ENCCLA 2027

Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro

ENCCLA em Debate:

Desafios, oportunidades e propostas para o sistema brasileiro de prevenção e combate à lavagem de dinheiro

DEPARTAMENTO DE RECUPERAÇÃO DE ATIVOS E COOPERAÇÃO JURÍDICA INTERNACIONAL
SECRETARIA NACIONAL DE JUSTIÇA
MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

EXPEDIENTE

Ministro da Justiça e Segurança Pública:

Wellington César Lima e Silva

Secretária Nacional de Justiça:

Maria Rosa Guimarães Loula

Diretor do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional - DRCI:

Marcelo Stopanovski

Coordenador-Geral de Articulação Institucional da Diretoria do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional - DRCI:

Guilherme Ayres Jameli

Coordenação de Enfrentamento à Lavagem de Dinheiro:

Maria Beatriz Pereira dos Santos Amaro

Organização:

Guilherme Ayres Jameli

Projeto gráfico e diagramação:

Lucas Leonardo de Souza

*É permitida a reprodução total ou parcial desta publicação desde que citada a fonte.



Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro

DEPARTAMENTO DE RECUPERAÇÃO DE ATIVOS E COOPERAÇÃO JURÍDICA INTERNACIONAL

SECRETARIA NACIONAL DE JUSTIÇA

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

Sumário

ENCCLA em Debate: Desafios, oportunidades e propostas para o sistema brasileiro de prevenção e combate à corrupção e à lavagem de dinheiro. 7

Desafios para a efetividade do sistema brasileiro de PLD/FTP: articulação público-privada em um ambiente financeiro digital e integrado. 12

Congelamento de criptoativos: da cooperação voluntária à expectativa regulatória. 20

Articulação público-privada no enfrentamento à lavagem de dinheiro, à fraude e às ameaças cibernéticas. 26

Prevenção À Lavagem De Dinheiro: Uma Análise Judicial Da Atuação Do Coaf. Desafios institucionais na apreciação dos RIF's. 33

Prevenir, Detectar e Evoluir: Os Desafios o Sistema Brasileiro de PLD/FTP. 411

O Combate à Corrupção, à Lavagem de Dinheiro e ao Financiamento do Terrorismo no Brasil: Novos desafios e a necessidade de uma cooperação ainda mais integrada. 50

O pagamento entre organizações criminosas como ponto de pressão no combate ao crime organizado transnacional. 59

Do dado ao ativo: a ENCCLA e o desafio de conectar os elos do sistema brasileiro de PLD/FT. 677

ENCCLA em Debate: Desafios, oportunidades e propostas para o sistema brasileiro de prevenção e combate à corrupção e à lavagem de dinheiro.

Secretaria Executiva da ENCCLA

Apresentação

Em 1998, com a promulgação da Lei nº 9.613, o Brasil deu um passo decisivo na construção de seu sistema de prevenção e combate à lavagem de dinheiro. Ao longo dos 28 anos seguintes, esse sistema passou por profundas transformações, impulsionadas pelo aperfeiçoamento do marco normativo, pelo fortalecimento das instituições, pelo desenvolvimento de capacidades técnicas e pela crescente integração entre os diferentes atores responsáveis por prevenir, identificar e reprimir a movimentação de recursos de origem ilícita.

Ao longo dessa trajetória, consolidou-se também uma compreensão fundamental: o enfrentamento à lavagem de dinheiro e à criminalidade organizada não pode se limitar à responsabilização individual dos envolvidos, mas deve alcançar sua dimensão econômica e patrimonial. Identificar fluxos financeiros ilícitos, compreender estruturas de ocultação patrimonial, interromper mecanismos de financiamento e recuperar os produtos e proveitos do crime são componentes essenciais de uma política pública capaz de comprometer a capacidade de atuação e reprodução das organizações criminosas.

Foi nesse contexto que, em 2003, surgiu a Estratégia Nacional de Combate à Lavagem de Dinheiro, posteriormente ampliada para incorporar o enfrentamento à corrupção e consolidada sob a denominação de Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA). Sua criação representou uma resposta à necessidade de superar a fragmentação da atuação estatal e construir uma agenda compartilhada entre instituições com competências distintas, mas responsabilidades complementares.

Desde sua origem, a ENCCLA fundamentou-se na convicção de que problemas complexos exigem soluções construídas coletivamente. Ao reunir instituições dos diferentes Poderes e esferas de governo, órgãos de controle e fiscalização e entidades parceiras, a Estratégia consolidou um modelo de articulação interinstitucional baseado no diálogo, na cooperação e na construção de consensos. Ao longo de mais de duas décadas, suas ações contribuíram para importantes avanços legislativos, para o desenvolvimento de instrumentos de investigação e inteligência financeira, para o fortalecimento dos mecanismos de cooperação e recuperação de ativos e para a ampliação das capacidades institucionais de enfrentamento à criminalidade. Entre os resultados dessa atuação, destacam-se:

- Programa Nacional de Capacitação e Treinamento para o Combate à Corrupção e à Lavagem de Dinheiro (PNLD);
- Rede Nacional de Laboratórios de Tecnologia contra Lavagem de Dinheiro — Rede-LAB;

- Cadastro de Clientes do Sistema Financeiro Nacional (CCS);
- Sistema Nacional de Bens Apreendidos (SNBA);
- Sistema de Investigação de Movimentações Bancárias (SIMBA);
- Cadastro de Empresas Inidôneas e Suspensas (CEIS).

Mais do que pelos resultados concretos de suas ações, a ENCCLA consolidou-se como um espaço singular de articulação e diálogo, no qual diferentes perspectivas, experiências e conhecimentos são reunidos em torno de desafios comuns. Ao promover o debate entre instituições públicas dos diferentes Poderes e esferas de governo, representantes da iniciativa privada, setores sujeitos às obrigações previstas na legislação de prevenção à lavagem de dinheiro e organizações da sociedade civil, a Estratégia favorece uma compreensão mais abrangente das vulnerabilidades e dos desafios do sistema brasileiro de prevenção e combate à lavagem de dinheiro. Essa diversidade de visões constitui um de seus principais diferenciais, permitindo a construção de diagnósticos mais consistentes e o desenvolvimento coletivo de soluções, por meio de uma metodologia baseada na cooperação, na valorização das contribuições de cada participante e na busca pelo consenso.

Essa capacidade de reunir diferentes perspectivas em torno de desafios comuns torna-se ainda mais relevante diante das profundas transformações do ambiente no qual atua o sistema brasileiro de prevenção e combate à lavagem de dinheiro. A digitalização da economia, o surgimento de novos produtos e serviços financeiros, a expansão dos ativos virtuais e a crescente complexidade das estruturas empresariais e patrimoniais impõem a necessidade de permanente avaliação e aperfeiçoamento dos mecanismos existentes. Paralelamente, a expansão econômica das organizações criminosas, sua inserção em atividades lícitas e a sofisticação de seus mecanismos de movimentação e ocultação de recursos impõem desafios crescentes às instituições públicas e privadas.

Passados 28 anos da promulgação da Lei nº 9.613/1998 e mais de duas décadas da criação da ENCCLA, é necessário reconhecer que, apesar dos importantes avanços normativos, institucionais e operacionais alcançados nesse período, a profundidade dessas transformações exige uma avaliação permanente da adequação e da efetividade do sistema brasileiro. Impõe-se, portanto, uma reflexão estratégica: **como preparar o sistema brasileiro de prevenção e combate à lavagem de dinheiro para os desafios dos próximos anos?**

Responder a essa questão exige um exame abrangente e crítico da arquitetura institucional, dos instrumentos e das práticas desenvolvidos ao longo desse período. Em que medida permanecem adequados aos riscos contemporâneos? Quais são suas principais vulnerabilidades? Onde estão as oportunidades de

aprimoramento? Como ampliar a integração entre seus componentes e aproveitar as possibilidades oferecidas pelas novas tecnologias? E, sobretudo, quais mudanças podem contribuir para aumentar a efetividade do sistema diante das transformações da economia e da criminalidade organizada?

É a partir dessa mesma lógica de articulação e valorização de diferentes perspectivas que o Ministério da Justiça e Segurança Pública, por meio da Secretaria Nacional de Justiça e do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, apresenta a publicação "ENCCLA em Debate: Desafios, oportunidades e propostas para o sistema brasileiro de prevenção e combate à lavagem de dinheiro".

A obra reúne reflexões de autoridades e profissionais de referência em diferentes campos de atuação, com o propósito de fomentar um debate qualificado sobre os desafios presentes e futuros do sistema brasileiro. Representantes da inteligência financeira, da regulação e supervisão, das instituições financeiras tradicionais, das *fintechs*, do setor de ativos virtuais, da investigação, do Ministério Público, do Poder Judiciário e da academia apresentam análises construídas a partir de suas respectivas experiências e áreas de especialização.

A pluralidade dessas contribuições constitui um dos principais valores da publicação. Ao reunir diferentes experiências e pontos de vista, **a obra pretende estimular a reflexão crítica sobre o funcionamento do sistema brasileiro de prevenção e combate à lavagem de dinheiro, contribuir para a identificação de suas vulnerabilidades e dos principais desafios a serem enfrentados nos próximos anos e fomentar o debate sobre possíveis caminhos para seu aperfeiçoamento.**

Não se pretende, com esta publicação, oferecer um diagnóstico único ou estabelecer uma agenda fechada de soluções, mas proporcionar um espaço de reflexão plural e propositiva. Os artigos reunidos expressam as análises e opiniões de seus autores, não representando necessariamente posicionamentos institucionais da ENCCLA ou do Ministério da Justiça e Segurança Pública. A liberdade de análise e a diversidade das contribuições são, precisamente, elementos fundamentais para o alcance dos objetivos desta iniciativa.

Ao mesmo tempo, o ENCCLA em Debate representa uma oportunidade de fortalecer a dimensão estratégica da ENCCLA, oferecendo subsídios para a identificação de desafios prioritários, a construção de agendas compartilhadas e o desenvolvimento de novas iniciativas voltadas ao aperfeiçoamento do sistema brasileiro. Ao promover esta publicação, o Ministério da Justiça e Segurança Pública reafirma seu compromisso com a cooperação institucional, a produção e disseminação de conhecimento e o aprimoramento contínuo das políticas públicas de prevenção e combate à corrupção e à lavagem de dinheiro.

Registramos nosso agradecimento aos autores, que generosamente compartilharam seus conhecimentos e experiências, e às instituições que, ao longo da trajetória da ENCCLA, contribuíram para a consolidação de uma rede nacional de cooperação comprometida com o enfrentamento da criminalidade e a proteção da sociedade brasileira.

Que esta publicação contribua não apenas para compreender o sistema que construímos, mas, sobretudo, para refletir sobre aquele que precisamos construir.

SECRETARIA EXECUTIVA DA ENCCLA

Desafios para a efetividade do sistema brasileiro de PLD/FTP: articulação público-privada em um ambiente financeiro digital e integrado.

Adriano Sekita

Resumo

O sistema brasileiro de prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação foi construído a partir de funções complementares de regulação, supervisão, inteligência financeira, investigação, persecução e recuperação de ativos. A transformação digital da economia, a velocidade dos pagamentos, a multiplicação de prestadores de serviços financeiros e a crescente sofisticação das organizações criminosas, porém, expõem limitações de um modelo excessivamente fragmentado e orientado ao cumprimento formal. Este artigo examina desafios prioritários para a efetividade do sistema brasileiro: compreensão compartilhada dos riscos, qualidade da informação financeira, visão integrada de redes e beneficiários finais, supervisão de novos modelos de negócio, uso responsável de tecnologia e mensuração de resultados. Sustenta-se que uma articulação público-privada estruturada, com base jurídica, governança e salvaguardas, pode transformar dados dispersos em conhecimento acionável. Propõe-se uma agenda gradual, apoiada na ENCCLA e nas competências do Banco Central do Brasil e do Coaf, com produção conjunta de tipologias, feedback estratégico, projetos-piloto e indicadores de efetividade.

Palavras-chave: PLD/FTP; articulação público-privada; Banco Central do Brasil; ENCCLA; inteligência financeira; supervisão baseada em risco; efetividade.

Um sistema maduro diante de riscos que mudaram de escala

O Brasil estruturou, desde a Lei nº 9.613/1998, um sistema no qual instituições financeiras e outros setores obrigados identificam clientes, mantêm registros, monitoram operações e comunicam situações suspeitas; o Coaf recebe e analisa informações financeiras; reguladores e supervisores definem e fiscalizam controles; e autoridades de investigação e persecução atuam sobre os ilícitos e seus resultados econômicos. Nesse sistema a ENCCLA (Estratégia Nacional de Combate à Corrupção e Lavagem de Ativos), criada em 2003, tornou-se espaço permanente de articulação entre órgãos com competências distintas.

Essa arquitetura permanece necessária, mas opera hoje em ambiente muito diferente daquele de 1998. Pagamentos instantâneos, instituições de pagamento, fintechs, plataformas digitais, ativos virtuais e apostas de quota fixa ampliaram os canais e a velocidade de circulação de recursos. Em paralelo, organizações criminosas diversificaram atividades, passaram a utilizar estruturas empresariais e patrimoniais mais complexas e aumentaram sua capacidade de transitar entre mercados ilícitos e lícitos. O convite para a publicação ENCCLA em Debate parte precisamente dessa mudança e propõe avaliar a adequação dos instrumentos atuais, suas vulnerabilidades, as oportunidades abertas pela tecnologia e as medidas capazes de elevar a efetividade do sistema.

O principal desafio não parece ser a ausência de atores ou de obrigações. É fazer com que os componentes existentes produzam uma visão comum dos riscos e respostas coordenadas. Dados cadastrais, alertas transacionais, comunicações de operações suspeitas, registros societários, informações fiscais, relatórios de inteligência e elementos de investigações são produzidos em pontos diferentes. Quando permanecem isolados, cada participante observa apenas uma fração da rede. O problema central é converter essa informação fragmentada em capacidade de prevenir, detectar e interromper fluxos ilícitos, preservando competências legais, sigilo e direitos fundamentais.

O GAFI traduz essa necessidade em padrões complementares. A Recomendação 1 exige identificação, avaliação e compreensão dos riscos; a Recomendação 2 requer coordenação nacional; as Recomendações 20 e 29 tratam das comunicações de operações suspeitas e das unidades de inteligência financeira; e a Recomendação 34 prevê orientação e feedback aos setores obrigados (FATF, 2012). A questão para o Brasil é como fazer essas funções trabalharem como sistema, e não como uma sucessão de obrigações independentes.

Desafios prioritários para a efetividade

Da quantidade de comunicações à qualidade da inteligência financeira: O modelo preventivo depende das informações produzidas pelos setores obrigados, mas o aumento do número de comunicações não demonstra, por si só, maior efetividade. Comunicações defensivas, narrativas genéricas e alertas sem contexto podem elevar custos e dificultar a priorização pela unidade de inteligência financeira. A literatura denomina esse problema de crying wolf: quando o sistema incentiva comunicação excessiva, o sinal relevante tende a se perder no volume (TAKÁTS, 2011). O desafio é elevar o valor informacional das comunicações, com indicação clara da atipicidade, dos sujeitos, das conexões e da lógica financeira observada.

Riscos digitais, velocidade e fragmentação institucional: A digitalização reduz fricções legítimas, mas também permite que recursos provenientes de fraudes e outros crimes percorram, em poucos minutos, múltiplas contas, instituições e classes de ativos. Controles organizados por produto ou por instituição podem não reconhecer uma operação que só se torna suspeita quando observada como rede. Isso exige integração entre prevenção a fraudes, segurança cibernética, conhecimento do cliente e monitoramento de PLD/FTP, além de mecanismos que permitam disseminar rapidamente novas tipologias. O desafio não é tratar inovação como risco em si, mas assegurar que a capacidade analítica acompanhe a velocidade e a interconexão do mercado.

Pessoas jurídicas, beneficiário final e infiltração na economia lícita: A utilização de empresas, cadeias societárias, interpostas pessoas e estruturas no exterior dificulta a identificação de quem controla ou se beneficia dos ativos. Informações de beneficiário final incompletas, desatualizadas ou distribuídas em bases incompatíveis reduzem a eficiência do conhecimento do cliente, da supervisão e das investigações. A avaliação mútua do Brasil pelo GAFI e pelo GAFILAT destacou a transparência de pessoas jurídicas e a disponibilidade tempestiva de informações adequadas, precisas e atualizadas como tema relevante para o aperfeiçoamento do sistema (FATF; GAFILAT, 2023). O avanço depende tanto da qualidade dos registros públicos quanto da validação e atualização realizadas pelas instituições obrigadas.

