais (licenças, produção, vendas) para identificar anomalias, falsificações de documentos e redes de pagamento ilegais, auxiliando os investigadores a focarem seus esforços em áreas de alto risco.

No âmbito do suporte a órgãos judiciais, a experiência da Justiça do Trabalho no Brasil serve como importante exemplo. Maximiliano Pereira de Carvalho e Marcos Vinícius Barroso (2019) demonstram como esse ramo judicial, ao lidar com altas taxas de congestionamento da execução, percebeu a intrínseca relação entre a dificuldade de cumprimento das sentenças e a ocultação e lavagem de bens.

A criação dos Núcleos de Pesquisa Patrimonial (NPPs) e a adoção de sistemas como o SIMBA (Sistema de Investigação de Movimentações Bancárias), que utiliza dados de instituições financeiras para análise e cruzamento de informações, foram passos importantes. A adesão à Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA) e a criação do Laboratório de Tecnologia contra Lavagem de Dinheiro (LAB-LD) no Conselho Superior da Justiça do Trabalho (LAB-CSJT) representam um vanguardismo, com o uso de *softwares* de alta capacidade para pesquisa, análise e tratamento de volumes massivos de dados.

De forma ampla, é possível visualizar que a IA pode ter papel fundamental para investigações financeiras complexas em diversos domínios, pois, como destaca Tatiana Tropina (2017), o *big data* (e, por extensão, a IA) equipa as agências de aplicação da lei com processos analíticos poderosos para melhorar abordagens proativas e reativas, identificando conexões entre informações aparentemente não relacionadas em investigações complexas, como as de crime organizado.

Essa capacidade de cruzar vastos conjuntos de dados de diferentes fontes, como registros bancários, dados de telecomunicações, informações de redes sociais e bases de dados públicas, permite que os investigadores construam uma

imagem mais completa das atividades criminosas, identifiquem suspeitos, rastreiem fundos e preparem casos mais robustos para a persecução penal, o que colabora de forma direta para a repressão desses delitos.

6 Desafios éticos, legais e regulatórios relativos ao uso da inteligência artificial na prevenção e repressão à lavagem de dinheiro

Apesar do imenso potencial da IA no combate à lavagem de dinheiro, sua implementação não é isenta de desafios complexos que exigem uma consideração cuidadosa e uma abordagem multidisciplinar.

Decerto, a integração da IA em sistemas tão sensíveis quanto os de prevenção e repressão a crimes financeiros levanta questões éticas, legais e regulatórias cruciais.

Um dos maiores desafios são os vieses algorítmicos, pois, na medida em que a IA aprende com dados históricos, se esses dados contiverem preconceitos ou refletirem desigualdades sociais e históricas, o algoritmo pode perpetuá-los ou até amplificá-los.

A esse respeito, Victor Sampaio Gondim e Gustavo Raposo Pereira Feitosa (2022) ilustram o problema com o caso do *software* COMPAS, utilizado na justiça criminal dos EUA, que apresentou uma "grave tendência racial", classificando indivíduos negros como de alto risco de reincidência a uma taxa duas vezes maior que a de brancos. Tais vieses, conforme os autores, não configuram uma "ação" com dolo por parte da IA, mas uma reprodução de padrões presentes nos dados de treinamento.

No contexto de lavagem de dinheiro, um modelo treinado com dados enviesados poderia direcionar a fiscalização de forma desigual ou falhar em identificar novos métodos de lavagem, gerando falsos positivos ou falsos negativos para grupos específicos.

Por isso, William Magnuson (2020) reforça que a dependência de dados tende a levar a resultados que perpetuam o *status quo*, incluindo preconceitos existentes no mercado.

Outra limitação crítica é a opacidade dos algoritmos, frequentemente referida como o problema da "caixa-preta", visto que muitos sistemas de IA, especialmente aqueles baseados em *deep learning*, operam de maneiras que, muitas vezes, nem mesmo seus criadores conseguem explicar detalhadamente.

Essa falta de transparência dificulta a compreensão da lógica por trás das decisões da IA, tornando impossível para os tomadores de decisão humanos entenderem o porquê de uma sinalização de fraude ou de uma liberação de transação.

