CAC COMTEXTO

EDIÇÃO Nº 05 – DEZEMBRO 2024

OAB PINHEIROS | COMISSÃO ANTICORRUPÇÃO E COMPLIANCE

EDITORES:
Renata F. Andrade (coordenação)
Pedro Roncarati

AUTORES:
Amanda Ribeiro Soares
Cecilia Choeri
Comitê de PLD
Juliana Batista de Vasconcelos
Renata Fonseca de Andrade

REVISORAS:
Aline Oliveira Silva
Mariana de Almada Jeveaux
Renata F. Andrade

FOTOGRAFIA: HELENA RUBANO

COMPLIANCE ANTI CORRUPÇÃO INOVAÇÃO

Editorial

RENATA FONSECA DE ANDRADE

Editora Coord. da CAC COMTEXTO
Presidente da Comissão de Anticorrupção
e Compliance -OAB/SP Pinheiros

Sempre em busca de conhecimento e contínua inovação e excelência, temos o prazer de apresentar a nova edição da CAC ComTexto. Nesta edição, focamos em Privacidade, anticrimes financeiros, Responsabilidade Social, Ambiental e Governança.

Sabemos que os desafios de nossa profissão estão nas tecnologias emergentes. Como adaptarmos as melhores práticas em mercados emergentes e cada vez mais digitalizados, mesmo os setores mais tradicionais da economia sem o uso da inteligência artificial e automação?

O poder computacional e os avanços tecnológicos nesses últimos anos estão rompendo as barreiras e estão transformando os negócios e a forma de organização econômica e social do mundo. Assim também os programas de compliance e os esforços contra a lavagem de dinheiro e a sustentabilidade precisam da tecnologia como aliada.

À medida que as empresas enfrentam desafios crescentes em ambientes regulatórios cada vez mais complexos, a tecnologia surge como uma aliada indispensável.

Agradecemos aos autores dessa edição que generosamente compartilham suas experiências e conhecimento em torno dos temas: ANTICORRUPÇÃO, COMPLIANCE e INOVAÇÃO. Parabéns a todos pela resiliência e dedicação.

Desafiamos os leitores ao discorrer as matérias com essa reflexão: Como explorar métodos inovadores e soluções tecnológicas que permitam uma gestão de riscos mais eficaz, que aumentem a transparência e melhorem a eficiência operacional?

Aproveitamos para agradecer aos nossos autores, cujas contribuições enriquecem nosso entendimento e nos impulsionam a buscar práticas ainda mais robustas e inovadoras. E a vocês, nossos leitores, por continuarem a nos acompanhar nesta jornada de conhecimento e evolução.

Dedicamos essa edição à Sociedade Brasileira em constante transformação. Boa leitura!

CAC COMTEXTO

ISSN 2675-8490

cac.oabpinheiros@gmail.com

A revista eletrônica CAC COMTEXTO é editada pela Editora Roncarati e distribuída gratuitamente.

RONCARATI EDITORA

EDITORA RONCARATI LTDA
Fone: (11) 9.1555-5591
www.editoraroncarati.com.br
contato@editoraroncarati.com.br

Sumário

2 **EDITORIAL**
Renata Fonseca de Andrade

4 **APRESENTAÇÃO**
Paulo Sergio Ferraz de Camargo

6 **PREFÁCIO DA 5ª EDIÇÃO**
Renata Fonseca de Andrade

7 **PARTE I**
INCLUSÃO E ACESSIBILIDADE: TORNANDO O PROGRAMA DE COMPLIANCE DISPONÍVEL PARA TODOS
Amanda Ribeiro Soares
Juliana Batista de Vasconcelos

16 **PARTE II**
PROTEÇÃO DE DADOS PESSOAIS E MEDIDAS DE PREVENÇÃO E COMBATE À LAVAGEM DE DINHEIRO
Cecília Choeri Coelho
Maira F. Martella
Renata F. Andrade

Apresentação

O futuro que se avizinha

Caminhamos para mais um final de ano e esse ano é especial, pois registra o encerramento de um ciclo. É o término da gestão à frente da OAB Pinheiros.

Por isso, é impossível não fazer um balanço desses últimos anos do trabalho desenvolvido na OAB Pinheiros. E do que se espera para o futuro.

Foram 06 seis anos muito intensos, de muito trabalho e muita luta. Período que ficou marcado pelo desafio da Pandemia do COVID 19 e pela nova sede da OAB Pinheiros.

A OAB Pinheiros se fortaleceu, promoveu inúmeros cursos, palestras, seminários. E esse trabalho não seria possível sem o apoio constante das Comissões. Tenho como certo que um dos segredos da OAB Pinheiros é a qualidade de suas Comissões.

E não podemos deixar de registrar, em especial, a excelência do trabalho desenvolvido pela Comissão de Anticorrupção e Compliance (CAC), liderada pela nossa antiga e fiel colaboradora, Renata Fonseca de Andrade. A CAC além de servir de exemplo para as demais Comissões

PAULO SERGIO FERRAZ DE CAMARGO

Presidente da OAB Pinheiros; Advogado empresarial; Mestre em Direitos Difusos e Coletivos pela Faculdade de Direito da Pontifícia Universidade Católica de São Paulo (PUC-SP); Especialista em Direito Processual Civil pela Faculdade de Direito da Pontifícia Universidade Católica de São Paulo (PUC-SP); Bacharel em Direito pela Faculdade de Direito da Pontifícia Universidade Católica de São Paulo (PUC-SP); Presidente da Ordem dos Advogados do Brasil – Subseção de Pinheiros; Conselheiro do Esporte Clube Pinheiros. Foi Presidente da Comissão de Cultura da Ordem dos Advogados do Brasil – Subseção de Pinheiros. Autor do livro Dano Moral Coletivo, pela Editora Almedina.

de Pinheiros, serviu de inspiração para a criação de Comissão de Anticorrupção e Compliance em outras Subseções, transcendendo, assim, os limites de Pinheiros.

Na minha visão o balanço é positivo e foi possível deixar a OAB Pinheiros em outro patamar, defendendo diuturnamente os direitos e interesses dos advogados de Pinheiros, trazendo muito mais serviços, apoio e qualidade aos nossos inscritos.

E o futuro acredito que para a OAB Pinheiros seja de renovação, com o ingresso de uma nova geração, mais jovem, conectada, trazendo mais tecnologia, garantindo o legado de inclusão e conhecimento que já é tradição em Pinheiros.

Do ponto vista pessoal, pretendo trilhar outros caminhos na vida institucional, sempre auxiliando no desenvolvimento da nossa classe, mas agora dedicando mais tempo para minha vida pessoal e para o escritório.

Serão tempos de mudanças. Mudanças positivas. Mudanças que demonstram uma transição democrática, com abertura de espaço, renovação de ideias e pessoas e com isso, certamente, quem ganha é a OAB Pinheiros.

Muito obrigado!

Prefácio da 5ª Edição

À medida que concluímos mais uma edição da Revista ComTexto, gostaríamos de refletir sobre os insights e aprendizados compartilhados em nossas páginas. Os artigos desta edição destacaram não apenas a importância, mas a necessidade urgente de integração entre Compliance, ESG e estratégias anti-lavagem de dinheiro em nossas práticas cotidianas.

Observamos como a inovação tecnológica está remodelando a sociedade e a economia, permitindo que organizações de todos os tamanhos fortaleçam seus negócios e com isso a necessidade de controles internos que respondam com mais eficácia às demandas regulatórias. A automação e a inteligência artificial, como vimos, não são mais apenas ferramentas facilitadoras, mas sim elementos essenciais para a sustentabilidade e integridade das operações corporativas.

À medida que o mundo continua a enfrentar mudanças rápidas e muitas vezes disruptivas, a adaptabilidade e a proatividade tornam-se qualidades indispensáveis. Portanto, encorajamos nossos leitores a não só absorver o conhecimento compartilhado, mas também a aplicá-lo, testá-lo e adaptá-lo às suas realidades específicas. A colaboração contínua e o intercâmbio de ideias serão vitais para navegarmos juntos nestes tempos desafiadores.

Agradecemos sinceramente a todos que contribuíram para esta edição e a você, leitor, por se juntar a nós em mais esse desafio de descoberta e inovação. Continuaremos a explorar temas que não apenas informam, mas também transformam nosso campo de atuação. Esperamos que você permaneça conosco, inspirado e informado, enquanto avançamos para futuras edições.

Até a próxima, com mais inovações, mais soluções e um compromisso renovado com a excelência.

RENATA FONSECA DE ANDRADE

Editora Coord. da CAC COMTEXTO
Presidente da Comissão de Anticorrupção e Compliance -OAB/SP Pinheiros

Parte I
Inclusão e acessibilidade: tornando o programa de compliance disponível para todos

AMANDA RIBEIRO SOARES

Gerente de Ética e Compliance da América do Sul e EUA. Advogada especialista em Penal Econômico, ESG, LGPD entre outros. Bacharel em Direito com láurea honrosa pela PUC-SP.

JULIANA BATISTA DE VASCONCELOS

Bacharel em Direito pela UFF e cursando MBA em Compliance pela Mackenzie, é consultora plena na KPMG e atua com projetos relacionados a Compliance.

Introdução

Com o advento da Lei Anticorrupção no panorama corporativo brasileiro, temos visto grandes evoluções com relação ao Programa de Compliance. A cada ano que passa, vamos ganhando experiência com a Lei Anticorrupção 12.846/13[1] e seu Decreto Regulamentador 11.129/22[2], bem como, se atentando as atualidades e riscos específicos.

É possível averiguar que essa evolução e atenção contribui para moldar o Programa de Compliance para que ele mitigue riscos importantes e torne a empresa cada vez mais conforme com os regulamentos, normas aplicáveis e boas práticas do mercado. Como exemplo, pode-se citar a evolução do canal de denúncias.

Desde que houve a necessidade de sua criação, as ferramentas de canal de denúncias e as práticas das empresas

1 BRASIL. Lei Nº 12.846, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Brasília, DF: Diário Oficial da União, 2013.

2 BRASIL. Decreto Nº 11.129, de 11 de julho de 2022. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. Brasília, DF: Diário Oficial da União, 2022.

em sua gestão evoluiu muito, tornando-o cada vez mais confiável e se tornando acessível a todos através de diferentes meios de comunicação. Os canais de denúncia de hoje em dia que já estão mais maduros, normalmente, estão disponibilizados 24 horas por dia, 7 dias por semana, o denunciante pode fazer uma denúncia anônima, existem políticas de não retaliação para o denunciante de boa-fé, pode ser feito online, por telefone, é gerido por um terceiro independente, e, a partir do recebimento da denúncia, há um protocolo para o seu tratamento, sendo garantida confidencialidade e imparcialidade no processo.

Contudo, mesmo com essa evolução e amadurecimento, é necessário considerar que há melhorias que podem ser realizadas. Embora estejamos vendo essa evolução da maturidade de legislação que auxilia a implementar um Programa de Compliance, muitas empresas ainda não implementaram ou se adaptaram para que o Programa seja verdadeiramente acessível a todos. Logo, dentre essas melhorias que podem ser realizadas, se preocupar e priorizar medidas, procedimentos e ferramentas, por exemplo, que auxiliam na inclusão e acessibilidade, é um passo extremamente importante para um mundo corporativo que a cada vez mais tem o foco em consciência e melhoria coletiva.

Nesse sentido, cabe ressaltar que mesmo sendo um conceito antigo (que surgiu em 2004), com a nova "onda" de reforço de medidas e gestão de ESG – *environment, social, governance* – o "S" (social) do ESG começou a ganhar protagonismo em ações gerais, principalmente, em grandes empresas. Os fatores ESG têm cada vez mais se tornado relevantes fazendo que as empresas se tornem socialmente mais engajadas. Mas, essa nova dinâmica e fator ESG precisam também serem aplicados no âmbito de Ética e Compliance. Por isso, a inclusão e a acessibilidade podem e devem ser consideradas uma evolução e uma necessidade em qualquer Programa de Compliance.

Quando um Programa de Compliance é inclusivo, ele atinge mais pessoas e abarca um melhor entendimento como um todo da cultura de Compliance. Sabemos que isso é fundamental para que tenhamos uma boa compreensão de políticas e procedimentos e uma maior efetividade do Programa. Não somente isso, essas ações trazem transparência para o Programa e permite o engajamento do "S" verdadeiramente.

Nesse breve artigo, portanto, será discutido algumas práticas que poderão ser implementadas num Programa de Compliance para que ele se torne acessível e inclusivo. Cabe ressaltar que essas premissas sempre deverão ser revisadas buscando o aprimoramento contínuo de cada Programa. Quanto mais avançamos na tecnologia e nos métodos de gestão do Programa, mais podemos nos adequar para assegurar que o Programa continue em constante evolução.

Por fim, cabe ressaltar que essas premissas podem ser aplicadas localmente e internacionalmente. Há desafios em gerir regiões que não são do Brasil, todavia, essas medidas que aqui serão expostas, poderão também ser aplicadas em Programas e gestão internacional. Basta a adequação cultural quando necessário.

A importância da inclusão no ambiente de trabalho e a necessidade de criar uma cultura de acessibilidade

A inclusão no ambiente de trabalho é essencial para a valorização de todos os profissionais e de suas diferenças e individualidades. Tendo em vista a existência de perfis diversos no mundo profissional, é dever de todas as empresas, independentemente do porte e localidade, analisar seus procedimentos, estruturas e seu dia a dia para assegurar que exista adaptabilidade e acessibilidade a todos para além do cumprimento de cotas e outras obrigações regulatórias.

Nesse sentido, observa-se uma ausência de interesses das empresas em cumprir essas obrigações regulatórias de uma maneira eficaz, ou seja, promover a integração desses colaboradores de forma que os profissionais sejam valorizados em suas funções e carreiras. Infelizmente, ainda existe o preconceito velado das empresas na contratação de profissionais com deficiência, com mais de 30 anos e mulheres com filhos. Inclusive, discute-se que muitas vezes esses profissionais são estigmatizados pelas organizações como pessoas improdutivas, bem como, há uma indisposição das empresas em realizar adaptações mínimas para permitir a acessibilidade e a integração plena desses colaboradores.

Nesse sentido, uma pesquisa realizada pela Page Personnel[3], empresa de recrutamento do grupo Michael Page, demonstra essa realidade de falta de acessibilidade, investimento e adaptações de profissionais com deficiência. Ilustra-se que dos 243 profissionais entrevistados foi constatado, por exemplo, que a maioria dessas pessoas (58%) ocupam cargos administrativos e muitos (36%) nunca foram promovidos. Ainda, a pesquisa destaca que não eram incluídos em reuniões, não eram desafiados, e há um relato que reforça o sentimento de que o colaborador era "contratação para cumprir tabela" sendo reconhecido apenas por sua deficiência e não por suas habilidades, conhecimento e profissionalismo.