Supervisão proporcional em um perímetro mais diversos: O crescimento de modelos digitais amplia o número e a diversidade de participantes sujeitos a controles. A resposta não deve ser a aplicação mecânica do mesmo programa a instituições com portes, produtos e exposições diferentes. A abordagem baseada em risco exige intensidade proporcional, mas também padrões mínimos claros e capacidade de identificar onde controles simplificados se tornam insuficientes. Nesse sentido, o desafio é combinar supervisão baseada em dados, conhecimento dos modelos de negócio e avaliação da efetividade concreta dos controles, sem reduzir a análise a evidências documentais.

Tecnologia com governança e explicabilidade: Inteligência artificial, análise de redes e aprendizado de máquina podem melhorar seleção de alertas e identificação de vínculos, mas modelos opacos ou treinados com dados inadequados podem ampliar falsos positivos, vieses e exclusão financeira. O GAFI reconhece oportunidades e riscos das novas tecnologias, enquanto o BIS destaca que SupTech e RegTech dependem de qualidade dos dados, validação, segurança e supervisão humana (FATF, 2021b; BROEDERS; PRENIO, 2018). A tecnologia deve aumentar a compreensão do risco, e não substituir a responsabilização dos decisores.

Medir resultados, e não apenas atividades: O sistema ainda tende a mensurar insumos e produtos intermediários, como número de alertas, comunicações, inspeções ou reuniões. Esses indicadores são úteis, mas não revelam se a inteligência produzida apoiou investigações relevantes, se riscos prioritários foram mitigados ou se vulnerabilidades foram corrigidas. A mensuração deve combinar dados quantitativos e avaliações qualitativas, evitando metas que incentivem comunicações automáticas, encerramento indiscriminado de relações ou concentração apenas em casos de menor complexidade.

Articulação público-privada como método de trabalho

Diante dos desafios colocados acima, a articulação público-privada pode desempenhar um papel fundamental para garantir um sistema de PLD/FTP mais efetivo. Ela não deve ser confundida com delegação de funções estatais nem com autorização geral para compartilhar dados protegidos. Trata-se de criar canais estruturados para que autoridades e setores obrigados construam uma compreensão comum dos riscos, produzam tipologias, aperfeiçoem indicadores e recebam feedback sobre a utilidade da informação encaminhada. No nível estratégico, podem ser compartilhados diagnósticos, tendências e sinais de alerta. No nível tático, podem ser examinados fenômenos delimitados. O compartilhamento operacional de dados identificados exige base jurídica específica, finalidade, controles de acesso, rastreabilidade e salvaguardas de sigilo e proteção de dados (FATF, 2017; FATF, 2021a).

Experiências estrangeiras demonstram o potencial e os limites desse modelo. A Joint Money Laundering Intelligence Taskforce, no Reino Unido, reúne autoridades e instituições financeiras em torno de ameaças prioritárias. A Fintel Alliance, coordenada pela unidade de inteligência financeira australiana, organiza projetos conjuntos de inteligência financeira. Em Singapura, a plataforma COSMIC permite, dentro de marco legal específico, o compartilhamento entre instituições participantes de informações sobre clientes que exibam múltiplos sinais de alerta. Nenhuma dessas soluções pode ser transplantada automaticamente. Todas indicam, contudo, que colaboração efetiva requer seleção de prioridades, regras de participação, segurança, capacidade analítica e avaliação de resultados.

No Brasil, a ENCCLA oferece ambiente adequado para desenvolver essa agenda porque reúne reguladores, supervisores, Coaf, autoridades de persecução e outros órgãos com competências complementares. A participação privada pode agregar conhecimento sobre produtos, comportamento transacional e limitações operacionais, especialmente na produção de tipologias e no desenho de respostas a ameaças emergentes. A decisão estatal e o acesso a informações protegidas, entretanto, devem permanecer submetidos às competências legais de cada autoridade.

O Banco Central do Brasil ocupa posição importante nessa articulação. A Circular nº 3.978/2020 incorporou a avaliação interna de risco, o conhecimento e monitoramento de clientes, a identificação do beneficiário final, a análise de operações suspeitas e a avaliação de efetividade como elementos dos programas das instituições autorizadas. A Carta Circular nº 4.001/2020 fornece exemplos de situações que podem indicar ilícitos, sem dispensar a análise contextual. Regulação e supervisão podem, assim, criar incentivos para que o setor privado

produza informação mais útil e utilize melhor o conhecimento disseminado pelas autoridades.

Uma agenda propositiva para o sistema brasileiro

O aperfeiçoamento do sistema de PLD/FTP por meio da articulação público-privada pode ocorrer de forma gradual, começando por iniciativas de menor complexidade jurídica e maior capacidade de gerar aprendizagem.

Primeiro, o país deve fortalecer a compreensão compartilhada dos riscos. Sínteses públicas da avaliação nacional de riscos, relatórios setoriais, tipologias anonimizadas e alertas tempestivos permitem que instituições convertam prioridades nacionais em avaliações internas, critérios de monitoramento e diligência reforçada. A metodologia do Banco Mundial para avaliações nacionais reforça a importância de combinar dados, conhecimento especializado e participação de diferentes atores (WORLD BANK, 2022).

Segundo, Coaf, supervisores e setores obrigados devem ampliar mecanismos de feedback. Não é necessário revelar investigações nem o destino de comunicações específicas. Orientações agregadas podem apontar lacunas recorrentes, características de narrativas úteis e riscos insuficientemente cobertos. Esse ciclo reduz comunicação defensiva e aproxima a obrigação de reportar de sua finalidade de produzir inteligência acionável.

Terceiro, a ENCCLA poderia promover projetos-piloto de articulação público-privada sobre ameaças delimitadas, por exemplo, redes de contas de passagem associadas a fraudes digitais ou uso de pessoas jurídicas sem atividade compatível. Cada piloto deveria definir participantes, finalidade, base jurídica, dados utilizados, controles de acesso, período de retenção, métricas e avaliação independente. O resultado mais valioso pode ser a tipologia, o indicador ou a melhoria de processo produzida, e não necessariamente o compartilhamento permanente de dados individualizados.

Quarto, é necessário melhorar a interoperabilidade e a qualidade das informações de clientes, pessoas jurídicas e beneficiários finais. Isso envolve padrões de dados, mecanismos de atualização, identificação de inconsistências e acesso tempestivo pelas autoridades competentes, com observância do sigilo e da proteção de dados. A articulação com o setor privado é relevante porque as instituições verificam essas informações no início e durante a relação de negócio e podem identificar divergências que não aparecem em uma única base.

Quinto, o sistema deve adotar um quadro comum de efetividade. Indicadores podem incluir tempo entre a identificação de uma ameaça e a

atualização dos controles; proporção de comunicações associadas a riscos prioritários; qualidade das narrativas e identificadores; capacidade de detectar redes multissetoriais; uso da inteligência em investigações; correção de vulnerabilidades e impactos sobre inclusão financeira. Nenhum indicador isolado é suficiente, mas um conjunto equilibrado permite verificar se a articulação gera resultados e não apenas novas estruturas.

Por fim, toda iniciativa deve incorporar salvaguardas desde o desenho: finalidade determinada, minimização de dados, segregação de acesso, auditabilidade, segurança cibernética, prevenção de conflitos de interesse, respeito concorrencial e revisão humana. A Lei Complementar nº 105/2001, a Lei nº 9.613/1998 e a Lei Geral de Proteção de Dados estabelecem limites que não impedem soluções colaborativas, mas exigem arquitetura jurídica e tecnológica proporcional ao risco.

Considerações finais

O sistema brasileiro de PLD/FTP dispõe de instituições, experiência e instrumentos relevantes, mas precisa adaptar sua forma de operar a uma economia mais digital e a organizações criminosas mais integradas. Os desafios centrais são conectar informações fragmentadas, elevar a qualidade da inteligência financeira, compreender estruturas societárias e beneficiários finais, supervisionar um perímetro diverso, empregar tecnologia com governança e medir resultados concretos.

A articulação público-privada pode contribuir para cada um desses desafios, desde que não seja tratada como fim em si mesma. Seu valor está em produzir melhor compreensão dos riscos, comunicações mais úteis, respostas mais rápidas e capacidade de identificar redes que atravessam instituições e setores. A ENCCLA pode funcionar como espaço de formulação e avaliação dessa agenda; o Banco Central pode aportar regulação, supervisão e conhecimento do sistema financeiro; o Coaf, sua perspectiva de unidade de inteligência financeira; e o setor privado, a observação cotidiana dos clientes, produtos e transações.

O futuro do sistema não depende simplesmente de acumular novas obrigações ou mais dados. Depende de converter informação em ação, com base jurídica, governança e confiança institucional. A melhoria contínua buscada pela ENCCLA exige que cada componente preserve suas competências, mas trabalhe orientado por riscos comuns e resultados verificáveis. Essa é a passagem necessária de um sistema predominantemente baseado em conformidade para um sistema efetivamente capaz de proteger a economia e atingir a dimensão financeira da criminalidade organizada.

Referências

- BANCO CENTRAL DO BRASIL. Circular nº 3.978, de 23 de janeiro de 2020. Brasília, DF: BCB, 2020a.
- BANCO CENTRAL DO BRASIL. Carta Circular nº 4.001, de 29 de janeiro de 2020. Brasília, DF: BCB, 2020b.
- BRASIL. Lei nº 9.613, de 3 de março de 1998. Brasília, DF: Presidência da República, 1998.
- BRASIL. Lei Complementar nº 105, de 10 de janeiro de 2001. Brasília, DF: Presidência da República, 2001.
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018.
- BROEDERS, Dirk; PRENIO, Jermy. Innovative technology in financial supervision: SupTech, the experience of early users. Basel: BIS, 2018.
- FATF. International standards on combating money laundering and the financing of terrorism and proliferation: the FATF recommendations. Paris: FATF/OECD, 2012.
- FATF. Private sector information sharing: role of financial information-sharing partnerships in detecting crime. Paris: FATF/OECD, 2017.
- FATF. Stocktake on data pooling, collaborative analytics and data protection. Paris: FATF/OECD, 2021a.
- FATF. Opportunities and challenges of new technologies for AML/CFT. Paris: FATF/OECD, 2021b.
- FATF; GAFILAT. Anti-money laundering and counter-terrorist financing measures: Brazil: mutual evaluation report. Paris: FATF/OECD, 2023.
- TAKÁTS, Előd. A theory of crying wolf: the economics of money laundering enforcement. Journal of Law, Economics, and Organization, v. 27, n. 1, p. 32-78, 2011.
- WORLD BANK. National money laundering and terrorist financing risk assessment toolkit. Washington, DC: World Bank, 2022.

ADRIANO SEKITA

Sobre o autor

Auditor, Chefe de Subunidade do Escritório de Consultoria e Representação Institucional em Conduta no Departamento de Supervisão de Conduta do Banco Central do Brasil. Mestre em Economia pela Universidade de Illinois e Contabilidade pela Universidade de Melbournee. Bacharel em Economia pela Universidade Estadual de Campinas.

Congelamento de criptoativos: da cooperação voluntária à expectativa regulatória.

Alexandre Senra
Marcelo Ribeiro de Oliveira

Introdução

Em 5 de outubro de 2026, a Conduit Technology, empresa norte-americana de pagamentos internacionais, processou a Tether em Nova York (*Conduit Technology, Inc. v. Tether Holdings S.A. de C.V. et al.*, 1:26-cv-08773, S.D.N.Y.). Segundo a Conduit, a Tether congelou cerca de 2,76 milhões de USDT de sua titularidade no contexto de uma investigação da Polícia Federal, embora o seu endereço não constasse da lista de endereços que a polícia havia pedido para congelar. A ação ainda não foi julgada, e a versão da Tether não é conhecida.

O caso ilustra um fenômeno que já não é marginal. A Tether afirma cooperar com mais de 340 agências de aplicação da lei em 65 países e já ter congelado mais de US$ 4,4 bilhões ligados a atividades suspeitas. O congelamento voluntário, realizado por emissores de *stablecoins* e por *exchanges* a partir de solicitações de autoridades, tornou-se, na prática, a primeira linha da recuperação de ativos virtuais. Em maio de 2026, a Suprema Corte de Israel reconheceu a legalidade desse tipo de solicitação, feita sem tratado, sem lei específica e sem ordem judicial prévia (ATAH 65435-03-26).

Pedir é, portanto, possível. O que ainda falta são regras para o que acontece depois do pedido. É sobre isso que propomos refletir.

Dois mecanismos, um mesmo efeito

Sob a expressão "congelar criptoativos" escondem-se dois mecanismos tecnicamente distintos.

O primeiro é o **congelamento de tokens pelo emissor**. Algumas *stablecoins*, como o USDT e o USDC, são criadas por contratos inteligentes que reservam ao emissor a função de bloquear endereços. O bloqueio é registrado na própria blockchain, em evento público e datado, e atinge os tokens mantidos naquele endereço, seja quem for o seu titular: cliente do emissor ou não, em autocustódia ou não. Esse mecanismo só existe para os ativos cujo código o prevê. Não há como congelar bitcoins na rede.

O segundo é o **bloqueio de saldos por uma *exchange***. Quem mantém criptoativos numa *exchange*, em regra, não é titular de criptoativos registrados em seu nome na blockchain. Os ativos ficam em carteiras da própria *exchange*, normalmente agregadas, e o cliente tem contra ela um crédito contado em criptoativos, lançado na sua contabilidade interna. Bloquear esse saldo é impedir que o cliente o movimente ou o saque. Nada acontece na blockchain. O mecanismo alcança qualquer ativo, inclusive bitcoins, mas apenas os clientes daquela *exchange*.

Juridicamente, os dois produzem efeito semelhante: a indisponibilidade de um patrimônio. Tecnicamente, diferem em quase tudo.

	Congelamento pelo emissor	**Bloqueio pela exchange**
Objeto	Tokens mantidos em um endereço na blockchain	Crédito do cliente, contado em criptoativos
Onde ocorre	No contrato inteligente do token (on-chain)	Na contabilidade interna da exchange (off-chain)
Quem alcança	Qualquer titular do endereço, cliente ou não	Apenas clientes da exchange
Ativos alcançados	Só tokens com função de bloqueio (ex.: USDT, USDC)	Qualquer ativo custodiado, inclusive bitcoin
Comprovação	Evento público e verificável na blockchain	Registro interno da exchange
Regime no Brasil	Cooperação voluntária (emissores estrangeiros)	Res. BCB nº 520/2025 (PSAVs no Brasil); cooperação voluntária (exchanges estrangeiras)

A distinção importa porque cada mecanismo tem um destinatário próprio, uma forma própria de comprovação e, como veremos, um tratamento regulatório próprio.

A virada regulatória

Até recentemente, os bloqueios de saldos praticados por *exchanges* eram tratados como faculdade contratual, legitimada pelos termos de uso e pela gestão de riscos da própria plataforma. A Resolução BCB nº 520/2025 muda essa perspectiva para as prestadoras de serviços de ativos virtuais (PSAVs) que atuam no Brasil. Seu art. 43, § 2º, VI, exige que elas estabeleçam "limites para transações e saques, bem como bloqueios temporários nos casos de transações e saques atípicos ou suspeitos", e o inciso VII impõe que essas ocorrências fiquem registradas à disposição do Banco Central. Paralelamente, no campo da prevenção a fraudes, a Resolução BCB nº 584/2026 incluiu na Resolução BCB nº 142/2021 uma retenção cautelar de 24 horas, a vigorar a partir de 1º de janeiro de 2027, para transferências de ativos virtuais destinadas a entidades no exterior que atuem nesse mercado ou a carteiras autocustodiadas, quando a operação superar o

equivalente a US$ 10 mil ou quando a análise de risco da instituição o indicar. Trata-se de quarentena para análise de risco, distinta do bloqueio por suspeita de ilícito, que ela expressamente não afasta.

