Compartilhamento de dados de pessoas politicamente expostas pelas instituições financeiras: uma proposta de modelo de gestão e mitigação de risco

Sharing data from people politically exposed by financial institutions: a proposal for a risk management and mitigation model

DOI: 10.34140/bjbv4n3-020

Recebimento dos originais: 06/05/2022
Aceitação para publicação: 30/06/2022

Alessandro Fernandes
Mestre em Gestão e Negócios pela Universidade do Vale do Rio dos Sinos – UNISINOS
Escola Gestão e Negócios UNISINOS
Av. Dr. Nilo Peçanha, 1600, Bairro Boa Vista
Porto Alegre – RS, CEP 91330-002
E-mail: alefernandesrs@gmail.com

João Zani
Doutor em Administração pela Universidade Federal do Rio Grande do Sul - UFRGS
Escola Gestão e Negócios UNISINOS
Av. Dr. Nilo Peçanha, 1600, Bairro Boa Vista
Porto Alegre – RS, CEP 91330-002

RESUMO

Para controlar todos os atos financeiros e comerciais usados para mascarar diversos ilícitos, o Brasil adotou um sistema de *colaboração compulsória entre o setor público e o privado*, *em que* profissionais e entidades que trabalham em setores mais usados por criminosos para ocultação de recursos devem notificar autoridades públicas sempre que tomarem conhecimento de operações suspeitas, principalmente pelas normas de Prevenção a Lavagem de Dinheiro e Financiamento ao Terrorismo. O compartilhamento de dados referentes a condição de Pessoas Expostas Politicamente (PEP) merece uma reflexão frente as limitações contidas na Lei Geral de Proteção de Dados (LGPD). Mesmo nos casos em que a LGPD não é aplicável, como nas atividades de investigação e repressão de infrações penais, estes procedimentos necessitam respeito aos princípios da boa-fé, finalidade, adequação e necessidade contidos nesta legislação, fazendo-se necessária a aplicação de estratégia de identificação e mitigação de riscos decorrentes desta partilha. Maior relevância ainda adquire o tema pelo fato de a adoção de políticas de *Open Banking* pelo Banco Central Brasileiro silenciar sobre o tema. O presente trabalho, em função de seus objetivos, conduziu-se como uma pesquisa bibliográfica, com abordagem exploratória e de natureza qualitativa. Construímos uma matriz de risco identificando e valorando as possíveis fragilizadas apontadas desta análise. Por fim, com base nos dados identificados nesta matriz, aplicamos o método 5W2H como ferramenta de mitigação de riscos. A severidade do impacto encontra-se em ponto crítico, principalmente pela maior atenção e potencial de ocorrência do ilícito por parte destes indivíduos, necessitando atenção total por parte da instituição financeira. Seu impacto de frequência é provável, considerando o critério elástico para sua classificação, exigindo a tomada das medidas para atenuação das ameaças. Apesar de sua alta criticidade, percebemos que as novas regras não tendem a inviabilizar os procedimentos atuais de controle, porém cada um destes pontos teve apurado seu grau de risco, através da utilização de matriz de risco, e apresentamos, utilizando análise baseada no método 5W2H, medidas necessárias para sua mitigação. Da mesma forma, a determinação dos valores (*how much*) necessários para implementação das providências apuradas pela aplicação do método 5W2H em cada instituição financeira também se constitui como limitação do presente trabalho, servindo de sugestão de pesquisa em estudos futuros.

Palavras-chave: Dados Sensíveis, Compartilhamento de Dados, Gestão de Risco.

ABSTRACT

In order to control all financial and commercial acts used to mask various illicit acts, Brazil has adopted a system of compulsory collaboration between the public and private sector, in which professionals and entities working in sectors most used by criminals to hide resources must notify authorities. public whenever they become aware of suspicious operations, mainly under the Anti-Money Laundering and Financing of Terrorism rules. The sharing of data regarding the condition of Politically Exposed Persons (PEP) deserves a reflection in view of the limitations contained in the General Data Protection Law (LGPD). Even in cases where the LGPD is not applicable, such as in the investigation and prosecution of criminal offenses, these procedures need to respect the principles of good faith, purpose, adequacy and necessity contained in this legislation, making it necessary to apply a strategy identification and mitigation of risks arising from this sharing. The topic is even more relevant due to the fact that the adoption of Open Banking policies by the Brazilian Central Bank is silent on the topic. The present work, due to its objectives, was conducted as a bibliographic research, with an exploratory approach and of a qualitative nature. We built a risk matrix identifying and valuing the possible weaknesses identified in this analysis. Finally, based on the data identified in this matrix, we apply the 5W2H method as a risk mitigation tool. The severity of the impact is at a critical point, mainly due to the greater attention and potential for the occurrence of the illicit on the part of these individuals, requiring full attention on the part of the financial institution. Its frequency impact is likely, considering the elastic criterion for its classification, requiring the taking of measures to mitigate threats. Despite its high criticality, we realized that the new rules do not tend to make the current control procedures unfeasible, but each of these points had its degree of risk determined, through the use of a risk matrix, and we present it, using analysis based on the 5W2H method. , necessary measures for its mitigation. Likewise, the determination of the values (how much) necessary to implement the measures determined by the application of the 5W2H method in each financial institution is also a limitation of the present work, serving as a research suggestion in future studies.

Keywords: Sensitive Data, Data Sharing, Risk Management.

1 INTRODUÇÃO

Para controlar todos os atos financeiros e comerciais usados para mascarar diversos ilícitos, o Brasil adotou um sistema de *colaboração compulsória entre o setor público e o privado, em que* profissionais e entidades que trabalham em setores mais usados por criminosos para ocultação de recursos devem notificar autoridades públicas sempre que tomarem conhecimento de operações suspeitas, como transações com altos valores em espécie ou depósitos fracionados (Rios, 2010).