Cabe aqui a reflexão: por que muitas empresas estão excluindo parcelas da população que poderiam agregar positivamente em suas empresas? Uma Pesquisa conduzida pela McKinsey[4] verificou que empresas com diversidade étnico cultural e de gênero foram mais lucrativas, bem como a Forbes[5] concluiu que equipes inclusivas tomam melhores decisões de negócio, bem como as tomam mais rapidamente.

Há que se repensar o modelo atual conduzido pelas empresas e não perpetuar a o comportamento retrógrado de excluir profissionais que poderiam agregar positivamente nas organizações, caso a cultura organizacional fosse diferente.

3 ATHAYDE, Bruno. "*Deficientes bem preparados são nivelados por baixo*". Exame, 2013. Documento eletrônico disponível em <https://exame.com/carreira/pra-cumprir-tabela/>; acessado em 17 de outubro de 2023.

4 DIXON-FYLE, Sundiatu. Et al. "*Diversity wins: How inclusion matters*". McKinsey & Company, 2020. Documento eletrônico, disponível em <https://www.mckinsey.com/~/media/mckinsey/featured%20insights/diversity%20and%20inclusion/diversity%20wins%20how%20inclusion%20matters/diversity-wins-how-inclusion-matters-vf.pdf> ; acessado em 01 de outubro de 2023.

5 LARSON, Erik. "*New Research: Diversity + Inclusion = Better Decision Making At Work*". Forbes, 2017. Documento eletrônico disponível em <https://www.forbes.com/sites/eriklarson/2017/09/21/new-research-diversity-inclusion-better-decision-making-at-work/?sh=7efoba3d4cbf >; acessado em 01 de outubro de 2023.

O mesmo pensamento vale para outras minorias. Essa evidente exclusão, baseada em preconceitos ocultos, leva a perda de grandes talentos que poderiam fazer uma diferença positiva na empresa.

Cabe ressaltar que há formas de transformar a cultura organizacional para que o preconceito não impeça a promoção da inclusão e da acessibilidade. Como exemplo, uma solução possível é a promoção de discussões e reflexões nas empresas sobre o *status quo* de seus quadros profissionais e a busca de uma maior participação dos colaboradores nesses fóruns com o intuito de quebrar paradigmas discriminatórios. A conscientização é uma ferramenta importantíssima para que seja discutido assuntos relevantes e para trazer compreensão, sensibilização e informação a todos os colaboradores.

Ainda, cabe a empresa, em seus processos do dia a dia, analisar seus procedimentos para trazer mais acessibilidade como um todo para o ambiente de trabalho e promover uma inclusão efetiva. A tecnologia, nesse caso, é uma poderosa aliada, que proporciona a independência e o rompimento de barreiras, bem como é possível implementar programas de "acompanhamento" para que os colaboradores integrantes de grupos de diversidade se sintam acolhidos e ouvidos. Eventuais sugestões de melhoria devem ser incentivadas, aceitas e implementadas, quando aplicáveis.

Nesse sentido, pensando na mudança e estrutura de cultura organizacional, o Programa de Compliance é um grande parceiro para as empresas. Por isso, compreender o que é um Programa de Compliance, os pilares nos quais está baseado e seu papel na inclusão é fundamental para a mudança do paradigma e implementação de ações necessárias.

O que é o programa de compliance e o papel do programa de compliance na inclusão

O Programa de Compliance, ou também conhecido como, Programa de Integridade, é um conjunto de mecanismos, como procedimentos, políticas e ferramentas, implementados em instituições públicas e privadas com o objetivo de prevenir, detectar e remediar a materialização de riscos como corrupção, fraude, conflitos de interesses, eventuais desvios de conduta e irregularidades.

Historicamente é possível observar que empresas de grande porte foram pioneiras na implementação de Programas de Integridade, sendo no cenário atual as organizações com maior maturidade em relação ao tema. Contudo, isso não significa que empresas de médio e pequeno porte não observaram a tendência, uma pesquisa conduzida pela KPMG em 2021[6] sobre a maturidade do Compliance no Brasil teve 47% dos seus respondentes empresas de pequeno e médio porte, demonstrando o interesse dessas organizações sobre o tema. Ao averiguar os benefícios que um Programa pode trazer para a empresa, bem como observando os incentivos regulatórios apresentados pela Legislação Anticorrupção Brasileira,

6 MELO, Emerson. Et al. "Pesquisa de Maturidade do Compliance no Brasil". KPMG, 2021. Documento eletrônico disponível em <https://www.editoraroncarati.com.br/v2/phocadownload/KPMG-pesquisa-maturidade-compliance-2021.pdf>; acessado em 19 de outubro de 2023.

essas empresas também iniciaram a implementação de Programas de Compliance adaptados à sua realidade.

Positivamente, essa observância pelas empresas tem contribuído significantemente para o combate a corrupção, fraude entre outras irregularidades. Observa-se que as ações dos Programas de Compliance são tradicionalmente voltadas para prevenção e detecção de questões relacionadas a corrupção e fraude, bem como riscos relacionados à imagem e reputação, contudo é possível notar que nos últimos anos questão relacionadas a esses temas mencionados não são a única preocupação dos Programas de Compliance.

Nesse ponto, cabe discorrer que programas de Compliance focados exclusivamente em questões "ABC" ("*anti bribery and corruption*"), ainda que sejam eficazes no atendimento a parâmetros regulatórios –como os que estão definidos no Decreto 11.129/22 e no *Evaluation of Corporate Compliance Programs* do *Department of Justice* dos Estados Unidos ("DoJ") –[7], não atendem suficientemente aos riscos de conduta aos quais as empresas estão expostas caso não considerem o perfil demográfico, bem como, inclusão e acessibilidade como parte de seu Programa. Isso ocorre, uma vez que a sociedade está em constante evolução trazendo novos riscos e novas necessidades de adaptabilidade. Não considerar os elementos expostos acima no Programa é não incluir ferramentas importantes que podem auxiliar em melhorias contínuas e que contribuiriam para mitigar, prevenir e detectar riscos e oportunidades.

Um Programa de Compliance bem estruturado, estabelecido e eficaz possui uma influência na cultura organizacional e na orientação da conduta cotidiana dos colaboradores da organização. É nesse sentido que pode ser observada a relevância dos Programas de Compliance na promoção da inclusão e no combate ao assédio e discriminação, se mostrando como uma forma inteligente de endereçar o tema através de mecanismos eficazes no controle de outros riscos relativos a condutas antiéticas. O Programa de Compliance efetivo é acessível a todos e promove a inclusão; consequentemente, a promoção de ações de inclusão no Programa de Compliance ajuda quebrar barreiras e preconceitos culturais e estruturais, além de mitigar riscos importantes.

Mediante o exposto, de uma forma generalista, um Programa de Compliance bem desenhado se estabelece, incluindo, mas não se limitando, sobre os seguintes elementos: (i) incentivo e exemplos da alta administração e gerência, bem como, promoção de uma cultura de ética, integridade e transparência disseminada em todos os níveis hierárquicos; (ii) avaliação regular e frequente de riscos de Compliance, (iii) políticas e procedimentos que estabeleçam diretrizes de conduta, (iv) treinamentos e comunicação sobre o tema, (v) avaliação do risco e *due diligence* de terceiros e de colaboradores, (vi) canal disponível para denúncias e procedimentos de investigação e (vii) monitoramento e aperfeiçoamento contínuo de processos de Compliance.

Há pontos de inclusão e acessibilidade que podem ser exploradas em cada

7 AMERICA, United States of. "Evaluation of Corporate Compliance Programs". U.S. Department of Justice, 2023. Documento eletrônico disponível em <https://www.justice.gov/criminal-fraud/page/file/937501/download">; acessado em 19 de outubro de 2023.

item enumerado acima. Entretanto, neste breve artigo, será ilustrado algumas ações de Compliance que podem ser realizadas, independentemente do porte da empresa, bem como, localidade, para se ter um Programa mais inclusivo e acessível.

Ações de compliance para acessibilidade e inclusão

Dentre os pilares de um Programa de Compliance, algumas ações e estruturas podem ser implementadas ou revisitadas buscando a melhoria contínua e a promoção da inclusão e acessibilidade. Nessa perspectiva, podem ser destacados os seguintes temas: governança de Compliance, treinamento e comunicação, políticas e canais de denúncia.

Com relação a governança de Compliance, a inclusão pode ser acentuada quando se traz mais diversidade para Comitês e Estruturas de Compliance. Conforme definido pelo IBGC[8], as boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas e contribuem para a qualidade da gestão da organização, sua longevidade e o bem comum.

Como parte da estrutura de governança, os Comitês de Compliance são essenciais para melhoria da gestão organizacional, demonstrar o comprometimento da alta gestão com a ética e a integridade e dar o tom da liderança (*tone at & from the top*). A implementação de Comitês inclusivos que sejam compostos, por exemplo, por diversidade de gênero, orientação sexual, orientação religiosa, étnico racial, de idade e perfis distintos promove que as decisões tomadas no âmbito desses colegiados sejam pautadas em vivências e realidades distintas, tornando, consequentemente, eventuais decisões mais isonômicas. Um Comitê diverso também traz mais legitimidade e realidade, já que diversos perfis podem representar diferentes parcelas de colaboradores dentro de uma empresa. Ou seja, se traz representatividade aos órgãos de governança.

No mais, considerando que a cada dia que passa estamos mais focados em um capitalismo de *stakeholders* e não de *shareholders* (ou seja, estamos cada vez mais olhando para as organizações como um todo, observando o interesse de todos, buscando criar valor a longo prazo ao observar a empresa como um só organismo e com um interesse em comum), trazer mais diversidade para os Comitês e Estruturas de Compliance tende a só agregar a esse conceito atrelado igualmente ao ESG.

Por outro lado, o treinamento e a comunicação também podem ser desenvolvidos à fim de garantir que colaboradores com perfis diversos consigam compreender e se conectar com o conteúdo dos treinamentos e comunicações de Compliance. A título exemplificativo, é possível realizar comunicações por e-mail, em murais (através de impressão física), por vídeos, gibis e até mesmo através da música. Os treinamentos, por exemplo, podem ser "gameficados", ou seja, transformados em jogos para torná-los mais lúdicos, realizados online e virtual, em múltiplas línguas (quando

8 IBGC. "Código das Melhores Práticas de Governança Corporativa – 6° edição". IBGC, 2023. Documento eletrônico disponível em <https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640>, acessado em 19 de outubro de 2023.

aplicável), em "pequenas pílulas", com tradução para libras, com ferramentas de audiodescrição, entre outros. O treinamento e a comunicação de Compliance é essencial para transmitir uma mensagem de ética, transparência e de inclusão. Como já mencionado anteriormente, são essenciais para questionar o *status quo,* trazer mudanças de pensamento e comportamento e para reforçar mensagens positivas.

Já observando as políticas, essas devem ser adaptadas para que todas as pessoas compreendam e tenham acesso ao seu conteúdo. Dentre essas adaptações, destaca-se que políticas e procedimentos precisam estar em um formato que permita o uso de ferramentas de acessibilidade, há necessidade de adaptá-las para que sejam fáceis e compreensíveis independentemente do nível hierárquico da pessoa, e, caso a empresa tenha locais internacionais, devem ser traduzidas para compreensão e inclusão de todos os indivíduos. Acessibilidade também é pensar que nem todos tem acesso à tecnologia, portanto, cópias físicas, quando aplicável ao perfil da empresa, precisam estar disponíveis e encontradas facilmente.

Com relação ao canal de denúncias, é possível criar estratégias que possibilitam o acesso de todos. Como exemplo, para deficientes visuais, criar ou adotar uma ferramenta de "talk-back" / um recurso para "ditar", letras maiores e mais espaçadas, são algumas ações simples que poderiam mudar a acessibilidade do canal. No caso de deficientes de fala ou auditivos, ter um recurso de libras e um *website* facilita o acesso para a denúncia.

Por outro lado, se considerarmos um perfil demográfico diverso, aqueles que não tem acesso a um computador poderiam ter acesso ao canal através de um número de telefone ao qual poderiam ligar. Nesse mesmo ponto, caso não tenham telefone celular ou internet disponível, disponibilizar um computador na empresa para que colaboradores tenham o recurso para usar o canal é fundamental para o incentivo de denúncias.

Da mesma forma, precisa ser considerado o país que o colaborador se encontra e o idioma. Em empresas internacionais, o ideal para garantir a inclusão adequada seria disponibilizar o canal de denúncias na língua materna dos colaboradores, possibilitando que esses se sintam confortáveis para reportar eventuais irregularidades.

Por fim, ressalta-se que o canal de denúncias também é uma ferramenta essencial na identificação de desvios de conduta e eventuais situações e/ou irregularidades que contribuem para uma desmotivação do profissional e que prejudiquem a promoção da inclusão na empresa. Tendo isso em vista, cabe a divulgação do canal de denúncias, ressaltando a não retaliação e a ferramenta como um canal seguro. A inclusão necessariamente implica o respeito, e, caso um colaborador esteja desrespeitando os demais, há que se ter uma ferramenta a qual os indivíduos se sintam seguros para reportar.

A cultura de uma empresa se torna acessível e inclusiva quando está aberta para os *feedbacks* dos colaboradores, bem como, ideias e sugestões. Ela se torna inclusiva, por exemplo, quando são incentivadas denúncias de irregularidades; se tem um procedimento para investigações imparciais e confidenciais/sigilosas, atribuindo confiança ao canal; se tem

políticas e procedimentos acessíveis e inclusivas; treinamentos e comunicações adaptáveis entre outros. São pequenas adaptações que podem ser realizadas e que fariam uma diferença imensurável para muitos profissionais.

Considerações finais – os benefícios de um programa de compliance acessível para todos

Diante do exposto, observar-se que a inclusão e acessibilidade, portanto, devem ser aliadas ao Programa de Compliance, tendo em vista os benefícios que uma cultura de diversidade pode trazer às empresas, bem como aos seus colaboradores. Investir em inclusão e acessibilidade, para que todos os colaboradores tenham o devido acesso e entendimento dos principais pilares que compõem o Programa, promove um maior engajamento, mitigação de riscos como um todo, além de aprimorar a efetividade e alcance do Programa.

Há que ressaltar, que se está investindo no sentimento de pertencimento da empresa, como também, assegurando que a Ética e o Compliance estão sendo devidamente permeados em todos os níveis hierárquicos. Além dos benefícios para a cultura de Compliance, pode-se mencionar também as vantagens para a produtividade, lucro e qualidade das decisões de negócio para as empresas que times de profissionais com diversidade acrescentam positivamente.