A mudança é relevante porque desloca o debate da esfera contratual para a regulatória. O bloqueio temporário deixa de ser uma faculdade exercida segundo os interesses patrimoniais ou reputacionais da plataforma e passa a ser um instrumento esperado, integrado aos controles de prevenção à lavagem de dinheiro e ao financiamento do terrorismo a que as PSAVs estão sujeitas desde que a Lei nº 14.478/2022 as incluiu entre os sujeitos obrigados da Lei nº 9.613/1998. Nas controvérsias judiciais, a pergunta deixa de ser se a plataforma tinha autorização contratual para bloquear e passa a ser se, diante dos elementos concretos disponíveis, ela cumpriu seus deveres de monitoramento e de gerenciamento de riscos.

Note-se, porém, que ambas as normas tratam apenas do segundo mecanismo: o bloqueio de saldos, pelas PSAVs, nas contas de seus clientes. O congelamento de tokens por emissores, quase todos estrangeiros, segue fora do alcance da regulação brasileira.

E a regulação não confere um cheque em branco. Os próprios termos da norma já carregam limites: se o bloqueio é "temporário", precisa de um horizonte de duração; se recai sobre operações "atípicas ou suspeitas", precisa de uma razão identificável.

Desafios

Dois mecanismos, dois regimes. O bloqueio de saldos por PSAVs que atuam no Brasil passou a ser expectativa regulatória. O congelamento de tokens por emissores e o bloqueio de saldos por *exchanges* estrangeiras seguem no plano da cooperação voluntária, sem canal definido nem prazo de resposta. Boa parte dos ativos relevantes para investigações brasileiras circula justamente por esses agentes.

Prazo, motivação e transparência. A Resolução nº 520 não define quanto tempo um bloqueio pode durar, como deve ser justificado nem a quem deve ser comunicado. Retenções prolongadas, sem fundamento conhecido e sem perspectiva de conclusão, enfraquecem a própria racionalidade que sustenta o poder de bloquear. E bloqueios que a autoridade desconhece dificilmente se convertem em medida judicial.

A ponte até o Judiciário. Qualquer dos dois mecanismos apenas imobiliza os ativos. Para que sejam transferidos ao Estado e, ao final, destinados ao

perdimento ou à reparação das vítimas, é necessária decisão judicial: sequestro (CPP, arts. 125 e seguintes) ou medida assecuratória da Lei nº 9.613/1998 (art. 4º). Quanto mais rápida e bem-informada for essa passagem, menor o tempo de restrição a quem, ao final, se revelar titular de boa-fé.

Propostas

As propostas abaixo dispensam alterações legislativas e procuram concentrar os deveres em quem bloqueia, não em quem pede. A solicitação voluntária funciona justamente por ser simples e rápida, e convém que continue assim.

Parâmetros para o bloqueio temporário das PSAVs. Sugerimos que o Banco Central, ouvidos os demais órgãos da ENCCLA, detalhe o art. 43, § 2º, VI, da Resolução nº 520, estabelecendo: (a) o dever de registrar o fundamento concreto do bloqueio; (b) um prazo máximo, findo o qual o bloqueio cessa, salvo ordem judicial; (c) a comunicação imediata ao COAF e, quando houver, à autoridade que solicitou o bloqueio, para que avalie a adoção de medida assecuratória; (d) a informação ao titular sobre a existência do bloqueio, preservado o sigilo da comunicação ao COAF e das investigações em curso; e (e) a liberação motivada, inclusive quando o titular demonstrar a licitude da operação. Bloqueios que vão além do pedido, por iniciativa da própria PSAV, deveriam ser prontamente informados à autoridade solicitante. A Resolução nº 584 mostra que o regulador já sabe fazer isso: para a retenção cautelar, definiu natureza, prazo, comunicação e registro documentado das decisões. Os bloqueios temporários da Resolução nº 520 pedem a mesma estrutura, com outra calibragem: prazos compatíveis com a gravidade dos indícios e comunicação ao titular nos termos do item (d).

Canais de contato. Do lado doméstico, cada PSAV autorizada deveria manter um canal dedicado para solicitações de autoridades, com prazo de resposta definido.

Um guia prático, de uso facultativo. Em vez de formulários obrigatórios, propomos que a ENCCLA elabore um guia de referência para as autoridades, distinguindo os dois mecanismos: que informações costumam ser úteis a um emissor (rede, contrato do token, endereços) e a uma *exchange* (cliente, endereços de depósito, transações), como confirmar que o congelamento foi efetivado e que providências levar ao juízo. No congelamento pelo emissor, por exemplo, a decisão judicial pode determinar a destruição dos tokens bloqueados e sua reemissão em carteira de custodiante nomeada pelo juízo; no bloqueio pela *exchange*, a transferência do saldo a essa custodiante. O guia serve para ajudar quem pede, não para criar requisitos.

Dados, a cargo das PSAVs. Não se gerencia o que não se mede. As próprias PSAVs, no reporte que já fazem ao Banco Central, poderiam informar o número de bloqueios, sua duração e seu desfecho: liberação, conversão em medida judicial ou outro. Esses dados permitiriam avaliar a efetividade do instrumento e corrigir distorções, como bloqueios excessivamente longos, sem acrescentar trabalho às autoridades de persecução.

Conclusão

O congelamento voluntário de criptoativos já é uma realidade, e funciona. A questão não é mais se as autoridades podem pedir ou se as empresas podem bloquear, mas como fazer com que esses bloqueios sejam eficazes na prevenção à lavagem de dinheiro e compatíveis com os direitos dos usuários de boa-fé.

A confiança no mercado depende simultaneamente de dois fatores: da capacidade das plataformas de impedir a circulação de ativos ilícitos e da previsibilidade de que usuários legítimos não ficarão sujeitos a bloqueios indefinidos ou imotivados. Segurança e fluidez não são objetivos antagônicos. O desafio é garantir que o bloqueio continue rápido para quem investiga e passe a ser previsível para quem é bloqueado.

Sobre os autores

Alexandre Senra. Procurador da República. Procurador-Chefe da Procuradoria da República no Espírito Santo e Coordenador do Grupo Executivo Criptoativos do MPF. Mestre em Direito. Certificado em blockchain pelo MIT (Massachusetts Institute of Technology) e em DeFi, NFTs e Metaverso pela University of Nicosia. Formador certificado pelo programa GLACY-e. Professor e palestrante sobre criptoativos desde 2020.

Marcelo Ribeiro de Oliveira. Advogado e Professor Universitário. Ex-Procurador da República. Pós-doutor em Direito pela Universidade de Salamanca, Doutor em Direito pela Universidade de Lisboa, Mestre em Direito e Estado e Bacharel em Direito pela Universidade de Brasília. Investigador Colaborador do Centro de Investigação de Direito Privado da Universidade de Lisboa.

ALEXANDRE SENRA

MARCELO RIBEIRO DE OLIVEIRA

Articulação público-privada no enfrentamento à lavagem de dinheiro, à fraude e às ameaças cibernéticas.

Antenor Madruga

A colaboração como norte

O enfrentamento à lavagem de dinheiro, à fraude e às ameaças cibernéticas exige colaboração entre instituições públicas, empresas, associações e academia. As capacidades necessárias estão distribuídas entre organizações que conhecem diferentes aspectos desses problemas e dispõem de meios distintos para agir. Reuni-las em torno de objetivos comuns é uma tarefa de construção institucional. Ainda é necessário desenvolver formas de participação que aproveitem o conhecimento e a iniciativa de todos os envolvidos.

Na prevenção à lavagem de dinheiro, a cooperação se expressa, em grande medida, no cumprimento de obrigações impostas pelo Estado aos particulares, como a comunicação de operações suspeitas. Esse componente é indispensável, mas o paradigma da colaboração tem alcance mais amplo. O setor privado e a academia podem contribuir com pesquisa, identificação de problemas, elaboração de propostas regulatórias e discussão sobre a própria atuação estatal. A experiência de quem opera serviços, desenvolve tecnologias e estuda os fenômenos deve participar da formulação das respostas públicas, e não apenas de sua execução.

A interação entre Estado e sociedade deve ser permanente. Essa aproximação precisa ocorrer por meios lícitos e transparentes, com respeito às atribuições de cada instituição, à diversidade dos interesses envolvidos e à prevalência do interesse público. Colaborar pressupõe reconhecer essas diferenças e criar condições para que o conhecimento circule e as decisões sejam mais bem informadas.

A experiência que vivi como primeiro coordenador da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA) reforçou em mim a convicção de que iniciativas dessa natureza dependem, sobretudo, das equipes que as constroem e lhes dão continuidade. O desafio era desenvolver uma estratégia de Estado, apartidária, capaz de reunir instituições distintas em torno de objetivos comuns. Sua continuidade ao longo de diferentes governos evidencia o valor desse esforço coletivo e de um método de colaboração que ultrapassa gestões e trajetórias individuais. A informalidade organizacional, o consenso na definição de metas e a responsabilidade por seu cumprimento permitiram articular órgãos autônomos em torno de uma agenda comum (Madruga, 2012, p. 34–35). Nessa experiência, o convite à participação de associações expressava a disposição de ampliar o debate.

Diagnósticos conjuntos e formulação de políticas

Fraude, lavagem de dinheiro e ataques cibernéticos podem compartilhar estruturas, agentes e meios tecnológicos. Contas, identidades, empresas e

infraestruturas digitais empregadas em uma dessas atividades podem também servir às demais. Essa sobreposição torna insuficiente uma análise compartimentada: um sinal que parece pouco relevante para uma equipe pode adquirir outro significado quando relacionado ao conhecimento de outra.

Uma visão integrada permite identificar conexões, aproveitar capacidades analíticas e tecnológicas e reduzir a duplicação de esforços. Por isso, as equipes de prevenção à fraude, de prevenção à lavagem e de cibersegurança precisam compreender as relações entre os riscos que enfrentam e articular seus diagnósticos e estratégias. A especialização ganha força quando inserida numa compreensão conjunta do problema, respeitados os limites jurídicos de cada atuação.

Essa visão encontra expressão na abordagem conhecida como FRAML, combinação de fraud e anti-money laundering, que integra prevenção à fraude e à lavagem de dinheiro. Seu valor está em conectar conhecimentos, equipes e capacidades tecnológicas para reconhecer relações que análises isoladas poderiam deixar escapar. A cibersegurança amplia essa perspectiva ao contribuir para a compreensão das vulnerabilidades e dos meios digitais utilizados nas atividades ilícitas.

Relatório conjunto do Grupo de Ação Financeira (GAFI/FATF), da INTERPOL e do Grupo Egmont destaca a complementaridade entre prevenção à fraude e à lavagem e apresenta orientações de cooperação entre essas áreas e a cibersegurança. Embora não empregue a sigla FRAML, o documento reforça a necessidade de superar a fragmentação das análises e articular capacidades para enfrentar a fraude cibernética e os fluxos financeiros a ela associados (FATF; INTERPOL; Egmont Group, 2023).

A necessidade de uma visão conjunta também ultrapassa os limites de cada organização. As empresas acompanham operações e vulnerabilidades; as autoridades reúnem experiências de regulação e investigação; a academia contribui com métodos para testar hipóteses e avaliar respostas. A cooperação permite confrontar essas perspectivas e construir diagnósticos que nenhuma instituição produziria isoladamente.

Esse conhecimento deve alimentar tanto a prevenção quanto a formulação das políticas públicas. A participação privada e acadêmica pode contribuir para identificar obrigações inexequíveis, lacunas regulatórias e alternativas de atuação. Cabe ao Estado avaliar essas contribuições e decidir no exercício de suas competências, por meio de procedimentos transparentes, abertos à diversidade de interesses e orientados ao interesse público.

A colaboração entre Estado e sociedade não exige necessariamente a edição de nova lei para cada iniciativa de escuta, debate técnico ou articulação. A construção conjunta de diagnósticos e propostas integra a dinâmica do Estado democrático e pode desenvolver-se no exercício de competências já existentes, observados a legalidade, a impessoalidade, a publicidade e os demais limites da atividade estatal.

A ordem jurídica brasileira oferece instrumentos para essa aproximação. No âmbito das agências reguladoras federais abrangidas pela Lei nº 13.848/2019, a análise de impacto regulatório deve, em regra, anteceder a adoção ou alteração de atos normativos de interesse geral, admitidas as hipóteses regulamentares de dispensa. As minutas e propostas de alteração desses atos submetem-se a consulta pública. Audiências públicas e outros meios participativos são facultativos, ressalvadas exigências da legislação específica. Esses instrumentos têm requisitos e âmbitos próprios, mas podem incorporar conhecimentos à decisão pública e dar continuidade e transparência à colaboração.

A qualidade dessa participação depende também de sua abertura. Empresas de diferentes portes, entidades representativas, pesquisadores, consumidores e vítimas podem revelar aspectos que escapam aos participantes mais estruturados. A transparência sobre interesses, financiamento de pesquisas e fundamentos das propostas ajuda a prevenir a captura da agenda. A cooperação deve acolher a divergência e permitir que a sociedade compreenda como as contribuições foram consideradas.

O trabalho entre equipes

A experiência da ENCCLA mostra como instituições autônomas podem construir uma agenda comum sem perder suas atribuições. O consenso na definição dos objetivos, a identificação dos responsáveis e o acompanhamento dos compromissos permitem transformar o diálogo em trabalho conjunto. Sua continuidade depende das equipes que preservam o conhecimento acumulado e dão seguimento às iniciativas, inclusive quando mudam os governos e seus dirigentes.

A aproximação entre equipes públicas, privadas e acadêmicas deve abrir caminho para pesquisas, propostas de capacitação, aperfeiçoamentos regulatórios e projetos de cooperação. Cada iniciativa precisa ter um propósito compreensível, interlocutores definidos e uma forma de acompanhar seu desenvolvimento. A flexibilidade do diálogo pode, assim, conviver com a responsabilidade pelos compromissos assumidos.

O Public-Private Partnership Toolkit Against Organized Fraud, do Escritório das Nações Unidas sobre Drogas e Crime (UNODC), reconhece diferentes modelos de parceria e vincula sua escolha à confiança institucional, aos marcos jurídicos, aos riscos setoriais e às capacidades disponíveis. A cooperação pode começar com fóruns e iniciativas delimitadas, avançando por etapas e projetos-piloto conforme os resultados e as necessidades identificadas. A institucionalização não é apresentada como destino obrigatório ou desejável para todas as parcerias (UNODC, 2026, p. 39–41 e 49–51). Para o Brasil, essas experiências oferecem referências a serem examinadas criticamente, com atenção às adaptações necessárias.

Os limites jurídicos e a proteção das pessoas

A cooperação exige distinguir atividades de diálogo e pesquisa daquelas que envolvem decisões públicas, informações protegidas ou medidas operacionais. A aproximação entre instituições não transfere competências nem amplia, por si só, as hipóteses legais de acesso a dados. Os instrumentos de parceria devem organizar o exercício das atribuições existentes e definir responsabilidades compatíveis com a finalidade de cada iniciativa.

O debate sobre políticas públicas pode apoiar-se em experiências, estudos e dados agregados, enquanto o intercâmbio de informações pessoais ou sigilosas exige exame específico de sua base jurídica, finalidade, necessidade e segurança. A confiança entre os participantes se fortalece quando cada um sabe o que pode compartilhar, com quem e para qual propósito.

Na prevenção à lavagem de dinheiro, a cooperação deve preservar os canais legais de comunicação ao Conselho de Controle de Atividades Financeiras (Coaf) e o dever de não dar ciência dessas comunicações às pessoas a que se refiram ou a terceiros. O acesso e o compartilhamento de informações financeiras devem observar o regime de sigilo e suas hipóteses legais de exceção. Nas atividades abrangidas pela Lei Geral de Proteção de Dados Pessoais (LGPD), o tratamento exige respeito aos princípios, às bases legais e às medidas de segurança, inclusive às regras sobre dados sensíveis, quando aplicáveis. O art. 4º, inciso III, exclui de seu âmbito o tratamento realizado exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou investigação e repressão de infrações penais. Essa exclusão remete a disciplina específica e não afasta as garantias e os limites dos §§ 1º e 2º, inclusive as restrições à atuação de pessoas jurídicas de direito privado. A existência de uma parceria não dispensa a identificação do fundamento jurídico e das condições aplicáveis ao compartilhamento.