A implementação do *Open Banking* no Brasil, inspirado em legislações vigentes na União Europeia, Hong Kong e Austrália, possibilita o compartilhamento de dados, produtos e serviços pelas instituições financeiras, a critério de seus clientes, por meio de abertura e integração de plataformas e infraestruturas de sistemas de informação, de forma segura, ágil e conveniente (BACEN, 2019).

Estas mudanças exigirão uma maior complexidade dos regulamentos atuais, uma vez que, justamente por sua contemporaneidade, amplia-se a dificuldade de identificar os riscos relacionais, principalmente no trato de dados referentes a clientes classificados como Pessoas Expostas Politicamente (PEP) pelas normas de Prevenção a Lavagem de Dinheiro e Financiamento ao Terrorismo.

O compartilhamento de dados referentes a condição de PEP merece uma reflexão frente a disposição contida na Lei Geral de Proteção de Dados (LGPD) que veta o compartilhamento de dados

sensíveis, cabendo discussão se esta condição se enquadra nessa proibição de partilha com demais instituições financeiras.

A adaptação às regras contidas na LGPD é uma preocupação de toda a sociedade, mas em especial das instituições bancárias, que necessitam de elevados volumes de dados para realizar análises para precificação dos produtos, para dosagem de seu apetite de riscos e, ainda, para a realização do processo de *Know Your Customer (KYC)*, numa economia de dados "interconectados por um sistema nervoso eletrônico" (Castells, 2013, p. 11).

Mesmo nos casos em que a LGPD não é aplicável, como nas atividades de investigação e repressão de infrações penais estes procedimentos necessito respeito aos princípios da boa-fé, finalidade, adequação e necessidade contidos nesta legislação, fazendo-se necessária a aplicação de estratégia de identificação e mitigação de riscos decorrentes desta partilha.

O presente trabalho, em função de seus objetivos, conduziu-se como uma pesquisa bibliográfica, com abordagem exploratória e de natureza qualitativa. Construímos uma matriz de risco identificando e valorando as possíveis fragilizadas apontadas desta análise. Por fim, com base nos dados identificados nesta matriz, aplicaremos o método 5W2H como ferramenta de mitigação de riscos.

OPEN BANKING

A adoção do *Open Banking* é mais uma etapa da Agenda BC#, que pretende, conforme percebe-se nas palavras do atual presidente do BACEN, Roberto Campos Neto, em um cenário de *Open Finance*:

> Já falamos em *Open Finance* e não mais em *Open Banking* porque é mais abrangente. Grande parte dos novos projetos do Banco Central está fora do mundo tradicional bancário. Há toda uma parte de finanças descentralizadas que vão ser conectadas juntamente com *Open Banking*, lembrando que o PIX se conecta ao *Open Banking*, que se conecta à moeda digital. Tudo isso faz parte de um arcabouço mais digital no futuro, onde vamos conseguir ver esses produtos navegando de forma transversal, com um custo de intermediação mais baixo (Campos Neto, 2021).

Há também uma definição "regulatória" de *Open Banking* com maior foco em transparência e que traz opções para correntistas, fazendo com que os bancos compartilhem cadastros e dados de referência (informações de origem interna e externa obtidas e usadas por diferentes partes de um banco) sobre clientes e produtos com terceiros. É possível que o *Open Banking* possa reformular os dados bancários do usuário das contas de pagamento, permitindo que empresas novas, inovadoras e modernas, compartilhem o cadastro construído pelas instituições financeiras tradicionais (Rohan, 2017).

O Brasil possui uma grande parcela da população ainda sem acesso a serviços financeiros e às condições atuais do mercado, com forte concentração, *spread* bancário elevado, incremento de cobrança de tarifas de serviços e a perspectiva de modernização regulatória, tornando-se especialmente atraentes para o investimento em *fintechs* que ofereçam soluções inovadoras (ABFINTECHS; PWC, 2018).

O modelo de *Open Banking* está diretamente associado a duas normativas jurídicas estrangeiras. Uma delas é a Diretiva 2015/2366 (União Européia, 2015) da União Europeia, responsável por alterar a regulação do sistema financeiro de pagamentos na Europa (*Second Paymment System Directive* – PSD2) e determinar a adoção de padrões tecnológicos pelos agentes de mercado que atuam neste ramo.

A segunda normativa trata da decisão da autoridade concorrencial britânica (CMA, 2017), dirigida aos principais atores do mercado financeiro do país, buscando interferir diretamente na estrutura tecnológica das instituições bancárias e na elevada taxa de concentração bancária (Goettenauer, 2018; Wilkinson, 2016).

IMPACTOS DA LGPD NO COMPARTILHAMENTO DE CADASTROS ENTRE INSTITUIÇÕES FINANCEIRAS

Importante ressaltar, ainda, que nenhuma discussão sobre compartilhamento de cadastros pode desconsiderar as regras previstas no texto da LGPD, uma vez que o Artigo 31 da Resolução Conjunta n.º 1 sublinha, ao final de sua redação, que a instituição participante é responsável "pelo cumprimento da legislação e da regulamentação e vigor" (BACEN; CMN, 2020).

Além disso, o fundamento legal do *Open Banking* já podia ser vislumbrado na própria LGPD (Trindade, 2021), conforme percebe-se da leitura de seu Artigo 18, inciso V, *in verbis*:

> Art. 18. O titular dos dados pessoais tem direito de obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> (...)
> V- A portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo da autoridade nacional, observados os segredos comercial e industrial (Brasil, 2018).