É papel daqueles que executam o Programa de Compliance trabalhar para que o Programa seja inclusivo para todos. Essa acessibilidade é intrínseca para que possamos continuar evoluindo e para que o Programa seja efetivo e continue agregando de forma positiva na cultura organizacional. Por isso, mediante todo o exposto neste artigo, quando for realizado o planejamento das prioridades de ações dos próximos anos de Ética e Compliance, espera-se que mais empresas tenham a conscientização sobre o tema e que coloquem em primeiro plano medidas que trazem inclusão e acessibilidade a todos.

BIBLIOGRAFIA

AMERICA, United States of. “Evaluation of Corporate Compliance Programs”. U.S. Department of Justice, 2023. Documento eletrônico disponível em <https://www.justice.gov/criminal-fraud/page/file/937501/download”>; acessado em 19 de outubro de 2023.

ATHAYDE, Bruno. “Deficientes bem preparados são nivelados por baixo”. Exame, 2013. Documento eletrônico disponível em <https://exame.com/carreira/pra-cumprir-tabela/>; acessado em 17 de outubro de 2023.

BRASIL. Decreto Nº 11.129, de 11 de julho de 2022. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. Brasília, DF: Diário Oficial da União, 2022.

BRASIL. Lei Nº 12.846, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Brasília, DF: Diário Oficial da União, 2013.

DIXON-FYLE, Sundiatu. Et al. “Diversity wins: How inclusion matters”. McKinsey & Company, 2020. Documento eletrônico, disponível em <https://www.mckinsey.

com/~/media/mckinsey/featured%20insights/diversity%20and%20inclusion/diversity%20wins%20how%20inclusion%20matters/diversity-wins-how-inclusion-matters-vf.pdf> ; acessado em 01 de outubro de 2023.

IBGC. "Código das Melhores Práticas de Governança Corporativa – 6° edição". IBGC, 2023. Documento eletrônico disponível em <https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640>, acessado em 19 de outubro de 2023.

LARSON, Erik. "New Research: Diversity + Inclusion = Better Decision Making At Work". Forbes, 2017. Documento eletrônico disponível em <https://www.forbes.com/sites/eriklarson/2017/09/21/new-research-diversity-inclusion-better-decision-making-at-work/?sh=7efoba3d4cbf >; acessado em 01 de outubro de 2023.

MELO, Emerson. Et al. "Pesquisa de Maturidade do Compliance no Brasil". KPMG, 2021. Documento eletrônico disponível em <https://www.editoraroncarati.com.br/v2/phocadownload/KPMG-pesquisa-maturidade-compliance-2021.pdf>; acessado em 19 de outubro de 2023.

Parte II
Proteção de dados pessoais e medidas de prevenção e combate à lavagem de dinheiro

CECÍLIA CHOERI COELHO

MAIRA F. MARTELLA

RENATA F. ANDRADE

O texto foi organizado por Renata Fonseca de Andrade, Maira Martela e Maria Cecilia Choeri. A coordenadora do grupo PLD, Maira Martella, organizou o texto a partir de contribuições e debates ocorridos com 18 integrantes do Comitê de PLD em coautoria com Renata Fonseca de Andrade e Cecilia Choeri, do Comitê de Proteção de Dados e Privacidade, do CWC – Compliance Women Committe.

Cecília Choeri Coelho: Advogada, sócia de Chediak Advogados. Doutora e mestre em Direito pela UERJ. Certificada em Compliance pela SCCE (CCEP-I). Especialista em Lei e Tecnologia (Universidade da Califórnia – Berkeley). Professora de diversas instituições e autora de artigos e capítulos de livros em temas de Compliance e proteção de dados.

Maira F. Martella: Advogada sócia da prática de Forense/FinCrime da Deloitte, com vasta experiencia em combater Crimes Financeiros e Fraude bem como realizar a prevenção à Corrupção e Lavagem de Dinheiro (ABAC/PLD), Fraudes Bancárias, investigações corporativas, recuperação de ativos nos mercados americano, europeu, africano e latino com foco em negócios, inovação e tecnologia. Coautora das seguintes publicações:- Guia Prático de Compliance: Conheça seu Robo – como aplicar a inteligência artificial aos pilares de Compliance, PLD e fraude; disponível pela Editora Gen/Forense; Série Mulheres: Compliance na Prática disponível pela Editora Volumes 1 e 2; e, CWC Compliance: artigo sobre Compliance e suas Origens – O contínuo impacto no Brasil do sistema norte-americano de combate à corrupção.

Renata F. Andrade – Advogada, conselheira administrativa, Certificada CCA/IBGC, Board Member at BoostInnovations AI. Diretora de Compliance e Proteção de Dados, Mestre pela University of Wisconsin-Madison School of Law, LLM-MLI USA (2006). Bacharel em Ciências Jurídicas e Sociais pela Faculdade de Direito da Universidade Mackenzie (1989) e especialização em Governo pela Escola de Governo, prof. Fábio Konder Comparato (2000). Presidente da Comissão de Anticorrupção e Compliance da OAB/SP Pinheiros. Especialista em Anticorrupção e Compliance, professora, realiza Seminários e Treinamentos Ativos nas áreas da Governança e Ética, Compliance, Relações Governamentais, Contratos, Mitigação de Riscos, Implementação de Programas de Compliance em atendimento à Legislação Anticorrupção (FCPA, UK Anti-Bribery Act e Lei Brasileira 12.846/2013), com ênfase na revisão e melhoria contínua de programas, sistemas e procedimentos, na mitigação de riscos legais, regulatórios e reputacionais. Professora em cursos de extensão na FECAP, LEC, IARC, ESENI, Professora em LLM e Pós Graduação das escolas de Direito da Universidade Mackenzie e Damásio-SP. Publicações: Manual de Compliance IARC, 2017; "Do Combate à Improbidade Administrativa", Ed. Almedina; "Direito, Cidadania e Compliance, Ed. Revista dos Tribunais, 2019; "Diretrizes do Compliance Financeiro", Ed. LEC, 2019; "Compliance em Perspectiva", Ed. D'Placido, 2019; Artigos publicados pela Ed. Roncarati e Revista LEC.

Introdução

O movimento de inclusão financeira digital ocorrido nos últimos anos trouxe benefícios a milhões de cidadãos no Brasil e no mundo, mas também revelou desafios e riscos. Nesse novo cenário, é crescente a preocupação com privacidade, criminalidade e segurança cibernética. São efeitos não intencionais da digitalização financeira, que envolvem o uso, necessariamente, de dados pessoais dos cidadãos.

Por essa razão, a preocupação com esses temas é mundial, e se dá sob diferentes lentes. Discussões sobre as conexões e desafios envolvendo prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo e da proliferação de armas de destruição em massa (PLD/FTP) e a temática da proteção de dados têm sido recorrentes nos fóruns mundiais e brasileiros, como no âmbito do Grupo de Ação Financeira (GAFI) – entidade que orienta ações de PLD/FTP para cerca de 200 jurisdições em todo o mundo. No Brasil, o Conselho de Controle de Atividades Financeiras (COAF), o Banco Central do Brasil (BC), a Comissão de Valores Mobiliários (CVM) e a Agência Nacional de Proteção de Dados (ANPD), bem como o setor privado e a academia, entre outros *stakeholders*, discutem com crescente interesse os possíveis conflitos entre essas legislações, medidas regulatórias e recomendações sobre as melhores práticas.

O cerne das discussões está em harmonizar as legislações e regulações emanadas por esses organismos e instituições sobre dois temas que parecem por vezes se contrapor, de forma a preservar os

bens jurídicos tutelados. Grosso modo, enquanto para fins de PLD/FTP o foco é no elemento coletivo e a regra de base é "quanto mais informações, melhor" (para a prevenção e o combate), para a proteção de dados, o foco está no elemento individual, de privacidade, e na restrição ao uso de informações. Em outras palavras, temos, em primeiro lugar, o aparente conflito, ou o necessário equilíbrio, entre transparência e privacidade, que envolve a disponibilização de informações pessoais.

Nesse contexto, um ponto crucial para PLD/FTP é a identificação do beneficiário final dos clientes que operam no sistema financeiro. A identificação de quem está por trás das operações das empresas é ponto crucial para se chegar aos criminosos que se utilizam do sistema financeiro para cometer os crimes. Esconder-se atrás de empresas ou entidades que possuem estruturas que dificultam a correta identificação dos criminosos é uma prática mundial. Por isso, igualmente, é uma recomendação do GAFI que os dirigentes das empresas e entidades sejam identificados, ainda que informalmente. A depender da forma como é realizada, a busca pela identificação do beneficiário final pode ser considerada uma interferência nos direitos da vida privada e da disposição de dados pessoais, entre eles renda, rendimentos, residência, assim como outros dados de identificação e/ou qualificação, essenciais para as análises de riscos e eventual identificação de irregularidades.

O esforço mundial pela identificação dos beneficiários finais das empresas que atuam no sistema financeiro está no centro das discussões envolvendo as questões de PLD/FTP e proteção de dados, mas não é o único ponto de tensão. Outro aspecto que vem levantando discussões e preocupações está no compartilhamento de dados pessoais e transacionais no caso de fraudes e golpes. O compartilhamento de dados, de forma geral, e seu uso, estão intrinsicamente ligados às questões de proteção de dados.

Outro ponto frequentemente discutido é a necessidade de consentimento na utilização de dados pessoais – e que pode perpassar tanto as questões de beneficiários finais quanto de fraudes e golpes, entre outros. Os defensores de linhas mais duras em PLD/FTP alegam que o consentimento raramente será obtido daqueles que intencionalmente visam a prática de crimes dessa natureza e que, por essa razão, a exigência de consentimento para qualquer utilização de dados pessoais e transacionais acabaria por impedir a efetividade e a tempestividade do combate aos crimes aqui discutidos, ou mesmo impossibilitar sua prevenção. Como, nessa hipótese, caberia ao cidadão a faculdade de alterar ou deletar seus dados pessoais, num extremo, a alteração em dados poderia dificultar, encobrir ou camuflar o caminho do dinheiro sujo e suas origens.

Como se esses pontos acima não fossem suficientes para erguer desafios ao tema aqui proposto, temos uma complexidade adicional quando entramos nas legislações, regulações e boas práticas sobre os assuntos. As fronteiras dessas regras e diferenças de maturidade e robustez não podem ser ignoradas. Regras de PLD/FTP possuem um componente de globalidade muito forte, pois as recomendações do GAFI são seguidas

como normas pelos seus países membros (ou deveriam ser seguidas, na maior medida possível). Já em termos de proteção de dados, não há um organismo que detenha um *enforcement* similar, e as legislações nacionais, embora sigam princípios mundiais, diferem muito de uma jurisdição para outra.

No mesmo sentido, são diferentes os graus de maturidade das legislações e regulações sobre os temas. Tomemos o Brasil como exemplo: enquanto somos parte do GAFI desde 2000, com uma 'Lei de Lavagem de Dinheiro' promulgada em 1998 (Lei 9.613/1998), a Lei Geral de Proteção de Dados (LGPD) veio duas décadas depois, com a promulgação da Lei 13.709/2018. Essa diferença de maturidade traz, por si só, assincronias e debates sobre suas aplicações, interpretações e entendimentos.

Todos esses pontos são relevantes e importantes – e em que pesem sejam desafiadores, não podemos nos furtar de seguir discutindo o impacto para as autoridades públicas, instituições privadas e, principalmente, para o cidadão.

É fundamental estressar discussões sobre a existência de real conflito sobre esses aspectos; eventual supremacia, por importância ou riscos implicados, de algum deles sobre o outro; possibilidade da adoção plena dos princípios de cada um deles, ou necessidade de flexibilização e abordagem nuançada; uso e destinação dos dados e relevância relativa do bem jurídico tutelado, entre outros.

E, claro, para avançarmos, é necessário que possamos aprender uns com os outros, entre diferentes jurisdições e instituições, para que as perspectivas se complementem. Para que cidadão e sociedade saiam ganhando, é fundamental estabelecer sinergias e conexões entre os fóruns internacionais, reguladores, supervisores e instituições afetadas pelas referidas legislações e regulações.

É nesse contexto que esse *whitepaper* se insere e para cujas discussões se pretende contribuir.

Arcabouço legal da prevenção à lavagem de dinheiro nas instituições financeiras

As diretrizes internacionais para a prevenção à lavagem de dinheiro (PLD) começaram a ser definidas na Convenção de Viena em 1988. No Brasil, a Lei nº 9.613 de 1998 foi um marco inicial, focando inicialmente no tráfico de entorpecentes. Desde então, a legislação e as normas regulatórias evoluíram e, no caso das instituições autorizadas a funcionar pelo Banco Central do Brasil, merecem atenção a Circular do Banco Central do Brasil nº 3.978, de 23 de janeiro de 2020 com ênfase no capítulo IX e a Carta Circular do Banco Central do Brasil, nº 4.001, de 29 de janeiro de 2020.

O arcabouço regulatório brasileiro exige que as pessoas obrigadas, descritas no artigo 9º, da Lei 9.613/98 (Lei de Lavagem de Capitais), implementem mecanismos robustos para prevenir, detectar e comunicar situações de risco de lavagem de dinheiro e financiamento ao terrorismo, a exemplo da criação de áreas específicas de governança de PLD-FT e o monitoramento de Pessoas Expostas Politicamente (PEP). A governança normativa abrange desde a identificação e

monitoramento de transações suspeitas até a comunicação obrigatória ao Conselho de Controle de Atividades Financeiras (COAF).

No âmbito do Sistema Financeiro Nacional, há algumas categorias principais de obrigações e responsabilidades relacionadas a PLD/FT, emanadas das próprias leis de base sobre o tema – Leis nº 9.613/1998 e nº 13.260/2016, e da regulamentação posta pelo Banco Central do Brasil (Circular nº 3.978/2020; Carta Circular nº 4.001/2020, entre outros normativos). Mencionem-se apenas 4 (quatro) dessas categorias:

1. obrigações gerais de "conhecer seu cliente", com captação e manutenção atualizada de dados cadastrais, identificação, qualificação e classificação de perfil econômico e dos riscos desses clientes relacionados a PLD/FT (Lei 9.613/1998, artigo 10; Circular 3.978/2020, artigos 1º, 10, 13, 16, 18 e 20);
2. obrigações de exercer "devida diligência" sobre as operações de clientes, em cotejamento com seu perfil econômico e com os produtos utilizados, também avaliados pelo risco (Lei 9.613/1998, artigo 11; Circular 3.978/2020, artigos 13, 38 a 46; Carta-Circular 4.001/2020);
3. obrigações de informar operações suspeitas ou atípicas à Unidade de Inteligência Financeira, o Conselho de Controle de Atividades Financeiras (Coaf) (Lei 9.613/1998, artigo 11; Circular 3.978/2020, artigos 48 e 50, e Carta-Circular 4.001/2020);
4. outras obrigações de monitoramento, remessa de informações, bloqueio ou constrangimento por força de comandos legais, judiciais, administrativos, ou de organismos com funções de vigilância sobre o tema.

Nas instituições financeiras, o combate à lavagem de dinheiro e ao financiamento ao terrorismo exige que sejam observadas alguns pilares fundamentais:

1. **Início de Relacionamento:** Identificação: Coleta e validação de informações básicas do cliente, confrontando com dados públicos e privados.

   - Qualificação: Verificação das informações compatíveis com o perfil de risco do cliente e a natureza do negócio, utilizando serviços de tecnologia que atualizam diariamente listas de PEP, tribunais e mídias desabonadoras.
   - Classificação: Segmentação dos clientes em categorias de risco (alto, médio, baixo, imaterial) baseada nas informações obtidas e no apetite ao risco da instituição.

2. **Monitoramento de Operações:** conforme o disposto na Circular 3978, as instituições financeiras devem implementar políticas e diretrizes que busquem coibir as práticas de lavagem de dinheiro e financiamento do terrorismo. Para tanto, é necessário identificar os clientes, classificar e monitorar as operações, sendo as

principais diretrizes relacionadas aos seguintes temas:

- Da coleta, verificação, validação e atualização de informações cadastrais, visando a conhecer os clientes, os funcionários, os parceiros e os prestadores de serviços terceirizados;
- Do registro de operações e de serviços financeiros;
- Do monitoramento, seleção e análise de operações e situações suspeitas;
- Da comunicação de operações ao Conselho de Controle de Atividades Financeiras (Coaf);
- Implementação de regras e controles para identificar transações atípicas e inconsistentes, considerando perfil econômico, valor transacionado e exposição negativa em mídia;
- Investimento em sistemas que geram alertas para movimentações suspeitas, facilitando a identificação de atividades ilícitas.

3. **Tratamento dos Alertas** – situações suspeitas devem ser analisadas, envolvendo diligências sobre as partes e transações, e fundamentação econômica para a elaboração de pareceres. O prazo máximo para conclusão das investigações é de 45 dias.
4. **Avaliação Interna de Risco (AIR)** – as empresas devem realizar uma avaliação interna de risco, identificando e avaliando os potenciais riscos de lavagem de dinheiro em suas operações.
5. **Abordagem Baseada em Risco (ABR)** – as empresas devem adotar uma abordagem baseada em risco para qualificar os clientes e parceiros.
6. **Política e procedimentos e controles internos** – Implementação de políticas, procedimentos e controles internos robustos para prevenir e detectar atividades suspeitas de lavagem de dinheiro.
7. **Comunicações ao COAF** – estabelecimento de mecanismos para reportar informações relevantes ao Conselho de Controle de Atividades Financeiras (Coaf) de acordo com as normas expedidas pelo Poder Executivo.

Prevenção à fraude no setor financeiro

Nos últimos anos, as inovações tecnológicas e um vasto arcabouço regulatório têm transformado significativamente a forma como as instituições financeiras enfrentam a prevenção a fraudes. A digitalização trouxe facilidades, mas também complexidade e novos desafios para identificar e validar informações dos clientes. A abertura de relacionamentos de forma majoritariamente digital exige que as instituições financeiras implementem camadas robustas de segurança desde o início do relacionamento com o cliente, até o monitoramento contínuo das transações.

INÍCIO DE RELACIONAMENTO

Na maioria das vezes, os clientes iniciam seu relacionamento com instituições

financeiras através de aplicativos de smartphones. Estes aplicativos proporcionam uma jornada intuitiva, onde os clientes preenchem cadastros, anexam documentos e tiram selfies para validação. Após o envio, um complexo sistema de prevenção a fraudes entra em ação, utilizando tecnologias avançadas e bases de dados especializadas para verificar a veracidade das informações fornecidas.

A verificação cadastral utiliza uma combinação de dados públicos e privados para avaliar o comportamento e a reputação digital do consumidor. Quanto mais dados forem coletados e confrontados, melhor será a precisão na validação das informações. Além disso, a autenticação de documentos e a vinculação da selfie ao conjunto de dados cadastrais ajudam a reduzir o risco de fraude, garantindo que apenas clientes legítimos iniciem o relacionamento.

MONITORAMENTO TRANSACIONAL CONTÍNUO

Após a fase de onboarding, o cliente começa a realizar transações financeiras que precisam ser monitoradas continuamente. Este monitoramento visa proteger tanto o cliente quanto a instituição contra fraudes e golpes. Fraudes ocorrem quando terceiros conseguem acessar e movimentar a conta do cliente sem seu envolvimento. Golpes, por outro lado, geralmente envolvem engenharia social, onde o cliente é induzido a fornecer suas credenciais ou realizar transações fraudulentas.

Para prevenir tais incidentes, as instituições implementam sistemas de monitoramento transacional que avaliam cada transação em tempo real. Estas avaliações utilizam um conjunto de regras e algoritmos para decidir sobre a continuidade da transação. Um exemplo clássico é a aprovação de uma transação de cartão de crédito em milissegundos, onde qualquer atraso pode impactar negativamente a experiência do cliente.

INTERSECÇÃO ENTRE PREVENÇÃO A FRAUDES E PLD-FT

Embora as áreas de prevenção a fraudes e PLD-FT operem de forma distinta, elas compartilham objetivos comuns no início do relacionamento com o cliente. Ambas as áreas utilizam verificações cadastrais para garantir a correta identificação e classificação de risco. No monitoramento transacional, fraudes confirmadas são relevantes para a área de PLD, permitindo uma análise mais rápida e eficaz.

Para maximizar a eficiência, é recomendável a integração de sistemas que compartilhem alertas automaticamente entre as áreas, evitando dependências de processos manuais. A colaboração entre as equipes através de reuniões regulares e comissões é essencial para criar uma cultura de proximidade e troca de informações.

O regulador tem incentivado essa integração, destacando a importância de ambas as áreas trabalharem juntas para fortalecer o combate aos crimes financeiros. A sinergia entre prevenção a fraudes e PLD-FT não só aumenta a eficácia dos controles internos, mas também assegura o cumprimento das normas regulatórias, proporcionando um ambiente mais seguro para as operações financeiras.[1]

1 Texto escrito e elaborado por: Zélia Souza e Raíssa Sanguinetti.

O problema da identificação do Beneficiário Final

A identificação do beneficiário final de uma pessoa jurídica se insere no universo amplo de obrigações relacionadas à devida diligência sobre clientes, que inclui sua identificação, qualificação e classificação conforme riscos. Nesse sentido, a qualificação do cliente pessoa jurídica inclui a análise da cadeia de participação societária até a identificação da pessoa natural caracterizada como seu beneficiário final. Isso porque o conceito de beneficiário final é central nos esforços globais de combate aos crimes financeiros, sobretudo de crimes tributários e de lavagem de capitais. O beneficiário final de uma estrutura em geral possui uma influência significativa sobre uma companhia, exercendo seu poder de decisão sobre os negócios da companhia de forma direta ou indireta, por meio de uma cadeia de participações e/ou controle societário. Além disso, é ele quem, em última instância, se beneficia dos seus ativos. A regulamentação em torno do tema tem por objetivo "descascar" as múltiplas camadas de participação e controle de uma estrutura com o objetivo de revelar a verdadeira natureza e identidade do beneficiário final.

O conceito de beneficiário final é, portanto, de suma importância para combater o crime financeiro pois traz a transparência necessária para conhecer uma empresa, sua composição societária e todas as pessoas físicas que possuem controle até a última instância, mesmo que não seja um representante legal da empresa, ou que não seja diretamente responsável pela administração. Este mecanismo visa evitar a ocultação de acionistas e, consequentemente, facilitar o combate a crimes financeiros.

De acordo com as Recomendações do FATF (Financial Action Task Force), o beneficiário final é qualquer indivíduo que possua ou controle mais de 25% da empresa ou que exerça o controle por meio de outros meios, como influência significativa ou controle sobre a gestão da empresa.

No Brasil, o conceito de beneficiário final surge a partir de regras do Bacen e é amplamente utilizado por outros órgãos reguladores como SUSEP e CVM, sendo os normativos mais atuais a Resolução Bacen nº 3978/2020, a Circular SUSEP nº 612/2020[2], a Resolução CVM nº 50[3] e a Instrução Normativa (IN) RFB nº 2119/2022, que manteve o conceito de beneficiário final como sendo:

(i) a pessoa natural que, em última instância, de forma direta ou indireta, controla ou influencia significativamente a entidade; ou

(ii) a pessoa natural em nome da qual uma transação é conduzida.

Considera-se haver influência significativa quando a pessoa natural, ainda que sem controlar a entidade:

(a) detém mais de 25% do seu capital social ou direitos de voto, direta ou indiretamente; ou

2 (*) Circular SUSEP nº 612/2020: "pessoa natural ou pessoas naturais que, isoladamente ou em conjunto, de forma direta ou indireta, possui(em), controla(m) ou influência(m) significativamente uma pessoa jurídica ou outro tipo de estrutura análoga

3 RESOLUÇÃO CVM Nº 50, DE 31 DE AGOSTO DE 2021: pessoa natural ou pessoas naturais que, em conjunto, possuam, controlem ou influenciem significativamente, direta ou indiretamente, um cliente em nome do qual uma transação esteja sendo conduzida ou dela se beneficie;"

(b) atuando individualmente ou em conjunto, direta ou indiretamente, detém ou exerce a preponderância nas suas deliberações sociais e o poder de eleger a maioria dos seus administradores.

Atualmente, o Brasil utiliza pelo menos dois mecanismos para garantir que as informações de beneficiários finais de pessoas jurídicas estejam disponíveis às autoridades competentes:

1. Cadastros mantidos por Instituições Financeiras (IF) e atividades e profissões não-financeiras designadas (APNFD): quando uma pessoa jurídica tem um relacionamento com uma IF ou APNFD, tais instituições devem identificar e tomar medidas razoáveis para verificar a identidade dos beneficiários finais de seus clientes que são pessoas jurídicas. Embora não seja obrigatório que uma PJ mantenha relacionamento com uma IF/APNFD, a maioria das pessoas jurídicas o faz, por exemplo, mantendo um relacionamento bancário para uso de uma conta corrente. Nesses casos, a Lei 9.613 (artigo 10) e a Circular BCB 3.978/2020 (artigos 28 e 67) estabelecem, para as instituições financeiras, a obrigatoriedade de manutenção de registros de transações, produtos e serviços contratados por um período de mínimo de dez anos, à disposição do Banco Central, o que compreende a identificação e qualificação de clientes, inclusive a informação sobre BFs.
2. Cadastro de CNPJ da Receita Federal do Brasil: as pessoas jurídicas devem identificar seu beneficiário final no Cadastro do CNPJ (Instrução Normativa da Receita Federal – IN RFB nº 2119/2022, artigo 4º). As pessoas jurídicas também devem registrar as pessoas autorizadas a representá-las, bem como a cadeia de participação societária até atingir as pessoas físicas caracterizadas como beneficiários finais. A IN n. 2119/2022 determina um prazo de 30 dias para entidades domiciliadas no Brasil e no exterior informarem seus beneficiários finais após a inscrição no CNPJ. A não apresentação dessas informações pode resultar na suspensão do CNPJ e no impedimento de realizar transações bancárias, como movimentação de contas correntes, aplicações financeiras e obtenção de empréstimos. Além disso, a IN n. 2119/2022 determina que o organograma da cadeia societária deve incluir informações detalhadas de cada integrante, como nome empresarial, país de origem, número de identificação fiscal e a identificação da pessoa natural beneficiária final ou a declaração da inexistência de tal pessoa. Este organograma deve ser registrado no órgão competente do país de origem ou assinado pelo representante legal da entidade estrangeira no Brasil.

Segundo o Relatório de Avaliação Mútua do Brasil pelo GAFI, publicado em

dezembro/2023, os maiores desafios para a adequada identificação dos beneficiários finais e o compartilhamento dessas informações em prol da necessária transparência para o eficiente combate a práticas ilícitas no Brasil são:

Não obrigatoriedade de identificação do beneficiário final para a maioria das PJs: Como mencionado acima, as pessoas jurídicas são obrigadas a fornecer informações de BF à Receita Federal do Brasil desde 2018. No entanto, há dispensa de prestação da informação para algumas entidades, partindo do pressuposto que suas informações já são públicas ou que seus titulares ou sócios mais influentes já são seus beneficiários finais. Isso se aplica, por exemplo, a empresas de capital aberto, empresários individuais e sociedades integradas exclusivamente por sócios pessoa física, em que pelo menos um deles possua mais de 25% do capital social.[4] Assim, cerca de 21 milhões de entidades (de um universo de cerca de 23 milhões) estão isentas de enviar informações de beneficiário final, principalmente com base em critérios de propriedade, ou seja, quando pessoas físicas possuem uma empresa por participação de mais de 25%, direta ou indiretamente. Nesse sentido, o número de entidades isentas, em relação ao universo de pessoas jurídicas é bastante relevante, especialmente quando atrelado à pouca ênfase na determinação dos graus de controle ou riscos específicos de PLD/FT.

Dificuldade de verificação das informações declaradas pelas empresas à RFB: Enquanto o Brasil assume que empreendedores individuais são os presumidos beneficiários finais, as autoridades competentes não têm mecanismos para avaliar se o elemento de controle está presente nessas e em outras naturezas jurídicas, a menos que haja uma investigação ativa, ou para monitorar suas atividades de acordo com as vulnerabilidades identificadas.

Dificuldade na completa identificação de BFs pelas IFs: Embora a compreensão dos requisitos de BF seja melhor em IFs de maior porte, a coleta de informações de BF continua a demandar melhorias. Algumas entidades obrigadas apresentam dificuldades em acessar informações precisas sobre o beneficiário final, além daquelas declaradas pelo cliente. Além disso, as IFs estão muito focadas em identificar o BF por meio da propriedade, e menos conscientes da necessidade de verificar o controle. Algumas IF implementam mecanismos de mitigação e melhores práticas para enfrentar esses desafios, solicitando documentos notariais adicionais, realizando visitas às dependências de entidades jurídicas e buscando acesso às bases de dados disponíveis, para comprovação e verificação cruzada.

Dificuldade no acesso a informações completas sobre os BFs por autoridades competentes: O principal instrumento disponível no Brasil atualmente é o registro de pessoas jurídicas do CNPJ, que inclui informações sobre todas as empresas que operam no país. Como visto, as pessoas jurídicas registradas no CNPJ devem declarar informações de beneficiário final à RFB, porém a maioria das empresas que operam no Brasil não adotam uma abordagem baseada em risco

4 BRASIL (Brasil). Domingues e Pinho. Beneficiários Finais: entenda como funciona essa obrigação. Artigo, [S. l.], 19 set. 2023. 1-1, p. 1-1. Disponível em: https://www.dpc.com.br/beneficiarios-finais-como-funciona/. Acesso em: 27 jun. 2024.

MATRIZ DE RISCO FOCADA NA TRANSPARÊNCIA DO BENEFICIÁRIO FINAL

Legal person or arrangement	Incorporation and dissolution	Identification, responsibility and rights of partners, quota holders and administrators	Transparency and control mechanisms	Beneficial Owner transparency	Vulnerability level
Joint venture partnerships	4,85	4,75	4,95	4,95	4,85
Closed joint-stock company	2,77	4,09	4,23	4,41	3,91
Limited Partnership by Shares	1,82	3,73	2,68	4,00	2,45
Football Anonymous Society	1,40	2,10	2,30	2,65	2,48
Association	2,06	2,17	3,11	2,39	2,62
Limited Liability Company	2,82	1,73	3,41	2,09	3,09
EIRELI	2,64	1,09	3,41	1,86	2,80
Individual Entrepreneur	3,45	2,14	3,23	1,82	3,52
Cooperative	1,18	1,50	2,14	1,77	1,82
Open joint-stock company	1,09	1,45	1,45	1,64	1,27
Foundation	1,13	1,69	1,38	1,63	2,63
Simple Partnersip	2,11	1,39	2,39	1,50	1,92
Limited Partnership	1,41	1,41	1,50	1,50	1,41
General Partnership	1,50	1,45	2,41	1,45	2,00
Simple Credit Company	1,50	1,23	1,86	1,41	2,43

Very low	Low	Medium	High	Very high
1,0 a 1,5	1,5 a 2,5	2,5 a 3,5	3,5 a 4,5	4,5 a 5

Fonte: 2023 FATF/OECD -GAFILAT (2023), Anti-money laundering and counter-terrorist financing measures – Brazil, Fourth Round Mutual Evaluation Report, FATF, Paris https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Mutualevaluations/Mer-Brazil-2023.html.

e, na prática, as informações de beneficiário final não são declaradas sistematicamente. Soma-se a isso a dificuldade das autoridades de obter informações de BF de sociedades anônimas e empresas estrangeiras. Além disso, as informações declaratórias de BF mantidas pela RFB estão sujeitas a sigilo fiscal, ou seja, não constam dos dados públicos disponibilizados pelo acesso geral à base de CNPJ e somente podem ser acessadas por autoridades competentes mediante ordem judicial, ou no contexto de investigações compartilhadas com a RFB, o que nem sempre garante a tempestividade.

Para exemplificar as dificuldades impostas pelas complicadas estruturas societárias na identificação de seu beneficiários final, a tabela a seguir apresenta resultado de estudo realizado no âmbito da ação 02/2022 da ENCCLA, que teve por objetivo avaliar o nível de risco de diferentes estruturas, a fim de diagnosticar os desafios e propor medidas para melhorar os requisitos de identificação do beneficiário final de acordo com a Recomendação 24 do GAFI – Transparência e Propriedade Corporativa.

Vale lembrar que, embora no Brasil a formação de empresas tenha sido simplificada nos últimos anos para facilitar os negócios, existem vários tipos de pessoas jurídicas que podem ser criadas de acordo com o Código Civil e legislações específicas, como a Lei das Sociedades Anônimas (nº 6.404/1976), a Lei sobre Sociedade Anônima de Futebol (nº 14.193/2021), a Lei sobre Cooperativas (nº 5.764/1971) e a Lei Complementar sobre Empreendedor Individual e Microempresários (nº 123/2006). Os principais tipos de pessoas jurídicas no Brasil são sociedades anônimas (S/A), criadas nos termos da Lei nº 6.404/1976, sociedades limitadas (Ltda), microempreendedor individual (MEI), sociedade individual (EIRELI), empresário Individual (EI), sociedade limitada unipessoal (SLU), sociedade em comandita por ações, além de parcerias, sociedades sem fins lucrativos e empresas que não adquirem personalidade jurídica, como sociedades em conta de participação (SCP).[5]

5 REIS, TIAGO. Pessoa Jurídica: entenda o que é e quais são os tipos de PJ no Brasil. Suno Artigos, [S. l.], p. 1-1, 27 ago. 2019. Disponível em: https://www.suno.com.br/artigos/pessoa-juridica/. Acesso em: 26 jun. 2024.

O Brasil tem feito esforços no sentido de simplificar e padronizar os procedimentos de registro de pessoas jurídicas, com destaque para a implementação da Redesim, que envolve a União, os 26 Estados e o Distrito Federal e os Municípios. A integração dos sistemas por meio da Redesim visa permitir a simplificação de procedimentos de registro, tanto empresarial quanto civil, e o atendimento às demais exigências administrativas e de natureza tributária, nos diferentes níveis da Federação.

Vale lembrar que o Brasil é membro do GAFI/FATF desde 1999 e passou por avaliações em 2000, 2004, 2010 e recentemente no final de 2023. Nesta última avaliação, o GAFI destacou que o Brasil deve continuar com os avanços e investimento no processo de identificação de pessoas, visto que um dos pontos de atenção é em relação ao risco devido às lacunas existentes no quadro jurídico e a algumas restrições no acesso à informação, que apesar dos esforços realizados até então não foram suficientes para saná-las.

O resultado imediato (RI) sobre a efetividade dos controles relacionados a pessoas e arranjos jurídicos foi classificado como moderado. Devido à estrutura existente, que depende muito dos dados disponíveis no banco de dados do CNPJ, o entendimento e a aplicação dos requisitos de beneficiário final são fortemente influenciados pelo conceito de propriedade e não de controle. Foi destacado que embora as autoridades competentes brasileiras coletem e processem informações básicas que estão publicamente disponíveis e acessíveis a todos, o acesso às informações declaratórias do beneficiário final à RFB é limitado pelos seguintes motivos:

(a) devido ao número reduzido de entidades que são obrigadas a declará-las; e
(b) devido à sua classificação como sigilo fiscal, o que significa que só está disponível por meio de ordem judicial ou no contexto de investigações conjuntas.

Apesar de existirem procedimentos notarizados e autenticação digital para assegurar a precisão das informações declaradas à Receita Federal do Brasil (RFB) e no Cadastro Nacional da Pessoa Jurídica (CNPJ), o Brasil ainda está em processo de aprimoramento da qualidade e integridade dos dados. As sanções por violações de conformidade são consideradas insuficientes, e os esforços para aumentar a precisão ainda são iniciais.[6]

6 Como forma de contribuir para o debate, apresentamos a seguir algumas recomendações para garantir a transparência das pessoas jurídicas e o acesso às informações sobre beneficiários finais (BF) por autoridades competentes no Brasil:
- Melhorar o entendimento do conceito de BF: As autoridades e entidades reguladas devem ter um conhecimento aprofundado sobre o conceito de beneficiário final.
- Revisão baseada em riscos: As isenções para declarar informações de BF à Receita Federal do Brasil (RFB) devem ser avaliadas e atualizadas periodicamente, com base em análises de risco.
- Aprimoramento dos mecanismos da RFB: A RFB deve melhorar os mecanismos para assegurar que as informações básicas e de BF sejam completas, precisas e atualizadas, aplicando sanções em casos de não conformidade.
- Recursos para a RFB: Devem ser alocados recursos humanos e de tecnologia da informação (TI) suficientes para permitir o monitoramento constante e a atualização dos bancos de dados do CNPJ e da RFB.
- Acesso tempestivo às informações de BF: As autoridades competentes devem ter acesso em tempo hábil às informações de BF para fins de inteligência e investigação, reexaminando até que ponto as informações do BF devem ser protegidas por sigilo fiscal.

Essas medidas são essenciais para fortalecer a integridade do sistema financeiro e prevenir o uso indevido das estruturas corporativas para atividades ilícitas como lavagem de dinheiro e financiamento do terrorismo.

A importância do levantamento de dados no combate aos crimes financeiros

O crime financeiro é uma prática que vem sendo cada vez mais combatida de forma coletiva, ou seja, embora cada pessoa, empresa e governo tenha sua responsabilidade individual, os melhores resultados vem sendo alcançados pelos esforços coletivos que vem ocorrendo em nível mundial, envolvendo autoridades, governos e, principalmente, a iniciativa privada, que é um grande propulsor de melhores práticas.

Entendendo a relevância de manter um sistema frequentemente atualizado, autoridades internacionais bem como entidades globais, como a ONU, há muitos anos desenvolvem listas de crimes financeiros como corrupção, lavagem de dinheiro e terrorismo. Atualmente existem cerca de mil listas públicas, a exemplo do que ocorre na Europa, em que há listas de sanções como a EU – *European Union Sanctions* ou INTERNATIONAL – INSAE-50-EU-WC (lista de empresas que possuem mais de 50% de acionistas pessoa física ou jurídica sancionados). Há, ainda, listas elaboradas no âmbito de determinados países, como aquelas produzidas no âmbito do OFAC, órgão do Departamento do Tesouro dos Estados Unidos, entre outras como:

- Na França: FRAFA – French Anti-Corruption Agency;
- Na Austrália: DFAT-AS – Dept Foreign Affairs – Autonomous Sanctions;
- No Reino Unido: FSA-UOF – Financial Conduct Auth – List of Unauthorized Overseas Firms;
- Na Suiça – FDFA – Federal Department of Foreign Affairs;
- Na Holanda: NLPOL – Dutch National Police Wanted.

Abaixo, a quantidade de listas disponíveis para consulta disponibilizadas por governos ou entidades globais, como Organizações das Nações Unidas (ONU), GAFI – FATF, União Europeia (EU):

LISTAS DISPONÍVEIS PARA CONSULTA DISPONIBILIZADAS POR GOVERNOS OU ENTIDADES GLOBAIS

Autoridade (país/entidade)	Total
USA	176
CANADA	62
EU	59
SWITZERLAND	37
UNKNOWN	36
UNITED KINGDOM	25
CHINA	22
INDIA	22
UN	22
AUSTRALIA	21
RUSSIAN FEDERATION	15
BRAZIL	13
PHILIPPINES	13
ISRAEL	12
JAPAN	12
FRANCE	11
MALAYSIA	11
SINGAPORE	10

Estas listas são formadas a partir de reportes obrigatórios de empresas privadas aos reguladores, ao sistema judiciário, bem como aos órgão reguladores como receita federal, reguladores de mercado financeiro, como bancos (incluindo as operações de câmbio), seguradoras, previdência privada, capitalização e meios de pagamento.

O levantamento de dados para fins de PLD/FTD no Brasil

Nos últimos 10 anos, foi notório o esforço e empenho dedicado pelos reguladores brasileiros, a exemplos dos reguladores europeus, em aumentar o nível de controle dos mercados sob sua supervisão, seja por recomendações do GAFI após as visitas técnicas ao país, ou pelo contexto do país que enfrentou diversas ações da polícia federal e procuradoria para combater o crime organizado.

A economia do Brasil movimenta muito capital de empresas estrangeiras que investem em diversos segmentos, em especial nos segmentos financeiros, o que indiscutivelmente exige que as empresas de capital privado tenham que atender não somente ao regulador local, mas também o regulador de suas casas matriz, que em grande maioria estão entre Europa e Estados Unidos. Por esta razão, não é incomum o sistema de governança e controles internos destas empresas serem avançados e com investimentos mais elevados.

Por oportuno, considerando os esforços governamentais e privados, é possível afirmar que atualmente os reguladores se valem de muitas informações de perfil de risco e comportamental dos clientes do mercado financeiro. Todavia, ao mesmo tempo que o regulador demanda ao mercado controles e reportes, o governo não disponibiliza bases com a acurácia necessária para suportar as entidades privadas no avanço de seus controles.

Há de se destacar o constante aumento de demandas regulatórias para as empresas privadas implementarem maiores controles sobre suas conexões, buscando sempre mais transparência e conhecimento de suas associações, sejam estas como cliente, prestadores de serviços, parceiros. O processo de "conheça seu..." é uma peça estruturante das empresas seja pelo impacto de riscos financeiros, reputacional e imagem, bem como o regulatório. Outrossim, para o avanço deste processo no Brasil, em especial, há uma dependência grande de entidades privadas, que apesar de seus melhores esforços, dependem de mídias, e buscas automáticas em sites governamentais, que podem não ter todos aos dados acessíveis.

No processo de '*onboarding*' de um parceiro/cliente, por não haver uma base nacional de composição societária até beneficiário final, as empresas se valem de serviços de *bureau* privados ou pedidos de cópia de estatuto social das empresas, que multas vezes não comprovam o beneficiário final. Isto acontece também porque as listas divulgada pelo governo são incompletas e com menos atualizações que aquelas oferecidas no mercado. É comum, ainda, que a lista de acordos de leniência do Brasil, encontrada no Portal da Transparência, não esteja atualizada com indicação dos acordos finalizados.

O governo do Estado do Rio de Janeiro possui uma lista publica denominada de BRPRORJ que é a lista de procurados do estado, lista esta que é válida e extremamente útil para o combate ao crime financeiro, mas insuficiente se considerarmos que o Brasil possui 27 estados e um distrito federal, ou seja, cobre uma parte muito pequena de procurados pelo país.

Cumpre ressaltar que não se pretende aqui incentivar a criação irrestrita e sem moderação de lista de combate a

crimes, mas sim demonstrar a importância de os entes governamentais e reguladores enriquecerem o mercado através da formação de uma base única, inclusive com mensuração de impacto. A criação deste canal oficial de obtenção de dados visa fortalecer os processos de '*onboarding*' das empresas, aumentar a acurácia, elevar o patamar dos controles realizados pelas empresas e principalmente, retroalimentar o sistema governamental com informações mais apuradas.

Todavia, se o levantamento de dados e o compartilhamento entre autoridades é fundamental para aprimorar o combate aos crimes financeiros, sobretudo o crime de lavagem de dinheiro, como se verá adiante, o tratamento desses dados deve se dar em estrita observância às novas leis de proteção de dados pessoais, o que muitas vezes revela pontos de tensão entre os regimes de combate a esse tipo de crime e os regimes de proteção aos direitos fundamentais dos cidadãos.

O tratamento de dados no mercado financeiro

O mercado financeiro brasileiro, por força da lei, requer dados cadastrais do cliente, tendo sempre a possibilidade de enriquecimento de dados, desde que comprovado o benefício ao cliente de tal ação. Atualmente muitas instituições financeiras se valem de extenso uso de tecnologia e inteligência artificial para obtenção de dados, padrões comportamentais e de consumo, e consequentemente apresentação de produtos e pacotes de serviços desenvolvidos ao perfil do cliente. O mercado financeiro não atua mais com pacotes pré-desenhados apenas de acordo com a segmentação do banco, mas sim considerando o perfil dos clientes.

Uma das principais razões pela qual a individualização dos dados se faz necessária é a aplicação correta das restrições e penalidades, visto que a avaliação de risco da empresa deve considerar o perfil e risco da empresa e o risco assumido por cada investidor, bem como a participação e tomada de decisão direta dele na empresa. O contrário também se faz verdadeiro, um pequeno acionista de uma empresa que esteja sob análise ou perfil de risco alterado não deve ser diretamente penalizado em sua análise de perfil de risco, deve ser avaliado o papel do indivíduo na companhia, seja para proteção de patrimônio ou de perfil de risco.

Desta forma a acuracidade é essencial para evitar a fragilidade do processo de '*onbording*' e é crucial para garantir os resultamos mais efetivos, e consequente evitar que os processos de combate a crimes financeiros sejam efetivos e tragam resultados sólidos.

Todavia, o setor financeiro deve observar, ainda, outras espécies de normas, que visam tutelar bens jurídicos diversos, como a privacidade e os direitos individuais. Cabe referir, com destaque, as normas que determinam o sigilo de operações de instituições financeiras, o denominado sigilo bancário (Lei Complementar nº 105/2001), e as normas de proteção a dados pessoais, a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709/2018). Tais legislações implicam em que as instituições que captam e gerem dados de seus clientes e usuários devem também observar outras ordens

de comandos, como aqueles de resguardar dados e tratá-los adequadamente, conforme os direitos de seus titulares.

A LC 105/2001 determina que as instituições financeiras conservarão sigilo de suas operações ativas e passivas e serviços prestados, e prevê as hipóteses em que o repasse ou o fornecimento de informações não constitui violação do dever de sigilo, bem como situações de obrigatório fornecimento, por força de comando legal ou de autoridade competente.

A LGPD, por sua vez, determina parâmetros para o denominado "tratamento de dados pessoais", com destaque para um elenco de princípios que devem ser observados, a teor de seu artigo 6º: finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, não-discriminação, entre outros. Dispõe ainda sobre requisitos para o mencionado tratamento, os direitos do titular dos dados, e regras gerais de segurança e boas práticas.

Dessa forma, as instituições financeiras devem cumprir os dispositivos da Lei de Sigilo Bancário e da LGPD, com intuito de proteger os dados de seus clientes, sem, contudo, comprometer suas ações que visam coibir os crimes de lavagem de dinheiro e financiamento do terrorismo.

Nesse contexto, fica evidente a magnitude do desafio de atender as regras de *compliance* relacionadas a PLD/FT, com as complexidades inerentes aos temas envolvidos e, ao mesmo tempo, garantir o respeito às regras de proteção à privacidade, no resguardo dos dados dos cidadãos. Trata-se de perseguir, a um só tempo, objetivos paralelos de combater a criminalidade e o uso para fins ilegais dos sistemas formais da economia, e de garantir a proteção a direitos individuais. Ambos, paz social via legalidade e respeito aos indivíduos, são bens jurídicos a serem valorizados, considerados com equilíbrio e ponderação no quotidiano das relações das empresas com seus clientes e a cidadania.

Nesse contexto, o vasto universo de instituições financeiras tem, ao longo dos últimos 25 anos, aperfeiçoado suas práticas e implementado controles internos e políticas, inclusive de treinamento de seus colaboradores, para o devido cumprimento à legislação e atendimento às obrigações mencionadas. A Supervisão de Conduta do Banco Central do Brasil tem, por sua vez, ampliado e reforçado seus instrumentos de supervisão sobre essas dimensões da *compliance* no que se refere às instituições financeiras sob sua supervisão, desde a edição da Lei 9.613/1998. Esses trabalhos levam em conta as recomendações e especificações técnicas de melhores práticas emanadas do Grupo de Ação Financeira (Gafi).

As medidas de PLD/FT diante da necessidade de proteção de dados pessoais

A Lei n. 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) é o diploma legal que, desde a sua entrada em vigor em 2020, regulamenta o tratamento de dados pessoais no país por pessoas naturais e jurídicas, no setor privado e na administração pública. A Lei estabelece que o tratamento de dados pessoais deve observar a boa-fé e uma série de princípios como finalidade, adequação, necessidade, livre acesso, qualidade dos dados,

transparência, segurança, prevenção, não discriminação e responsabilização. Além disso, exige dos agentes de tratamento que somente processem dados nas hipóteses legais que elenca em seus artigos 7º e 11º, como para o cumprimento de uma obrigação legal, para atendimento a seus legítimos interesses ou com o consentimento do titular dos dados. Para garantir a proteção dos dados – direito fundamental que somente após a LGPD veio a ser insculpido na Constituição Federal por meio da Emenda Constitucional nº 115/2022 – a Lei prevê, ainda, uma série de direitos em relação aos dados, como o direito de obter informações sobre as atividades de tratamento e sobre o compartilhamento de seus dados, entre outros.

Como já antecipado ao longo desse artigo, as ações de PLD/FTD envolvem, por sua natureza, uma série de atividades que dependem do processamento de dados das pessoas naturais envolvidas a fim de identificar atividades suspeitas, como é o caso das ações que visam identificar o beneficiário final de uma transação ou estrutura. Assim, se por um lado, essas medidas são cruciais para se chegar aos indivíduos que se utilizam do sistema financeiro para cometer crimes, por outro, a busca pela identificação do beneficiário final pode resultar em uma interferência desproporcional na sua vida privada e violar a proteção de seus dados pessoais, que podem incluir desde dados de identificação e/ou de qualificação, até sua renda, rendimentos, residência, partes relacionadas, entre outros.

O mesmo acontece em relação aos representantes legais da pessoa jurídica que, ao optar por assumir essa posição, passam a se submeter a um conjunto de obrigações e responsabilidades que podem limitar a proteção de seus dados pessoais em determinadas circunstâncias. No contexto da investigação de um crime, por exemplo, não somente a proteção de dados do beneficiário final como a de seu representante legal pode ser relativizada. As autoridades competentes, como a Polícia Federal, o Ministério Público e o COAF, têm o poder de requisitar informações e dados pessoais necessários para a investigação (Brasil, 1998). Embora a identificação do representante legal e do beneficiário final sejam essenciais para a segurança financeira, há um equilíbrio delicado entre proteger a privacidade dos clientes e combater atividades ilícitas.

De um modo geral, o tratamento de dados pessoais no regime da prevenção e combate à lavagem de capitais envolve uma grande quantidade de dados do cliente, do seu representante legal e do beneficiário final, tendo as instituições financeiras, assim como as demais pessoas obrigadas, o dever de conservar tais dados por longos períodos.

Diante desse problema, passamos a analisar as seguir os principais aspectos da proteção de dados pessoais no Brasil, a partir do confronto das disposições da Lei n. 13.709/2018 (a LGPD) e os mecanismos atualmente utilizados pelas autoridades para identificação de pessoas envolvidas em crimes financeiros, sobretudo para fins de PLD/FT.

Base Legal para o Tratamento de Dados

A Lei 13.709/2018 determina em seus artigos 7° e 13°, que o tratamento

de dados pessoais e de dados pessoais sensíveis, respectivamente, deve se dar mediante uma das hipóteses legais previstas na Lei, sem a qual o tratamento será considerado ilícito. Como regra, o fundamento de licitude para o tratamento dos dados de clientes, beneficiários finais e representantes legais da pessoa jurídica pelas pessoas obrigadas no âmbito das regras de PLD/FT será aquele previsto no artigo 7º, II e no artigo 11º, II, a, os quais autorizam o tratamento de dados pessoais para o cumprimento de obrigação legal ou regulatória pelo controlador. Nesse caso, está se falando da pessoa jurídica obrigada, segundo a Lei 9.613/98, como a bolsa de valores, seguradoras, corretoras de seguros e as entidades de previdência complementar ou de capitalização, administradoras de cartões de crédito, bancos, entre outros.

Neste sentido, em princípio, não há que se falar na necessidade de obter consentimento do representante legal ou beneficiário final de uma empresa para que forneça seus dados pessoais nesse caso uma vez que há hipótese legal que permite o tratamento sem a gestão desse consentimento. Nesse ponto, vale afastar qualquer entendimento no sentido que o consentimento deve prevalecer em relação às demais bases legais, uma vez que não há hierarquia entre elas, devendo ser adotada a que melhor se adequa ao caso concreto.

Sendo assim, conquanto que a pessoa obrigada trate dados pessoais de seus clientes para atender a normas de PLD/FTD previstas em diplomas legais e atos normativos que os regulamentam, essas atividades de tratamento serão consideradas lícitas. Ocorre, entretanto, que não basta que se aponte uma hipótese legal compatível com o processamento; este tem que atender aos princípios elencados na LGPD para que seja considerado válido.

Princípios da LGPD

Em atendimento ao princípio da *finalidade*, expresso no artigo 6º, I, da LGPD, os dados coletados somente poderão ser utilizados com o intuito de prevenção e combate à lavagem de dinheiro, não devendo ser utilizados para outras finalidades pelas pessoas obrigadas, como para a promoção de seus produtos ou serviços, por exemplo. A discussão, na realidade, vai além da mera coleta dos dados pessoais pelas pessoas obrigadas porque, no âmbito regulatório da prevenção à lavagem de dinheiro, em casos de suspeitas, há a obrigatoriedade de comunicação e compartilhamento dos dados com o COAF, atividades que são também consideradas formas de tratamento dos dados e devem, da mesma forma, ser realizadas no limite da LGPD.

Além disso, o propósito do tratamento deve ser específico, isto é, não é compatível com a LGPD a coleta generalizada de dados para possível descoberta de um ou mais crimes, o chamado *fishing expedition*. Esse tipo de prática se trata também de violação ao princípio da necessidade, como se verá a seguir.

No âmbito de PLD/FT, há diversos atos normativos que delimitam a extensão do tratamento de dados requerido para fins de prevenção ao crime, como as Circulares BC 3978/20, CVM 50/20, SUSEP 612/20. Além disso, cada autoridade deve detalhar como será a captura e a obtenção desses dados, a verificação

e validação, como serão utilizadas as informações pessoais posteriormente e quem poderá ter acesso, além de informar como será a guarda destes dados, o prazo, além da certificação de que os dados pessoais não serão disponibilizados para outros fins e não serão utilizados indevidamente.

Vale lembrar que a necessidade de conhecer informações a respeito de operações suspeitas bem como dados cadastrais da pessoa jurídica não justifica necessariamente a individualização das pessoas naturais eventualmente relacionadas o que, para ocorrer, deve ser justificada pela finalidade pretendida, definidas medidas de proteção e levada a conhecimento do titular. Desta forma, o perfil da pessoa natural, seja bancário, de investimentos, ou qualquer outro não deve ser utilizado indiscriminadamente com a mera justificativa de analisar o perfil de risco da empresa.

O princípio da finalidade deve também orientar e limitar posteriores atividades de tratamento por outras autoridades que possam vir a ter acesso aos dados pessoais recebidos pelas unidades de inteligência financeira, como ocorre nas hipóteses de compartilhamento de dados entre o COAF, a RFB e o Ministério Público. Ademais, ainda que se trate de atividade de tratamento realizada em razão de obrigação legal ou regulamentar, prescindindo de consentimento do titular, seu propósito deve ser explícito e informado ao titular. Nesse aspecto, é importante destacar, ainda, a necessidade de atuar com transparência na relação com os titulares. O atendimento ao princípio da *transparência*, fundamental na disciplina do tratamento de dados pessoais, destina-se a garantir a confiança dos cidadãos nos processos. Aliado ao princípio da finalidade, ele garante ao titular o direito de conhecer os motivos que levam à necessidade de coleta e uso de seus dados pessoais, que dados serão tratados, quem terá acesso, se haverá transferência a terceiros, as categorias de destinatários, prazo de guarda, base legal de tratamento, entre outras informações de seu interesse. Ou seja, permitem que os titulares dos dados compreendam os propósitos, forma e extensão do tratamento, e se oponham a esses processos, quando possível. Naturalmente, essa obrigação é, muitas vezes, conflitante com o sigilo que em geral é necessário em investigações dessa natureza, revelando-se como uma dos principais motivos de tensão entre a legislação de proteção de dados pessoais e as regras de PLD-FT.

O princípio da transparência possui uma outra vertente não mesmo importante no caso dos processos envolvendo PLD-FT: o titular deve ter informações claras e diretas sobre os responsáveis pelo tratamento de seus dados pessoais, isto é, sobre os agentes de tratamento e o Encarregado, devendo ter acesso a seus dados de contato e identidade. Essa obrigação se comunica diretamente com a necessidade de *accountability* por parte dos agentes de tratamento e de se garantir a efetivação dos direitos dos titulares, sobre o que comentaremos mais adiante.

Além disso, o tratamento dos dados deve se limitar ao mínimo necessário para o cumprimento da obrigação legal ou regulamentar, considerando a finalidade pretendida (art 6, III, da LGPD) que, no caso, envolve um interesse público. O atendimento a esse critério se dará

sempre na medida do que a lei determina, ou seja, a lei deverá determinar a coleta e entrega de dados pertinentes, proporcionais e não excessivos em relação às finalidades de PLD/FT, bem como determinar os responsáveis pelo tratamento, o tipo de dados pessoais que devem ser coletados, os titulares dos dados em questão, as autoridades com as quais os dados pessoais devem ser compartilhados, os prazos de guarda e conservação e outras medidas que garantam a licitude do tratamento e a proteção dos dados.

Direitos dos clientes, representantes legais e beneficiários finais como titulares de dados

Um outro pilar fundamental da LGPD que revela dificuldades quando se trata de PLD-FT é o atendimento aos direitos dos titulares. Como qualquer outro titular de dados, o cliente, o beneficiário final e o representante legal da pessoa jurídica possuem direitos em relação a seus dados, que podem ser exercidos em relação aos agentes de tratamento, quer sejam eles as pessoas obrigadas pela Lei de Lavagem de Capitais, quer sejam as autoridades que tem acesso aos dados em razão da comunicação de operações suspeitas. O responsável pelo tratamento deve facilitar o exercício dos direitos do titular dos dados, entre eles:

- Confirmar a existência de tratamento de dados pessoais.
- Acessar os dados pessoais que estão sendo tratados.
- Corrigir dados incompletos, inexatos ou desatualizados.
- Solicitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados de forma inadequada.
- Realizar a portabilidade dos dados para outro fornecedor de serviço ou produto, observando segredos comerciais e industriais.
- Revogar o consentimento dado anteriormente.

Além disso, o titular de dados pode peticionar junto à Autoridade Nacional de Proteção de Dados (ANPD) em relação aos seus dados e se opor a tratamentos realizados sem consentimento, caso a LGPD não seja cumprida.

Como se observa, alguns desses direitos podem se revelar difíceis de serem atendidos no contexto de prevenção à lavagem de dinheiro, sob pena de comprometerem a eficiência das medidas de PLD/FTD, sobretudo quando os dados são tratados já no contexto de atividades de investigação e persecução penal, como veremos a seguir.

Tratamento de dados para fins penais

Embora a LGPD seja de aplicação abrangente a todas as pessoas jurídicas e pessoas naturais que tratam dados com fins econômicos, inclusive na administração pública, o legislador excetuou de sua aplicação as atividades de tratamento realizadas para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, deixando a cargo de legislação específica a previsão

de medidas proporcionais e estritamente necessárias ao atendimento do interesse público nessa seara (art. 4º, III e § 1º, da LGPD). Dessa forma, encontram-se atualmente em discussão algumas propostas de lei para tratar do tema, como o Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal e o PL 1515/2022.

Esse tratamento diferenciado se justifica porque embora a LGPD tenha estabelecido diretrizes rigorosas para a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, bem como uma série de direitos e condições para assegurar a proteção de dados pessoais, essa proteção não é absoluta e pode ser relativizada em situações específicas, como no processo penal ou em investigações criminais, incluindo aquelas relacionadas a crimes de lavagem de dinheiro. Dessa forma, em razão do interesse público envolvido, é razoável esperar que, sob certas condições, as autoridades tenham o poder de requisitar informações e dados pessoais necessários para uma investigação criminal, por exemplo, desde que pautem sua atuação pelos princípios da proporcionalidade, necessidade, sigilo, confidencialidade e devido processo legal. A proteção de dados de um representante legal ou beneficiário final deve ir até o ponto em que não comprometa a efetividade das investigações, do processo penal e a segurança coletiva. É necessários equilibrar a privacidade individual com a segurança coletiva. A chave está na implementação de medidas proporcionais, transparentes e seguras que respeitem os direitos fundamentais dos indivíduos enquanto combatem atividades ilícitas.

Assim, além das condições gerais já mencionadas acima para o tratamento de dados pessoais pelas autoridades públicas, quando se trata de matéria criminal, a proteção de dados encontra os seguintes limites:

Proporcionalidade e necessidade: as autoridades devem garantir que a coleta e o tratamento dos dados sejam proporcionais e necessários para a investigação. Apenas os dados essenciais para a elucidação do crime devem ser acessados. A proporcionalidade é um princípio constitucional que deve ser observado para evitar abusos no tratamento de dados.

Sigilo e confidencialidade: as informações obtidas durante uma investigação devem ser tratadas com sigilo e confidencialidade, evitando a exposição indevida dos dados pessoais. A confidencialidade é um elemento essencial para a proteção da privacidade, mas pode ser relativizada em casos de interesse público superior. Assim, as comunicações realizadas ao COAF e ao órgão regulador setorial, por exemplo, devem ser sigilosas. Isso é necessário para não comprometer as investigações e o bloqueio de ativos. Embora não seja possível avisar ao cliente, é recomendável que as entidades sigam políticas de Prevenção à Lavagem de Dinheiro (PLD) e Combate ao Financiamento do Terrorismo (CFT). Dessa forma, todos os que se relacionam com essas entidades saberão, de antemão, da possibilidade de comunicação das operações suspeitas.

Devido processo legal: as investigações devem seguir o devido processo legal, respeitando os direitos e garantias fundamentais dos indivíduos. No entanto, a urgência e a natureza sigilosa das investigações podem dificultar a observância

estrita desses princípios, especialmente quando é necessário agir rapidamente para evitar a destruição de provas.

Transparência e informação: sempre que possível, os titulares dos dados devem ser informados sobre o tratamento de seus dados, exceto quando a comunicação possa comprometer a investigação. A transparência é um princípio fundamental para a proteção de dados, mas pode ser mitigada em casos de investigações criminais.

Direitos dos titulares: Na prática, nem todos os direitos previstos na LGPD podem ser exercidos contra o COAF. Em certas etapas, a existência do tratamento para fins de inteligência financeira é sigilosa, mesmo para o titular dos dados. Isso significa que nem sempre o titular dos dados terá direito a informações prévias específicas sobre o início do tratamento, o compartilhamento de seus dados por um sujeito obrigado ao COAF, nem sobre a difusão de um Relatório de Inteligência Financeira (RIF) pelo COAF aos órgãos de persecução criminal, salvo depois de se tornar pública a investigação ou o processo penal.

Com relação a esse último ponto, vale destacar que o COAF é uma unidade de inteligência financeira e, a princípio, não realiza investigação ou atua em segurança pública ou qualquer fase do processo penal. Dessa forma, quando realiza atividades de tratamento de dados se submete à LGPD em todos os seus aspectos.

De todo modo, observa-se que é necessário haver um equilíbrio entre privacidade e proteção de dados pessoais, de um lado, e segurança pública e efetividade das atividades das autoridades criminais, de outro. No combate à lavagem de dinheiro e crimes financeiros, em geral, as autoridades devem adotar que garantam a efetividade que se pretende em termos de combate ao crime, o mesmo tempo em que sejam respeitados os direitos fundamentais dos indivíduos. Isso inclui:

- Avaliação de Impacto: Realizar avaliações de impacto sobre a proteção de dados antes de implementar novas medidas de vigilância financeira. As avaliações de impacto são ferramentas essenciais para identificar e mitigar riscos à privacidade.
- Medidas de Segurança: Adotar medidas técnicas e administrativas para proteger os dados pessoais durante as investigações. A segurança dos dados é um requisito indispensável para a proteção da privacidade.
- Supervisão e Controle: Estabelecer mecanismos de supervisão e controle para garantir que as investigações sejam conduzidas de acordo com a lei e os princípios de proteção de dados. A supervisão é crucial para assegurar a conformidade com as normas de proteção de dados.

O compartilhamento de dados obtidos pelo COAF com autoridades de persecução penal

Recentemente, o STF decidiu, no julgamento do Recurso Extraordinário (RE) 1.055.941/SP (com repercussão geral – tema 990), que é constitucional

o compartilhamento de relatórios de inteligência financeira do COAF com autoridades de persecução penal, sem a necessidade de autorização judicial prévia. O STF entendeu que o COAF pode compartilhar dados com autoridades de persecução penal sem autorização judicial desde que o sigilo das informações seja mantido e os procedimentos sejam formalmente instaurados. Isso significa que as informações devem ser compartilhadas de maneira oficial e registrada, garantindo a possibilidade de controle posterior. A decisão foi fundamentada na interpretação do artigo 15 da Lei 9.613/1998 (Lei de Lavagem de Dinheiro). O mesmo entendimento foi adotado pelo ministro relator, Cristiano Zanin, na Reclamação Constitucional 61.944, para permitir o envio de dados do COAF às autoridades policiais sem necessidade de autorização judicial prévia. De todo modo, o sigilo das informações deve ser rigorosamente mantido, não sendo permitido o compartilhamento informal de informações, isto é, sem registro oficial. Para garantir a integridade das investigações e a proteção dos dados pessoais envolvidos é crucial, ainda, que haja responsabilidade e transparência no processo.

Cooperação Internacional

A LGPD permite a remessa de dados pessoais ao exterior em algumas hipóteses expressamente previstas na Lei (art. 33 da LGPD), inclusive quando o destinatário for um país ou organismo internacional que proporcione um grau de proteção de dados pessoais adequado, similar ao previsto na LGPD. O compartilhamento transfronteiriço de dados também é permitido quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e persecução, de acordo com os instrumentos de direito internacional.

Assim, as informações transferidas internacionalmente entre as Unidades de Inteligência Financeira (UIFs) de diferentes países devem ser tratadas e protegidas com o mesmo nível de confidencialidade aplicável às informações obtidas de fontes nacionais. Todas as operações de tratamento devem observar critérios de segurança e confidencialidade, e os dados recebidos só podem ser usados para as finalidades acordadas ou previstas em leis e regulamentos. Para isso, as UIFs devem ter regras que garantam a segurança e o sigilo das informações recebidas, incluindo procedimentos adequados para coleta, processamento, armazenamento, disseminação e proteção dos dados, além do acesso a essas informações.

As orientações de Egmont quanto à segurança e à confidencialidade das informações devem ser seguidas, assim como as Recomendações 29 e 40 do GAFI. Essas orientações exigem que as informações recebidas pelas UIFs sejam usadas apenas para o fim solicitado ou autorizado. Se houver necessidade de usar os dados para outros fins, inclusive na persecução criminal no exterior, deve haver autorização prévia da UIF remetente.

O Princípio 30 de Egmont exige que os funcionários das UIFs sejam adequadamente capacitados para lidar com os dados que gerenciam, especialmente para as operações de tratamento e divulgação

de informações sensíveis ou confidenciais. Todas as unidades de inteligência devem instituir mecanismos de segurança digital, incluindo a limitação de acesso físico às suas instalações e a restrição e controle de acesso aos seus sistemas informáticos e bases de dados.

Para reforçar o requisito da finalidade do tratamento dos dados, o Princípio 32 de Egmont exige que as informações recebidas pelas UIFs sejam usadas apenas para o fim solicitado ou autorizado. Se houver necessidade de usar os dados para outros fins, inclusive na persecução criminal no exterior, deve haver autorização prévia da UIF remetente.

Direito Comparado

COREIA DO SUL

Em 1953, a Coreia do Sul passou por um rápido desenvolvimento econômico e financeiro após o fim temporário da Guerra da Coreia com o Acordo de Armistício. Após esse acontecimento, o Governo Sul-Coreano introduziu e continuou a desenvolver um quadro financeiro sofisticado e, atualmente, é a décima maior economia do mundo. A Unidade de Informação Financeira da Coreia ("koFIU") é a principal agência responsável pela implementação cumprimento e aplicação da legislação AML/CFT na Coreia do Sul. A KoFIU recebe relatórios de operações suspeitas, assim como o COAF, no Brasil e os encaminha para outros organismos responsáveis pela aplicação da lei para investigar, rever, analisar e comunicar as conclusões.

O país passou a fazer parte do GAFI no ano de 1996, porém, sua primeira avaliação foi realizada em 2008 e, mais recentemente, em 2020. O último relatório observou que houve uma melhoria significativa desde a sua avaliação anterior e concluiu que "a Coreia do Sul dispõe de um quadro jurídico sólido para combater o branqueamento de capitais e o financiamento do terrorismo e para confiscar os fundos envolvidos, mas precisa de fazer mais para impedir de impedir o governo e os funcionários públicos de branquear o produto da da corrupção".[7]

De um lado, a Coréia do Sul possui mecanismos legais de Prevenção à Lavagem de Dinheiro contendo:

(i) Verificação de "conheça seu..." garantindo que a diretoria da instituição financeira ou entidade regulamentada deve supervisionar os sistemas de controle interno para AML/FT;

(ii) A Instituição Financeira deve ter um diretor de relatórios encarregado de relatar movimentações suspeitas com supervisão diária dos protocolos KYC e, ao mesmo tempo, educar e treinar os funcionários sobre AML.

(iii) Ao existir movimentações financeiras suspeitas, a entidade regulamentada deve preparar e registrar um reporte para o KoFIU quando suspeitar que uma transação financeira possa ser ilegal ou que haja uma tentativa de lavagem de dinheiro.

(iv) Uma instituição financeira ou entidade regulamentada deve iniciar os procedimentos de verificação de KYC quando um cliente

7 Documents – FATF (https://www.fatf-gafi.org). Acesso em 26 de junho de 2024.

> abrir uma nova conta ou busca concluir uma transação que exceda KRW 1.000.000 para ativos virtuais e US$ 10.000 para transações de câmbio.

De outro, desde 2011, a Lei de Proteção de Informações Pessoais da Coreia do Sul impõe diversas normas para proteção de dados. Dessa forma, ao entrar em contato com dados para identificação de potenciais criminosos, o agente precisa garantir medidas técnicas, administrativas e físicas necessárias para a segurança dessas informações.

A legislação de proteção de dados pessoais informa que há quatro entidades com competências relacionadas à proteção de dados: (1) a Comissão de Proteção de Informações Pessoais, (2) o Ministério do Interior, que regula as questões gerais de proteção de dados ao abrigo da Lei de Proteção de Informações Pessoais, (3) a Comissão de Comunicações da Coreia que regula as questões de privacidade relacionadas a provedores de serviço online e (4) a Comissão de Serviços Financeiros, que regula as questões de privacidade relacionadas à indústria de serviços financeiros.[8]

É imprescindível citar o desafio das entidades regulamentadas e instituições financeiras em identificar os envolvidos nos crimes de Lavagem de Dinheiro e financiamento ao terrorismo, haja vista que a Legislação da Coréia do Sul informa que: "Artigo 3º (nº1): "(1) O controlador de informações pessoais deve tornar a finalidade do processamento de informações pessoais explícita e especificada e deve coletar o mínimo de informação pessoal, legal e justamente, na medida do necessário para tal finalidade.". Dessa maneira, a lei coreana menciona que a coleta de informações pessoais, para a realização de uma finalidade de utilização, deva ser mínima[9].

O desafio é inerente ao assunto e, portanto, assim como os demais países, é necessário que haja certa cautela no tratamento de dados, sem que ocorra desfalque nas informações e condutas de identificação de criminosos.

CHINA

A China, país integrante do GAFI desde 2007, possui um arcabouço legal de prevenção a Lavagem de Dinheiro. Em junho de 2021, o Banco Popular da China (PBoC) publicou a Lei contra Lavagem de Dinheiro (AML) alterada para comentários do público. Em 2023, ela foi incluída no plano de trabalho legislativo do Conselho de Estado. Em 23 de abril de 2024, o projeto de alteração da Lei Antilavagem de Dinheiro (a "AML alterada") foi apresentado ao Comitê Permanente do Congresso Nacional do Povo para deliberação legislativa inicial, representando um avanço substancial no processo legislativo.

O Artigo 3 da referida legislação foi alterado para indicar que as entidades

8 CONFEDERAÇÃO NACIONAL DA INDÚSTRIA (Brasil). EM BUSCA DE SOLUÇÕES: ATRIBUTOS DE AUTORIDADES DE PROTEÇÃO DE DADOS EFICAZES. Proteção de dados, [S. l.], p. 1-1, 1 jul. 2024. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/64/e0/64e0fce7-d49e-4b43-83aa-ab21000 8b66a/em_busca_de_solucoes_ago2017_v3.pdf. Acesso em: 28 jun. 2024.

9 MARQUES, Ana Vitória Cavalcante de Carvalho. A relação entre a lei brasileira 13.709/18 e o arcabouço jurídico para proteção de dados pessoais do Japão e da Coreia do Sul a partir do modelo TLICS. 2021. 130 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Brasília, 2021.

estabeleçam sistemas sólidos de prevenção de riscos. Ademais, os artigos 5 e 36 enfatizam as obrigações das entidades e indivíduos no trabalho de AML, incluindo a cooperação com verificações de *due diligence* e a comunicação de transações suspeitas. As instituições financeiras têm o direito de tomar medidas contra qualquer pessoa que se recuse a cooperar. Caso não haja cooperação, as referidas instituições podem sofrer sanções estipuladas em lei.[10]

De acordo com o relatório de 2021 do FAFT sobre a China, o país "fez progressos para abordar as deficiências acima mencionadas" em suas iniciativas de AML, e os novos requisitos são mais um passo para garantir regulamentações AML/KYC robustas. Os novos requisitos são chamados de Medidas Administrativas para Instituições Financeiras sobre Investigações de Due Diligence do Cliente e Manutenção de Informações de Identidade do Cliente e Registros de Transações.

De acordo com as alterações realizadas em 2021, as entidades obrigadas precisam coletar e manter: (i) Nome; (ii) Gênero; (iii) Nacionalidade; (iv) Ocupação; (v) Endereço e (vi) Número de identificação. Da mesma forma, as empresas precisam manter informados, de acordo com a modificação, o beneficiário final.

É importante citar que em caso de investigações suspeitas de Lavagem de Dinheiro, o beneficiário final é importante para identificação da ação criminosa. Porém, assim como nos demais países, existe a Legislação de Proteção à Informação Pessoal (PIPL) promulgada em 2021.

Dessa forma, a Lei de Proteção de Informações Pessoais da China, em seu artigo 44, determina que os titulares têm direito de limitar o tratamento de seus dados pessoais. Dessa forma, assim como no Brasil, existe certa dificuldade de detalhar toda a cadeia societária até o beneficiário final. Nesse sentido, é importante que haja o "conheça seu...." para compreender a natureza do negócio, como o setor, as jurisdições, o tipo e o valor das transações e os produtos ou serviços que oferecem; compreender a estrutura de propriedade e controle do negócio e, principalmente identificar os beneficiários finais.

Em conclusão, apesar do desafio de respeitar as informações pessoais e identificar possíveis criminosos, o país deve seguir as recomendações do Gafi que compreendem identificar o beneficiário e adotar medidas razoáveis para verificar a identidade de tal beneficiário, de forma que a instituição financeira obtenha conhecimento satisfatório sobre quem é o beneficiário.

Outros temas atuais – Lavagem de dinheiro em operações com criptomoedas

Criptomoedas "são unidades monetárias de base criptografada utilizadas para fazer pagamentos e transferências de forma digital e operadas por usuários."[11]

10 JUNHE LLP (China). Organização. Client Briefing: An Overview of the Draft Amendment to the Anti-Money Laundering Law. LEXOLOGY, [S. l.], p. 1-1, 9 maio 2024.

11 O QUE são criptomoedas?. Valor Investe, [S. l.], p. 1-1, 5 abr. 2019. Disponível em: https://valorinveste.globo.com/mercados/cripto/noticia/2019/04/05/o-que-sao-criptomoedas.ghtml. Acesso em: 1 jul. 2024.

Além disso, as criptomoedas empregam tecnologia de *blockchain* e criptografia para assegurar a validade das transações e a criação de novas unidades de moeda. Existem diversas Criptomoedas, tais como, mas não se limitando a Bitcoin, Ethereum, Binance coin, Cardano, Tether, Solana, XRP, Polkadot, Dogecoin e USD Coin. A moeda Bitcoin é uma criptomoeda descentralizada, um dinheiro eletrônico para transações diretas ponto-a-ponto (peer-to-peer, ou P2P), realizadas sem intermediários, e que são gravadas em um banco de dados distribuído e público denominado blockchain.[12]

As principais características das criptomoedas que favorecem seu uso para a lavagem de dinheiro são a descentralização, a "*pseudoanonimidade*" e a globalidade[13]:

(i) A criptomoeda é descentralizada haja vista que ela é criada e transacionada sem a necessidade de intermediários. As transações podem ser feitas diretamente entre adquirente e vendedor, são então verificadas por todos os usuários e inscritas em um banco de dados público, o blockchain. Sob o ponto de vista de PLD/FT, é importante dar luz ao fato de que inexiste uma autoridade central a quem apelar em caso de investigação ou suspeita de atividade criminosa.

(ii) A "*pseudononimidade*" traduz-se no fato de que, apesar de não ser anônimo, as transações garantem um grau de privacidade. De acordo com Heloisa Estellita "ao abrir uma conta a pessoa não tem de se identificar e basta o acesso à internet e a um cliente de BTC para gerar um par de chaves e um endereço e ter acesso a transações. Ademais, uma mesma pessoa pode ter diversos endereços, pois a capacidade de criação de endereços pelo wallet a partir do par de chaves é ilimitado. Isso agrega maior privacidade às transações"[14].

(iii) A globalidade se caracteriza pelo fato de que as transações podem ser realizadas globalmente sem qualquer obstáculo.

Em uma situação hipotética, o criminoso poderia obter criptomoedas com valores provenientes da prática de infração penal anterior com dinheiro em espécie por meio da aquisição em *exchanges* (intermediadoras entre vendedores e compradores de ativos digitais). Além disso, o indivíduo poderia gerar infinitas chaves públicas, mudando o endereço das criptomoedas sem que o usuário perca o controle sobre elas. Também se pode usar os endereços de terceiros ou mesmo de agentes financeiros. O que não é passível de conhecimento, como dito, é a identidade dos usuários.

12 ESTELLITA, HELOISA. Bitcoin e lavagem de dinheiro: uma aproximação. JOTA, [S. l.], p. 1-16, 7 out. 2019.

13 Cf. FATF. Guidance for a risk-based approach: virtual assets and virtual asset service providers. 2019. Disponível em: www.fatfgafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtualassets.html (acesso em 23/09/2019) Cf. também FERNÁNDEZ BERMEJO, Daniel (org.). Blanqueo de capitales y TIC: marco jurídico nacional y europeo, modus operandi y criptomonedas – Ciberlaundry. informe de situación. Navarra: Thompson ReutersAranzadi, 2019, p. 81-82.

14 ESTELLITA, HELOISA. Bitcoin e lavagem de dinheiro: uma aproximação. JOTA, [S. l.], p. 1-16, 7 out. 2019.

No Brasil, a regulamentação doa ativos virtuais é recente. A Lei 14.478/22 – regulamentada pelo Decreto n. 11.563/2023 – que determina as diretrizes e princípios que devem ser observados na prestação de serviços de ativos virtuais (criptomoedas), alterou a Lei nº 9.613/98 passando a prever aumento de pena nos crimes de lavagem de dinheiro, no montante de 1/3 a 2/3, quando cometidos de forma reiterada e realizados por meio da utilização de ativo virtual.

No campo internacional, o Financial Crimes Enforcement Network (FinCEN), órgão do Departamento do Tesouro dos Estados Unidos especializado na análise de operações financeiras para fins de PLD-FT, vem tornando mais rígidas as regras aplicáveis às criptomoedas com o objetivo de conferir maior segurança nessas transações e prevenir a ocorrência de crimes. Entre outras regras, a regulamentação sujeita às *exchanges* a registro como prestadores de serviços monetários, bem como ao cumprimento das normativas de combate à lavagem de dinheiro. Observa-se, portanto, como, apesar de embrionária, a proteção da sociedade em torno dos criptoativos está se desenvolvendo e ganhando maior arcabouço legal.

Conclusão

A partir da análise detalhada sobre a intersecção entre a proteção de dados pessoais e as medidas de prevenção e combate à lavagem de dinheiro, ressaltamos a importância crescente do rigoroso cumprimento das normativas legais que as regem. A abordagem que as instituições financeiras devem adotar frente ao arcabouço legal da prevenção à lavagem de dinheiro vai além da obrigação de observância regulatória, e nos desafia à oportunidade estratégica rumo à escalabilidade, segurança cibernética e governança de dados, para fortalecer a confiança e a segurança do setor financeiro nacional e global.

A Lei Geral de Proteção de Dados (LGPD) traz consigo princípios constitucionais essenciais a garantir privacidade e segurança dos dados pessoais, e exige uma estrutura legal robusta para o tratamento desses dados em contextos complexos para além do relacionamento comercial, estendendo-se a situações penais. Garantir a legitimidade do tratamento de dados e a segurança jurídica dos cliente e da sociedade, são cruciais para o equilíbrio entre a proteção de dados, as exigências de conformidade e as práticas de due diligence fundamentais ao combate da lavagem de dinheiro e crimes financeiros.

Os direitos dos titulares de dados, clientes, representantes legais e beneficiários finais devem ser moldurados pela transparência e o controle do tratamento das informações e dados pessoais, para a manutenção da integridade dos dados no sistema financeiro.

O compartilhamento de dados obtidos pelo COAF com autoridades de persecução penal e a cooperação internacional são aspectos que destacam a complexidade e a importância da interação entre regimes de proteção de dados e o combate à lavagem de dinheiro. Estes processos devem ser realizados de maneira que respeite tanto os direitos dos titulares dos dados quanto as necessidades de investigação e prevenção de crimes financeiros.

A discussão reflete a interdependência entre a segurança da informação e a integridade financeira, sublinhando a necessidade de um equilíbrio cuidadoso entre privacidade, segurança e conformidade regulatória. Conforme as instituições financeiras e os órgãos reguladores avançam, a harmonização desses princípios será fundamental para assegurar que as práticas de proteção de dados e as estratégias de combate à lavagem de dinheiro evoluam de forma a proteger tanto os consumidores quanto às instituições e o sistema financeiro global.

As instituições financeiras devem se adaptar, inovar e colaborar, não apenas para atender à legislação existente, mas para serem proativas na prevenção de ameaças futuras, garantindo um ambiente seguro e confiável para todos os stakeholders envolvidos.

REFERÊNCIAS

- Almeida, J. (2021). Transparência e Proteção de Dados. São Paulo: Editora Jurídica.
- Brasil. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018.
- Brasil. (1998). Lei nº 9.613, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores e a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei.
- Costa, M. (2019). Proporcionalidade e Proteção de Dados. Rio de Janeiro: Editora Jurídica.
- Ferreira, L. (2021). Supervisão e Conformidade na Proteção de Dados. Brasília: Editora Jurídica.
- Nunes, R. (2019). Segurança de Dados e Privacidade. Porto Alegre: Editora Jurídica.
- Prado, G. (2018). Devido Processo Legal e Investigações Financeiras. Belo Horizonte: Editora Jurídica.
- Rodrigues, A. (2020). Avaliações de Impacto na Proteção de Dados. Curitiba: Editora Jurídica.
- Silva, T. (2020). Confidencialidade e Interesse Público. Recife: Editora Jurídica.
- Supremo Tribunal Federal (STF):
- Decisão do Recurso Extraordinário (RE) 1.055.941/SP: Disponível em: STF
- Reclamação Constitucional 61.944: Disponível em: STF
- Lei 9.613/1998 (Lei de Lavagem de Dinheiro):
- Texto integral da Lei: Disponível em: Planalto
- Lei Geral de Proteção de Dados (LGPD):
- Lei 13.709/2018: Disponível em: Planalto
- Emenda Constitucional nº 115:
- Texto integral da Emenda: Disponível em: Planalto
- Medida Provisória 1.158/2023:
- Texto integral da Medida Provisória: Disponível em: Planalto
- Princípios de Egmont:
- Princípios para o Intercâmbio de Informações entre Unidades de Inteligência Financeira: Disponível em: Egmont Group
- Recomendações do GAFI (Grupo de Ação Financeira):

- 40 Recomendações do GAFI: Disponível em: FATF-GAFI
- Artigos e Comentários:
- ARAS, Vladimir; LUZ, Ilana Martins. Comentários à Lei de lavagem de dinheiro. In: PINHEIRO, Igor Pereira. Leis penais especiais comentadas na visão do STF, STJ e TSE. Leme, SP: Mizuno, 2021.
- BADARÓ, Gustavo Henrique Righi Ivahy; BOTTINI, Pierpaolo Cruz. Lavagem de dinheiro: aspectos penais e processuais penais: comentários à Lei 9.613/1988, com as alterações da Lei 12.683/2012. 2019.
- ESTELLITA, Heloisa. O RE 1.055.941: um pretexto para explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo COAF. In: Revista de Direito Público, vol. 18, n. 100, Out-Dez/2021.
- Documents – FATF (https://www.fatf-gafi.org). Acesso em 26 de junho de 2024.
- CONFEDERAÇÃO NACIONAL DA INDÚSTRIA (Brasil). EM BUSCA DE SOLUÇÕES: ATRIBUTOS DE AUTORIDADES DE PROTEÇÃO DE DADOS EFICAZES. Proteção de dados, [S. l.], p. 1-1, 1 jul. 2024. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/64/e0/64e0fce7-d49e-4b43-83aa-ab21000 8b66a/em_busca_de_solucoes_ago2017_v3.pdf. Acesso em: 28 jun. 2024.
- MARQUES, Ana Vitória Cavalcante de Carvalho. A relação entre a lei brasileira 13.709/18 e o arcabouço jurídico para proteção de dados pessoais do Japão e da Coreia do Sul a partir do modelo TLICS. 2021. 130 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Brasília, 2021.
- JUNHE LLP (China). Organização. Client Briefing: An Overview of the Draft Amendment to the Anti-Money Laundering Law. LEXOLOGY, [S. l.], p. 1-1, 9 maio 2024.
- Link: https://uplexis.com.br/blog/artigos/como-identificar-um-beneficiario-final/. Acesso em 01 de julho de 2024.
- BRASIL (Brasil). Domingues e Pinho. Beneficiários Finais: entenda como funciona essa obrigação. Artigo, [S. l.], 19 set. 2023. 1-1, p. 1-1. Disponível em: https://www.dpc.com.br/beneficiarios-finais-como-funciona/. Acesso em: 27 jun. 2024.
- SR. CORONEL ARMANDO. PL 1515 de 2022. [S. l.], 5 jan. 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274. Acesso em: 1 jul. 2024.
- O QUE são criptomoedas?. Valor Investe, [S. l.], p. 1-1, 5 abr. 2019. Disponível em: https://valorinveste.globo.com/mercados/cripto/noticia/2019/04/05/o-que-sao-criptomoedas.ghtml. Acesso em: 1 jul. 2024.
- ESTELLITA, HELOISA. Bitcoin e lavagem de dinheiro: uma aproximação. JOTA, [S. l.], p. 1-16, 7 out. 2019.

• Cf. FATF. Guidance for a risk--based approach: virtual assets and virtual asset service providers. 2019. Disponível em: www.fatfgafi.org/publications/fatfrecommendations/documents/Guidance--RBA-virtualassets.html (acesso em 23/09/2019) Cf. também FERNÁNDEZ BERMEJO, Daniel (org.). Blanqueo de capitales y TIC: marco jurídico nacional y europeo, modus operandi y criptomonedas – Ciberlaundry. informe de situación. Navarra: Thompson ReutersAranzadi, 2019, p. 81-82.