A qualidade da informação também integra a proteção das pessoas. Um alerta pode indicar a necessidade de investigação, sem comprovar a prática de um ilícito. Por isso, a cooperação deve prever meios de avaliar a confiabilidade dos

dados, corrigir registros e revisar conclusões equivocadas. A ampliação da capacidade de análise precisa vir acompanhada de responsabilidade sobre os efeitos que essas análises produzem.

A colaboração também exige avançar na discussão sobre formas de análise conjunta que permitam reconhecer conexões entre informações dispersas, com governança, segurança e respeito aos direitos das pessoas. O Projeto Aurora, do Bank for International Settlements (BIS), oferece uma referência experimental. Em prova de conceito com dados sintéticos, explorou análises colaborativas e tecnologias de preservação da privacidade para identificar padrões de lavagem entre instituições e fronteiras (BIS, 2023). Essa experiência contribui para discutir possibilidades técnicas da cooperação, sem substituir o exame do ordenamento brasileiro.

O desafio é identificar quais informações podem ser utilizadas, por quais participantes, para quais finalidades e sob quais garantias. Avançar nessa análise permite construir formas juridicamente seguras de colaboração, preservando os sigilos aplicáveis e os direitos das pessoas.

Compromissos comuns e avaliação dos resultados

Uma agenda de cooperação precisa traduzir objetivos comuns em compromissos acompanháveis. Cada iniciativa deve identificar o problema a enfrentar, a contribuição esperada dos participantes e os responsáveis por seu desenvolvimento. Os instrumentos de organização devem ser proporcionais à atividade: uma pesquisa conjunta, uma proposta regulatória e um projeto operacional exigem cuidados distintos. Essa disciplina pode preservar a flexibilidade da articulação e evitar a criação de estruturas desnecessárias.

A avaliação deve considerar o que a parceria pretende alcançar. Na pesquisa, importa saber se o conhecimento produzido esclareceu problemas e informou decisões; na capacitação, se foi aplicado; nos projetos operacionais, se houve melhoria na resposta e na proteção das pessoas. O número de reuniões, participantes ou informações compartilhadas descreve atividade, mas não demonstra, isoladamente, resultados. A prestação de contas deve explicitar avanços, dificuldades e limites da evidência, permitindo corrigir rumos e sustentar a colaboração ao longo do tempo.

ANTENOR MADRUGA

Sobre o autor

Coordenador científico do Foro Internacional Antifraude, presidente do Conselho da Zela Trust, sócio-fundador do Madruga BTW e pesquisador de pós-doutorado na

Faculdade de Tecnologia da UnB. Doutor em Direito Internacional pela USP, ocupou os cargos de Secretário Nacional de Justiça e Advogado da União, além de integrar o COAF. Foi diretor do DRCI e um dos idealizadores e primeiro coordenador da ENCCLA.

Prevenção à Lavagem de Dinheiro: Uma Análise Judicial Da Atuação do Coaf.

Desafios institucionais na apreciação dos RIF's

Fausto De Sanctis
Desembargador Federal do TRF3

Introdução

A lavagem de dinheiro é um fenômeno criminoso complexo, dada a capacidade de agentes criminosos infiltrar capitais ilícitos na economia formal, comprometendo a integridade dos mercados financeiro e empresarial, bem como a ordem socioeconômica. O marco normativo central de repressão a essa prática no ordenamento jurídico brasileiro é a Lei nº 9.613, de 03.03.1998, com suas alterações posteriores, cujo tipo penal está previsto especificamente em seu artigo 1º.

A comprovação do delito, em regra, dada a dificuldade de obtenção de provas diretas da lavagem de dinheiro, deve ser extraída de dados externos e objetivos, tais como incremento patrimonial injustificado e operações financeiras anômalas que sirvam de lastro a esse acréscimo. Usualmente tais operações são estruturadas de forma complexa e fragmentada em camadas, com o propósito de dissimular sua origem e dificultar o rastreamento pelos mecanismos de registro e comunicação legalmente exigidos.

A eficácia do sistema punitivo estatal não depende exclusivamente da atuação do Poder Judiciário e dos órgãos de persecução penal, mas também de um microssistema preventivo que tem no Conselho de Controle de Atividades Financeiras (COAF) sua peça-chave.

O COAF, Unidade de Inteligência Financeira (UIF) do Brasil, recepciona, analisa e dissemina informações sobre operações financeiras suspeitas, encaminhando tais informações às autoridades policiais, ao Ministério Público e a outros órgãos competentes, conforme a natureza da operação analisada.

Neste viés, compreender as vulnerabilidades operacionais e normativas que circundam o sistema de prevenção, bem como os desafios a que se sujeitam os magistrados na valoração probatória dos Relatórios de Inteligência Financeira (RIF's), é tarefa necessária para o aprimoramento das políticas públicas e da cooperação interinstitucional.

O Conselho de Controle de Atividades Financeiras (COAF) e o Modelo Preventivo Brasileiro

O modelo brasileiro de prevenção à lavagem de dinheiro adota a técnica da regulação por setores de atividade econômica, impondo a diversos agentes o dever de compliance, cadastro, manutenção de registros e, particularmente, a comunicação de operações suspeitas ao COAF, nos termos dos artigos 9º a 11 da Lei nº 9.613/1998. Submetem-se a esse regime, entre outros, as instituições

financeiras, os integrantes do mercado de capitais e as sociedades seguradoras, bem como profissionais e entidades de setores não financeiros, tais como contadores, tabeliães e registradores (Cartórios) e aqueles que exercem atividades de compra e venda de imóveis.

Merece ressalva, nesse contexto, a situação dos advogados, cuja sujeição ao dever de comunicação de operações suspeitas é tema de controvérsia jurídica e institucional ainda não pacificada, tendo em vista o sigilo profissional e as prerrogativas da advocacia asseguradas pela Lei nº 8.906, de 04.07.1994 (Estatuto da OAB), que fundamentam a discussão da categoria à submissão irrestrita a esse regime regulatório.

Do ponto de vista judicial, os Relatórios de Inteligência Financeira (RIF's) produzidos pelo Conselho de Controle de Atividades Financeiras (COAF) consubstanciam elementos informativos de relevo para a persecução penal.

O Supremo Tribunal Federal, em sede de repercussão geral (RE 1.055.941, Tema 990, Relator Ministro Dias Toffoli, Tribunal Pleno, DJE de 18.03.2021), assentou ser constitucional o compartilhamento direto e espontâneo, pela Unidade de Inteligência Financeira, de dados bancários e fiscais e de outras informações submetidas a sigilo com os órgãos de persecução penal, sem autorização judicial prévia, desde que tal compartilhamento decorra do exercício regular das atribuições legais e regulamentares da própria Unidade de Inteligência Financeira, no âmbito do fluxo de produção e disseminação do RIF disciplinado pela Lei nº 9.613/1998, e não de requisição desvinculada desse procedimento próprio.

Trata-se de transferência do dever de confidencialidade e, não, propriamente, de quebra de sigilo, inclusive porque a própria lei de regência (Lei nº 9.613/1998) impõe ao COAF obrigação de comunicação às autoridades competentes para a instauração dos procedimentos cabíveis, quando concluir pela existência de crimes previstos nesta Lei, de fundados indícios de sua prática, ou de qualquer outro ilícito (inteligência do art. 15), tratando-se esse tipo de compartilhamento de mero mecanismo de cooperação institucional entre órgãos estatais igualmente sujeitos ao dever de confidencialidade.

A dispensa de autorização judicial, nesses termos, não equivale à relativização genérica do sigilo bancário e fiscal, tampouco substitui o regime de quebra de sigilo por via judicial nas hipóteses em que este seja exigido por força de outras disposições legais e constitucionais. Impõe-se, de todo modo, a preservação do sigilo dos dados compartilhados no âmbito dos autos da investigação, com acesso restrito às autoridades legalmente competentes.

É relevante ressaltar, também, que remanesce discussão sobre a possibilidade de aplicação do entendimento firmado no bojo do Tema de Repercussão Geral nº 990 às hipóteses em que, ao invés do compartilhamento espontâneo dos relatórios financeiros pelo COAF e/ou Receita Federal, há requisição direta da Polícia ou do Parquet, por vezes, sem que haja prévia instauração de procedimento de investigação formal.

Para esses casos, prevalece, atualmente, o posicionamento adotado em decisão liminar proferida pelo Ministro Alexandre de Moraes, em 27.03.2026, no bojo do Recurso Extraordinário nº 1.537.165 (Tema de Repercussão Geral nº 1404 ainda pendente de julgamento definitivo pelo Plenário do STF), cujos efeitos são vinculantes e prospectivos (ex nunc), a qual estabeleceu, por ora, seis requisitos obrigatórios para a validade e/ou legitimidade da requisição direta de RIF's por parte da Polícia ou do Ministério Público, quais sejam: (a) somente poderão ser fornecidos RIF's quando houver procedimento formal instaurado (inquérito, PIC ou processo administrativo/judicial sancionador), com finalidade claramente delimitada; (b) a requisição deve conter identificação objetiva do investigado ou sujeito sancionável, com comprovação formal da instauração do procedimento; (c) é exigida pertinência temática estrita entre o RIF solicitado e o objeto da apuração, vedado uso genérico prospectivo ou exploratório; (d) fica proibida a fishing expedition, vedando o uso do RIF como primeira ou única medida investigativa; (e) ordens judiciais e pedidos de CPI/CPMI também devem observar rigorosamente esses requisitos; (f) são expressamente vedadas requisições para procedimentos preliminares não sancionadores; (g) o descumprimento desses requisitos torna o RIF prova ilícita, com invalidação e desentranhamento, inclusive de provas derivadas, nos termos do art. 5º, LVI, da Constituição Federal.

Frise-se, contudo, que tal discussão não foi, até o presente momento, definitivamente resolvida pelo Plenário do Supremo Tribunal Federal, de maneira que a aplicação desses critérios é, ainda, provisória, considerando-se os efeitos vinculantes e prospectivos (ex nunc) da referida medida liminar concedida no bojo do Recurso Extraordinário nº 1.537.165 (Tema de Repercussão Geral nº 1404).

Em suma, observados tais requisitos, o RIF constitui elemento informativo apto a embasar a instauração de investigação preliminar e, eventualmente, a formação da opinio delicti para o oferecimento de denúncia, quando corroborado por outros elementos de convicção. Não se admite, todavia, que o RIF seja tomado como fundamento autossuficiente ou prova plena para a persecução penal, tendo em vista sua natureza de elemento meramente informativo, que demanda, para fins de formação de juízo condenatório, confirmação por meios de prova produzidos sob o crivo do contraditório e da ampla defesa.

Principais Vulnerabilidades e os Desafios do Judiciário na Apreciação dos RIF's

Apesar da evolução legislativa e estrutural do sistema brasileiro de prevenção à lavagem de dinheiro, a persecução penal e a análise judicial de casos dessa natureza frequentemente esbarram em vulnerabilidades operacionais, normativas e jurisdicionais que fragilizam a efetividade do sistema como um todo.

Em primeiro lugar, observa-se a existência de vulnerabilidades nos mecanismos de prevenção à lavagem de dinheiro, especialmente no que diz respeito à supervisão e ao cumprimento das obrigações preventivas por determinados setores não financeiros. Enquanto o setor bancário e financeiro possui estruturas de compliance e apresenta elevado volume de comunicações ao COAF, os setores não financeiros, como o mercado imobiliário, o comércio de bens de luxo, as joalherias e os prestadores de serviços societários, registram índices expressivamente menores de comunicação, em certa medida pela ausência ou deficiência de regulação e de supervisão desses setores.

Estes dados podem ser identificados pelo volume de comunicações efetuadas pelos setores obrigados entre 1998 e 2025 (cf. Relatório de Gestão Integrado 2025 do COAF – p. 29, disponível em: https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/rgi 2025.pdf/@@display-file/file, acesso em 08.10.2026).

Essa assimetria dá origem a verdadeiras zonas cinzentas, nas quais capitais de origem ilícita ingressam com relativa facilidade na economia real, sem a devida triagem pelos mecanismos preventivos legalmente previstos.

Em segundo lugar, destaca-se o desafio probatório enfrentado pelos magistrados na valoração dos Relatórios de Inteligência Financeira. Por constituir produto de inteligência financeira, e não auto de infração ou peça de inquérito policial tradicional, o RIF frequentemente apresenta dados macroscópicos, agregados e sintéticos sobre movimentações atípicas.

Impõe-se ao julgador, nesse contexto, transitar pela linha tênue entre reconhecer o RIF como ponto de partida legítimo para a instauração de investigações e evitar que condenações ou medidas cautelares se fundamentem exclusivamente em dados genéricos de inteligência financeira, sem que estes sejam submetidos ao crivo da instrução probatória e do contraditório judicial.

Soma-se a isso a necessidade de rigor analítico na distinção entre a fishing expedition, investigação genérica e desprovida de individualização de suspeita, vedada pelo ordenamento jurídico, e o uso legítimo dos alertas produzidos pelo COAF como fundamento inicial de apuração, de modo a conciliar a proteção das

garantias fundamentais do investigado com a efetividade do combate à criminalidade econômica.

Por fim, a proliferação de empresas de fachada, de holdings patrimoniais sem substância econômica e o uso crescente de criptoativos e de arranjos tecnológicos descentralizados impõem desafios severos à rastreabilidade dos fluxos financeiros ilícitos.

Tais fenômenos dificultam tanto o trabalho analítico desenvolvido pelo COAF quanto a compreensão técnica desses instrumentos por parte dos julgadores, exigindo constante atualização institucional e capacitação técnica para o enfrentamento adequado dessas novas modalidades de dissimulação patrimonial.

Sugestões para o Aprimoramento e Mitigação de Riscos

Para fortalecer a barreira preventiva e subsidiar de forma mais eficiente a atuação do Poder Judiciário e do Ministério Público, sugerem-se as seguintes medidas estruturais:

Fortalecimento tecnológico e uso de inteligência artificial pelo COAF: no exercício das atribuições previstas no artigo 14 da Lei nº 9.613/1998, é recomendável a expansão da capacidade de cruzamento automatizado de grandes bases de dados e o emprego de algoritmos preditivos e de inteligência artificial para identificação de padrões complexos de desvio e de camadas de ocultação patrimonial, com vistas à produção de Relatórios de Inteligência Financeira mais analíticos e inteligíveis ao magistrado. Tal expansão tecnológica deve observar os limites impostos pela Lei Geral de Proteção de Dados (Lei nº 13.709, de 14.08.2018), bem como com o reconhecimento, pelo Supremo Tribunal Federal, da proteção de dados pessoais como direito fundamental autônomo (vide ADI 6387 MC-Ref, Relatora Ministra Rosa Weber, Tribunal Pleno, DJe-270 DJ e 12.11.2020).

Embora a LGPD não tenha por finalidade disciplinar requisitos para o afastamento dos sigilos constitucionalmente protegidos, ela reforça a necessidade de que toda atividade de coleta, tratamento, compartilhamento e armazenamento de dados pessoais observe os princípios da finalidade, adequação, necessidade, segurança, transparência, responsabilização e prestação de contas (arts. 6º e 23 da LGPD). Assim, mesmo nas hipóteses em que o ordenamento jurídico autoriza o acesso a informações bancárias, fiscais ou comunicacionais sem prévia autorização judicial, como ocorre, por exemplo, em determinados procedimentos administrativos fiscais, nas investigações conduzidas por Comissões Parlamentares de Inquérito ou no compartilhamento institucional de informações admitido pelo Supremo Tribunal Federal no Tema de Repercussão Geral nº 990,

permanece incólume o dever de preservação da confidencialidade dos dados, os quais somente poderão ser utilizados para as finalidades legalmente previstas, vedado seu emprego abusivo, desproporcional ou desvinculado do interesse público que justificou seu tratamento.

Capacitação contínua de magistrados em criptoativos e finanças complexas: recomenda-se a promoção, por meio da Escola Nacional de Formação e Aperfeiçoamento de Magistrados (ENFAM) e das escolas judiciais regionais, de programas de formação especializada voltados à compreensão de estruturas financeiras sofisticadas, mercados globais e tecnologias financeiras descentralizadas, de modo a assegurar maior segurança jurídica na apreciação de medidas cautelares e na formação do juízo de mérito em processos relacionados à lavagem de dinheiro.