O primeiro projeto de regulamentação envolvendo questões do mundo *online* foi apresentado em 2009 e ficou conhecido como Marco Civil da Internet[1], sendo transformado em lei em 2014. Apesar de um foco diferente do texto da LGPD, foi pioneiro na delimitação de direitos e deveres para os usuários e fornecedores de serviços na internet, estabelecendo diretrizes para a atuação do governo brasileiro perante o assunto. No final de 2010, surgiram as primeiras propostas de criação de uma regulamentação específica sobre atividades envolvendo o uso e armazenamento de dados pessoais.

Em 2015, o Governo Federal realizou um debate público com vários setores da sociedade, que resultou na elaboração do primeiro Anteprojeto de Lei de Proteção dos Dados Pessoais, com clara inspiração no texto da GDPR[2], buscando estabelecer uma relação de proteção de direitos e garantias fundamentais da pessoa natural, mediante a harmonização e atualização de conceitos, mitigando riscos e

1 Lei n.º 12.965 de 23 de abril de 2014: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
2 Regulamento Geral sobre a Proteção de Dados, que trata do direito sobre a privacidade e proteção dos dados pessoais, aplicável a todos os indivíduos na União Europeia.

estabelecendo regras bem definidas sobre o tratamento de dados pessoais, fundando um marco regulatório setorial com a aprovação da Lei n.º 13.709, de 14 de agosto de 2018 (Maldonado; Blum, 2020), conforme se percebe pela transcrição abaixo:

> (...) assume o papel de principal legislação existente sobre o tema, incluindo o estabelecimento de fundamentos e princípios que transpassam a própria lei, norteando e aclarando o pensamento jurídico (Cots; Oliveira, 2019, p. 39).

A finalidade da LGPD busca abarcar os dados pessoais, tanto em sentido estrito quanto à informação obtida, na medida em que o desiderato principal da lei é a proteção de direito fundamental ligado à personalidade, trazendo conceitos de privacidade e proteção de dados pessoais (Botelho, 2020).

O compartilhamento de dados, proposto pelo *Open Banking*, tem sua forma e limites regulados pelo Artigo 5° da Resolução Conjunta n.°1 (BACEN; CMN, 2020), conforme texto abaixo colacionado:

> Art. 5° O Open Banking abrange o compartilhamento de, no mínimo:
> I - dados sobre (…)
> c) cadastro de clientes e de seus representantes; (…)
> §4º O compartilhamento de dados do cadastro que trata o inciso I, alínea "c" do caput, deve abranger:
> I - os dados fornecidos diretamente pelo cliente ou obtidos por meio de consulta a bancos de dados de caráter público ou privado, exceto:
> a) os dados classificados como dado sensível pela legislação;
> b) as notas ou pontuações de crédito;
> c) as credenciais e outras informações utilizadas com o objetivo de efetuar as autenticações do cliente; e
> II - o último dado disponível, com discriminação da data de sua obtenção (BACEN; CMN, 2020).

A LGPD prima pela busca de um ponto de equilíbrio na manutenção do desenvolvimento econômico e tecnológico de modelos de negócios inovadores, com a garantia da inviolabilidade de direitos constitucionais do cidadão (Maldonado, Blum, 2020).

DUE DILIGENCE E *KNOW YOUR CUSTOMER* (KYC)

Preliminarmente, é importante destacar a diferença entre *Due Diligence* e KYC. Ao tratar de *Due Diligence,* o escritório sobre drogas e crime das Nações Unidas expressa o seguinte entendimento:

> As medidas de Due Diligence (CDD) a serem tomadas são as seguintes:
> a) Identificar o cliente e verificar a identidade desse cliente usando dados, ou informações de fontes confiáveis e independentes;
> b) Identificar o beneficiário e tomar medidas razoáveis para verificar a identidade do beneficiário, de modo que a instituição financeira fique satisfeita por saber quem é o beneficiário dos recursos. No caso de pessoas jurídicas deve-se ainda tomar medidas razoáveis para compreender sua estrutura de propriedade e controle;
> c) Obtenção de informações sobre o objetivo e a natureza pretendida da relação comercial;
> d) Realização de devida diligência contínua sobre a relação comercial e análise das transações realizadas ao longo desse relacionamento para garantir que as transações que estão sendo conduzidas são consistentes com o conhecimento da instituição sobre o cliente, seus negócios e perfil de risco, incluindo, quando necessário, a origem dos fundos (United Nations, s.d.).

Due Diligence pode ser traduzido como "diligência prévia", referindo-se ao procedimento em que se busca todas as informações de um determinado cliente (Mclaughlin; Pavelka, 2013) .

Já o processo de KYC é a linha mestra da política de aceitação de cliente, objetivando inibir a entrada ou a manutenção de clientes que tenham suas atividades ligadas ao crime de lavagem de dinheiro (Callegari; Weber, 2017), conforme detalha o Artigo 13 da Circular n.º 3.978/2020 do BACEN:

> Art. 13. As instituições mencionadas no art. 1º devem implementar procedimentos destinados a conhecer seus clientes, incluindo procedimentos que assegurem a devida diligência na sua identificação, qualificação e classificação (BACEN, 2020).

Podemos afirmar que Due Diligence se refere a processos mais vinculados a regras de conformidade técnica, enquanto KYC vincula-se a procedimentos centrados na aferição de sua efetividade (BACEN, 2018).

Mesmo que a coleta dos documentos para início da relação negocial enquadre-se em procedimentos mais vinculados ao conceito de *Due Diligence,* é inegável que esta oportunidade de contato é uma ocasião ímpar para coletar informações necessárias para cumprir regras de efetividade próprias ao KYC.

Porém, mesmo antes da implantação do *Open Banking*, percebe-se um processo de digitalização das operações em todo o Sistema Financeiro, possibilitando cada vez mais a realização de cadastros e operações em um ambiente digital, através de canais alternativos ao atendimento em agências físicas, o que já criava obstáculos a esta oportunidade de realmente conhecer o cliente.

Independente da origem dos dados cadastrais, a instituição financeira deve, em função das obrigações decorrentes da Circular n.º 3.978/2020 da BACEN, tomar todos os procedimentos necessários para qualificar seus clientes, conforme percebe-se pela leitura do artigo abaixo citado:

> Art. 18. As instituições mencionadas no art. 1º devem adotar procedimentos que permitam qualificar seus clientes por meio da coleta, verificação e validação de informações, compatíveis com o perfil de risco do cliente e com a natureza da relação de negócio.
> § 1º Os procedimentos de qualificação referidos no caput devem incluir a coleta de informações que permitam avaliar a capacidade financeira do cliente, incluindo a renda, no caso de pessoa natural, ou o faturamento, no caso de pessoa jurídica.
> § 2º A necessidade de verificação e de validação das informações referidas no § 1º deve ser avaliada pelas instituições de acordo com o perfil de risco do cliente e com a natureza da relação de negócio.
> § 3º Nos procedimentos de que trata o caput, devem ser coletadas informações adicionais do cliente compatíveis com o risco de utilização de produtos e serviços na prática da lavagem de dinheiro e do financiamento do terrorismo.
> § 4º A qualificação do cliente deve ser reavaliada de forma permanente, de acordo com a evolução da relação de negócio e do perfil de risco.
> § 5º As informações coletadas na qualificação do cliente devem ser mantidas atualizadas.
> § 6º O Banco Central do Brasil poderá divulgar rol de informações a serem coletadas, verificadas e validadas em procedimentos específicos de qualificação de clientes (BACEN, 2020).

2 METODOLOGIA

O presente trabalho, em função de seus objetivos, conduziu-se como uma pesquisa documental, com abordagem exploratória e de natureza qualitativa.

A pesquisa documental se aproxima da pesquisa bibliográfica, residindo sua diferença na natureza das fontes. Enquanto a pesquisa bibliográfica foca em contribuições de diversos autores sobre um tema, a pesquisa documental recorre a documentos que ainda não receberam tratamento analítico (Oliveira, 2007). Neste trabalho nos propomos a uma análise da legislação pertinente aos dois temas centrais deste trabalho: o ilícito de lavagem de dinheiro e a regulamentação da Lei Geral de Proteção de Dados.

Construímos uma matriz de risco identificando e valorando as possíveis fragilizadas apontadas desta análise, uma vez que a identificação de possíveis riscos é um pré-requisito para um eficiente gerenciamento e mitigação de seus danos (Kaplan; Leonard; Mikes, 2020).

Com base nos dados identificados nesta matriz, aplicaremos o método 5W2H como ferramenta de mitigação de riscos. O nome 5W2H vem das palavras em inglês: *what, why, who, where, when, how e how much*, e constitui-se como um instrumento vastamente utilizado para que se realize um plano de ação eficaz, possibilitando colocar em prática medidas mitigadores de eventuais riscos (Silva, 2009).

Em função de se tratar de um estudo que pretende analisar as instituições financeiras de forma genérica, sem distinção de porte ou forma de funcionamento, optamos por não determinar valores necessários para implementação dos procedimentos de mitigação de risco, estabelecendo como "a determinar" para o campo *how much.*

PESSOAS EXPOSTAS POLITICAMENTE

Pessoas expostas politicamente (PEP) são, na definição do Artigo 1°, § 2° da Circular n.º 3.339 (BACEN, 2006):

> Consideram-se pessoas politicamente expostas os agentes públicos que desempenham ou tenham desempenhado, nos últimos cinco anos, no Brasil ou em países, territórios e dependências estrangeiros, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo (BACEN, 2006).

A circular 3.978/2020 da BACEN, em seu Artigo 27, estabelece os procedimentos que as instituições financeiras devem tomar para qualificação de PEP:

> Art. 27. As instituições mencionadas no art. 1º devem implementar procedimentos que permitam qualificar seus clientes como pessoa exposta politicamente.
> § 1º Consideram-se pessoas expostas politicamente:
> I - os detentores de mandatos eletivos dos Poderes Executivo e Legislativo da União;
> II - os ocupantes de cargo, no Poder Executivo da União, de:
> a) Ministro de Estado ou equiparado;
> b) Natureza Especial ou equivalente;
> c) presidente, vice-presidente e diretor, ou equivalentes, de entidades da administração pública indireta; e