Jennifer L. Bauer (2018) argumenta que essa opacidade protege os processos e resultados de uma revisão significativa, criando o risco de uma "ditadura de dados", em que resultados são aceitos cegamente sem questionamento. Essa característica é uma preocupação substancial, já que, no caso de falhas, a falta de explicabilidade compromete a responsabilização e a melhoria contínua do sistema.

Ademais, a questão da responsabilidade é um problema muito complexo na aplicação da IA em contextos legais e criminais. Helena Folgueira de Campos Vieira (2024) aponta para um vácuo de responsabilidade devido à natureza *sui generis* da IA e seu aprendizado autônomo. Por sua vez, Samuel Ebel Braga Ramos e Cathiani M. Bellé (2022) argumentam, com base na teoria significativa do delito, que a IA não pode ser considerada um agente ativo para fins penais no Brasil, pois não possui vontade ou consciência, elementos essenciais para o dolo e a culpabilidade. Consequentemente, a responsabilidade penal recai sobre os seres humanos (programadores, operadores) ou empresas.

No âmbito da responsabilidade civil, Gustavo da Silva Melo (2021) defende que as cláusulas gerais da lei civil brasileira são suficientes para responsabilizar o fornecedor de IA por falhas, inclusive pelo "risco do desenvolvimento", já que a autoaprendizagem e imprevisibilidade da IA são características esperadas da tecnologia.

Por outro lado, Helena Folgueira de Campos Vieira (2024) propõe a teoria da omissão imprópria, responsabilizando humanos que, por negligência em seus deveres de supervisão e controle, falham em evitar resultados lesivos causados pela IA.

Maksim Karliuk (2018) também aborda essa dificuldade, explorando diferentes analogias para a responsabilidade da IA, mas conclui que a imprevisibilidade de sistemas autônomos e a dificuldade de determinar a responsabilidade são desafios persistentes.

Essas discussões revelam a necessidade de fixar marcos legais claros para atribuir responsabilidade em casos de falha da IA.

Além dos vieses e da questão da responsabilidade, há o risco de a própria IA ser instrumentalizada para fins ilícitos. Nils Christopher Köbis *et al* (2022) cunharam o termo "corrupt AI", que descreve o abuso de sistemas de IA por detentores de poder para ganho privado.

Isso pode se manifestar em "design corrupto" (sistemas projetados intencionalmente para fins ilícitos, como *deepfakes*), "manipulação corrupta" (exploração de vulnerabilidades em sistemas existentes, como a captura algorítmica) ou "aplicação corrupta" (reaproveitamento de IA benigna para vigilância em massa ou *microtargeting*[8] político).

Essas características, combinadas com a autonomia e escalabilidade da IA, podem tornar os crimes financeiros ainda mais sofisticados e difíceis de rastrear, criando um desafio para a PLD/FTP.

Camino Kavanagh (2019) também destaca a natureza de uso duplo (*dual-use*) das aplicações de IA, o que dificulta o controle de seu desenvolvimento e regulamentação, além de ressaltar a expansão de ameaças cibernéticas em sistemas críticos dependentes de IA.

---

[8] *Microtargeting* é a prática de segmentar e direcionar mensagens, conteúdos ou propaganda para grupos muito específicos e reduzidos de pessoas, baseado em dados detalhados sobre seus comportamentos, preferências, vulnerabilidades e características pessoais. O *microtargeting* político representa uma "aplicação corrupta" de IA, ou seja, usar tecnologia inicialmente benigna (algoritmos de recomendação, análise de dados) para fins manipulatórios e antidemocráticos.