Integração interinstitucional avançada: sugere-se o aprofundamento dos canais de comunicação e interoperabilidade entre o COAF, as Polícias Judiciárias, o Ministério Público, o Poder Judiciário e as Receitas Estadual e Federal, dentre outros, nos termos da cooperação já prevista no artigo 14, § 2º, da Lei nº 9.613/1998, com o objetivo de reduzir o intervalo temporal entre a identificação de operação financeira atípica e a adoção de medidas cautelares patrimoniais, tais como o sequestro, hipoteca legal e o arresto de bens, sem prejuízo da atuação de estruturas interinstitucionais já existentes, como a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA).

Conclusão

A prevenção à lavagem de dinheiro no Brasil, tendo o Conselho de Controle de Atividades Financeiras (COAF) como eixo central de inteligência financeira, constitui instrumento indispensável para a higidez do sistema econômico e para a efetividade da justiça penal. O diagnóstico desenvolvido ao longo deste estudo revelou vulnerabilidades que fragilizam a atuação estatal em seus diferentes níveis: as deficiências nos mecanismos de prevenção e supervisão de determinados setores não financeiros, a complexidade probatória enfrentada pelo Judiciário na valoração dos Relatórios de Inteligência Financeira, os desafios impostos pela proliferação de estruturas societárias opacas e pelo uso de criptoativos e tecnologias financeiras descentralizadas.

Nesse cenário, a modernização tecnológica do COAF, a capacitação continuada dos magistrados para a compreensão de arranjos financeiros sofisticados e a integração interinstitucional entre os órgãos de inteligência financeira, persecução penal e Poder Judiciário despontam como medidas

estruturais necessárias ao fortalecimento do sistema de prevenção e repressão à lavagem de dinheiro.

Tal fortalecimento, todavia, não pode prescindir da observância das garantias constitucionais do processo penal. O reconhecimento do RIF como legítimo ponto de partida para a instauração de investigações não autoriza, por si só, a fundamentação de condenações ou de medidas cautelares patrimoniais em dados genéricos e desprovidos de individualização, sob pena de comprometimento do devido processo legal e do contraditório.

O desafio que se impõe ao Estado brasileiro é, portanto, o de harmonizar a eficácia da persecução penal em matéria de lavagem de dinheiro com a estrita observância das garantias fundamentais do investigado, de modo a assegurar, simultaneamente, a efetividade do combate à criminalidade econômica e a integridade do sistema de justiça.

FAUSTO DE SANCTIS

Sobre o autor

Desembargador Federal do TRF3. Doutor em Direito Penal pela Faculdade de Direito da Universidade de São Paulo. Como especialista em legislação de combate ao crime de lavagem de dinheiro (e crimes do colarinho branco), ficou à frente da 6ª Vara Federal Criminal da capital, especializada em crimes contra o sistema financeiro nacional e em lavagem de dinheiro.

Prevenir, Detectar e Evoluir: Os Desafios o Sistema Brasileiro de PLD/FTP.

Guilherme Ayres Jameli

A construção do sistema de prevenção e combate à lavagem de dinheiro.

A partir das décadas de 1980 e 1990, consolidou-se na comunidade internacional uma compreensão que transformaria as estratégias de enfrentamento à criminalidade organizada: combater essas organizações exigia não apenas identificar e responsabilizar seus integrantes, mas também alcançar os recursos financeiros que sustentavam suas atividades. Os lucros obtidos com o crime permitiam financiar novas operações, ampliar estruturas criminosas, corromper instituições e expandir sua influência sobre a economia e a sociedade. Privar as organizações criminosas desses recursos seria, portanto, uma medida essencial para comprometer sua capacidade de atuação e reprodução.

Essa visão impulsionou a construção de compromissos internacionais. A Convenção de Viena, de 1988, estabeleceu medidas relacionadas à criminalização da lavagem de dinheiro, ao confisco de bens e à cooperação entre países. Em 1989, foi criado o Grupo de Ação Financeira (GAFI/FATF), que publicou, no ano seguinte, suas primeiras 40 Recomendações, posteriormente consolidadas como padrões internacionais para os sistemas nacionais de prevenção e combate à lavagem de dinheiro.

No Brasil, a Lei nº 9.613/1998 criminalizou a lavagem de dinheiro, estabeleceu obrigações preventivas para determinados setores econômicos e criou o Conselho de Controle de Atividades Financeiras (Coaf). Ao longo das décadas seguintes, esse sistema incorporou novos instrumentos e medidas voltadas também ao financiamento do terrorismo e da proliferação de armas de destruição em massa, passando a ser conhecido como sistema de PLD/FTP.

A arquitetura do sistema de PLD/FTP e o papel central dos sujeitos obrigados.

Esse sistema baseia-se na premissa de que a movimentação de recursos ilícitos exige o uso de instrumentos econômicos legítimos, como contas bancárias, operações de câmbio e constituição de empresas. Para evitar a detecção, as organizações criminosas simulam atividades lícitas, conferindo aparência de regularidade à ocultação e circulação desses valores.

Tais operações costumam deixar rastros financeiros, comerciais e patrimoniais que podem ser analisados em busca de inconsistências e padrões indicativos de atividades ilícitas (red flags). No entanto, a maior parte dessas informações não está imediatamente disponível às autoridades públicas, estando sob o controle dos entes privados que executam ou intermediam os serviços, a exemplo de instituições financeiras, casas de câmbio, contadores e empresas do comércio de bens de luxo. Esses agentes econômicos ocupam, portanto, uma

posição privilegiada para observar determinadas transações e identificar comportamentos atípicos.

Em razão dessa capacidade de observação, foi atribuído aos agentes econômicos mais expostos ao risco de utilização de seus serviços para fins ilícitos um papel central no sistema de PLD/FTP. Denominados sujeitos obrigados, esses agentes devem adotar medidas para identificar e conhecer seus clientes, monitorar operações e comunicar situações suspeitas às autoridades competentes. As comunicações realizadas pelos sujeitos obrigados constituem o principal insumo para a produção de inteligência financeira, subsidiando a atuação do Estado na identificação e investigação de atividades ilícitas, na persecução penal e na recuperação de ativos de origem criminosa.

Além dos sujeitos obrigados, o sistema de PLD/FTP depende da atuação de outros três grupos de atores: os órgãos reguladores e supervisores, a unidade de inteligência financeira e os órgãos responsáveis pela investigação e persecução penal.

Os órgãos reguladores e supervisores, como o Banco Central, a Comissão de Valores Mobiliários (CVM), a Superintendência de Seguros Privados (Susep) e o Coaf, nos setores de sua competência, estabelecem normas e procedimentos de prevenção à lavagem de dinheiro, orientam os setores obrigados e fiscalizam o cumprimento das obrigações legais e regulamentares.

A Unidade de Inteligência Financeira (UIF), função exercida no Brasil pelo Coaf, recebe e analisa as comunicações encaminhadas pelos sujeitos obrigados, integrando-as a informações de outras fontes para identificar vínculos, movimentações e padrões indicativos de atividades ilícitas. Os resultados dessas análises são consolidados em Relatórios de Inteligência Financeira (RIFs), disseminados às autoridades competentes quando identificados fundados indícios de lavagem de dinheiro ou de outros ilícitos pertinentes. Por fim, os órgãos de investigação e persecução penal, especialmente as polícias e os Ministérios Públicos, utilizam essas informações, juntamente com outros elementos, para aprofundar investigações, identificar envolvidos, rastrear recursos e promover a responsabilização dos autores e a recuperação de ativos de origem criminosa, com a participação do Poder Judiciário nas medidas sujeitas à sua competência.

Estado atual do sistema de PLD/FTP: maturidade e desafios

O grau de maturidade do sistema nacional de PLD/FTP é evidenciado pela abrangência dos setores obrigados pela Lei de Lavagem de Dinheiro e pelos expressivos números da inteligência financeira no país. Após sucessivas reformas, o art. 9º da referida lei alcança desde os setores bancário, securitário e de valores mobiliários até a negociação de imóveis, bens de luxo, joias, obras de arte, ativos

virtuais, juntas comerciais, além de serviços de auditoria e consultoria, dentre outros. Em 2025, esses agentes encaminharam ao Coaf mais de 7,6 milhões de comunicações de operações, viabilizando a produção de mais de 20 mil RIFs.

É difícil exagerar a relevância desse arranjo para o combate à corrupção, aos ilícitos financeiros e ao crime organizado no Brasil: praticamente todas as grandes investigações conduzidas no país nos últimos anos fundamentaram-se nos dados e análises produzidos por esse sistema.

Apesar desse cenário, uma série de desafios se apresenta para a manutenção e a ampliação da efetividade do sistema nacional de PLD/FTP, os quais podem ser divididos em dois grandes grupos. O primeiro diz respeito a pontos de melhoria interna na execução do modelo já estabelecido, refletindo setores e atores que ainda não alcançaram a maturidade esperada. O segundo grupo abrange questões estruturais decorrentes de falhas ou da desatualização da arquitetura de PLD/FTP frente às novas dinâmicas criminosas, tecnologias e transformações econômicas ocorridas.

Quanto ao primeiro grupo, sobressai a constatação de que nem todos os setores incluídos no sistema de PLD/FTP atingiram o mesmo grau de maturidade no cumprimento de suas obrigações, gerando lacunas que favorecem a circulação de capitais ilícitos. É preciso reconhecer que o dinheiro de origem criminosa possui uma tendência implícita de fluir pelos caminhos de menor resistência — ou seja, por canais que ofereçam menores obstáculos, menor risco de identificação, maior velocidade e menor custo para a lavagem.

No ecossistema de PLD/FTP, esses caminhos de menor resistência manifestam-se de forma evidente na disparidade de maturidade entre os diversos setores obrigados. Essa assimetria sistêmica pode ser atribuída a três fatores principais:

- **Assimetria de maturidade e expertise regulatória:** Os níveis de capacitação e de aprofundamento técnico também variam acentuadamente entre os órgãos supervisores. Enquanto o conhecimento regulatório em PLD alinha-se diretamente ao *core business* de entidades como Banco Central, CVM, Susep e o próprio Coaf, ele representa uma atribuição periférica e distante das competências tradicionais de reguladores de outros setores, como a ANM (no setor mineral) ou o IPHAN (no comércio de obras de arte e antiguidades), gerando discrepâncias na qualidade e no rigor das normas, assim como na fiscalização de seus supervisionados.
- **Assimetria de recursos entre negócios:** O universo de sujeitos obrigados perante a lei de lavagem de dinheiro é extremamente heterogêneo. Ele

abrange desde grandes instituições financeiras — com centenas de funcionários dedicados ao *compliance*, alto investimento em capacitação e sistemas tecnológicos de ponta para detecção de anomalias — até microempresas que comercializam joias, veículos ou obras de arte, muitas vezes com recursos limitados e desconhecimento sobre como seus negócios podem ser explorados para a lavagem de capitais por terceiros.

- **Disparidade de porte institucional e universo informacional:** A disparidade não se manifesta apenas entre diferentes setores, mas também dentro de um mesmo setor. A capacidade de identificação de ilícitos é fortemente influenciada pelo acesso a dados e pelo aprendizado contínuo. A título de exemplo, instituições financeiras de grande escala, que chegam a administrar carteiras com dezenas de milhões de clientes, operam com um volume massivo de dados multissetoriais. Essa capilaridade lhes confere robustez estatística para identificar desvios comportamentais, reconhecer padrões e aprimorar continuamente seus modelos de detecção de *red flags*. Em contrapartida, instituições de menor porte sofrem com a escassez de dados informacionais comparativos, o que restringe severamente sua capacidade de reconhecer e mitigar operações sofisticadas de lavagem de dinheiro.

Quanto ao segundo grupo, as questões estruturais decorrem de falhas e da desatualização da arquitetura de PLD/FTP frente às profundas transformações econômicas, tecnológicas e comportamentais ocorridas.

Um primeiro desafio resulta da expansão dos instrumentos de circulação de valores para além das estruturas financeiras tradicionais. O desenvolvimento dos criptoativos, das plataformas de apostas, dos mercados de ativos digitais e de serviços de monetização e transferência de valores criou novas possibilidades de circulação econômica, nem sempre submetidas aos mesmos mecanismos de controle do sistema financeiro convencional. No mercado de ativos virtuais, por exemplo, transferências podem ocorrer diretamente entre carteiras digitais, sem a participação de uma instituição intermediária sujeita a obrigações de monitoramento em cada etapa. Outras atividades digitais, como plataformas de jogos e determinados serviços de conteúdo e entretenimento, também permitem o armazenamento, a transferência e a conversão de valores por meio de créditos ou ativos digitais.

Paralelamente, ocorreram transformações profundas dentro do próprio ecossistema financeiro formal. A expansão das *fintechs*, das instituições de pagamento e dos mecanismos de transferência instantânea ampliou o acesso aos serviços financeiros, reduziu custos e conferiu maior velocidade às operações. Embora representem avanços importantes, essas características também

permitem a rápida dispersão de recursos ilícitos, criando um descompasso acentuado entre a velocidade das transações e o tempo necessário à identificação, comunicação e análise de operações suspeitas.

A multiplicação das instituições e a facilidade de abertura de contas acentuaram, por sua vez, o problema da fragmentação informacional. Um mesmo indivíduo pode distribuir suas movimentações entre diversas entidades, de modo que cada uma delas detenha acesso apenas a uma parcela fragmentada de sua atividade financeira. Operações aparentemente regulares quando analisadas isoladamente podem revelar padrões suspeitos quando examinadas em conjunto. Essa fragmentação reduz a capacidade de observação individual dos sujeitos obrigados e é frequentemente explorada por meio do uso cruzado de múltiplas contas, pessoas interpostas e transferências sucessivas de valores.

Outro desafio crítico está relacionado à crescente acessibilidade das estruturas patrimoniais e financeiras internacionais. Em anos recentes, a constituição de empresas *offshore*, *trusts* e contas no exterior tornou-se mais simples, rápida e barata. A título de exemplo, por menos de mil dólares e em um único dia é possível abrir uma empresa *offshore* de forma remota em jurisdições de elevado grau de sigilo. Esse baixo custo e a facilidade operacional vêm ampliando o uso dessas ferramentas — antes restritas a organizações criminosas sofisticadas e grandes esquemas de corrupção —, permitindo que grupos de menor porte e indivíduos passem a utilizá-las para sonegar tributos e ocultar patrimônio de bloqueios judiciais. Para as organizações de maior porte, essa facilidade viabiliza a criação em massa de estruturas *offshore* "descartáveis".

Por fim, mesmo diante dessas transformações tecnológicas e de mercado, permanece um desafio associado a um dos mecanismos mais tradicionais de movimentação de recursos: o dinheiro em espécie. Em novembro de 2026, o valor de cédulas e moedas em circulação no Brasil ultrapassava R$ 383 bilhões, segundo o Banco Central, com aproximadamente R$ 264 bilhões concentrados em notas de R$ 100 e R$ 200 — as mais cobiçadas para a circulação de recursos ilícitos. A popularização, a velocidade, o reduzido custo e a segurança apresentados por meios digitais de pagamento, a exemplo do Pix, levantam fundados questionamentos sobre se a manutenção de um volume tão elevado de papel-moeda em circulação não estaria associada predominantemente à sonegação fiscal, à movimentação de recursos ilícitos e à ocultação de capitais, explorando a ausência de rastreabilidade inerente à circulação de recursos em espécie.

Um sistema que precisa aprender e se atualizar

Como ilustrado anteriormente, o sistema de PLD/FTP opera em um ambiente de transformações permanentes, no qual o próprio aperfeiçoamento dos controles impulsiona os agentes envolvidos em atividades ilícitas a buscar setores menos supervisionados, novos instrumentos ou mecanismos que dificultem sua identificação. Para enfrentar esse dinamismo, o sistema precisa ser permanentemente avaliado e aperfeiçoado, sustentando-se em diagnósticos técnicos rigorosos capazes de identificar resultados, vulnerabilidades e oportunidades de melhoria. A qualidade desses diagnósticos é diretamente proporcional à amplitude e à diversidade das fontes de informação que os fundamentam.