d) Grupo Direção e Assessoramento Superiores (DAS), nível 6, ou equivalente;
III - os membros do Conselho Nacional de Justiça, do Supremo Tribunal Federal, dos Tribunais Superiores, dos Tribunais Regionais Federais, dos Tribunais Regionais do Trabalho, dos Tribunais Regionais Eleitorais, do Conselho Superior da Justiça do Trabalho e do Conselho da Justiça Federal;
IV - os membros do Conselho Nacional do Ministério Público, o Procurador-Geral da República, o Vice-Procurador-Geral da República, o Procurador-Geral do Trabalho, o Procurador-Geral da Justiça Militar, os Subprocuradores-Gerais da República e os Procuradores Gerais de Justiça dos Estados e do Distrito Federal;
V - os membros do Tribunal de Contas da União, o Procurador-Geral e os Subprocuradores-Gerais do Ministério Público junto ao Tribunal de Contas da União;
VI - os presidentes e os tesoureiros nacionais, ou equivalentes, de partidos políticos;
VII - os Governadores e os Secretários de Estado e do Distrito Federal, os Deputados Estaduais e Distritais, os presidentes, ou equivalentes, de entidades da administração pública indireta estadual e distrital e os presidentes de Tribunais de Justiça, Tribunais Militares, Tribunais de Contas ou equivalentes dos Estados e do Distrito Federal; e
VIII - os Prefeitos, os Vereadores, os Secretários Municipais, os presidentes, ou equivalentes, de entidades da administração pública indireta municipal e os Presidentes de Tribunais de Contas ou equivalentes dos Municípios.
§ 2º São também consideradas expostas politicamente as pessoas que, no exterior, sejam:
I - chefes de estado ou de governo;
II - políticos de escalões superiores;
III - ocupantes de cargos governamentais de escalões superiores;
IV - oficiais-generais e membros de escalões superiores do Poder Judiciário;
V - executivos de escalões superiores de empresas públicas; ou
VI - dirigentes de partidos políticos.
§ 3º São também consideradas pessoas expostas politicamente os dirigentes de escalões superiores de entidades de direito internacional público ou privado.
4º No caso de clientes residentes no exterior, para fins do disposto no caput, as instituições mencionadas no art. 1º devem adotar pelo menos duas das seguintes providências:
I - solicitar declaração expressa do cliente a respeito da sua qualificação;
II - recorrer a informações públicas disponíveis; e
III - consultar bases de dados públicas ou privadas sobre pessoas expostas politicamente.
§ 5º A condição de pessoa exposta politicamente deve ser aplicada pelos cinco anos seguintes à data em que a pessoa deixou de se enquadrar nas categorias previstas nos §§ 1º, 2º, e 3º.
§ 6º No caso de relação de negócio com cliente residente no exterior que também seja cliente de instituição do mesmo grupo no exterior, fiscalizada por autoridade supervisora com a qual o Banco Central do Brasil mantenha convênio para troca de informações, admite-se que as informações de qualificação de pessoa exposta politicamente sejam obtidas da instituição no exterior, desde que assegurado ao Banco Central do Brasil o acesso aos respectivos dados e procedimentos adotados (BACEN, 2020).

A legislação brasileira é aderente à Convenção das Nações Unidas contra a Corrupção (Brasil, 2006), que recomenda expressamente que cada país adote as medidas necessárias, no sentido de exigir das instituições financeiras que funcionam em seu território que desenvolvam controles internos, a fim de verificar a identidade dos clientes, determinem os beneficiários finais dos recursos depositados, e intensifiquem seu escrutínio de toda conta solicitada ou mantida pelo nome de pessoas que desempenhem ou tenham desempenhado funções públicas eminentes, de seus familiares e estreitos colaboradores – as chamadas Pessoas Politicamente Expostas (Salvo, 2010), conforme os termos da Recomendação 12 da GAFI.

> Recomendação 12. Pessoas expostas politicamente
> As instituições financeiras deveriam, em relação às pessoas expostas politicamente (PEPs) estrangeiras, além das medidas normais de devida diligência ao cliente, ser obrigadas a:
> (a) ter sistemas adequados de gerenciamento de riscos para determinar se o cliente ou beneficiário é pessoa exposta politicamente;
> (b) obter aprovação da alta gerência para estabelecer (ou continuar, para clientes existentes) tais relações de negócios;
> (c) adotar medidas razoáveis para estabelecer a origem da riqueza e dos recursos; e
> (d) conduzir monitoramento reforçado contínuo da relação de negócios.
> As instituições financeiras deveriam ser obrigadas a adotar medidas razoáveis para determinar se um cliente ou beneficiário é uma PEP ou pessoa que ocupa função importante em uma organização internacional. Nos casos de relações de negócios de mais alto risco com essas pessoas, as instituições financeiras deveriam ser obrigadas a aplicar as medidas referidas nos parágrafos (b), (c) e (d).
> As exigências para todas as PEPs também se aplicam a familiares ou pessoas próximas dessas PEPs (FATF, 2019b).

Atendendo a esta recomendação, o COAF resolveu que as pessoas arroladas no Artigo 9º da Lei 9.613[3] deverão adotar as providências previstas nesta Resolução, para o estabelecimento de relação de

3 Art. 9º Sujeitam-se às obrigações referidas nos arts. 10 e 11 as pessoas físicas e jurídicas que tenham, em caráter permanente ou eventual, como atividade principal ou acessória, cumulativamente ou não:
I - a captação, intermediação e aplicação de recursos financeiros de terceiros, em moeda nacional ou estrangeira;
II – a compra e venda de moeda estrangeira ou ouro como ativo financeiro ou instrumento cambial;
III - a custódia, emissão, distribuição, liquidação, negociação, intermediação ou administração de títulos ou valores mobiliários.
Parágrafo único. Sujeitam-se às mesmas obrigações
I – as bolsas de valores, as bolsas de mercadorias ou futuros e os sistemas de negociação do mercado de balcão organizado;
II - as seguradoras, as corretoras de seguros e as entidades de previdência complementar ou de capitalização;
III - as administradoras de cartões de credenciamento ou cartões de crédito, bem como as administradoras de consórcios para aquisição de bens ou serviços;
IV - as administradoras ou empresas que se utilizem de cartão ou qualquer outro meio eletrônico, magnético ou equivalente, que permita a transferência de fundos;
V - as empresas de arrendamento mercantil (*leasing*), as empresas de fomento comercial (*factoring*) e as Empresas Simples de Crédito (ESC);
VI - as sociedades que efetuem distribuição de dinheiro ou quaisquer bens móveis, imóveis, mercadorias, serviços, ou, ainda, concedam descontos na sua aquisição, mediante sorteio ou método assemelhado;
VII - as filiais ou representações de entes estrangeiros que exerçam no Brasil qualquer das atividades listadas neste artigo, ainda que de forma eventual;
VIII - as demais entidades cujo funcionamento dependa de autorização de órgão regulador dos mercados financeiro, de câmbio, de capitais e de seguros;
IX - as pessoas físicas ou jurídicas, nacionais ou estrangeiras, que operem no Brasil como agentes, dirigentes, procuradoras, comissionárias ou por qualquer forma representem interesses de ente estrangeiro que exerça qualquer das atividades referidas neste artigo;
X - as pessoas físicas ou jurídicas que exerçam atividades de promoção imobiliária ou compra e venda de imóveis;
XI - as pessoas físicas ou jurídicas que comercializem joias, pedras e metais preciosos, objetos de arte e antiguidades;
XII - as pessoas físicas ou jurídicas que comercializem bens de luxo ou de alto valor, intermedeiem a sua comercialização ou exerçam atividades que envolvam grande volume de recursos em espécie;
XIII - as juntas comerciais e os registros públicos;
XIV - as pessoas físicas ou jurídicas que prestem, mesmo que eventualmente, serviços de assessoria, consultoria, contadoria, auditoria, aconselhamento ou assistência, de qualquer natureza, em operações:
a) de compra e venda de imóveis, estabelecimentos comerciais ou industriais ou participações societárias de qualquer natureza;
b) de gestão de fundos, valores mobiliários ou outros ativos;
c) de abertura ou gestão de contas bancárias, de poupança, investimento ou de valores mobiliários;
d) de criação, exploração ou gestão de sociedades de qualquer natureza, fundações, fundos fiduciários ou estruturas análogas;
e) financeiras, societárias ou imobiliárias; e
f) de alienação ou aquisição de direitos sobre contratos relacionados a atividades desportivas ou artísticas profissionais;
XV - pessoas físicas ou jurídicas que atuem na promoção, intermediação, comercialização, agenciamento ou negociação de direitos de transferência de atletas, artistas ou feiras, exposições ou eventos similares;
XVI - as empresas de transporte e guarda de valores;
XVII - as pessoas físicas ou jurídicas que comercializem bens de alto valor de origem rural ou animal ou intermedeiem a sua comercialização; e
XVIII - as dependências no exterior das entidades mencionadas neste artigo, por meio de sua matriz no Brasil, relativamente a residentes no País (BRASIL, 1998).

negócios e o acompanhamento de operações ou propostas de operações realizadas pelas Pessoas Politicamente Expostas (COAF, 2007).

A regulamentação do *Open Banking* veta, de forma expressa em seu Artigo 5°, II (BACEN; CMN, 2020), o compartilhamento dos dados classificados como sensíveis pela legislação vigente – no caso a LGPD –, cabendo uma discussão se este diploma legal poderá ser empecilho para compartilhamento de informações de clientes classificados de PPE[4].

> Art. 5° Para fins desta lei, considera-se:
> (...)
> II – Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado à pessoa natural; (BRASIL, 2018).

Parece-me que, neste caso, mesmo nas situações em que se trata de dados sensíveis, como as de ocupantes de cargo de presidência e tesouraria de diretórios nacionais de partido (art. 27, § 1°, VI da Circular BACEN 3.978/2020), aplicam-se as hipóteses de dispensa de aplicação, contidas no Artigo 4° da LGPD.

Entendo que estes dados deverão ser objeto de compartilhamento pelo *Open Banking*, mesmo que as regras de ressarcimentos contidos no Capítulo V, Seção VI, da Resolução Conjunta n. 1 (BACEN; CMN, 2020), vetem qualquer cobrança por sua disponibilização, uma vez que no Artigo 5°, I, c, § 4º, I é expresso:

> O compartilhamento de dados do cadastro que trata o inciso I, alínea "c" do caput, deve abranger:
> I- os dados fornecidos diretamente pelo cliente ou obtidos por meio de consulta a bancos de dados de caráter público ou privado (BACEN; CMN, 2020).

Pessoas expostas politicamente (PEP) são alvo de especial preocupação nos procedimentos para prevenção à lavagem de dinheiro, sendo, inclusive, objeto de preocupação da Recomendação de n.º 12 da GAFI, exigindo cuidados adicionais para o estabelecimento de relação de negócios e o acompanhamento de operações ou propostas de operações por elas realizadas, não se aplicando qualquer limitação decorrente da LGPD.

3 RESULTADOS E DISCUSSÕES

A LGPD apresenta, em seu artigo 4°, as hipóteses em que suas determinações não devem limitar o compartilhamento de dados, e o inciso III, d, abaixo transcrito, é totalmente pertinente à presente discussão:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> (...)
> III - realizado para fins exclusivos de:(...)
> d) atividades de investigação e repressão de infrações penais; ou
> (...) (BRASIL, 2018).

4 A condição de PPE não consta do rol de informações cadastrais obrigatórias de compartilhamento pelo *Open Banking*, limitando a regular os casos em que o cliente ocupa atualmente uma das ocupações listadas pela circular 3.978/2020 BACEN.

Pela leitura do texto legal, pode-se concluir que a LGPD não regula a necessidade de coleta de dados para atividades de investigação e repressão de infrações penais, e este entendimento engloba o processo de KYC, que vincula as instituições financeiras a um modelo de colaboração compulsória e*ntre o setor público e o privado em que as instituições financeiras,* devendo notificar autoridades públicas sempre que tomarem conhecimento de operações suspeitas vinculadas a ocorrência de ilícito de lavagem de dinheiro e financiamento ao terrorismo (Badaró; Bottini, 2016; Estellita; Tumbiolo, 2020).

Porém, esta disposição não exclui as instituições financeiras de atentar para limitações em seu tratamento, conforme percebemos pela leitura de seu artigo 7°, § 6, respeitando em especial os princípios da boa-fé, finalidade, adequação e necessidade[5].

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> (...)
> § 6°: "eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular
> (...) (BRASIL, 2018).

Assim, frente às demais exigências decorrentes da LGPD, as instituições deverão revisar e adequar suas estruturas de *compliance*, orientadas para a prevenção de lavagem de dinheiro, garantindo a adoção de boas práticas que permitam tratamento certo, adequado e transparente dos dados pessoais (Guariento, 2021), determinando assim a Matriz de Risco descrita na Figura 1 que segue abaixo, localizando os riscos decorrentes do compartilhamento de dados cadastrais de clientes classificados como PEP:

5 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL, 2018).

Figura 1 – Matriz de Risco

Matriz de Risco (Impacto x Frequência)			Frequência (Probabilidade de Ocorrência)			
			(1) EXTREMAMENTE REMOTA	(2) REMOTA	(3) PROVÁVEL	(4) POSSÍVEL
			1	2	3	4
Impacto (Severidade)	(4) CRÍTICO	4	4	8	PEP 12	16
	(3) SEVERO	3	3	6	9	12
	(2) MODERADO	2	2	4	6	8
	(1) REDUZIDO	1	1	2	3	4

Fonte: Elaborado pelo autor (2021) com base em Allen, 2013.

A severidade do impacto encontra-se em ponto crítico, principalmente pela maior atenção e potencial de ocorrência do ilícito por parte destes indivíduos, necessitando atenção total por parte da instituição financeira. Seu impacto de frequência é provável, considerando o critério elástico para sua classificação, exigindo a tomada das medidas descritas no Quadro 1 para atenuação das ameaças.

Quadro 1 – Método 5W2H

Método 5W2H – PEP		
5W	*What*	Implementar medidas adicionais de validação de veracidade de dados compartilhados referente a clientes PEP.
	Who	Diretoria responsável pela condução do PLD e adaptação ao *Open Banking.*
	Where	Todas as unidades da instituição financeira.
	When	Medidas devem ser implementadas sempre que a instituição receber cadastros compartilhados.
	Why	Para manter abordagem baseada em risco aderente à implementação do *Open Banking.*
2H	*How*	Através da revisão de processos e procedimentos relativos ao recebimento de cadastros de terceiros.
	How Much	A determinar.

Fonte: Elaborado pelo autor (2021) com base em Silva, 2009.

Por sua importância junto aos métodos de controle, seria recomendável a criação de uma lista unificada, de caráter colaborativo e de acesso irrestrito a todas as instituições participantes pela Unidade de Inteligência Financeira Nacional, no caso o COAF. Frisa-se que já existe uma lista PEP COAF, mas percebe-se que esta lista é de difícil acesso e consulta e, principalmente, não é tão completa como a fornecida por birôs externos. Sua aplicação garantiria uma atuação uniformizada das instituições financeiras, atuando diretamente na mitigação do risco de desconsiderar esta condição dos clientes em sua atuação negocial.

Quadro 2 – Método 5W2H – Lista PEP

Método 5W2H – Lista PEP		
5W	*What*	Criação de lista nacional atualizada e acessível contendo relação de clientes PEP.
	Who	COAF e/ou FEBRABAN.
	Where	Todas as Instituições Financeiras.
	When	Imediatamente.
	Why	Unificar a base e uniformizar o tratamento entre as instituições bancárias.
2H	*How*	Centralização de dados cadastrais através de padronização de dados por parte da Unidade de Inteligência Financeira Nacional.
	How Much	A determinar.

Fonte: Elaborado pelo autor (2021) com base em Silva, 2009.

Percebe-se, ainda, que a condição de PEP tem potencial para agravar a criticidade dos cuidados exigidos pela LGPD para o tratamento dos dados compartilhados, ou ainda daqueles passíveis de compartilhamento.

4 CONSIDERAÇÕES FINAIS

O presente estudo buscou identificar e analisar a ocorrência de riscos decorrentes do compartilhamento de dados de clientes classificados na condição de PEP através da confecção de uma matriz de riscos para dimensionar, onde ponderou-se as disposições dos regulamentos legais sobre o tema.

Importante frisar que, conforme podemos perceber da análise da Figura 1, o ponto de análise localizara em quadrante de controle de situação crítica, necessitando que tanto as instituições financeiras como autoridades reguladoras se dediquem ao desenvolvimento de controles de elevada certeza, para garantir a mitigação dos seus impactos.

Apesar de sua alta criticidade, percebemos que não tende a inviabilizar os procedimentos atuais de controle, porém cada um destes pontos teve apurado seu grau de risco, através da utilização de matriz de risco, e apresentamos, utilizando análise baseada no método 5W2H, medidas necessárias para sua mitigação.

A utilização de birôs para validar os dados compartilhados para composição de Lista de Clientes PRP se constitui como ferramenta essencial para validação dos dados de controle. Os entraves que a LGPD pode exercer sobre estas empresas parceiras é uma limitação da pesquisa, uma vez que não incluídas nos objetivos do trabalho, constituindo-se em tema relevante para pesquisas posteriores.

Da mesma forma, a determinação dos valores (*how much*) necessários para implementação das providências apuradas pela aplicação do método 5W2H em cada instituição financeira também se constitui como limitação do presente trabalho, servindo de sugestão de pesquisa em estudos futuros.

REFERÊNCIAS

Allen, C. (2013). Risky Bussiness: How to Build a Risk Matrix, 518 kb, ePub.

ABFINTECHS – Associação Brasileira de Fintechs, & PWC – Price Water House Coopers Brasil Ltda. (2018). Pesquisa Fintech Deep Dive. 2018.

BACEN – Banco Central do Brasil. (2006). Circular n. 3.339, de 22 de dezembro de 2006: Dispõe acerca dos procedimentos a serem observados pelos bancos múltiplos, bancos comerciais, caixas econômicas, cooperativas de crédito e associações de poupança e empréstimo para o acompanhamento das movimentações financeiras de pessoas politicamente expostas. Brasília: Banco Central do Brasil.

BACEN – Banco Central do Brasil. (2018). Relatório de Estabilidade Financeira. Brasília.

BACEN – Banco Central do Brasil. (2020). Circular n. 3.978, de 23 de janeiro de 2020: Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016. Brasília: Banco Central do Brasil.

BACEN – Banco Central do Brasil; CMN – Conselho Monetário Nacional. (2020) Resolução conjunta n. 1, de 04 de maio de 2020: Dispõe sobre a implementação do Sistema Financeiro Aberto (*Open Banking*). Brasília: Banco Central do Brasil. Diário Oficial da União.

Botelho, M. C. (2020) A LGPD e a proteção de dados pessoais de crianças e adolescentes. Revista Direitos Sociais e Políticas Públicas: UNIFAFIBE, vol. 8, pp. 197-231. http://dx.doi.org/10.25245/rdspp.v8i2.705.

Brasil. (1998). Lei n. 9.613, de 3 de março de 1998: Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. Brasília: Diário Oficial da União.

Brasil. (2006). Decreto n. 5.687, de 31 de janeiro de 2006: Promulga a Convenção das Nações Unidas contra a Corrupção, adotada pela Assembleia-Geral das Nações Unidas em 31 de outubro de 2003 e assinada pelo Brasil em 9 de dezembro de 2003. Brasília: Diário Oficial da União.

Brasil (2011). Lei n. 12.414, de 09 de junho de 2011: Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília: Diário Oficial da União.

Brasil. (2018). Lei n. 13.709, de 14 de agosto de 2018: Lei Geral da Proteção de Dados (LGPD), com redação dada pela Lei n. 13.853 de 08 de julho de 2019. Brasília: Diário Oficial da União.

Callegari, A. L.; WEBER, A. B. (2017). Lavagem de Dinheiro. 2. ed. rev. atual. e ampl. São Paulo: Atlas.

Campos Neto, R. (2021). *Open Banking*. Brasília. Twitter: @BancoCentralBR.

Castells, M. (2013). A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar.

CMA – Competetion & Markets Authority. (2017). Remedie Implementation Programme Board (RIPB). Londres.

COAF – Conselho de Atividades Financeiras. (2007). Resolução COAF nº 16 de 28/03/2007: Dispõe sobre os procedimentos a serem observados pelas pessoas reguladas pelo COAF, na forma do § 1º do artigo 14 da Lei 9.613, de 3 de março de 1998, relativamente a operações ou propostas de operações realizadas por pessoas politicamente expostas.

Cots, M.; Oliveira, R. (2019). Lei Geral de Proteção de dados pessoais comentada. 2. ed. São Paulo: Revista dos Tribunais.

Estellita, H.; Tumbiolo, M. (2020). LGPD e programas de prevenção à lavagem de dinheiro. Jota.

FATF – Financial Action Task Force. (2019). The FATF Recommendations. Paris: France.

Goettenauer, C. (2018). *Open banking* e teorias da regulação da internet. São Paulo: Revista de Direito Bancário e do Mercado de Capitais, v. 82, pp. 109-130.

Kaplan, R. S.; Leonard, H. B. D.; Mikes, A. (2020). Os riscos que você não prevê: que fazer quando não existe manual. Harvard Business Review Brasil. pp. 20-26.

Maldonado, V. N.; Blum, R. O. (2020). LGPD: Lei Geral de Proteção de Dados Comentada [livro eletrônico]. Ver., atual. e ampl. São Paulo: Thomson Reuters Brasil.

Mclaughlin, J. S.; Pavalka, D. (2013). The use of customer due diligence to combat money laundering. Accountancy Business and Public Interest, pp. 57–84.

Oliveira, M. M. (2007). Como fazer pesquisa qualitativa. Petrópolis: Vozes.

Rios, R. S. (2010). Direito Penal Econômico: advocacia e lavagem de dinheiro: questão de dogmática jurídico-penal e de política criminal. São Paulo: Saraiva.

Rohan, P. (2017). Open Banking Strategy Formation. Califórnia: Create Space Independent Publishing Platform.

Salvo, M. (2010) O Combate à Lavagem de Dinheiro como Inibidor da Corrupção no Brasil: custos e benefícios dos controles internos na fiscalização das pessoas politicamente expostas. *UC Berkeley: Berkeley Program in Law and Economics*

Silva, G. G. M. P. (2009). Implantando a manufatura enxuta: Um método estruturado, p. 157. Dissertação (Mestrado em Engenharia da Produção). Programa de Pós-Graduação em Engenharia de Produção, UFSC, Florianópolis.

Trindade, M. G. N. (2021). Open Banking: Trinômio Portabilidade-Interoperabilidade-Proteção de Dados Pessoais no Âmbito do Sistema Financeiro. Lisboa: Revista Jurídica Luso-Brasileira, pp. 1159-1188. ISSN: 2183-539X.

União Europeia. (2015). Diretiva 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.1093/2010, e que revoga a Diretiva 2007/64/CE. Jornal Oficial das Comunidades Europeias.

United Nations. (s.d). Office on Drugs and Crime. Money Laundering and The Financing of Terrorism: The United Nations response. Vienna.

Wilkinsons, D. (2016). Open Banking and the API Economy. FinTech Network.