De acordo com o autor, no relatório *"New Tech, New Threats, and New Governance Challenges"*, publicado pelo *Carnegie Endowment for International Peace*, a IA situa-se num contexto de "dual-use" (duplo uso) pois é uma tecnologia cujas capacidades são inerentemente ambivalentes, podendo servir tanto ao progresso civil e econômico quanto a propósitos militares ou maliciosos. O autor ressalta que essa dualidade cria um desafio de governança sem precedentes, pois as mesmas inovações que otimizam a medicina, as comunicações e a infraestrutura podem ser redirecionadas para usos prejudiciais, como a automação de ataques cibernéticos mais rápidos e sofisticados, o desenvolvimento de Sistemas de Armas Autônomas Letais (LAWS) – que operam sem intervenção humana significativa – e a implementação de mecanismos de vigilância e controle social que corroem a privacidade. Além disso, Kavanagh adverte que a IA pode ser explorada de maneira nociva para desestabilizar democracias por meio da desinformação (como *deepfakes*) e para aprofundar injustiças sociais via vieses algorítmicos, transformando a opacidade técnica e a autonomia das máquinas em vetores de risco que ameaçam a segurança internacional e os direitos fundamentais (Kavanagh, 2019).

Outro ponto relevante refere-se à privacidade e à proteção de dados, que são preocupações primordiais. Como a IA em PLD/FTP lida com vastas quantidades de dados pessoais e financeiros, Romulo Greco et al (2023) levanta questões cruciais sobre a invasão do cotidiano e a necessidade de mecanismos de controle e conformidade com leis de proteção de dados, como a LGPD.

Nesse aspecto, Gustavo da Silva Melo (2021) ressalta que a IA representa o ápice da preocupação com a privacidade, dada sua capacidade de vigilância e persuasão. A dependência de grandes volumes de informações pela IA também envolve "proteção de dados, privacidade e outros princípios e valores, como equidade e igualdade, autonomia, transparência, responsabilidade e devido processo".

Portanto, equilibrar a necessidade de acesso a dados para combater crimes com a proteção dos direitos individuais à privacidade é um dilema central. Diante desses desafios, reconhece-se a indispensabilidade de regulamentação e governança da IA. Romulo Greco *et al* (2023) mencionam iniciativas como o *EU Artificial Intelligence Act* e o PL nº 21/2020[9], no Brasil, que buscam estabelecer parâmetros para o uso ético e transparente da IA.

Camino Kavanagh (2019) destaca a proliferação de princípios, valores e padrões de ONGs, governos e fóruns multilaterais, que buscam guiar o desenvolvimento e uso da IA. William Magnuson (2020) argumenta que os reguladores já possuem uma ampla gama de leis, mas que a regulamentação precisa se adaptar para auditar algoritmos, garantir a explicabilidade, mitigar preconceitos e abordar a IA adversária, que consiste em técnicas que exploram vulnerabilidades em sistemas de IA, com o objetivo de enganar, manipular ou

[9] O mencionado Projeto de Lei restou declarado "prejudicado" e foi arquivado na Câmara dos Deputados, em 20/01/2025, em decorrência da aprovação de substitutivo ao Projeto de Lei nº 2.338/2023 no Senado Federal. No momento da revisão deste trabalho, em março/2026, o referido projeto está em apreciação na Câmara dos Deputados, aguardando parecer do relator da Comissão Especial, tendo sido aprovados requerimentos para a realização de audiências públicas sobre a matéria.

perturbar o funcionamento de modelos de IA, fazendo com que produzam resultados incorretos ou indesejados.

Portanto, a criação de estruturas regulatórias claras, que definam os limites e riscos aceitáveis da IA, e que exijam auditorias de modelos, transparência de dados e código, e responsabilidade legal, é essencial para preencher o "vácuo de responsabilidade".

Por fim, o fator humano permanece crucial. Tatiana Tropina (2017) enfatiza que as ferramentas de *big data* não são a resposta; são apenas uma parte da resposta. Os resultados da IA precisam ser analisados, interpretados e contextualizados por humanos que formulam as perguntas certas e tomam as decisões finais.

Nesse sentido, William Magnuson (2020) alerta para o excesso de confiança e os vieses cognitivos humanos que podem levar à dependência excessiva das recomendações da IA.

Assim sendo, a IA deve ser compreendida como uma ferramenta de apoio, empoderando os analistas humanos com *insights* e alertas, mas sem substituir a análise crítica, a supervisão e o discernimento ético e jurídico, que permanecem responsabilidades indelegáveis dos seres humanos.

7 Perspectivas futuras e recomendações

O futuro da IA na prevenção e repressão à lavagem de dinheiro é promissor, mas dependerá criticamente da capacidade de mitigar os desafios existentes e de promover um desenvolvimento e uso responsável da tecnologia.

Sem dúvida, a IA continuará a evoluir rapidamente, com avanços em *machine learning*, processamento de linguagem natural e visão computacional que permitirão análises ainda mais sofisticadas e em tempo real de dados financeiros e comportamentais.

Uma das principais perspectivas é o desenvolvimento contínuo da IA de forma mais robusta e explicável (XAI). A superação da "caixa-preta" é fundamental para construir confiança nos sistemas de IA. A XAI permitirá que os analistas e investigadores compreendam a lógica por trás das decisões do algoritmo, validem os resultados e corrijam vieses, o que é essencial para a auditabilidade, a atribuição de responsabilidade e a aceitação legal.

O relatório da *Transparency International* (2017) já criticava a falta de transparência e o acesso limitado a dados sobre PLD/FTP. Para que a IA seja verdadeiramente eficaz, é necessário um fluxo de dados mais robusto e transparente entre instituições financeiras, órgãos reguladores e agências de aplicação da lei.

Desse modo, investimentos em pesquisa e desenvolvimento para XAI são cruciais para que a IA não apenas detecte, mas também justifique suas conclusões, tornando-se uma aliada transparente no processo de tomada de decisão humana. Para tanto, a colaboração público-privada e a troca de informações são imperativas.

Federico Paesano (2023) recomenda aumentar a cooperação com empresas de análise de *blockchain* e provedores de serviços de ativos cripto para agilizar o compartilhamento de informações e a resposta a ordens de congelamento. A criação de plataformas seguras e padronizadas para a troca de dados, utilizando IA para anonimização e garantia da privacidade, pode otimizar a detecção de padrões de lavagem em escala global.

Ademais, a educação e capacitação de profissionais são igualmente importantes. A IA não substitui o ser humano, mas o complementa. É fundamental treinar analistas de *compliance*, investigadores, promotores e juízes para entender as capacidades e limitações da IA, interpretar seus *insights* e tomar decisões informadas.

Nesse ponto, relevante a conclusão de Romulo Greco *et al* (2023) no sentido de que "os limites da inteligência artificial somos nós que colocamos", enfatizando a necessidade de que pesquisadores e operadores do Direito acompanhem o uso dessas tecnologias, criando normas e regras para ajustar seu uso.

Também deve-se considerar que a lavagem de dinheiro é um crime adaptável, e os criminosos também usarão a IA para sofisticar seus métodos. Em vista disso, as soluções de IA para PLD/FTP devem ser constantemente atualizadas e testadas contra novas tipologias e potenciais "corrupt AI" ou ataques adversários.

Assim, evidencia-se que é essencial manter um equilíbrio delicado entre inovação e segurança, o que exige um ciclo contínuo de pesquisa, desenvolvimento e implementação de contramedidas.

Deve-se, também, avaliar como a IA pode ser uma importante ferramenta para executar as recomendações do GAFI para prevenção à lavagem de dinheiro: avaliação de riscos e abordagem baseada no risco, devida diligência do cliente (CDD/KYC), pessoas politicamente expostas (PEPs), comunicação de transações suspeitas, entre outras.

Finalmente, a criação de um arcabouço regulatório e ético robusto é a pedra angular para o sucesso da IA na PLD/FTP. Como sugerido por Helena Folgueira de Campos Vieira (2024), é necessária uma regulamentação clara que defina os limites e riscos aceitáveis da IA, além de medidas de governança corporativa e *compliance* para a correta manutenção e calibração dos sistemas.

Essa regulamentação deve ser ágil e adaptável para acompanhar a evolução tecnológica, garantindo a proteção da privacidade, a equidade, a transparência e a responsabilidade em todas as etapas do ciclo de vida da IA.

8 Conclusão

A lavagem de dinheiro representa uma ameaça global de magnitude avassaladora, cujos métodos tradicionais de prevenção e repressão mostram-se cada vez mais ineficazes diante da sofisticação dos criminosos e da hiper-globalização. Nesse cenário, o uso da inteligência artificial surge como uma ferramenta promissora e indispensável, capaz de processar vastos volumes de dados e identificar padrões complexos em escala inatingível para a análise humana. Contudo, o pleno potencial dessa tecnologia exige um arcabouço

regulatório e ético robusto, que impeça a aceitação cega de resultados e garanta que a inovação sirva à justiça financeira de forma transparente e responsável.

A implementação da IA enfrenta desafios éticos, legais e regulatórios significativos, como os vieses algorítmicos exemplificados pelo software COMPAS, a opacidade dos sistemas conhecidos como "caixa-preta" e a complexa atribuição de responsabilidade jurídica. Diante disso, é indispensável que os marcos regulatórios estabeleçam parâmetros claros para o uso ético da tecnologia, a exemplo das iniciativas do *EU Artificial Intelligence Act*. Tais normas devem ser capazes de auditar algoritmos, garantir a explicabilidade e mitigar preconceitos, além de abordar a IA adversária e o risco de "corrupt AI", em que o design ou a aplicação da tecnologia são instrumentalizados para fins ilícitos. A regulamentação precisa ainda harmonizar o combate aos fluxos financeiros ilícitos com a proteção de dados e a privacidade previstos na LGPD, evitando que a vigilância automatizada resulte em uma ditadura de dados que ignore princípios como equidade, autonomia e devido processo.

No âmbito da conformidade legal, a adoção da IA explicável (XAI) revela-se como o pilar fundamental para permitir que as máquinas não apenas sinalizem suspeitas, mas racionalizem seu padrão de comportamento. Isso torna a decisão compreensível e auditável para os analistas humanos, garantindo a conformidade ética necessária para a validação das investigações.

A experiência internacional e as recomendações do GAFI indicam que a regulamentação deve focar na avaliação de riscos e na devida diligência em setores vulneráveis, como criptomoedas, mercado imobiliário e de luxo. É essencial que as normas promovam a colaboração público-privada e a troca transparente de informações entre instituições financeiras, órgãos reguladores e o COAF. O uso de *Big Data* e modelos preditivos em tempo real deve ser incentivado para superar as limitações das ferramentas tradicionais, permitindo a detecção de tipologias complexas como a lavagem de dinheiro baseada no comércio (TBML).

Finalmente, o fator humano permanece como o elemento crucial e indelegável na supervisão desses sistemas. A IA deve ser compreendida como uma ferramenta de apoio que empodera os investigadores, mas que não substitui o discernimento ético e a análise crítica humana na tomada de decisões finais.

Referências

BAUER, Jennifer L. The necessity of auditing artificial intelligence algorithms, *Social Science Research Network*, ago. 2018. Disponível em: https://ssrn.com/abstract=3218675. Acesso em: 10 out. 2025.

BERTOLINO, José Rodolfo Juliano. Compliance e responsabilidade penal da pessoa jurídica: o programa de autorregulação como uma atenuante criminal. *Revista de Direito Penal Econômico e Compliance*, v. 4, n. 16, p. 45-66, out./dez. 2023.

BRASIL. COAF. *O Coaf no sistema de PLD/FTP*. Assuntos, 25 ago. 2020 (atualizado em 15 mar. 2024). Disponível em: https://www.gov.br/coaf/pt-br/assuntos/o-sistema-de-prevencao-a-lavagem-de-dinheiro/o-coaf-no-sistema-de-prevencao-e-combate-a-lavagem-de-dinheiro. Acesso em: 10 out. 2025.

BRASIL. COAF. *Normas de PLD/FTP de outros supervisores*. Legislação e normas, 27 out. 2020 (atualizado em 24 fev. 2026). Disponível em: https://www.gov.br/coaf/pt-br/centrais-de-conteudo/legislacao-e-normass/normas-de-outros-supervisores. Acesso em: 25 fev. 2026.

BRASIL. Tribunal Regional Federal da 3ª Região. *Apelação Criminal 5000329-51.2021.4.03.6181*, Relator Desembargador Federal Fausto de Sanctis, j. 07/08/2025, DJe 14/08/2025. Disponível em: https://web.trf3.jus.br/acordaos/Acordao/BuscarDocumentoPje/332817659. Acesso em: 25 fev. 2026.

CARVALHO, Maximiliano Pereira de; BARROSO, Marcos Vinícius. Combatendo a corrupção e a lavagem de dinheiro: a experiência da justiça do trabalho. *Revista de Direito do Trabalho*, vol. 45, n. 198, p. 19-32, fev. 2019.

CHAKRABORTY, Anirban; SHARMA, Shilpa. Machine learning in artificial intelligence. *International Journal of Advanced Research in Engineering and Technology,* v. 11, n. 6, p. 392-399, jun. 2020. Disponível em: https://iaeme.com/MasterAdmin/Journal_uploads/IJARET/VOLUME_11_ISSUE_6/IJARET_11_06_035.pdf. Acesso em: 10 out. 2025.

CREUZ, Luís Rodolfo Cruz E. COAF, lavagem de dinheiro e o mercado imobiliário: questões relevantes relacionadas às práticas e às atividades no mercado imobiliário e normas brasileiras de prevenção à lavagem de dinheiro. *Revista Tributária e de Finanças Públicas*, vol. 19, n. 101, p. 325-340, nov./dez. 2011.

DE SPIEGELEIRE, Stephan; MAAS, Matthijs; SWEIJIS, Tim. What is artificial intelligence? In: *Artificial intelligence and the future of defense:* strategic implications for small- and medium-sized force providers. Hague Centre for Strategic Studies, p. 25-42, 2017. Disponível em: http://www.jstor.com/stable/resrep12564.7. Acesso em: 10 out. 2025.

ESOIMEME, Ehi Eric. Identifying and reducing the money laundering risks posed by individuals who have been unknowingly recruited as money mules. *Social Science Research Network*, jun. 2020. Disponível em: https://ssrn.com/abstract=3752095. Acesso em: 10 out. 2025.

FABIÁN CAPARRÓS, Eduardo A. *El delito de blanqueo de capitales*. Madri: Colex, 1998.

GONDIM, Victor Sampaio; FEITOSA, Gustavo Raposo Pereira. Algoritmização da justiça criminal: uma análise do aplicativo Compas e seus vieses. *Revista Brasileira de Ciências Criminais*, v. 30, n. 188, p. 447-470, fev. 2022.

GRECO, Romulo; ALVES, Débora Longo; MATTEU, Ivelise Fonseca de. Inteligência artificial, quais os limites? *Revista de Direito Constitucional e Internacional*, v. 31, n. 136, p. 153-164, mar./abr. 2023.

HEYWOOD, Max; EBRARD, Jessica. International standards: the FATF recommendations and the G20 beneficial ownership principles. *In*: *Tainted treasures:* money laundering risks in luxury markets. Transparency International, p. 20-29, 2017. Disponível em: http://www.jstor.com/stable/resrep20576.10. Acesso em: 10 out. 2025.

JOJARTH, Christine. Money laundering: motives, methods, impact, and countermeasures. *In*: STIFTUNG, Heinrich-Böll; SCHÖNENBERG, Regine (Eds.). *Transnational organized crime*: analyses of a global challenge to democracy, p. 18-33, 2013. Disponível em: https://www.jstor.org/stable/j.ctv1fxh0d.5. Acesso em: 10 out. 2025.

KARLIUK, Maksim. Ethical and legal issues in artificial intelligence. *In*: *International and Social Impacts of Artificial Intelligence Technologies*. Working Paper No. 44. Moscou: Russian International Affairs Council (RIAC), p. 43-49, 2018. Disponível em: https://ssrn.com/abstract=3460095. Acesso em: 10 out. 2025.

KAVANAGH, Camino. Artificial intelligence. *In: New tech, new threats, and new governance challenges*: an opportunity to craft smarter responses? Carnegie Endowment for International Peace, p. 13-22, 2019. Disponível em: http://www.jstor.com/stable/resrep20978.5. Acesso em: 10 out. 2025.

KÖBIS, Nils Christopher; STARKE, Christopher; EDWARD-GILL, Jaselle. The corruption risks of artificial intelligence. *Transparency International*, 2022. Disponível em: https://www.jstor.org/stable/resrep43028. Acesso em: 10 out. 2025.

KOWALCZYK-HOYER, Barbara; HEYWOOD, Max; SIMEONE, Gabriele. Introduction: corruption, banks and anti-money laundering data. *In*: Top Secret: countries keep financial crime fighting data to themselves. *Transparency International*, p. 2-6, 2017. Disponível em: https://www.jstor.org/stable/resrep20589.3. Acesso em: 10 out. 2025.

MAGNUSON, William. Artificial financial intelligence. *Harvard Business Law Review*, v. 10, n. 2, p. 337-382, 2020. Disponível em: https://ssrn.com/abstract=3403712. Acesso em: 10 out. 2025.

MELO, Gustavo da Silva. Violação à privacidade causada por entes dotados de inteligência artificial. *Revista de Direito e as Novas Tecnologias*, v. 13, p. 1-12, out./dez. 2021.

NAVES, José Paulo Micheletto. O crime de lavagem de dinheiro no mercado de luxo. *Revista de Direito Penal Econômico e Compliance*, v. 2, n. 7, p. 29-51, jul./set. 2021.

OLIVEIRA, William Terra de. A criminalização da lavagem de dinheiro (aspectos penais da Lei 9.613 de 1º de março de 1998). *Revista Brasileira de Ciências Criminais*, v. 6, n. 23, p. 111-129, jul./set. 1998.

PAESANO, Federico. Cryptocurrencies and money laundering investigations. *Basel Institute on Governance, 2023.* Disponível em: https://www.jstor.org/stable/resrep52987. Acesso em: 10 out. 2025.

RAMOS, Samuel Ebel Braga; BELLÉ, Cathiani M. Teoria significativa do delito e inteligência artificial: uma releitura do conceito de ação nos crimes de preconceito. *Revista Brasileira de Ciências Criminais*, n. 190, p. 93-114, maio/jun. 2022.

RUIVO, Marcelo Almeida. O bem jurídico protegido no crime de lavagem de dinheiro. *Revista Brasileira de Ciências Criminais*, n. 206, p. 101-126, jan./fev. 2025.

SANTOSO, Topo *et al*. Corruption and money laundering. *In*: SANTOSO, Topo *et al*. *A guide to investigation and indictment using an integrated approach to law enforcement*. Center for International Forestry Research, p. 27-61, 2011. Disponível em: http://www.jstor.com/stable/resrep02129.8. Acesso em: 10 out. 2025.

SMITH, Peter. The magnitude of money laundering. *In*: SMITH, Peter. *Money laundering*: from environmental crime. Igarape Institute, p. 2-4, 2023. Disponível em: https://www.jstor.org/stable/resrep51368.4. Acesso em: 10 out. 2025.

SOUZA, Artur de Brito Gueiros; COELHO, Cecília Choeri da Silva. Questões atuais na prevenção da lavagem de dinheiro. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 165, p. 41-69, mar. 2020.

TONIN, Alexandre Baraldi. *Compliance*: uma visão do *compliance* como forma de mitigação de responsabilidade. *Revista dos Tribunais*, v. 1046, p. 359-377, dez. 2022.

TROPINA, Tatiana. Big data: tackling illicit financial flows. *In*: DE BUSSER, Els et *al*. *Big data:* a twenty-first century arms race. Atlantic Council, p. 41-52, 2017.

Disponível em: https://www.jstor.org/stable/resrep03719.8. Acesso em: 10 out. 2025.

VIEIRA, Helena Folgueira de Campos. Responsabilidade penal por delitos cometidos por inteligência artificial. *Revista de Direito Penal Econômico e Compliance*, v. 5, n. 19, p. 37-49, jul./set. 2024.

Z/YEN. Anti-money laundering requirements: costs, benefits and perceptions. *City Research Series Number Six*. Corporation of London, 2005. Disponível em: https://www.zyen.com/media/documents/AMLR_FULL.pdf. Acesso em: 10 out. 2025.

FLUXO EDITORIAL:

- Data de submissão: 16 out. 2025
- Data de aprovação: 30 mar. 2026
- Data de publicação: 06 abr. 2026

- Avaliação: por pares dupla-anônima
- Pareceristas: 2 (dois)
- Editor Chefe: José Carlos Francisco