Em face desse cenário, a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA) — principal rede brasileira de articulação institucional para o desenvolvimento de soluções no combate a esses crimes — tem muito a contribuir. Reunindo aproximadamente 90 órgãos e entidades dos Poderes Executivo, Legislativo e Judiciário, do Ministério Público e de diferentes esferas federativas, além de contar com a colaboração de organizações da sociedade civil, especialistas externos e sujeitos obrigados, a ENCCLA já se provou capaz de construir diagnósticos, propostas de mudanças normativas e instrumentos concretos, a exemplo de guias de investigação, sistemas e bases de dados indispensáveis para o ecossistema de PLD/FTP. Entre suas realizações, destacam-se a criação do Programa Nacional de Capacitação e Treinamento para o Combate à Corrupção e à Lavagem de Dinheiro (PNLD) e da Rede Nacional de Laboratórios de Tecnologia contra Lavagem de Dinheiro (Rede-LAB), ambos decisivos para elevar a efetividade do sistema nacional nas últimas duas décadas.

Como atual curador da ENCCLA, no âmbito da Coordenação-Geral de Articulação Institucional do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (CGAI/DRCI/SENAJUS/MJSP), apresento algumas iniciativas que estamos conduzindo para enfrentar os desafios mencionados e impactar positivamente a efetividade do sistema de PLD/FTP:

Portal Nacional de Tipologias de Lavagem de Dinheiro. Desenvolvimento de uma plataforma destinada a reunir e disponibilizar tipologias de lavagem de dinheiro e sinais de alerta, com contribuições contínuas de órgãos públicos e sujeitos obrigados. Além de permitir o mapeamento de tendências e subsidiar diagnósticos e ações de capacitação, o Portal buscará ampliar o acesso ao conhecimento sobre os mecanismos utilizados para lavar recursos ilícitos. Essa iniciativa é especialmente relevante para os sujeitos obrigados de menor porte e com recursos limitados para investir em estruturas especializadas de PLD/FTP,

contribuindo para reduzir as disparidades na capacidade de detecção e aprimorar a produção de inteligência financeira.

Reformulação do PNLD. Em 2027, o PNLD Básico passará por uma atualização de formato e conteúdo, enquanto o PNLD Avançado, voltado aos agentes públicos diretamente envolvidos no enfrentamento à lavagem de dinheiro, adotará uma abordagem mais prática, com maior atenção às tipologias contemporâneas, incluindo a utilização de criptoativos e estruturas *offshore*. Também está previsto o lançamento do PNLD Setorial, com capacitações específicas para os diferentes setores obrigados, abordando os riscos, as tipologias e os sinais de alerta relacionados às suas atividades. A iniciativa busca enfrentar uma das principais vulnerabilidades do sistema: a desigualdade de conhecimento técnico e de capacidade de identificação de operações suspeitas entre os agentes econômicos.

ENCCLA: Pesquisa em Foco. Criação de um periódico dedicado à publicação de pesquisas científicas sobre prevenção e combate à lavagem de dinheiro e temas correlatos. A iniciativa pretende aproximar o Estado das universidades e instituições de pesquisa, estimular estudos sobre problemas prioritários para o sistema nacional de PLD/FTP e ampliar a produção e disseminação de conhecimentos capazes de subsidiar políticas públicas baseadas em evidências.

Além dessas medidas, a ENCCLA pode e deve ser utilizada pelos reguladores nacionais de PLD como instrumento de apoio ao desenvolvimento de diagnósticos, procedimentos e normativos setoriais.

De forma semelhante, a Estratégia também deve contribuir para o enfrentamento de questões mais amplas, que podem exigir mudanças na própria arquitetura do sistema de PLD/FTP. Como superar a crescente fragmentação das informações financeiras? Seria necessário desenvolver mecanismos que permitam maior compartilhamento de dados entre sujeitos obrigados e ampliar a integração entre instituições públicas e privadas? Quais novas atividades econômicas e formas de circulação de valores devem ser incorporadas ao sistema de prevenção? Como enfrentar os riscos apresentados por instrumentos concebidos para dificultar a identificação dos envolvidos e o rastreamento das transações, como determinadas criptomoedas de privacidade (*privacy coins*)?

São questões que exigem análises técnicas aprofundadas, participação de diferentes setores e avaliação das consequências das possíveis soluções. Ao reunir essas capacidades em um espaço permanente de articulação, a ENCCLA está singularmente preparada e posicionada para desempenhar um papel decisivo na construção das respostas necessárias para que o sistema brasileiro de PLD/FTP

continue evoluindo e ampliando sua efetividade diante das transformações da economia e da criminalidade organizada.

GUILHERME AYRES JAMELI

Sobre o autor

Coordenador de Articulação Institucional do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do Ministério da Justiça e Segurança Pública. Oficial de inteligência, atuou como analista e gestor em setores dedicados à análise de ilícitos financeiros (lavagem de dinheiro e financiamento do terrorismo) e Inteligência corporativa. Conselheiro do Conselho de Controle de Atividades Financeiras entre 2024 a 2026. Mestre em Contabilidade, Controladoria e Finanças pela Universidade Federal de Minas Gerais. Especialista em Controle, Detecção e Desvio de Recursos Públicos (UFLA/CGU).

O Combate à Corrupção, à Lavagem de Dinheiro e ao Financiamento do Terrorismo no Brasil: Novos desafios e a necessidade de uma cooperação ainda mais integrada.

Luiz Paulo Azevedo Bittencourt

Introdução

Em 2025, as perdas globais decorrentes de fraudes e golpes financeiros alcançaram aproximadamente US$ 579 bilhões. Mais preocupante ainda é o fato de que apenas 0,2% desses recursos foram recuperados (Nasdaq Verafin, 2026). A pergunta que emerge desse cenário é inevitável: quantos desses valores continuam financiando organizações criminosas, alimentando novos crimes e ampliando estruturas de lavagem de dinheiro ao redor do mundo?

Em um ambiente marcado pela instantaneidade das transações financeiras, pela expansão dos ativos virtuais, pela crescente sofisticação do crime organizado e pelo uso cada vez mais intenso da inteligência artificial tanto por instituições quanto por criminosos, torna-se legítimo questionar se os mecanismos construídos ao longo das últimas décadas continuam evoluindo na mesma velocidade das ameaças que pretendem enfrentar.

Passadas quase três décadas da promulgação da Lei nº 9.613/1998 (Brasil, 1998), o Brasil construiu um sistema robusto de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo. Ao longo desse período, o país aperfeiçoou sua legislação, fortaleceu os mecanismos de inteligência financeira, ampliou a capacidade de supervisão e consolidou uma rede de cooperação entre instituições públicas e privadas.

Criada em 2003, a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA) consolidou-se como o principal fórum de articulação institucional do país sobre o tema. Ao reunir órgãos de investigação, inteligência financeira, regulação, controle, supervisão e representantes do setor privado, a Estratégia contribuiu para o desenvolvimento de políticas públicas, marcos normativos e instrumentos operacionais que fortaleceram significativamente o sistema brasileiro de prevenção e combate à criminalidade financeira (Brasil, 2026b).

O ambiente em que esse sistema opera, entretanto, transformou-se profundamente. Diante do novo cenário, torna-se fundamental refletir sobre os desafios que se apresentam e sobre os caminhos necessários para preservar a efetividade do sistema construído ao longo das últimas décadas.

Um Ambiente de Riscos em Rápida Transformação

As organizações criminosas contemporâneas diferem significativamente daquelas que motivaram a construção dos primeiros sistemas modernos de prevenção à lavagem de dinheiro.

Hoje, muitas delas operam de forma empresarial, utilizam tecnologias sofisticadas, movimentam recursos em diferentes países e atuam simultaneamente em mercados lícitos e ilícitos. Além do tráfico de drogas, passaram a explorar atividades como crimes ambientais, contrabando, fraudes financeiras, apostas eletrônicas, comércio internacional ilícito, mineração ilegal e crimes cibernéticos.

O objetivo da inteligência criminosa não é apenas ocultar recursos obtidos ilegalmente. Busca-se administrar, proteger, multiplicar e reinserir esses recursos na economia formal, construindo poder econômico e ampliando a capacidade de influência das organizações criminosas.

Nesse contexto, a lavagem de dinheiro deixou de ser uma etapa acessória da atividade ilícita e passou a representar um instrumento estratégico para a sobrevivência e expansão dessas organizações criminosas.

Essa lógica está sintetizada em uma das expressões mais conhecidas da investigação financeira: *follow the money*. A premissa é simples, mas poderosa. Seguir os fluxos financeiros frequentemente permite compreender melhor uma estrutura criminosa do que a análise isolada dos crimes praticados. Ao rastrear recursos, torna-se possível identificar beneficiários finais, operadores financeiros, empresas de fachada e conexões invisíveis entre diferentes integrantes de uma organização.

Não por acaso, o sistema financeiro ocupa posição estratégica no combate à criminalidade organizada. É por meio da inteligência financeira, dos mecanismos de monitoramento e das políticas de prevenção à lavagem de dinheiro que se torna possível identificar relações suspeitas, interromper fluxos ilícitos e enfraquecer economicamente organizações criminosas.

Capacidades e Desafios

O Brasil vem fortalecendo suas capacidades institucionais. O Conselho de Controle de Atividades Financeiras (Coaf) consolidou-se como um dos pilares do sistema nacional de prevenção à lavagem de dinheiro e ao financiamento do terrorismo. Em 2026, o órgão já acumula mais de 12 mil Relatórios de Inteligência Financeira (RIFs), além de registrar milhares de intercâmbios de informações com autoridades nacionais. Esses números evidenciam a crescente relevância da inteligência financeira para subsidiar investigações e apoiar ações de recuperação de ativos (COAF, 2026).

O fortalecimento institucional também pode ser observado na publicação do Decreto nº 12.892/2026 (Brasil, 2026a), que ampliou significativamente a

estrutura do Coaf, elevando seu quantitativo de cargos e funções de confiança de 75 para 101 posições.

Outro avanço importante foi a promulgação da Lei nº 15.358/2026 (Brasil, 2026c), conhecida como Lei Antifacção, que fortaleceu instrumentos de enfrentamento às organizações criminosas e reforçou a compreensão de que o combate ao crime organizado exige atuação coordenada entre inteligência financeira, investigação, supervisão, persecução penal e segurança pública.

Os valores subtraídos globalmente, citados no começo deste artigo, revelam que a fraude financeira se tornou um dos principais mecanismos de geração de recursos para a criminalidade organizada. Além disso, fraudes, golpes financeiros, ataques cibernéticos, furtos de credenciais e extorsões digitais frequentemente constituem crimes antecedentes da lavagem de dinheiro. Os recursos obtidos por essas práticas precisam ser ocultados, movimentados e reinseridos na economia formal, alimentando estruturas de lavagem de dinheiro e fortalecendo economicamente organizações criminosas.

Assim, o crescimento das fraudes digitais não representa apenas um risco para indivíduos e empresas. Representa também um fator de ampliação dos riscos de lavagem de dinheiro e de fortalecimento do crime organizado transnacional.

Sob essa perspectiva, o combate à lavagem de dinheiro não deve ser compreendido apenas como uma etapa posterior à ocorrência dos crimes financeiros. Trata-se de uma estratégia fundamental para interromper o ciclo econômico da criminalidade, dificultando que recursos obtidos por meio de fraudes, ataques cibernéticos e outras atividades ilícitas sejam convertidos em patrimônio aparentemente lícito.

Inteligência Artificial: Aliada e Ameaça

Poucas tecnologias têm potencial de transformação comparável ao da inteligência artificial. Instituições financeiras, órgãos de controle e entidades de supervisão já utilizam intensivamente IA para identificação de padrões suspeitos, monitoramento transacional, análise de relacionamentos e gestão de riscos.

Entretanto, as organizações criminosas também vêm incorporando essas ferramentas. *Deepfakes*, clonagem de voz, identidades sintéticas, automação de ataques e engenharia social potencializada por IA já representam ameaças concretas para empresas, governos e cidadãos.

Segundo a CrowdStrike (2026), as operações conduzidas por agentes criminosos apoiados por inteligência artificial cresceram 89% em 2025 em relação ao ano anterior. A tecnologia vem sendo utilizada para acelerar ataques,

automatizar fraudes, aperfeiçoar campanhas de phishing e ampliar significativamente a capacidade de evasão de controles.

Os impactos dessas práticas vão além das perdas financeiras imediatas. Em muitos casos, os recursos obtidos por meio dessas fraudes tornam-se objeto de processos subsequentes de lavagem de dinheiro, reforçando a conexão cada vez mais estreita entre criminalidade cibernética e os ilícitos financeiros.

Nesse ambiente, tecnologia e cooperação tornaram-se elementos inseparáveis. Quanto maior a velocidade dos ataques, mais importante se torna a capacidade de compartilhamento tempestivo de informações entre instituições públicas e privadas.

O Grande Desafio: Conectar as Peças do Sistema

O principal desafio contemporâneo, certamente, não reside na ausência de instituições ou instrumentos. O Brasil dispõe de órgãos especializados, bases de dados, inteligência financeira e mecanismos regulatórios sofisticados. O desafio está na capacidade de integrar essas diferentes peças.

Informações relevantes, muitas vezes, permanecem dispersas, sem padrões ou processos que permitam adequado intercâmbio. Conhecimentos especializados ficam concentrados em instituições específicas e experiências bem-sucedidas nem sempre são compartilhadas com a rapidez necessária.

Enquanto isso, organizações criminosas operam de forma integrada, colaborativa e altamente adaptável. A resposta institucional precisa evoluir na mesma direção. O compartilhamento seguro e tempestivo de informações, aliado a mecanismos robustos de governança e proteção de dados, tornou-se condição indispensável para aumentar a efetividade do sistema. Nesse contexto, a cooperação entre instituições públicas e privadas ganha importância estratégica.

A ENCCLA e os Desafios da Próxima Década

É justamente nesse cenário que a ENCCLA demonstra sua relevância. Sua principal contribuição não está apenas na formulação de ações anuais, mas na capacidade de reunir diferentes instituições em torno de objetivos comuns e construir soluções compartilhadas para problemas complexos.

Os desafios atuais exigem um novo salto evolutivo: mais fluidez, maior interoperabilidade, compartilhamento mais intenso de informações, uso crescente de inteligência artificial e implementação mais rápida das medidas aprovadas.

Também exigem olhar para riscos ainda emergentes. Nas últimas décadas, conceitos como *Know Your Customer* (KYC), *Know Your Employee* (KYE) e *Know Your Supplier* (KYS) tornaram-se fundamentais para a gestão de riscos de lavagem de dinheiro. O avanço dos agentes autônomos de inteligência artificial sugere que, em breve, as organizações devem incorporar um novo conceito: ***KYA – Know Your Agentic***, ou "Conheça seu Agente de Inteligência Artificial".

À medida que agentes autônomos assumam funções relevantes em processos de conformidade, monitoramento e tomada de decisão, será necessário monitorar seu desempenho, compreender seus modelos de funcionamento e prevenir manipulações, vieses intencionais, alucinações induzidas e outras vulnerabilidades capazes de comprometer controles internos.

As organizações criminosas historicamente demonstram elevada capacidade de adaptação tecnológica. Nesse contexto, não é difícil imaginar tentativas de exploração de agentes autônomos utilizados por empresas e governos, seja por meio de manipulação de dados, introdução de vieses ou comprometimento silencioso de processos decisórios.

A governança da inteligência artificial tende a ocupar posição cada vez mais relevante nos programas de integridade e gestão de riscos, exigindo monitoramento contínuo, auditoria, validação e curadoria permanente dos modelos utilizados.

A contribuição do Banco do Brasil

Ao longo da trajetória da ENCCLA, o Banco do Brasil consolidou-se como um dos participantes mais ativos da Estratégia, acumulando 72 participações em ações desde sua criação (Brasil, 2026d).

Esse protagonismo reflete o compromisso da instituição com a integridade, a sustentabilidade e o fortalecimento das políticas de prevenção à lavagem de dinheiro. Em 2025, o Banco do Brasil foi reconhecido pela Corporate Knights como o banco mais sustentável do planeta pela sexta vez, no *ranking* Global 100 das Corporações Mais Sustentáveis do Mundo. Na edição de 2025, o Banco também alcançou a 17ª posição entre todas as empresas avaliadas globalmente, consolidando sua posição de destaque em sustentabilidade, governança, gestão de riscos e responsabilidade corporativa (Banco do Brasil, 2025; Corporate Knights, 2025).

A participação ativa do Banco do Brasil na ENCCLA, face à sua natureza de sociedade de economia mista, possui forte simbolismo ao apontar caminhos efetivos para o combate à corrupção, à lavagem de dinheiro e ao financiamento do

terrorismo mediante atuação integrada dos setores público e privado, especialmente em um ambiente cada vez mais complexo e digital.

Conclusão

O sistema brasileiro de combate à corrupção, à lavagem de dinheiro e ao financiamento do terrorismo alcançou elevado grau de maturidade institucional. Entretanto, as ameaças evoluíram. O crime organizado tornou-se mais sofisticado, mais tecnológico e mais internacionalizado, enquanto fraudes financeiras, crimes cibernéticos e inteligência artificial passaram a integrar um mesmo ecossistema de riscos, gerando recursos ilícitos que posteriormente alimentam estruturas complexas de lavagem de dinheiro.

Diante desse cenário, torna-se necessário fortalecer a integração entre instituições públicas e privadas, ampliar o compartilhamento de informações, utilizar de forma responsável as novas tecnologias e acelerar a implementação de soluções capazes de responder à velocidade das transformações em curso.

A experiência das últimas décadas demonstra que a efetividade do combate à corrupção, à lavagem de dinheiro e ao financiamento do terrorismo depende cada vez menos da atuação isolada de instituições individuais e cada vez mais da capacidade coletiva de operar como um verdadeiro sistema.

Se o crime organizado atua em rede, a resposta também precisa ocorrer em rede. O fortalecimento da ENCCLA, o aprofundamento da cooperação entre os diversos integrantes do sistema, o compartilhamento seguro de informações, a valorização da inteligência financeira e o uso ético e responsável da inteligência artificial constituem elementos essenciais para que o Brasil continue preparado para enfrentar os desafios crescentes de um ambiente econômico, financeiro e tecnológico em constante transformação.

Referências

ABREU, Allan de. *Cocaína*: a rota caipira. Rio de Janeiro: Record, 2017.

BRASIL. Banco Central do Brasil. Instrução Normativa BCB nº 761, de 9 de julho de 2026. Brasília, DF, 2026.

BRASIL. Banco Central do Brasil. Resolução BCB nº 1, de 12 de agosto de 2020. Institui o arranjo de pagamentos Pix e aprova o seu Regulamento. Brasília, DF, 2020.

BRASIL. Banco Central do Brasil. Resolução BCB nº 587, de 18 de setembro de 2026. Brasília, DF, 2026.

BRASIL. Conselho Monetário Nacional; Banco Central do Brasil. Resolução Conjunta nº 6, de 23 de maio de 2023. Brasília, DF, 2023.

FINANCIAL ACTION TASK FORCE (FATF). *Guidance on Correspondent Banking Services*. Paris: FATF/OECD, out. 2016. Disponível em: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Correspondent-Banking-Services.pdf.

FINANCIAL ACTION TASK FORCE (FATF). *Investigating Professional Money Laundering, Underground Banking, and the Use of Hawala and Other Similar Service Providers*. Paris: FATF/OECD, set. 2026a. Disponível em: https://www.fatf-gafi.org/en/publications/Methodsandtrends/pml-underground-banking-hawala-hossps.html.

FINANCIAL ACTION TASK FORCE (FATF). *Virtual Assets*: Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs. Paris: FATF/OECD, jul. 2026b. Disponível em: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/7th-targeted-update-on-implementation-fatf-standards-vas-vasps-2026.pdf.coredownload.pdf.

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL (GAFI). *Anti-money laundering and counter-terrorist financing measures – Brazil*: Mutual Evaluation Report. Paris: FATF; GAFILAT, dez. 2023. Disponível em: https://www.fatf-gafi.org/en/publications/Mutualevaluations/Brazil-mer-2023.html.

LAGARDA, G.; VERASTEGUI LIRA, P. *Do Warnings Change Behavior?* Money-Laundering, Grey-Listing by the FATF, and Cross-Border Financial Flows. Working Paper. Washington, D.C.: Banco Interamericano de Desenvolvimento (BID), abr. 2026. DOI: 10.18235/0014029. Disponível em: https://publications.iadb.org/en/do-warnings-change-behavior-money-laundering-grey-listing-fatf-and-cross-border-financial-flows.

SERAPIÃO, Fabio; PILLE, Letícia. Líder da máfia explica uso de doleiro para pagar traficantes; ouça. *Metrópoles*, Brasília, 11 mar. 2025. Disponível em: https://www.metropoles.com/colunas/fabio-serapiao/lider-da-mafia-italiana-usa-doleiro-para-pagar-traficantes-ouca.

LUIZ PAULO AZEVEDO BITTENCOURT

Sobre o autor

Head de Segurança Institucional do Banco do Brasil e diretor setorial do Comitê de Prevenção a Fraudes da Febraban. Mestre em Administração com MBA em Gestão de Riscos e Compliance, MBA em Finanças e MBA em Comunicação Organizacional. Possui certificações internacionais em Inovação, Controles Internos, PLD/FTP, Sanções Internacionais e Prevenção a Fraudes.

O pagamento entre organizações criminosas como ponto de pressão no combate ao crime organizado transnacional.

Maurício Sambuichi
Oto Montagner

Introdução

O crime organizado transnacional se sustenta em transações econômicas de alta complexidade. Para que um carregamento de cocaína deixe os países produtores andinos e chegue às ruas da Europa, por exemplo, é preciso que indivíduos de diferentes culturas, dispersos pelo mundo, atuem de forma complementar. No percurso, esses atores negociam preços e padrões de qualidade, monitoram a carga e definem operadores e locais. É da eficiência desses processos que depende a alta lucratividade do negócio.

Esses negócios envolvem custos de transação, demandando recursos para reduzir riscos entre as partes. No crime organizado transnacional, esse ônus é amplificado por duas características. A ilicitude impede o acesso a contratos formais e tribunais, de modo que as negociações ocorrem em um ambiente de alta incerteza e assimetria informacional. A transnacionalidade, por sua vez, acrescenta a cada fronteira cruzada novas complexidades e as exigências próprias de cada jurisdição. Entre todas essas etapas, uma se destaca como gargalo estrutural: o pagamento.

Levar um produto ilícito de um país A a um país B já é, por si só, uma operação complexa. O negócio, no entanto, só se completa quando a organização em B paga sua parceira em A, e dois fatores principais tornam esse momento especialmente sensível. O primeiro é a rastreabilidade. Um pagamento que deixe rastros pode expor não apenas a transação, mas toda a rede que a sustenta. O segundo é a desconfiança. Sem garantias formais de que a outra parte cumprirá o combinado, o pagamento se torna um dos pontos em que a cooperação entre organizações criminosas é posta à prova. Não por acaso, investigações documentam tensões em grupos criminosos provocadas por trapaças, ou pela mera suspeita delas, justamente na liquidação (SERAPIÃO; PILLE, 2025; ABREU, 2017).

Nenhuma operação pode dispensar o pagamento, e nele se concentram riscos de exposição e de quebra de confiança. Trata-se, portanto, de uma vulnerabilidade estrutural das cadeias de suprimento ilícitas que toda rede criminosa transnacional precisa resolver.

Para contornar o gargalo, a movimentação dos recursos através do sistema financeiro costuma ser delegada a operadores especializados que se utilizam de produtos, canais e serviços existentes. O caixa desses operadores mistura fluxos comerciais, remessas legítimas e produto de crime, combinando, no mesmo canal, quem move recursos lícitos e quem lava dinheiro. Muitos atuam por meio de negócios de aparência regular, como importação, exportação e câmbio; e usam a

rede bancária e empresas de fachada para liquidar saldos entre si. Assim, sem a devida detecção, a parte visível do sistema financeiro enxerga apenas operações comerciais e transferências comuns.

Entre os produtos utilizados para mascarar os reais beneficiários da transação, estão contas em que o titular movimenta recursos de terceiros ou em que há mistura de recursos de diversos beneficiários, como, por exemplo, as chamadas "contas-bolsão" no Brasil e as *payable-through account* ou *nested account* disponibilizadas através da relação entre bancos de jurisdições diferentes (*correspondent banking*).

Já os criptoativos são utilizados pela dificuldade da rastreabilidade do titular da carteira digital e beneficiário final dos recursos. Cada carteira é identificada por um código, que pode ser criada em quantidades ilimitadas. No caso das carteiras não custodiadas (*unhosted wallets*), o próprio usuário é responsável pela guarda dos ativos, sem intermediação de instituição regulada. A identificação dos beneficiários finais ocorre nos pontos de contato com o sistema financeiro, como as prestadoras de serviços de ativos virtuais (VASPs) na abertura da conta e/ou na movimentação de recursos.

Dentre os canais e serviços utilizados pelas redes criminosas estão os serviços de transferência de valor (*Money or Value Transfer Services*) que vão de prestadores regulados e licenciados a redes informais, que também utilizam canais legais, como IBANs virtuais (vIBANs) para receber dos clientes e liquidar saldos. As comissões dos operadores ilegais variam, em geral, entre cerca de 0,5% e 5% do valor transferido, mas são explicitamente baseadas em risco: transferências de recursos suspeitos de origem criminosa pagam taxas maiores, para remunerar o risco de detecção, a responsabilidade penal e a possibilidade de sanções (FATF, 2026a).

A complexidade inerente à movimentação de recursos abre espaço para que intervenções voltadas a gerar instabilidade nesse ponto elevem ainda mais os custos de transação das organizações criminosas. Quanto mais elas precisam sofisticar seus mecanismos de pagamento, maior o ônus imposto.

Elevar o risco e a incerteza associados a essas transações reduz a eficiência das redes criminosas e comprime a lucratividade de seus negócios, limitando sua capacidade de expansão e de infiltração. Sob essa perspectiva, o objetivo é tornar sistematicamente mais difícil e arriscado movimentar recursos.

As instituições financeiras reguladas e autorizadas a operar, como bancos e instituições de pagamento, são a primeira linha de defesa na identificação e na interrupção do fluxo financeiro ilegal. Os reguladores e a lei os obrigam a identificar

os clientes, manter cadastros e registros atualizados e comunicar operações suspeitas às unidades de inteligência financeira, como o COAF. Na regulação bancária, isso significa analisar a cadeia societária até o beneficiário final, qualificar o cliente conforme o risco e a natureza da relação, avaliar sua capacidade financeira e analisar o propósito e finalidade das operações. A ideia é que com isso as transações e clientes sejam rastreáveis de origem a destino e finalidade correspondente à capacidade financeira.

No entanto, esse desenho possui duas fragilidades. A primeira é a efetividade dos controles dentro das próprias instituições reguladas, que podem não ter a capacidade de identificar e/ou não comunicar transações provindas de recursos ilícitos. A segunda é a infiltração de entidades não reguladas, que operam no sistema financeiro regulado se utilizando de produtos e canais que, sem a devida diligência, ocultam os reais beneficiários e origem dos recursos.

Para fortalecer o combate destas cadeias ilícitas, deve-se aprimorar os controles e enforcement no pagamento entre organizações criminosas, um dos seus gargalos estruturais. Para isso, há três frentes de atuação:

1. A cooperação entre entidades reguladas e o regulador se mostra fundamental para a identificação e prevenção de transações ilícitas. As redes criminosas misturam recursos e estruturas societárias às redes reguladas, abrindo a possibilidade de identificação pelas autoridades e pelas instituições obrigadas a manter controles de PLD/FT, sanções e prevenção a fraudes.
2. Maiores controles e diligência em produtos, canais e instituições que permitem a liquidação de valores de terceiros, elevando o custo dos operadores ilegais e reduzindo a eficiência do pagamento entre entidades criminosas.
3. Redução de arbitragem regulatória entre países, uma vez que as organizações criminosas migram para onde a regulação é mais frágil e a detecção de pagamentos ilícitos é menos efetiva. Como resposta, o Grupo de Ação Financeira Internacional (GAFI) avalia a aderência dos países aos padrões de controle do sistema financeiro e, ao identificar deficiências estratégicas, exige um plano de ação para corrigi-las. A entrada nas listas do GAFI eleva o custo de operar com a jurisdição e pode reduzir os fluxos financeiros que ela recebe, o que a incentiva a corrigir as deficiências (LAGARDA; VERASTEGUI LIRA, 2026).

Conclusão e recomendações

Tão complexo quanto levar a mercadoria ilícita do ponto A ao ponto B é pagar por ela. No pagamento, a rede se expõe e a confiança entre as organizações é posta à prova, o que o torna uma vulnerabilidade estrutural das cadeias ilícitas transnacionais e um ponto de pressão para o combate ao crime organizado. Para resolvê-lo, essas organizações recorrem a operadores especializados, que misturam fluxos lícitos e ilícitos e se valem de produtos, canais e serviços do sistema financeiro regulado para burlar a identificação dos beneficiários finais. É nesse ponto que o combate aos crimes financeiros deve atuar, já que identificar e interromper o fluxo de dinheiro entre as organizações desestabiliza a confiança entre elas, compromete a liquidação das transações e enfraquece o próprio negócio criminoso.

No Brasil, as instituições financeiras reguladas identificam e monitoram clientes e operações com base em uma abordagem baseada em risco, que só se mantém eficaz se for recalibrada de forma constante com informações sobre como as redes atuam. Sem pretensão de esgotar o tema, propomos três recomendações, uma para cada frente apresentada.

Na frente da cooperação e da detecção, a primeira recomendação é ampliar a capacidade analítica do COAF. O órgão recebe comunicações que citam pessoas, empresas e sócios e pode cruzar esses dados para mapear as conexões entre eles e identificar redes que uma comunicação isolada não revela. Ampliar essa capacidade exige mais analistas e tecnologia, como já apontado na avaliação mútua do GAFI (2023), e dados estruturados nas comunicações. Mais do que produzir essa inteligência, é preciso compartilhá-la. Nos casos em que o COAF conclui haver indícios de lavagem, deve-se alertar as instituições financeiras, em formato que preserve o sigilo das investigações, de modo que possam recalibrar suas avaliações de risco e a classificação de seus clientes, e permitir que as próprias instituições compartilhem entre si indícios de lavagem, nos moldes do que a Resolução Conjunta nº 6/2023 prevê para fraudes e do registro de suspeita de fraude no DICT, previsto no Regulamento do Pix (Res. BCB 1/2020, na redação da Res. BCB 587/2026), com base legal, salvaguardas de privacidade e direito de contestação.

Na frente da rede de produtos e canais utilizada pelos operadores especializados para liquidar os pagamentos, a segunda recomendação é avançar na regulação para dar maior rastreabilidade às transações realizadas nessa rede, de modo que as instituições financeiras reguladas, que são a primeira linha de defesa na identificação de indícios de lavagem e na interrupção do fluxo ilegal, consigam identificar todas as partes envolvidas. É nessa rede que a identificação

dos beneficiários finais é mais vulnerável (FATF, 2016; 2026a; 2026b), o que a torna inerentemente mais arriscada, e a medida busca reduzir a mistura de recursos lícitos e ilícitos. As boas práticas do GAFI indicam o caminho, que inclui licenciar ou registrar os prestadores e agir contra os não autorizados; divulgar as sanções aplicadas e estatísticas anonimizadas por canal e setor; estender os controles a setores facilitadores, como casas de câmbio, prestadores de ativos virtuais e comércio exterior; e adotar um "modelo de barreiras", que atribui a cada etapa da cadeia de lavagem uma medida e uma autoridade responsável, como na Bélgica (FATF, 2026a).

Na frente da arbitragem, a terceira recomendação é avaliar o risco pela rota do pagamento, considerando os países e canais envolvidos, e não apenas a presença do país nas listas do GAFI. Como as redes migram para onde a regulação é mais frágil (FATF, 2026a), uma rota pode ser de alto risco mesmo sem passar por jurisdições listadas, já que as listas dependem de ciclos de avaliação e de períodos de observação e olham o país, não o canal. A regulação brasileira já associa medidas reforçadas às jurisdições com deficiências identificadas pelo GAFI (IN BCB 761/2026), e propõe-se complementá-la com avaliações mútuas, que mostram a fragilidade de países ainda não listados, e com tipologias, que descrevem como os esquemas operam. Propõe-se também que o COAF direcione seus pedidos a unidades de inteligência financeira de outros países conforme as rotas e jurisdições de maior risco para o Brasil, ponto de melhoria apontado na avaliação mútua do GAFI (2023), para acompanhar o dinheiro além da fronteira.

Em conjunto, as três recomendações atuam sobre o mesmo ponto de pressão, pois a cooperação amplia a capacidade de identificar as redes; a regulação dessa rede de produtos e canais reduz o espaço para misturar recursos lícitos e ilícitos; e a atenção ao risco das rotas e à troca de informações entre países limita a migração para onde o controle é mais frágil. Quanto mais difícil e arriscado for pagar, menores a confiança e a eficiência entre as organizações, e maior a contribuição do combate aos crimes financeiros para enfraquecer o crime organizado transnacional.

Referências

ABREU, Allan de. *Cocaína*: a rota caipira. Rio de Janeiro: Record, 2017.

BRASIL. Banco Central do Brasil. Instrução Normativa BCB nº 761, de 9 de julho de 2026. Brasília, DF, 2026.

BRASIL. Banco Central do Brasil. Resolução BCB nº 1, de 12 de agosto de 2020. Institui o arranjo de pagamentos Pix e aprova o seu Regulamento. Brasília, DF, 2020.

BRASIL. Banco Central do Brasil. Resolução BCB nº 587, de 18 de setembro de 2026. Brasília, DF, 2026.

BRASIL. Conselho Monetário Nacional; Banco Central do Brasil. Resolução Conjunta nº 6, de 23 de maio de 2023. Brasília, DF, 2023.

FINANCIAL ACTION TASK FORCE (FATF). *Guidance on Correspondent Banking Services*. Paris: FATF/OECD, out. 2016. Disponível em: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Correspondent-Banking-Services.pdf.

FINANCIAL ACTION TASK FORCE (FATF). *Investigating Professional Money Laundering, Underground Banking, and the Use of Hawala and Other Similar Service Providers*. Paris: FATF/OECD, set. 2026a. Disponível em: https://www.fatf-gafi.org/en/publications/Methodsandtrends/pml-underground-banking-hawala-hossps.html.

FINANCIAL ACTION TASK FORCE (FATF). *Virtual Assets*: Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs. Paris: FATF/OECD, jul. 2026b. Disponível em: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/7th-targeted-update-on-implementation-fatf-standards-vas-vasps-2026.pdf.coredownload.pdf.

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL (GAFI). *Anti-money laundering and counter-terrorist financing measures – Brazil*: Mutual Evaluation Report. Paris: FATF; GAFILAT, dez. 2023. Disponível em: https://www.fatf-gafi.org/en/publications/Mutualevaluations/Brazil-mer-2023.html.

LAGARDA, G.; VERASTEGUI LIRA, P. *Do Warnings Change Behavior?* Money-Laundering, Grey-Listing by the FATF, and Cross-Border Financial Flows. Working Paper. Washington, D.C.: Banco Interamericano de Desenvolvimento (BID), abr. 2026. DOI: 10.18235/0014029. Disponível em: https://publications.iadb.org/en/do-warnings-change-behavior-money-laundering-grey-listing-fatf-and-cross-border-financial-flows.

SERAPIÃO, Fabio; PILLE, Letícia. Líder da máfia explica uso de doleiro para pagar traficantes; ouça. *Metrópoles*, Brasília, 11 mar. 2025. Disponível em: https://www.metropoles.com/colunas/fabio-serapiao/lider-da-mafia-italiana-usa-doleiro-para-pagar-traficantes-ouca.

Sobre os autores

Mauricio Sambuichi. Gerente de PLD/FT e Oversight de Prevenção a Fraudes do Banco ABC Brasil e Deputy MLRO e Deputy AMLCO da filial Cayman Islands. Ex-Gerente na PwC, em Financial Crime e Integrity Due Diligence. Bacharel em Relações Internacionais pela PUC-SP e pós-graduado em Economia Empresarial pela FGV-SP, com especializações em Economia (FIPE/USP) e Risk Management (B3 Educação).

Oto Montagner. Professor Agregado da Escola de Relações Internacionais da Fundação Getulio Vargas (FGV RI) e doutor em Economia Aplicada pela ESALQ-USP. Sua pesquisa concentra-se no crime organizado transnacional, com ênfase nas dinâmicas estratégicas, nas estruturas de governança e nas interações entre organizações criminosas em diferentes países. Utiliza principalmente teoria dos jogos e modelagem formal para investigar esses fenômenos.

MAURICIO SAMBUICHI

OTO MONTAGNER

Do dado ao ativo: a ENCCLA e o desafio de conectar os elos do sistema brasileiro de PLD/FT.

Ricardo Andrade Saadi
Presidente do Conselho de Controle de Atividades Financeiras (COAF)

Introdução

Acompanho a ENCCLA desde suas primeiras reuniões. Participei delas como representante da Polícia Federal e, anos depois, já à frente do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do Ministério da Justiça, coordenei os trabalhos da Estratégia por sete anos. Hoje, na presidência do COAF, observo o sistema a partir de outro ponto da cadeia: o lugar em que as comunicações dos setores obrigados se transformam em inteligência financeira.

Essa trajetória me leva a uma convicção e a uma tese. A convicção é que a ENCCLA é o espaço mais adequado para decidir os próximos passos do sistema brasileiro de prevenção e combate à lavagem de dinheiro, porque foi nela que boa parte dos passos anteriores foi decidida. A tese é que a efetividade do sistema dependerá menos de criar novos deveres ou de aumentar o número de comunicações e mais de conectar melhor os elos que já existem — do dado comunicado pelo setor obrigado ao ativo efetivamente retirado do crime.

O método ENCCLA: problemas reais, soluções construídas em conjunto

A ENCCLA tem um desenho singular. Ela coloca à mesma mesa instituições dos três Poderes, dos três níveis da Federação e da sociedade civil para que, juntas, definam quais são, naquele momento, os principais problemas do país no combate à corrupção e à lavagem de dinheiro. Definidas as prioridades, formam-se grupos de trabalho encarregados de resolver o problema ou de propor caminhos para sua solução.

O método é simples e, por isso mesmo, eficaz. Ele parte de problemas concretos, distribui a responsabilidade entre quem tem competência para agir e produz entregas verificáveis. Os resultados falam por si. Da ENCCLA nasceu o Programa Nacional de Capacitação e Treinamento para o Combate à Corrupção e à Lavagem de Dinheiro (PNLD), que formou milhares de agentes públicos em todo o país. Dela saíram projetos e anteprojetos cujos textos foram, em parte, aproveitados em leis estruturantes, como a reforma da Lei de Lavagem de Dinheiro, em 2012, a Lei de Organizações Criminosas e a Lei Anticorrupção, ambas de 2013.

A Estratégia também enfrentou problemas de natureza operacional. Um exemplo é o estímulo à criação dos Laboratórios de Tecnologia contra a Lavagem de Dinheiro (LAB-LD), que levaram capacidade de processamento e análise de grandes volumes de dados a polícias, Ministérios Públicos e outros órgãos, e que hoje funcionam em rede.

Há, porém, uma característica que considero mais importante do que qualquer produto isolado: a ENCCLA é uma estratégia de Estado, e não de governo. Ao longo de mais de duas décadas, independentemente de quem estivesse à frente do Executivo, seus integrantes técnicos mantiveram o foco em identificar e resolver os problemas reais do país. É essa continuidade que a credencia a liderar a próxima etapa.

Diagnóstico: um sistema que produz muito e precisa converter mais

A Lei nº 9.613/1998 criou, ao mesmo tempo, um crime, um conjunto de deveres e uma instituição. O crime de lavagem deu ao Estado um instrumento para alcançar o produto da atividade ilícita. Os deveres de identificação, registro e comunicação transformaram parte relevante do setor privado em sentinela do sistema. E o COAF foi concebido como o ponto de encontro entre esses dois mundos. Vinte e oito anos depois, essa arquitetura continua correta em suas linhas gerais. O que mudou foram a escala, a velocidade e a sofisticação do ambiente em que ela opera.

Na ponta de entrada, o sistema é maduro. A base de dados do COAF reúne mais de 65 milhões de comunicações de operações. Em 2025, a unidade produziu 20.548 Relatórios de Inteligência Financeira (RIFs), 9,5% a mais que em 2024 e mais de seis vezes o volume de 2014. Na supervisão dos setores sob sua responsabilidade direta, foram instaurados 786 processos administrativos sancionadores no mesmo ano, com multas que somaram R$ 96,9 milhões.

A avaliação mútua do Brasil pelo GAFI (FATF), concluída em 2023, reconheceu esses avanços — entre eles, o papel da ENCCLA como espaço de coordenação e a qualidade da inteligência financeira produzida. O mesmo

relatório, contudo, apontou onde a cadeia perde força: número reduzido de analistas diante do volume recebido; investigações de lavagem que raramente resultam em processos e condenações compatíveis com o perfil de risco do país; resultados de confisco em tráfico de drogas, crime organizado e fraudes aquém da dimensão desses riscos; acesso limitado e pouco ágil a informações de beneficiário final; e lacunas na supervisão de alguns setores não financeiros.

O quadro é o de um sistema forte na captação de dados e na produção de inteligência, mas que ainda converte pouco desse esforço em resultado final. Cada elo foi aperfeiçoado, em grande medida, de forma isolada. O desafio dos próximos anos é otimizar a cadeia inteira — precisamente o tipo de problema que nenhuma instituição resolve sozinha e para o qual a ENCCLA foi criada.

Desafios: onde a cadeia perde força

Volume sem foco. O crescimento das comunicações é, em parte, sinal de maturidade. Mas carrega o risco da comunicação defensiva: operações reportadas mais para afastar responsabilidade do que por efetiva suspeita. Quando os indicadores de todos os atores se baseiam em quantidade, o sistema tende a produzir ruído em escala e a diluir os sinais que realmente importam.

O crime dentro da economia formal. A Operação Carbono Oculto, deflagrada em agosto de 2025, expôs o problema com clareza. Segundo a Receita Federal, uma única instituição de pagamento movimentou mais de R$ 46 bilhões entre 2020 e 2024, e ao menos 40 fundos de investimento, com patrimônio estimado em R$ 30 bilhões, eram usados para ocultar os reais beneficiários dos negócios de uma facção criminosa no setor de combustíveis. A lição é que o crime organizado já utiliza estruturas reguladas e aparentemente legítimas — contas de pagamento, contas-bolsão, fundos e sociedades empresárias. O risco se concentra nos interstícios entre supervisores, produtos e jurisdições. Avanços como a regulamentação dos prestadores de serviços de ativos virtuais e o novo regime das apostas de quota fixa mostram que o sistema reage; mostram também que a regulação tende a correr atrás da inovação.

Supervisão fragmentada. Quase duas dezenas de setores obrigados estão distribuídos entre supervisores com capacidades, metodologias e prioridades distintas. Ao COAF cabe supervisionar os setores sem regulador próprio — como joias e metais preciosos, bens de luxo e alto valor e fomento mercantil —, espalhados por todo o território. Sem matriz de risco comum, o mesmo grupo econômico pode ser visto por partes, sem que nenhum supervisor enxergue o todo.

Beneficiário final tardio. A informação existe, mas não chega com a rapidez necessária. Em casos de camadas societárias e fundos, o tempo para identificar quem efetivamente controla uma estrutura é, muitas vezes, o tempo que os recursos levam para desaparecer.

A ausência de retorno. Nem a unidade de inteligência sabe, de forma sistemática, quais RIFs resultaram em investigação, bloqueio ou confisco, nem o setor obrigado sabe quais de suas comunicações foram úteis. Sem esse retorno, ninguém calibra o próprio trabalho, e o sistema não dispõe de uma métrica comum de efetividade.

Tecnologia dos dois lados. Pagamentos instantâneos, abertura digital de contas e contas de passagem permitem pulverizar recursos em segundos. Se o Estado continuar analisando em ritmo manual um fluxo que ocorre em tempo real, a distância entre o crime e a resposta tenderá a crescer.

Propostas: conectar os elos

As propostas a seguir partem de um critério comum: aumentar a conversão do esforço já existente em resultado, em vez de simplesmente acrescentar obrigações. Todas se prestam ao método ENCCLA — problema definido, responsáveis identificados e entregas mensuráveis.

Da quantidade à relevância das comunicações. Adotar indicadores de qualidade das comunicações por setor e por instituição, com retorno periódico e individualizado aos setores obrigados; construir tipologias e sinais de alerta em conjunto com o setor privado; e revisar comunicações automáticas de baixo valor analítico, liberando capacidade para o que de fato indica risco.

Parcerias público-privadas de inteligência. Experiências como o JMLIT, no Reino Unido, o FinCEN Exchange, nos Estados Unidos, e a ACIP, em Singapura, demonstram o valor do compartilhamento estruturado de informações sobre ameaças prioritárias. O Brasil pode institucionalizar um modelo próprio, com base legal adequada, salvaguardas de sigilo e foco em temas definidos, como facções criminosas, fraudes eletrônicas e crimes ambientais. Compliance não é adversário do Estado; é parte da linha de frente.

Inteligência aumentada por tecnologia. O que os LAB-LD representaram para a investigação, a inteligência artificial pode representar agora para toda a cadeia. É preciso investir de forma contínua em triagem automatizada, análise de redes e cruzamento de bases, com governança: rastreabilidade das decisões, explicabilidade dos modelos, supervisão humana e proteção de dados. A tecnologia deve ampliar a capacidade do analista, não substituir o seu juízo.

Fechar lacunas de perímetro e coordenar a supervisão. Reforçar a supervisão sobre os setores obrigados e, em paralelo, criar uma instância permanente de coordenação entre supervisores, com matriz de risco comum, troca de informações, ações conjuntas e sanções proporcionais e dissuasivas.

Beneficiário final acessível e confiável. Um cadastro de beneficiários finais só cumpre sua função se for verificado, atualizado e acessível de forma direta e tempestiva pelas autoridades competentes, inclusive a unidade de inteligência financeira, com regras claras de acesso e responsabilização.

Capacidade institucional, capacitação e presença territorial. Inteligência financeira é atividade intensiva em conhecimento especializado. O fortalecimento do quadro de pessoal do COAF, com carreira e estrutura compatíveis com suas atribuições, é condição para as demais propostas. O PNLD mostrou que capacitação em escala muda a qualidade do sistema; uma nova geração de formação, voltada a ativos virtuais, análise de dados e investigação patrimonial, seria sua continuidade natural. A presença territorial também importa: as unidades regionais do COAF em São Paulo e no Rio de Janeiro, e a nova unidade em Foz do

Iguaçu, na tríplice fronteira, aproximam a inteligência financeira dos setores supervisionados, das autoridades locais e das dinâmicas regionais de risco.

Conclusão

O sistema brasileiro de prevenção e combate à lavagem de dinheiro foi construído de forma coletiva, e é dessa forma que precisará evoluir. Quem acompanhou a ENCCLA desde o início sabe que a articulação entre instituições produziu resultados que nenhuma delas alcançaria sozinha — leis, programas de capacitação, laboratórios e, sobretudo, uma cultura de cooperação que sobreviveu a sucessivos governos.

O próximo passo é deslocar o foco do desempenho de cada instituição para o desempenho da cadeia: perguntar não apenas quantas comunicações foram recebidas ou quantos relatórios foram produzidos, mas quanto desse esforço chegou ao fim do caminho. Sugere-se, nesse sentido, que a ENCCLA considere, entre suas próximas ações, a construção do painel nacional de efetividade, a estruturação de um modelo brasileiro de parceria público-privada de inteligência e o mapeamento das lacunas de perímetro e supervisão evidenciadas pelos casos recentes envolvendo o crime organizado.

Um sistema de PLD/FTP se mede, ao final, por sua capacidade de impedir que o crime desfrute de seus lucros. A ENCCLA já demonstrou que sabe transformar problemas reais em soluções concretas. Conectar os elos — do dado ao ativo — é o desafio à altura dessa trajetória.

RICARDO ANDRADE SAADI

Sobre o autor

Presidente do Conselho de Controle de Atividades Financeiras (COAF). Delegado de Polícia Federal. Mestre e Doutor em Direito Político e Econômico (Universidade Presbiteriana Mackenzie).

ENCCLA 2027

Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro

DEPARTAMENTO DE RECUPERAÇÃO DE ATIVOS E COOPERAÇÃO JURÍDICA INTERNACIONAL
SECRETARIA NACIONAL DE JUSTIÇA
MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO