CAC COMTEXTO

EDIÇÃO Nº 03 - NOVEMBRO 2020

OAB PINHEIROS | COMISSÃO ANTICORRUPÇÃO E COMPLIANCE

EDITORES:
Renata F. Andrade (coordenação)
Mariana de Almada Jeveaux
Pedro Roncarati

REVISORES:
Aline de Oliveira Silva
Igor Fernandez de Moraes

AUTORES:
Adriana Babi
Amanda dos Santos Figueiredo
Amanda Kathleen Di Marchi Peçanha
Ana Caroline Ferreira
Claudia da Costa Bonard de Carvalho
Edmo Colnaghi Neves
Gabriela de Ávila Machado
Isabella Zampini Veneroso
Juliana Fosalusa da Silva
Julio Cesar Chaves
Mariana de Almada Jeveaux
Michelle Fernanda de Oliveira Souza
Pedro Ackel
Rafael Sgoda Tomazeti
Rhaiza de Souza

COMPLIANCE ANTI CORRUPÇÃO INOVAÇÃO

ARCHER

Solução líder GARTNER para

- **Compliance, Controles Internos e PLD**
- **Riscos Operacionais e Corporativos**
- **Riscos de TI e Segurança**
- **Continuidade dos Negócios**
- **Gestão de Terceiros**
- **Auditoria**

contato@athenasolucoes.com
athenasolucoes.com

Conte com Athena a maior provedora de Professional Services para RSA Archer do Brasil

ATHENA
SOLUÇÕES INTELIGENTES

Editorial

RENATA FONSECA DE ANDRADE

Advogada – Brasil e Estados Unidos; Mestre pela University of Wisconsin-Madison School of Law, LLM-MLI USA; Bacharel em Direito pela Universidade Mackenzie; Presidente da Comissão de Anticorrupção e *Compliance* da OAB/SP Pinheiros.

Esse ano 2020 é atípico e exige muita resiliência. Resiliência física, mental e ética. Os profissionais de *Compliance* também sentiram em suas vidas, empresas e atividades todos os desafios e angústias próprias da crise global que ultrapassamos. Muitos perderam familiares, amigos e também parte substancial de suas receitas e empregos.

Todos vivemos esse momento com a esperança de superação da crise, de dias melhores e torcendo para sairmos dessa mais fortalecidos. A Comissão Anticorrupção e *Compliance* – CAC OAB/SP Pinheiros permanece cumprindo sua missão, mantendo as reuniões temáticas, as recomendações em audiências públicas e estudos permanentes no âmbito da ética, anticorrupção e *compliance*, e assim apresentamos a 3ª Edição da CAC COMTEXTO.

Agradecemos aos autores dessa 3ª edição que generosamente compartilham suas experiências e conhecimento em torno dos temas: ANTICORRUPÇÃO, *COMPLIANCE* e INOVAÇÃO. Parabéns a todos pela resiliência e dedicação.

Nós, da CAC OAB/SP Pinheiros, dedicamos essa edição à Sociedade Brasileira em constante transformação.

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) 3071-1086
www.editoraroncarati.com.br
contato@editoraroncarati.com.br

Índice

Apresentação

2020 – Um ano desafiador

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.

Mais uma vez tenho a honra de ser convidado pela Comissão de Anticorrupção e *Compliance* da OAB Pinheiros (CAC), para escrever em sua revista.

Revisitando os artigos anteriores me deparei com um artigo cheio de expectativa para 2020, planejando eventos e reuniões, organizando comissões e grupos de trabalho e, finalmente, no âmbito específico do *compliance* se preparando para a entrada em vigor da Lei Geral de Proteção de Dados (LGPD).

E, eis que de supetão, nos deparamos com um 2020 avassalador que colocou todos os nossos planos de ponta cabeça. Ao invés de reuniões e eventos, tivemos o distanciamento social. Abruptamente migramos do presencial para o virtual. E, até mesmo, a entrada em vigor da LGPD foi feita de forma confusa e desordenada.

Em que pese as dificuldades que 2020 nos reservou, é certo que em momentos como esses em que temos que demonstrar nossa resiliência e capacidade de reação. E aqui está a CAC trabalhando, conseguindo editar mais uma revista, mantendo o excelente trabalho e fortalecendo o estudo do *Compliance* e da Anticorrupção.

São exemplos como esse que nos enche de ânimo para continuar trabalhando em prol da nossa classe e do fortalecimento da cultura e das instituições jurídicas.

Agradeço pelo empenho de todos os integrantes da CAC por continuarem o trabalho voluntário diante de tanta adversidade e, também, registro meu agradecimento a todos os colaboradores da terceira edição da revista.

Prefácio

Compliance – Anticorrupção – Desafio 2020

FABYOLA EN RODRIGUES

Sócia das áreas Penal Empresarial e de Compliance, Fabyola En Rodrigues lidera o Departamento Criminal Empresarial de Demarest. Possui mais de 20 anos de experiência e alta especialização: doutora em Direito Criminal Empresarial e mestre em Direito Criminal pela PUC-SP e especialista em Crime Empresarial pela FGV. E Vice-Presidente da Comissão de Anticorrupção e Compliance da Ordem dos Advogados do Brasil, Subseção de Pinheiros (OAB-SP), membro do Comitê de Anticorrupção da American Bar Association (ABA), membro do Comitê de Crimes Transnacionais do International Bar Association (IBA) e membro do Comitê de Compliance do Instituto dos Advogados de São Paulo (IASP)

No decorrer desse ano ímpar de 2020, a Comissão de Anticorrupção e Compliance da OAB/Pinheiros não apenas manteve a interação entre todos os seus integrantes, como aumentou o fluxo de reuniões, e discussões valendo-se da adaptabilidade aos recursos virtuais, permitindo assim um aumento importante na presença de novos integrantes em suas reuniões.

Nessa terceira edição, o livro reúne 10 artigos contendo abordagens diversas, com temas da maior atualidade, bem como fundamentais a todo programa eficiente de *Compliance*.

A coletânea contou com a coordenação da Renata Andrade, Mestre pela University of Wisconsin-Madison School of Law, LLM-MLI USA; Bacharel em Direito pela Universidade Mackenzie e Presidente da Comissão.

Participam da obra os autores Adriana Balbi, Amanda Figueiredo, Amanda Kathleen Di Marchi Peçanha, Ana Caroline Ferreira, Claudia Carvalho, Edmo Colnaghi Neves, Gabriela Machado, Juliana Fosaluza da Silva, Julio Cesar Chaves Cocolichio, Mariana Jeveaux, Michelle Fernanda de Oliveira Souza, Pedro Teixeira Leite Ackel, Rafael Sgoda Tomazeti, Rhaiza de Souza.

Na última década temos acompanhado importantes mudanças legislativas trazendo uma crescente responsabilização para o empresário, não apenas na esfera administrativa, civil, mas em especial criminal.

Determinando a importância da gestão dos negócios com foco na mitigação dos riscos, valorizando o envolvimento da alta administração na definição das políticas de governança, nos treinamentos de Compliance, na definição da comunicação.

A comunicação nunca ocupou um papel tão central no mundo.

O Brasil vivenciou na última década uma mudança expressiva de percepção em relação a questões essenciais como cumprimento a lei e combate à corrupção. Operações como a Lava Jato, representam uma mudança de paradigma relevante para toda a sociedade.

Isto porque, mais do que depositar no Judiciário expectativas sobre o controle da corrupção, mudanças foram vistas nos compromissos assumidos pelas empresas em alterar o quadro da alta administração, implementando eficientes programas de integridade e gestão de risco.

Em março do presente ano, em menos de duas semanas, inúmeras empresas públicas e privadas tiveram que se organizar para instituir o regime de trabalho remoto, milhares de pessoas tiveram que administrar o exercício das suas profissões em meio a dinâmica do lar.

E o regime de teletrabalho passou a ser exercido através de ferramentas como o zoom, Microsoft Teams, Hangouts, Whatsapp, Skype, entre outras. E através dessas mesmas ferramentas os departamentos de Compliance tiveram que dar continuidade às investigações em curso, quer seja realizando entrevistas, quer seja concluindo pela apresentação de denúncias às autoridades judiciais.

A pandemia trouxe flexibilidade para as regras de contratação com o poder público e nesse momento de regime de exceção, as empresas precisam redobrar ainda mais os requisitos internos, buscando documentar todo o processo para evitarem um envolvimento em um futuro escândalo de corrupção.

Embora o momento seja de urgência e se tenha necessidade em estabelecer uma comunicação rápida, as empresas devem investir tempo e tecnologia na proteção dos dados. O sequestro de dados ou "ransonware" aumentou exponencialmente durante a pandemia, assim como as fraudes cibernéticas e fake news, demandando uma reação imediata do departamento jurídico e uma ação preventiva ao departamento de Compliance.

A pandemia coloca em permanente "teste" a área de compliance das empresas, trazendo situações novas que precisam de respostas rápidas em um contexto de muitas regras flexibilizadas e outras tantas novas como a LGPD que entrou em vigência.

Nos artigos constantes nessa obra coletiva vocês poderão encontrar abordagens específicas sobre os pontos acima abordados, entre outros, boa leitura a todos.

Os Desafios do Combate à Lavagem de Dinheiro em um Mundo Pandêmico

ADRIANA BABI BENETTI DE SOUZA

Mestre em Ciências Sociais – PUCSP (2012), Pós-Graduada em Administração de Empresas – FAAP (2001), Graduada em Comunicação Social – FAAP (1999). Possui mais de 15 anos de experiência em área de *Compliance*, atuando nos segmentos financeiro e da saúde. Atualmente é associada da consultoria 2ic *Compliance*, foi head de *Compliance* do Royal Bank of Canada e trabalhou como *Compliance* Officer no banco JP Morgan, na Itaú Seguros, no Banco Votornatim e no Banco HSBC, também atuou como Consultora de Investimentos, Cross Border Referral e Gerente de Produtos.

Em um cenário de pandemia cheio de incertezas os esforços estão direcionados para a busca da normalidade, e o que sabemos é que por algum tempo ainda viveremos esse "novo normal", mas como conceituar a realidade atual na perspectiva do combate à Lavagem de Dinheiro e do Financiamento do Terrorismo (LD/FT)?

Lavagem de Dinheiro e Terrorismo

Em termos gerais o crime de a lavagem de dinheiro consiste na transformação de recursos obtidos de forma ilícita em recursos lícitos, no Brasil é regulamentado pela Lei 9.613, de março de 1998, é importante pontuar que o delito de lavagem de dinheiro tem aspectos acessórios e necessita ter uma conexão com um crime derivado ou dependente, logo um crime anterior, do qual decorreu a obtenção de vantagem financeira, nesta perspectiva, ilegal. Entre os setores sujeitos a norma estão a maioria dos agentes e entidades que atuam em atividades relacionadas ao Sistema Financeiro Nacional, assim como os setores de bens de luxo, cartões de crédito ou credenciamento, *factoring* e securitização de ativos, títulos ou recebíveis

mobiliários, joias, pedras e metais preciosos, direitos de transferências de atletas e artistas, remessas alternativas de recursos, serviços de assessoria, consultorias, auditoria, aconselhamento e assistência.

Enquanto que o terrorismo consiste na prática de atos criminosos pretendidos ou calculados para provocar um estado de terror no público em geral, este último, normatizado pela Lei 13.260 de março de 2016, que não só regulamentou o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, e tratando de disposições investigatórias e processuais, mas também reformulando o conceito de organização terrorista, alterando normativos preambulares.

Os terroristas financiam suas atividades de diversas formas e buscam angariar recursos tanto através de fontes ilícitas como também de fontes aparentemente lícitas, como organizações não governamentais, e empresas regulares, por intermédio de fraudes, do contrabando, do comércio ilegal de drogas e de armas, entre outros crimes. De acordo com o *Institute for Economics and Peace (IEP),* os dados sobre o terrorismo mundial têm apresentando quedas, em seu último relatório, *Global Terrorism Index,* de 2019 o instituto constatou a redução significativa nos indicadores de mortes, segundo a publicação o número absoluto dos casos totalizou o montante de 15.952, representando uma queda de 52% em comparação ao indicador de 2014, evidenciando o declínio acentuado da atividade terrorista. Muito embora a intensidade do terrorismo tenha diminuído a amplitude não reduziu, os indicadores de 2018 apontam que ao menos um incidente terrorista foi registrado em 103 países, ademais cerca de 71 países sofreram pelo menos uma fatalidade no mesmo período, destacando a necessidade de ações continuadas para o combate positivo do terrorismo, concomitantemente se olharmos para os indicadores de lavagem de dinheiro, verificamos que o produto do crime lavado, anualmente, chega a atingir um volume que varia de 2% a 5% do PIB do planeta, cerca de 1,6 a 4 trilhões de dólares por ano, segundo estimativas do escritório de Drogas e Crimes da Nações Unidas (UNODC).

Principais Organismos

Entre as entidades dedicadas ao combate à lavagem de dinheiro e crimes relacionados é importante salientar o papel do Financial Action Task Force/Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI), cooperação internacional de carácter informal, estabelecida inicialmente como uma força-tarefa de ação financeira para conter os fluxos financeiros associados a drogas e ao tráfico, no âmbito da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). No campo nacional a relevância fica com o Conselho de Controle de Atividades Financeiras (COAF), que tem como finalidade coordenar, disciplinar, aplicar penas administrativas, receber, examinar e identificar as ocorrências suspeitas de atividades de lavagem de dinheiro, e com a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA), principal articulador das discussões e arranjos entre os três poderes e o Ministério Público, nas esferas, Federal, Estadual e Municipal, além de formular políticas públicas e soluções voltadas para o combate à lavagem de dinheiro e crimes relacionados, a ENCCLA elabora inúmeras ações direcionadas para a produção de conhecimento, capacitação, o desenvolvimento de estruturas e sistemas, bem como o avanço e aperfeiçoamento de normas.

A Lavagem de Dinheiro e a Pandemia

Embora o crime de lavagem de dinheiro possa estar frequentemente associado ao terrorismo, invariavelmente outras

atividades criminosas o precedem, a realidade atual deixa essa situação cada vez mais evidente, e de acordo com o documento publicado em maio deste ano pelo GAFI, *COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses,* essa nova dinâmica, isto é a crise de saúde pública – COVID19, comprovou a conexão entre os mais diversos crimes e a lavagem de dinheiro, e não só permitiu a avaliação assertiva sobre o impacto da crise na sociedade, mas também propiciou o melhor direcionamento e a adoção de medidas preventivas pelas jurisdições impactadas. A publicação que não representa oficialmente a posição do grupo, contou com informações recebidas de mais de 200 integrantes, entre os quais encontravam-se países membros, órgãos regionais, organizações observadoras, como o Fundo Monetário Internacional, o Banco Mundial e a Organização das Nações Unidas. O material tem um viés qualitativo e teve como pilar central a análise dos documentos compartilhados pelos próprios membros da rede global, o objetivo central da publicação é auxiliar a sociedade na busca por respostas céleres para as ameaças acerca da lavagem de dinheiro e crimes relacionados.

Entre as tendências verificadas ficou constatado que os trabalhos e a interação remota assumiram um papel protagonista durante a crise, a migração de colaboradores do ambiente corporativo para o ambiente residencial certamente sinalizam uma mudança de rumo para as relações de trabalho, da mesma maneira trabalhos considerados menos essenciais acabaram, houve também o crescimento nas vendas online e o aumento surreal das demandas por produtos e serviços de saúde, como os insumos e equipamentos de proteção e equipamentos médicos, principalmente respiradores. Outro fator observado durante o levantamento foi a manutenção das operações de bancos e instituições financeiras, embora os bancos tenham apresentado limitação na oferta de serviços presenciais, as mesmas permaneceram estáveis, concomitantemente ocorreu o redirecionamento dos recursos públicos para o setor da saúde, já os setores voltados para o comércio global, as viagens, e o turismo foram extremamente prejudicados.

Esse novo ambiente também afetou o crime organizado, que em função da nova perspectiva, redirecionou e intensificou seus esforços para outras frentes, como os crimes cibernéticos, entre eles a exploração de grupos vulneráveis, o tráfico humano, assim como a exploração de crianças no ambiente virtual. O documento ainda retratou o aumento notável na recorrência dos crimes de fraude, especialmente aqueles em que falsários se passam por colaboradores de serviços oficiais, com a intenção de aplicar golpes, assim como aqueles em que há a utilização de intermediários para a aquisição de produtos, neste último caso, incidindo sobre os ventiladores pulmonares importados, cujos preços foram extremamente inflacionados, a adulteração de insumos e equipamentos, a arrecadação de recursos para instituições de caridades falsas e até mesmo a oferta de investimentos fraudulentos entre outros. Na esfera dos crimes cibernéticos, o que se viu foi o aumento nas denúncias relativas aos ataques do tipo *phishing*, prática fraudulenta que consiste no envio de e-mails falsos e atribuídos a empresas reconhecidas, com o intuito de obter informações pessoais, como senhas e números de cartão de crédito, assim como a utilização de softwares maliciosos, *ransonware*, usados para a paralisação de sistemas, extorsão, e cobrança de resgates. Paralelamente, ocorreu um aumento das denúncias referentes a corrupção, desvios de fundos governamentais e de organismos de assistência financeira internacional, em especial por meio de transações remotas, muito em

consequência da falta de familiaridade dos usuários com as plataformas online. A desaceleração econômica, amplamente percebida, o aumento das transações físicas em dinheiro, a comercialização de ativos virtuais, as práticas envolvendo *insider trading* e a maior volatilidade da indústria financeira, assim como o financiamento do terrorismo também estão entre as considerações reportadas e analisadas no documento.

As informações consolidadas e os relatos, assim como as práticas adotadas pelos membros do GAFI possibilitaram a elaboração tempestiva de recomendações para os países membros e demais governantes, entre as quais estão: a necessidade de se estabelecer um movimento de coordenação doméstico eficaz, ou seja, os países devem avaliar internamente e apropriadamente os riscos e o impacto da crise COVID-19 em seus sistemas de prevenção e combate à lavagem de dinheiro e de crimes relacionados, igualmente devem endereçar de forma correta os riscos identificados, tanto no setor privado mas principalmente na esfera pública, inclusive no que tange a participação das unidades de inteligência. Outras questões como o fortalecimento da comunicação com o setor privado e a maior proatividade na aplicação das medidas de prevenção, detecção e combate, o encorajamento do uso de metodologias baseadas em risco e o incentivo ao uso de soluções inovadoras – capazes de identificar clientes na integração e durante a realização de transações, assim como o apoio as opções de meios de pagamento eletrônico e digital, também foram reportadas.

As observações ressaltam que o foco nos mais diversos segmentos também deve ser objeto de atenção dos governantes, em algumas jurisdições constatou-se uma dedicação maior a prevenção dos crimes envolvendo jogos online e transações com moedas e metais preciosos, como o ouro, deixando um pouco de lado os esforços e a atenção ao setor financeiro, especialmente aquelas englobando transações em espécie. Além das transações atípicas identificadas, como a realização de saques e o imediato repasse de recursos públicos, muitas jurisdições adotaram boas práticas criando grupos de trabalho e relatórios específicos para lidar com os crimes relativos a crise de saúde, a compreensão e a formação de parcerias entre os países, assim como as parcerias públicas e privadas também foi percebida como algo essencial, o diferencial dos países na prevenção e no combate dos crimes, com isso o documento sublinha a relevância da cooperação entre os países, sobretudo no que diz respeito ao reporte das unidades de inteligência, em especial aquelas relativas aos desenvolvimentos ou quaisquer interrupções operacionais que possam afetar as respostas de cooperação internacional ao secretariado do *Grupo Egmont*, organização internacional que facilita a cooperação e o compartilhamento de informações entre as unidades de inteligência, da mesma forma foi dada ênfase ao monitoramento do setor privado, visto que o prolongamento da crise pode abalar o funcionamento e a atuação dos agentes reguladores.

Após a publicação do referido documento o COAF emitiu uma nota de esclarecimento sobre a atuação da instituição no contexto da crise de saúde pública. No comunicado, a instituição informou que "vem trabalhando de forma vigilante e coordenada, promovendo a interação com outros órgãos da administração pública e com os setores obrigados", na ocasião, além dos indicadores sobre as comunicações suspeitas recebidas dos setores obrigados (189) e das autoridades competentes (121), a instituição divulgou os principais sinais de alerta detectados no país, sendo alguns deles convergentes com a experiência reportada pelo relatório do GAFI, e outros específicos, na perspectiva interna

as suspeitas recaem sobre: a obtenção de empréstimo por funcionários de empresas de equipamentos médicos com o objetivo de transitar recursos possivelmente desviados de contratos administrativos, com a posterior devolução dos valores à empresa empregadora ou empresas associadas, a contratação com dispensa de licitação e o superfaturamento de preços por empresas com características de fachada e intermediadoras, a pronta transferência de recursos públicos a terceiros sem relacionamento financeiro aparente, e que originalmente seriam destinados à compra de equipamentos ou insumos para o combate à pandemia, a transferência de recursos para servidores públicos por empresas que receberam pagamentos decorrentes de contratos administrativos, ordens de pagamento do exterior justificadas como comissões por vendas de máquinas hospitalares por pessoa sem histórico de atuação no ramo, a criação de empresas de fachada em nome de familiares para transitar recursos desviados, fraudes no pagamento de auxílio emergencial, assim como a realização de saques em espécie imediatamente após o recebimento de repasses de recursos públicos.

Os impactos apontados no documento do GAFI e pelo COAF não representam a totalidade dos desafios que o Brasil tem pela frente, as medidas para o enfrentamento da emergência de saúde pública definidas pela Lei n.º 13.979 e pelas normas relacionadas, expressam a fragilidade e as lacunas existentes, e representam uma ameaça adicional na detecção e punição dos crimes de lavagem de dinheiro e relacionados, em especial no que corresponde a dispensa do processo de licitação para aquisição ou contratação de bens e serviços, e a flexibilização na estimativa de preços das situações tidas como excepcionais, como por exemplo as hipóteses de contratação, em caráter eventual de fornecedor de bem ou prestador de serviço, mesmo impedido por sanções ou suspensões.

Recomendações Nacionais e Internacionais

A última avaliação mútua do Brasil, relatório do GAFI baseado nas 40 recomendações referentes ao combate à lavagem de dinheiro e nas 9 recomendações especiais sobre financiamento do terrorismo, realizada em 2010 apresentou críticas contundentes ao país, na ocasião a visão da entidade foi de que a estrutura de criminalização é deficitária, segundo a avaliação o sistema apresentava complexidade e limitação de recursos, especialmente em relação as estatísticas sobre investigações, denúncias e condenações, assim como o comprometimento da capacidade de processar e obter condenações finais por lavagem de dinheiro.

A resposta do Brasil veio em 2012 através das alterações realizadas na lei de Lavagem de Dinheiro, entre os aspectos reformulados estão a eliminação do rol de crimes antecedentes, que converteu em criminosa a lavagem de quaisquer proventos de crimes ou contravenções, a ampliação da lista de agentes sujeitos ao registro e reporte de transações suspeitas para o regulador ou unidade de inteligência, de forma a abranger além de instituições financeiras outras entidades assemelhadas, o que incluiu também filias de empresas brasileiras no exterior, a exigência para a criação de políticas e controles internos compatíveis com o porte das operações, assim como a necessidade do cadastro no órgão regulador, fiscalizador ou no COAF, compreendendo também a declaração de não ocorrência de fatos passíveis de serem reportados (declaração negativa), igualmente a obrigatoriedade da comunicação prévia de transferências internacionais e saques em espécie.

Quando ampliamos o foco e observamos outros países membros é possível afirmar que o desafio não está só com o Brasil,

nessa empreitada o país não caminha sozinho, a atualização do documento intitulado *"International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation"* também do GAFI, ocorridas em 2012, trouxe indicadores bem razoáveis e preocupantes para os mais de 150 países membros que participaram da pesquisa, de acordo com a revisão apenas 1% apresentaram um alto nível de eficiência nos programas de prevenção e combate à lavagem de dinheiro e combate ao financiamento do terrorismo, os demais apresentaram níveis substanciais, moderados ou baixos, respectivamente 24%, 32% e 18%, tal resultado trouxe à tona o debate acerca do que ainda precisa ser feito, e entre as mudanças reveladas ficou clara a necessidade de fortalecimento das estruturas usadas para detectar, prevenir e punir crimes financeiros, com isso, além de mudar o escopo da avaliação de acompanhamento direcionando seus esforços para as áreas onde os países atingiram níveis baixos ou moderados, o grupo quer assegurar que os países membros tenham leis, regulamentos e organismos apropriados, capazes de avaliar se as medidas são eficazes e os resultados esperados serão entregues.

Próxima Avaliação

O Brasil passará por outra avaliação mútua do GAFI a partir de janeiro de 2021, neste contexto é possível afirmar que o país vem empregando esforços e adotando medidas não só objetivando a manutenção no grupo mas também focando no atendimento das exigências e das demandas trazidas recentemente pelas discussões ocorridas no plenário de Paris, tais como, a necessidade de reforço das estruturas normativas e o maior controle das práticas PLD/FT pelos países. Internamente, já é possível constatar algumas das medidas adotadas ao longo desse período e que estão voltadas para o cumprimento das exigências, entre as quais podemos destacar a publicação da Lei 13.810, de março de 2019, que estabelece o bloqueio de bens de pessoas e organizações ligadas a crimes de LD/FT e o Decreto 10.270 de março de 2020, que instituiu o Grupo de Trabalho de Avaliação de Riscos de LD/FT e Financiamento da Proliferação de Armas de Destruição em Massa no âmbito nacional, o grupo será responsável por elaborar diagnósticos para identificar, avaliar e compreender os riscos no país, com o propósito de subsidiar ações de órgãos e entidades competentes, e deverá elaborar a sua primeira avaliação no intervalo de um ano, o COAF também irá coordenar as ações que serão desenvolvidas no âmbito do Ministério Público Federal, conforme menciona a Portaria 195, de março de 2020, e a aceitação do convite pelo Ministério viabilizará a obtenção de diversos dados estatísticos sobre as principais ameaças que os crimes de lavagem de dinheiro e relacionados têm para o país, esse último grupo será composto por membros e servidores das Câmaras Criminal, de Meio Ambiente e Patrimônio Cultural, de Combate à Corrupção e de Sistema Prisional e de Controle Externo da Atividade Policial, além dos integrantes das Secretarias de Cooperação Internacional (SCI), da Secretaria de Perícia Pesquisa e Análise (SPPEA), e da Secretaria de Estado Justiça e Cidadania (SEJUD).

A avaliação também mobilizou os agentes reguladores do Sistema Financeiro Nacional, tanto o Banco Central (BACEN), como a Comissão de Valores Mobiliários (CVM) e a Superintendência de Seguros Privados (SUSEP), publicaram novas normas que não só atualizam mas também modernizam as diretrizes relativas a prevenção e combate à lavagem de dinheiro, principalmente no que tange as suas políticas, a avaliação interna de risco, os procedimentos para a identificação e diligência de clientes, parceiros e colaboradores, o registro de

operações, o monitoramento de operações e situações suspeitas, assim como medidas que assegurem a implementação, a adequação e a avaliação da efetividade destes procedimentos e controles internos. Entre as exigências, estão aquelas que disparadamente irão impactar e demandar uma atenção especial da indústria financeira como a avaliação do risco de lavagem de dinheiro e a avaliação da efetividade dos programas, em outras palavras, o setor financeiro precisa mudar o enfoque dado ao gerenciamento da prevenção a lavagem de dinheiro, isto é, sair do padrão detectivo e migrar para uma condição proativa. Com isso em mente, os agentes do sistema financeiro devem integrar organicamente ideias, mecanismos, requisitos de controle de risco, da mesma maneira, desenvolver uma gestão de negócios unificada a gestão de risco, propiciando o estabelecimento de uma estrutura sólida e uma gestão compatível e efetiva, as novas diretrizes estão internamente dispostas nas Circulares Nº 3.978 do BACEN e Nº 612 da SUSEP e na Instrução Normativa Nº 617 da CVM.

Outro indicativo de que o Brasil tem se empenhado na agenda LD/FT está na comissão de juristas que irá propor mudanças para a Lei de Lavagem de Dinheiro, a equipe de trabalho foi criada pelo presidente Câmara dos Deputados, Rodrigo Maia (DEM-RJ), e será presidida pelo ministro do Supremo Tribunal Federal, Alexandre de Moraes, o foco inicial do grupo será elaborar um anteprojeto que delimite e estabeleça diretrizes que contemplem as medidas investigativas e processuais e também propor mudanças legislativas que assegurem o intercâmbio e o compartilhamento de informações entre os órgãos competentes e de inteligência, lado a lado, em tramitação encontra-se o projeto de Lei N° 4516, do Senador Arolde de Oliveira (PSD/RJ) que recomenda a inclusão das pessoas físicas ou jurídicas que prestem serviços de advocacia ou de consultoria jurídica no rol de pessoas sujeitas aos mecanismos de controle e prevenção à lavagem de dinheiro, embora não seja precursor o projeto do senador coloca o Brasil em linha com as diretrizes internacionais.

Outras Crises

Nem tudo é empenho, as seguidas reestruturações do COAF, agora dispostas na Lei 13.974 de janeiro de 2020, a exoneração do diretor-geral da Polícia Federal, Maurício Valeixo e a saída do ministro da Justiça, Sergio Moro representaram um golpe na credibilidade do país, não só sentido pelo mercado financeiro, que na ocasião viu o índice bovespa, principal indicador do desempenho médio das cotações das ações negociadas na bolsa de valores brasileira despencar mais de 6%, chegando a 74.681 pontos, enquanto a moeda americana atingiu o patamar de R$ 5,60, mas também no âmbito internacional, representando um abalo na imagem interna e externa do país.

O ministro Sergio Moro é uma referência mundial no combate à corrupção, e tem seu trabalho reconhecido por inúmeras entidades, inclusive como uma das personalidades mais influentes da década, pelo Financial Times, e certamente a sua saída terá um peso na condução da agenda anticorrupção do país, algo que já estamos vivenciando, seja pela interferência da política nas instituições anticorrupção, ou através da influência no Judiciário. Recentemente, a confirmação do entendimento pela 2ª Turma do Supremo Tribunal Federal, de que delatados podem questionar acordos de delação premiada para se defender, corroborou com essa percepção, segundo o relator, o ministro Gilmar Mende "a proteção jurisprudencial a acordos de delação serviu para blindar ilegalidades", essa entre outras questões foram objeto da denúncia

feita pela organização não governamental, Transparência Internacional ao GAFI, não sendo essa a primeira denúncia contra o Brasil, em 2019 o Sindicato Nacional dos Auditores-Fiscais da Receita Federal do Brasil, já havia feito uma queixa sobre os retrocessos institucionais no combate à corrupção e à lavagem de dinheiro em território brasileiro, assim como sobre o conhecimento e impacto das decisões do Supremo Tribunal no trabalho de investigação criminal no país.

Inexplicavelmente, a crise brasileira e a certa morosidade por parte do Brasil em atender as diretrizes internacionais, não colocam o país numa situação menos desconfortável do que a vivenciada pelos Estados Unidos, os escândalos envolvendo o vazamento de documentos internos do Financial Crimes Enforcement Network, FINCEN, unidade de inteligência ligada ao departamento do tesouro dos Estados Unidos, ocorridos nos últimos cinco anos, apontam que alguns dos maiores bancos do mundo permitiram que criminosos movimentassem dinheiro sujo além fronteira. Os documentos mencionam um montante de cerca e 2 trilhões de dólares em transações e demonstram ainda como os oligarcas russos usaram os bancos para evitar sanções que deveriam impedi-los de colocar o dinheiro no ocidente. Em resposta, a unidade de inteligência americana, FINCEN, publicou uma proposta de regulamentação, *Advanced Notice For Proposed Rulemaking,* cujo período para comentários encerrará próximo ao final deste ano, aumentando a preocupação em torno do assunto visto que nenhuma nova regra será proposta até a referida data. A imprensa americana é unânime em afirmar que os regulamentos existentes e os processos de conformidade dos bancos são insuficientes, tal situação irá impactar e mobilizar a indústria para o fato de que desenvolver uma cultura sedimentada no princípio da abordagem baseada em risco é um caminho sem volta, suscitando a necessidade do reforço nos processos de diligência dos clientes, base para a gestão efetiva, a prevenção, detecção e o combate à lavagem de dinheiro e crimes relacionados, a preocupação com o monitoramento das transações em tempo real passará a ser fundamental, a avaliação do risco em produtos e a necessidade de ferramentas de tecnologia de informação avançada entrarão na ordem do dia. Nesse sentido, existe uma oportunidade para o Brasil se antecipar e fazer o dever de casa, abrandando a possibilidade de incorrer nos mesmos erros que o vizinho, Estados Unidos, no que tange a resposta do GAFI sobre o ocorrido, a instituição informou ter conhecimento dos relatos da imprensa, assim como sobre a divulgação dos documentos da FINCEN, mas informou que não iria comentar nada sobre o teor dos relatórios, uma vez que as informações produzidas pelas unidades de inteligência têm caráter confidencial, um dos princípios do Grupo Egmont.

Apesar dos avanços com as pesquisas científicas e a perspectiva para a conclusão de vacinas eficazes, ainda estamos vivendo em um mundo pandêmico, e embora o retorno à normalidade seja algo previsível, teremos também que lidar com o legado da adoção de medidas repentinas e irrefletidas adotadas pela maioria dos governantes em função da crise de saúde. Nos próximos anos, o Brasil terá um longo caminho a percorrer, considerando as diretrizes e trabalhos internacionais, o cenário pandêmico, as crises internas e além fronteira, a economia e seus desdobramentos, neste contexto as perspectivas para o combate à Lavagem de Dinheiro serão no mínimo desafiadoras.

Notas

O Grupo de Ação Financeira Internacional, GAFI, em inglês, Financial Action Task Force, ou FATF, é um agrupamento governamental internacional de carácter informal,

criado em 1989, com propósito de desenvolver e promover políticas nacionais e internacionais de combate à lavagem de dinheiro e ao financiamento do terrorismo.

O grupo criou um guia com 40 recomendações para que os países signatários adotem padrões e promovam a efetiva implementação de medidas legais, regulatórias e operacionais de combate a crimes que ameaçam o sistema financeiro.

O Conselho de Controle de Atividades Financeiras, COAF, órgão criado no âmbito do Ministério da Fazenda, foi instituído pela Lei 9.613, de 1998, e atua eminentemente na prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo. O §1º do artigo 14 da lei também atribuiu ao Coaf a competência de regular os setores econômicos para os quais não haja órgão regulador ou fiscalizador próprio.

O Grupo Egmont é uma organização internacional que facilita a cooperação e o compartilhamento de informações entre as unidades nacionais de inteligência financeira para investigar e impedir a lavagem de dinheiro e o financiamento do terrorismo.

Referências bibliográficas

INSTITUTE FOR ECONOMICS & PEACE. Global Terrorism Index 2019: Measuring the Impact of Terrorism, Sydney, Novembro 2019. Disponível em: http://visionofhumanity.org/reports (accessed Date Month Year).

FATF (2020), COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses, FATF, Paris, France, Maio 2020. Disponível em: www.fatf-gafi.org/publications/methodandtrends/documents/covid-19-ML-TF.html.

FATF (2012-2019), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, Junho 2019. Disponível em: www.fatf-gafi.org/recommendations.html.

Modelo das Três Linhas: o Papel da Primeira Linha nas Políticas de PLD/FT em Instituições Financeiras

AMANDA KATHLEEN DI MARCHI PEÇANHA

Bacharel em Relações Internacionais pela Universidade Anhembi Morumbi e cursando MBA em Governança em *Compliance* pela Universidade Federal de São Carlos. Atua desde 2017 no mercado financeiro, trabalhando em grandes bancos internacionais nas áreas de Onboarding, Middle Office e *Compliance*/ AML. Também possui experiência internacional reportando diretamente para a corretora do BTG Pactual situada nos Estados Unidos. Atualmente é membro da Comissão Anticorrupção e *Compliance* da OAB/SP Pinheiros e da Comissão de Estudos de *Compliance* da OAB/São Paulo.

MICHELLE FERNANDA DE OLIVEIRA SOUZA

Bacharela em Relações Internacionais com ênfase em Gestão Financeira pela UAM e cursando MBA de Gestão em *Compliance* pela UFSCar. Atuante no setor bancário há dois anos, com experiência em front e middle office. Co-autora do artigo "As Políticas de PLD-CFT no Brasil e a Influência do FATF/GAFI" (2019), publicado na Revista de Direito Bancário e do Mercado de Capitais (RDB), pela Thomson Reuters.

Introdução

Diante de escândalos, fraudes e um sistema regulatório cada vez mais desenvolvido ao longo dos últimos anos, os *stakeholders* e autoridades do governo voltam às atenções ao risco como um fator

concomitante aos objetivos corporativos. Especialmente em um contexto criado pelo "novo normal", que também mudou as formas de trabalho e agitou as dinâmicas interpessoais impondo relações à distância e exposição a novos riscos.

Com a responsabilização das empresas e dos altos escalões, cresce cada vez mais a necessidade de promover um ambiente integrado e alinhado em todos os níveis para buscar a otimização de resultados mitigando riscos, responsabilizando individualmente cada linha de colaboração.

O Modelo COSO e o Modelo de Três Linhas (IIA) dizem respeito à abordagem e gestão de riscos voltada para o controle interno da organização. É com base nisso que esse artigo se propõe a refletir sobre esses modelos, analisando de que forma cada papel pode contribuir para mitigar os riscos reputacionais e regulatórios no cumprimento de suas funções, trazendo as definições e responsabilidades de cada linha e enfatizando a relevância da primeira linha (representada por *front office*, *middle Office* e *back office*) sendo este o primeiro contato da relação cliente-instituição. Não obstante, explicitaremos, de modo prático, cenários possíveis de percepção de risco na primeira linha para prevenção de lavagem de dinheiro e combate ao financiamento do terrorismo.

O COSO (*Committee of Sponsoring Organizations*)

O COSO (*Committee of Sponsoring Organizations*) é uma organização privada sem fins lucrativos que tem como objetivo principal a criação de estruturas, recomendações e guias para gestão de riscos, controles internos com foco em prevenir e reduzir fraudes corporativas além de desenvolver melhorias para governança organizacional. (COSO, 2020)

O comitê propõe o gerenciamento de riscos com uma visão voltada à estrutura integrada da organização. Foca em três objetivos: operacionais; relatórios confiáveis; e conformidade legal. No enfoque operacional, preocupa-se em abranger todo o complexo organizacional. A organização introduz novas perspectivas à análise de risco ao envolver todos os setores empresariais do maior ao menor nível, ao invés de olhar apenas o que se relaciona com regulamentações e relatórios, o que até então protagonizava as áreas de controle.

THE IIA (*The Institute of Internal Auditors*)

The Institute of Internal Auditors (IIA) é uma associação profissional internacional fundada em 1941 com o objetivo de estruturar e formalizar a condição profissional do auditor interno. Sediada nos Estados Unidos, está presente em mais de 160 países abordando os campos de auditoria interna, gerenciamento de riscos, governança, controle interno, auditoria de TI, educação e segurança. (The Institute of Internal Auditors, 2020).

Revisão do modelo das três linhas

Existem vários conceitos acerca do Modelo de Três Linhas.A companhia Brasiliano Interisk, por exemplo, que atua no mercado de soluções para gestão de riscos, descreve o quão imprescindível é, tendo um contexto cada vez mais complexo de riscos, que sejam promovidos esforços coordenados para garantir conformidade com os planejamentos. A empresa define o modelo da seguinte forma:

> "As Três Linhas de Defesa são um modelo de Governança Corporativa de atuação da área de gestão de riscos, *compliance*, controles internos e auditoria que organizam as funções de cada linha e descentraliza o processo de controle, dando aos usuários dos processos operacionais e estratégicos a responsabilidade primária de realizar o respectivo controle, com supervisão para que haja cobertura em todos os níveis da empresa". (BRASILIANO INTERISK, 2019).

Em julho de 2020, o IIA liberou o Modelo das Três Linhas, uma revisão do modelo das Três Linhas de Defesa. Considerado uma evolução por compreender todo o corpo administrativo, demonstrando de forma clara as responsabilidades e funções, inclusive da gestão executiva e auditoria interna. (Instituto dos Auditores Internos do Brasil, 2020).

Deste modo, de acordo com o Instituto dos Auditores Internos do Brasil, o Modelo de Três Linhas ajuda as organizações a identificarem as melhores estruturas e processos para cumprimento de objetivos e auxilia na facilitação da governança e gerenciamento de riscos.

Um ponto importante que foi adicionado à revisão do modelo é o reforço à relevância da criação de estruturas e procedimentos necessários para prestações de contas através de uma supervisão corporativa no qual garante integridade, transparência e liderança. Além de obter uma definição mais clara das responsabilidades do órgão de governança, para uma governança assertiva e eficiente, estando alinhados com o propósito da companhia.

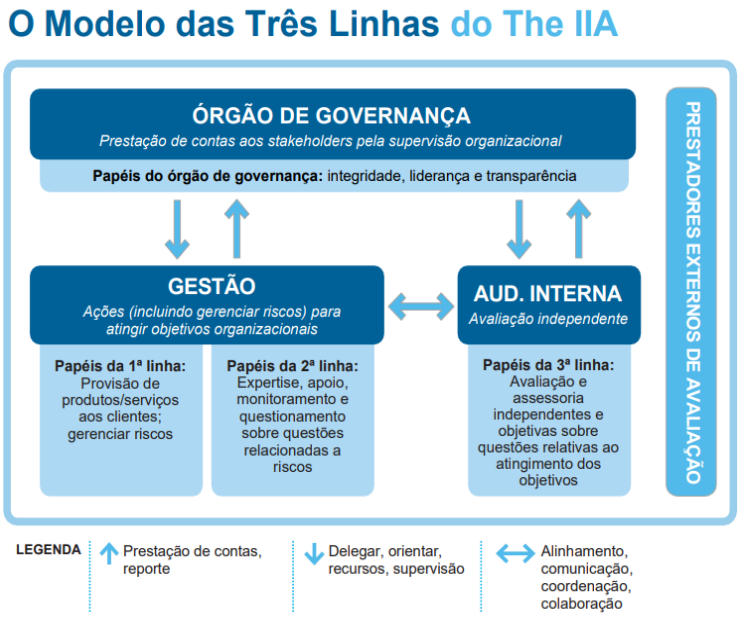
Nesse contexto, a Alta Administração fica responsável pela supervisão e monitoramento dos processos de gestão de risco, sendo atendido pelos resultados provenientes de todas as áreas envolvidas, o que compreende a Primeira e a Segunda Linha.

A Primeira Linha tem ligação direta à gestão operacional, sendo aliada à entrega de produtos/serviços ao cliente. Em suma, compreende as atividades do *front*, *middle* e *back office* e inclui funções de suporte ao cliente. O modelo enfatiza a responsabilidade da gerência de riscos, que devem ser alinhados junto ao corpo diretivo.

Em paralelo, na Segunda Linha concentram-se nas funções complementares que detêm conhecimento e fornecem apoio e monitoramento sobre as questões de riscos, em suporte interno que assegura o funcionamento das atividades. São exemplos as áreas de *Legal*, *Compliance*, Controles Internos, Tecnologia da Informação, Segurança e Qualidade.

Já na Terceira Linha, situam-se as funções de auditoria interna, responsáveis por avaliar com independência a Primeira e a Segunda Linha. É onde acontecem inspeções, investigações, remediações e reportes à Alta Administração para promover acurácia e segurança.

Na figura abaixo, o IIA explicita seu modelo das três linhas de forma didática, demonstrando os fluxos e divisões das três linhas adicionando o órgão de governança como supervisor organizacional:



Fonte: The Institute of Internal Auditors, 2020[1]

1 Disponível em: <https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf>, Acesso em: 05 outubro 2020.

O IIA baseia-se em seis princípios para adequar as circunstâncias aos objetivos organizacionais dentro deste contexto. Nos Princípios 1 e 2, fala-se da governança e em seu papel, levando como premissa uma tomada de decisão voltada a analisar, planejar, monitorar e revisar o alinhamento com os riscos paralelamente aos objetivos. No Princípio 3, esclarecendo os papéis da primeira e segunda linha enfatizando a importância do gerenciamento de riscos como prioridade da gerência, que deve ser guiada pelos riscos associados aos objetivos definidos em alinhamento com a governança.

Já nos princípios 4 e 5, a abordagem é voltada aos papéis da terceira linha salientando a necessidade de autonomia nessa linha. A FERMA (Federação das Associações Europeias de Gestão de Riscos) reafirma a importância dessa imparcialidade, argumentando que a auditoria interna independente e profissional contribui ativamente para uma governança corporativa altamente eficaz e deve fazer parte das melhores práticas.

Por último, no princípio 6 é evidenciado a necessidade de comunicação, cooperação e colaboração em esforço coletivo entre os papéis e as linhas, reforçando a intenção do modelo em promover uma estrutura integrada.

A importância da primeira linha para prevenção à lavagem de dinheiro e financiamento ao terrorismo

A partir dos conceitos e divisões das três linhas, a entidade obtém a capacidade de identificar variados riscos, incluindo estratégicos; financeiros; imagem e reputação; legais e regulatórios ou de conformidade; operacionais; e socioambientais. Neste sentido, abordaremos o risco de lavagem de dinheiro e combate ao financiamento ao terrorismo demonstrando sua intrínseca relação a uma adequada gestão de riscos corporativa.

Conforme já apresentado, o Modelo de Três Linhas tem a função de gerenciar os riscos de forma coletiva. Cada um com sua atribuição e responsabilidade faz parte da gestão de riscos suscetíveis aos negócios. Contudo, o enfoque neste artigo será na primeira linha de defesa, uma vez que as relações cliente-instituição se iniciam nesse contexto.

Para exemplificar as ações e prevenções que devem ser analisadas pela primeira linha, dividiremos por funções, sendo estas *front office*, *middle office* e *backoffice*[2].

A área de *front office,* amplamente representada pelo comercial ou gerência de relacionamento, é responsável pela prospecção e carteira de clientes. Por esta razão, é necessário o conhecimento inicial dos riscos de lavagem de dinheiro e do financiamento do terrorismo que cada cliente potencialmente poderia representar para a instituição. Ao contatar um novo cliente, é imprescindível focar não somente em sua capacidade financeira e patrimonial, assim como no potencial desse relacionamento gerar lucro para a instituição, mas também na mensuração dos respectivos riscos de LDFT. Isso envolve conhecer a procedência e histórico do cliente,assim como a origem de seus recursos e, na exatidão da definição, gerir todo o relacionamento deste cliente durante sua permanência na instituição.

Além disso, algumas informações cadastrais iniciais são identificadas primariamente pelo *front*. Tendo isso em destaque, é válido lembrar que é logo nesta primeira etapa que se inicia o processo de KYC

2 A segmentação de front, middle e back office é um padrão de governança em instituições financeiras submetidas ao Art. 9º da Lei 9.613/98.

(*Know Your Customer*)[3]. Antes que a checagem de antecedentes ou de veracidade das informações ocorra no *middle*, é o *front* quem tem contato direto com o cliente e fornece dados iniciais como atuação profissional do prospecto, capacidade financeira e patrimonial, perfil de investimento e origem dos bens. Adicionalmente, é o *front* quem colhe dados complementares e esclarecimentos caso necessário.

Todo o processo iniciado pelo *front office* deve estar alinhado com os documentos entregues para análise, por exemplo: um cliente pessoa jurídica prospectado possui um balanço com indicadores muito superiores ao tamanho e capacidade da empresa. Quando o *front* conhece seu cliente de fato, pode-se previamente identificar fatores suspeitos quanto ao risco do cliente. Sem prejuízo disso, o gerente de relacionamento, também deve acompanhar a conformidade do *suitability*[4] e tendo em vista as movimentações e aos produtos bancários utilizados. Neste sentido, é capaz de identificar quando seu cliente pretende operar além do seu perfil de investimentos, de forma atípica.

Após a prospecção, são necessários procedimentos para cadastrar o cliente nos sistemas da instituição, essa função é comumente responsabilidade do *middle office*, ou, dependendo da estrutura da instituição, da área de Cadastro. Assim como o *front* deve conhecer o cliente ao prospectar, a área de *middle* analisa criticamente a documentação do cliente, representando uma ponte entre o cliente e a instituição**.** Atuando tanto na abertura de relacionamento, quanto nas atualizações e suporte ao cliente.

Ao analisar as documentações e a forma que são entregues já é possível ter uma percepção inicial de possíveis indícios de: documentos fraudados, omissão de informações, pressão externa para abertura da conta com urgência, resistência ao providenciar informações necessárias para o início de relacionamento e/ou atualização cadastral, fornecimento de informação falsa ou de difícil ou oneroso entendimento e validação, incluindo identificação do respectivo beneficiário final, e omissão de participações societárias em empresas, sendo muitas vezes de segmentos sensíveis[5].

Outros exemplos práticos, citados no artigo "Governança, risco e *compliance*: papéis fundamentais na prevenção a lavagem de dinheiro e combate à corrupção" são:

> Informação de mesmo endereço comercial por diferentes pessoas jurídicas ou organizações, sem justificativa razoável para tal ocorrência; representação de diferentes pessoas jurídicas ou organizações pelos mesmos procuradores ou representantes legais, sem justificativa razoável para tal ocorrência; informação de mesmo endereço residencial ou comercial por pessoas naturais, sem demonstração da existência de relação familiar ou comercial. (Pablo Jesus de Camargo Correia, 2018).

Em algumas instituições, a área m*iddle office* também é responsável pela análise prévia de *due diligence*, ou seja, uma verificação, muitas vezes por meio de uma ferramenta

3 O Conheça seu Cliente (KYC – Know Your Customer) é um programa contínuo, que tem por objetivo minimizar os riscos legais e reputacionais da instituição. Envolve completo entendimento do cliente e de suas necessidades em especial, o conhecimento do cliente quanto a sua avaliação de risco, assim como do processo de identificação de seu beneficiário final.

4 Em Guia de PLDFT publicado em 02/10/2020, a ANBIMA cita o dever de adequação dos produtos, serviços e operações de acordo com o perfil de disposição ao risco do cliente encontram-se na ICVM 539/2013 e na Resolução n° 3694 do Banco Central. Disponível em:<http://www.cvm.gov.br/legislacao/instrucoes/inst539.html> e <https://www.bcb.gov.br/pre/normativos/res/2009/pdf/res_3694_v3_P.pdf.>. Acesso em: 04/10/2020.

5 A ABBI (Associação Brasileira de Bancos Internacionais) elenca quais são setores mais visados no processo de Lavagem de Dinheiro segundo o COAF (Conselho de Controle de Atividades Financeiras): Instituições Financeiras; Paraísos fiscais e centros "offshore"; Bolsas de Valores; Companhias Seguradoras; Mercado Imobiliário; Metais Preciosos; Jogos e Sorteios. Disponível em:<http://www.abbi.com.br/praticasdeprevencao.html>. Acesso em 03/10/2020.

de pesquisa, no qual se examina o histórico do cliente, idoneidade, negativações, mídias negativas e averiguação em listas, como por exemplo, a lista de pessoas naturais e jurídicas e entidades os quais os ativos estão sujeitos à indisponibilidade devido resoluções do Conselho de Segurança das Nações Unidas ou de orientação de seus comitês de sanções, de requerimento de outro país ou de designação nacional[6]. Não obstante, é realizada a verificação por definição da ICVM 617[7] e da Circular nº3978 do Banco Central[8] se o cliente é considerado uma pessoa politicamente exposta[9].

Ainda que, após analise dos documentos e pesquisas em nome do cliente, seja preciso o escalamento de aprovações para segunda linha, como aval dos times de *Compliance* e Legal, a percepção inicial de fatores suspeitos são levantados pela primeira linha.

Por sua vez, posteriormente à abertura de relacionamento, a área de suporte, *back office*, é responsável pelas transações, custódia e movimentações dos ativos e fluxos financeiros dos clientes. Prematuramente, já é possível identificar fatores suspeitos, por exemplo: quanto aos montantes de valores, sucessivos depósitos de valores exatos ou similares, origem e destino dos recursos, reincidência das movimentações e cadastramento de múltiplas contas no mesmo período, irregularidades ou não entrega da documentação regulatória para o registro das operações, como casos em que não é possível identificar o beneficiário final da operação, solicitações de urgências e alteração dos dados da conta destino de forma repentina, na tentativa de mascarar o rastro do dinheiro pelo sistema financeiro, transpondo seus intermediários. **(**Pablo Jesus de Camargo Correia, 2018)

Assim como o front conhece o cliente, o *middle office* conhece a documentação e histórico do cliente, o *back office* conhece as transações e histórico de movimentações do cliente. E mais uma vez, ainda que as movimentações suspeitas sejam escaladas, via sistema ou por reporte dos colaboradores para a segunda linha, o time de *back office* é o primeiro nível de identificação de situações contestáveis quanto às transações dos clientes.

Conclusão

Levando em conta as novas regulamentações do escopo de instituições financeiras, como a ICVM 617 e a Circular nº 3978 do Banco Central, é reforçada a necessidade de cada instituição compreender e mapear os riscos dos clientes para além das questões regulatórias e obrigações legais. Para tanto, o IIA aborda no Modelo de Três Linhas a indispensabilidade de gerenciar riscos, sugerindo a sinergia entre todas as linhas da instituição com a Alta Administração

6 Lei 13810/2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Lei/L13810.htm> Acesso em: 04 de outubro de 2020.

7 A Comissão de Valores Mobiliários (CVM) dispõe uma instrução sobre a prevenção à lavagem de dinheiro e ao financiamento do terrorismo no âmbito do mercado de valores mobiliários. Disponível em: <http://www.cvm.gov.br/legislacao/instrucoes/inst617.html>. Acesso em 03/10/2020.

8 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. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3978&fbclid=IwAR21-uzbGw6GEf7Wu4W-TaKUmmyf4Gdd8tOrEZQDlhSCdjYeZq7wTJKI_Z8>, Acesso em 03/10/2020.

9 Resolução nº 29/2017 do Conselho de Controle de Atividades Financeiras (COAF), pessoas politicamente expostas compreendem: detentores de mandatos elegíveis aos Poderes Executivo e Legislativo da União; presidentes e tesoureiros de partidos políticos; agentes públicos diretos ou indiretos, inclusive ministros e diretores de entidades da administração pública que desempenham ou tenham desempenhado, nos cinco anos anteriores, no Brasil ou em países, territórios e dependências estrangeiras, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e estreitos colaboradores; ocupantes de escalões superiores em empresas públicas. Disponível em: <http://www.fazenda.gov.br/orgaos/coaf/legislacao-e-normas/normas-coaf/resolucao-no-29-de-7-de-dezembro-de-2017-1>. Acesso em: 04 de outubro 2020.

para mapear os riscos de acordo o apetite e disposição, mensurando riscos e os custos de suas consequências em face ao lucro. Valendo-se do método da ABR (Abordagem Baseada em Riscos)[10]no mapeamento dos riscos, é possível que a instituição consiga aliar o arcabouço regulatório e de recomendações com o entendimento dos riscos envolvidos em cada negócio.

Muitas vezes o conhecimento das melhores práticas, definições, conceitos regulatórios e possíveis pontos de atenção ficam concentrados na segunda e terceira linha, disseminando uma cultura que responsabiliza somente as áreas *Compliance, Legal,* Controles Internos e Auditores Internos pelos riscos. Não obstante, esse pensamento normalmente concentra a ideia de que somente a segunda e terceira linha são capazes de identificar informações suspeitas.

O IIA se contrapõe nesse sentido, ao demonstrar a importância de alinhamento desde a Alta Administração em se inteirar e entender os riscos em *Tone at the Top*[11]. Nas linhas seguintes, a gestão é responsabilizada por ajudar a Alta Administração a disseminar as informações para todos os níveis[12], gerando no ambiente generalizado da companhia uma cultura de defesa e gestão riscos, onde todos sabem seu papel e tem responsabilidade sobre os riscos de lavagem de dinheiro e/ou financiamento ao terrorismo.

Demonstrou-se anteriormente o papel primordial da primeira linha na identificação de riscos e PLD/FT, uma vez que o conhecimento de pontos importantes sobre o cliente inicia-se desde a prospecção. Nesse sentido, é também nessa linha que ocorre o contato direto com o cliente por parte do *front*, que, além de ter conhecimento sobre os produtos e transações do cliente, colhe dados primários que serão utilizados pelo *middle* e *back* na análise, cadastro e manutenção do relacionamento.

Na atualidade, o cenário da pandemia colaborou para aumentar as atenções aos riscos, uma vez que mudaram as formas de trabalho e incrementaram riscos inéditos ou riscos que eram diminutos e nesse contexto foram maximizados. Com a migração massiva de pessoas ao *home office* e o aumento de métodos e ferramentas digitais e eletrônicas em transações à distância, logo no primeiro dia de abril, o presidente do GAFI[13] fez um comunicado alertando seus membros, incluindo o Brasil, sobre os novos riscos e encorajando a colaboração no mapeamento de vulnerabilidades. No mês seguinte, o GAFI publicou um relatório identificando os novos desafios, boas práticas e políticas responsivas às novas ameaças[14].

Finalmente, o novo modelo das Três Linhas do IIA de junho de 2020 surge como uma

10 A metodologia Abordagem Baseada em Risco (ABR) tem como objetivo assegurar que as instituições apliquem medidas de PLDCFT proporcionais ao risco do uso dos serviços em crimes de lavagem de dinheiro e financiamento do terrorismo. Ela sinaliza onde e de que forma os recursos devem ser investidos internamente, além de orientar a adoção de procedimentos compatíveis ao perfil de cada cliente. Disponível em: https://www.amlreputacional.com.br/editorial/as-8-principais-recomendacoes-do-gafi-para-fortalecer-seus-processos-de-pldft/. Acesso em 27/09/2020.

11 De acordo com VENTURA, Leonardo Henrique de Carvalho (2018), Tone at the Top envolve não apenas a participação da diretoria da entidade, mas também sua continuidade e efetividade. O autor cita que "a Alta Direção deve patrocinar Mecanismos de Integridade e Sistemas de *Compliance*, servindo de exemplo direto aos funcionários para que seus atos sejam "imitados" naturalmente, por admiração, lealdade ou mesmo por receio.".

12 A importância da governança também é destacada em exemplos como FCPA, UK BRIBERY ACT, OCDE e U.S. Federal Sentencing Guidelines. Disponível em: https://jus.com.br/artigos/66732/ferramentas-de-*compliance*-tone-at-the-top. Acesso em 03/10/2020.

13 O Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FATF) é uma organização intergovernamental cujo propósito é desenvolver e promover políticas nacionais e internacionais de combate à lavagem de dinheiro e ao financiamento do terrorismo. Disponível em: <http://www.fazenda.gov.br/assuntos/atuacao-internacional/prevencao-e-combate-a-lavagem-de-dinheiro-e-ao-financiamento-do-terrorismo/gafi>. Acesso em: 04/10/2020.

14 Disponível em: <https://www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html>. Acesso em: 03/10/2020.

proposta coerente e necessária, pois traz à tona a necessidade estratégica de promover a cooperação no âmbito complexo das instituições no combate aos riscos, não só para atender às questões legais, como também para assegurar a perpetuidade do negócio.

Referências bibliográficas

ANBIMA. Guia ANBIMA de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo. Disponível em: <https://www.anbima.com.br/data/files/60/10/AC/B5/3 59E471074E33B47092BA2A8/Guia ANBIMA-PLDFT.pdf.>. Acesso em: 04/10/2020.

ABOUT US. **COSO, The Committee of Sponsoring Organizations of the Treadway**. Commission. Disponível em: <https://www.coso.org/Pages/aboutus.aspx>. Acesso em: 02/10/2020.

CHAMBERS, Richard. Novo modelo das três linhas do IIA oferece evolução tempestiva de uma ferramenta confiável. **Instituto dos Auditores Internos do Brasil**. 2020. Disponível em: <https://iiabrasil.org.br//noticia/novo-modelo-das-tres-linhas-do-iia-oferece-evolucao-tempestiva-de-uma-ferramenta-confiavel>. Acesso em: 26/09/2020.

CIRCULAR N° 3.978. **Banco Central do Brasil**. 2020. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3978&fbclid=IwAR21-uzbGw6GEf7Wu4W-TaKUmmyf-4Gdd8tOrEZQDlhSCdjYeZq7wTJKI_Z8>. Acesso em: 02/10/2020.

Comunicado do presidente do GAFI sobre Covid-19 e medidas de combate ao financiamento ilícito. **Ministério da Economia**. 2020. Disponível em: <http://www.fazenda.gov.br/orgaos/coaf/publicacoes/comunicado-do-presidente-do-gafi-sobre-covid-19-e-medidas-de-combate-ao-financiamento-ilicito>. Acesso em: 28/08/2020.

CORREIA, Pablo. Governança, risco e *compliance*: papéis fundamentais na prevenção a lavagem de dinheiro e combate à corrupção. **JUS.COM**. 2018. Disponível em: <https://jus.com.br/artigos/65116/governanca-risco-e-*compliance*-papeis-fundamentais-na-prevencao-a-lavagem-de-dinheiro-e-combate-a-corrupcao>. Acesso em: 28/09/2020.

COVID-19 related Money Laundering and Terrorist Financing: Risks and Policy Responses. **FATF-GAFI**. 2020. Disponível em: <https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf>. Acesso em: 01/10/2020.

Detalhando o modelo de Governança: Como funcionam as 3 linhas de Defesa. **Brasiliano Interisk: Inteligência em riscos**. 2019. Disponível em: <https://www.brasiliano.com.br/22-tres-linha-de-defesa>. Acesso em: 28/09/2020.

GAMEIRO, João. Risco crescente de lavagem de dinheiro durante a pandemia de Covid-19. **Trench Rossi Watanabe**. 2020. Disponível em: <https://www.trenchrossi.com/3r/risco-crescente-de-lavagem-de-dinheiro-durante-a-pandemia-de-covid-19/:~:text=Al%C3%A9m%20disso%2C%20a%20ado%C3%A7%C3%A3o%20de,a%20popula%C3%A7%C3%A3o%2C%20mas%20que%2C%20por>. Acesso em: 02/10/2020.

Guidance on the 8th EU Company Law Directive. **FERMA / ECIIA**. Disponível em: <https://www.iia.nl/SiteFiles/ECIIA%20FERMA.pdf>. Acesso em: 27/09/2020.

LUCENA, Gustavo. Crimes financeiros e a pandemia de Covid-19: Crise reforça necessidade de uma estrutura robusta de governança. **Deloitte**. 2020. Disponível em: <https://www2.deloitte.com/br/pt/pages/risk/articles/crimes-financeiros-covid-19.html>. Acesso em: 03/10/2020.

Modelo das três linhas do IIA 2020: Uma atualização das três linhas de defesa. **Instituto dos Auditores Internos do Brasil**. 2020. Disponível em: <https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf>. Acesso em: 25/09/2020.

The Institute of Internal Auditors. 2020. Página inicial. Disponível em: <https://na.theiia.org/Pages/IIAHome.aspx>. Acesso em: 01/10/2020.

Implicações do Dever de Vigilância na Atuação dos Gestores do Programa de *Compliance* e suas Responsabilidades como Garantidores

AMANDA SANTOS DE FIGUEIREDO

Advogada e palestrante, graduada em Direito pela Universidade Federal do Rio de Janeiro (UFRJ), pós graduada em Ciências Penais e Criminologia pelo Instituto de Criminologia e Política Criminal (ICPC), Mestranda em Direito Penal, Direitos Humanos e Segurança Pública pela Universidad de Salamanca (Espanha). Especialista em Anticorruption *Compliance* pela University of Pennsylvania e pela LEC, em *Compliance* e Governança Corporativa, e em LGPD pela ESA OAB/RJ.

A necessidade de implementar e fomentar uma cultura de *compliance* decorre da prática de se delegar às empresas as funções de vigilância que seriam próprias do Estado, no que tange à prevenção de ilícitos, através da chamada autorregulação regulada[1]. Neste sentido, pensar em *Compliance* significa pensar em autovigilância, sendo então de suma importância conhecer os alicerces e limites das questões referentes às responsabilidades oriundas da posição de garantidor, bem como das atribuições inerentes às relações pautadas no Princípio da Confiança.

Busca-se por meio desta breve explanação trazer reflexões sobre os deveres e as responsabilidades oriundas das atribuições dos dirigentes das empresas, e de cada um que ocupa diferentes níveis na organização, para que seja possível pensar nos cuidados que envolvem a contratação de terceiros e as delegações de funções. Muitas vezes é difícil definir o grau de responsabilidade de quem supervisiona as atividades e do executor do ato praticado em uma estrutura empresarial onde as funções se mesclam, e não há como realizar um controle direto sobre todas as situações que ali dentro ocorrem.

1 Enforced self-regulation, também chamada de corregulação, diz respeito a uma forma de regulação estatal do mundo empresarial, subordinada a fins ou interesses públicos pré-determinados pelo Estado no interesse em reorientar sua atuação por um intervencionismo à distância". COCA VILA, Ivó. ¿Programas de Cumplimiento como forma de autorregulação regulada? In: SILVA SÁNCHEZ, Jesús-María; FERNÁNDEZ, Raquel (Orgs.). Criminalidad de Empresa y *Compliance*. prevención y reacciones corporativas. Barcelona: Atelier, 2013. p. 43-75, p. 51.

A posição de garantidor de quem possui a função de vigilância

Quando alguém que deveria estar sendo supervisionado em sua função comete um ilícito, a responsabilidade recai também sobre o garantidor, que possuía o dever de vigilância daquela pessoa no desenrolar de determinadas atividades. Isto ocorre no âmbito penal em certos casos que, por determinação legal, uma pessoa é tida como garantidora, ou seja, responsável por agir em situações que sua omissão acarretará algum dano[2].

Nestes casos, o responsável, caso fique inerte diante da necessidade, responderá como se tivesse cometido determinado ilícito. Logo, bombeiros, policiais e afins, são garantidores para resguardar os direitos dos cidadãos em situações de emergência, ou seja, não podem se quedar omissos, deles se exige um especial agir, bem como os diretores de empresa devem ser responsáveis pelos atos por ela praticados, todavia, como eles não são executores diretos de todas as atividades, lhes incumbe como garantidores, dever de vigilância sobre as situações que ocorrem no desenrolar de todas as funções inerentes ao atuar empresarial.

Delegação de competência e dever de supervisão

A partir da identificação da posição de garantidor há que se verificar a questão da delegação de competência, pois a delegação faz surgir uma transferência e uma transformação de posição de garantia. Ocorre a transferência pois faz surgir para o delegado a posição de garantia, e juntamente ocorre a transformação, tendo em vista que a posição de garantidor do delegante passa a ser residual.

Nestas hipóteses em que há uma delegação de funções, não há mais um dever de controle direto sobre os focos de risco para o delegante. A ele somente incumbe a função de selecionar corretamente alguém para figurar na posição de delegado, bem como formá-lo e informá-lo para que possua meios adequados à sua missão, todavia recai ainda sobre o delegante o dever de vigilância das atividades do delegado.

Atividades perigosas exigem maior vigilância para manter os riscos dentro do limite permitido, ao passo que atividades que não sejam comumente reconhecidas como perigosas, somente serão puníveis quando o superior hierárquico fique omisso diante de um risco que se conhecia, que tinha alta probabilidade de ocorrer e de superar o risco permitido.

No Direito alemão, os diretores e membros do Conselho de Administração da empresa são considerados, majoritariamente, garantidores das atividades realizadas por seus subordinados. Este pensamento não apresenta muita coerência posto que a posição de garantidor surge nas hipóteses em que se busca resguardar direitos diante de situações perigosas ou para controlar pessoas perigosas que não sejam responsáveis por seus atos, tais quais os inimputáveis. Considerando os funcionários da empresa como pessoas plenamente capazes, portanto, auto responsáveis por seus atos, não se adequa a hipótese de atribuir responsabilidade a outrem pelos atos por elas praticados.

Esta posição da doutrina germânica justifica a função de garantidor com base no domínio hierárquico do superior, ou seja,

2 Artigo 13 do Código Penal Brasileiro (...) § 2º - A omissão é penalmente relevante quando o omitente devia e podia agir para evitar o resultado. O dever de agir incumbe a quem: a) tenha por lei obrigação de cuidado, proteção ou vigilância; b) de outra forma, assumiu a responsabilidade de impedir o resultado.

diante de sua possibilidade fática e jurídica de dar ordens, na superioridade de informações que possui. Ela tem como intuito a garantia de controle da própria organização, pois compreende-se como dever da Pessoa Jurídica controlar os perigos oriundos da sua organização.

Já no Direito espanhol, se considerarmos a transferência da posição de garantia em um contexto individual, não há que se falar em dever de vigilância. Por exemplo, se alguém assume a custódia do filho de outrem e delega esta custódia a um terceiro escolhido corretamente, ele não precisará vigiar o desempenho das funções deste terceiro[3]. Hipótese que não se coaduna com a previsão dada no âmbito empresarial, em que se exige um dever de vigilância àquele que tenha delegado sua função, ainda que de forma cuidadosa.

Determinadas relações se regem ainda pela separação de esferas, também chamada de estrita competência, onde não se exige uma vigilância da conduta daquele que realiza atividades na empresa conjuntamente com outrem. Nestes casos, cada um é responsável pelo seu atuar, não havendo a posição de garantidor. É o que vigora nas relações entre diretores situados no mesmo plano horizontal, em que há uma ideia de neutralidade, onde não é possível se exigir uma extensão do dever em função do conhecimento.

A questão não é pacífica ao se analisar as relações existentes entre membros do Conselho de Administração. Existem decisões do Tribunal Espanhol que sustentam que entre eles não há um dever de vigilância recíproco, e outras que defendem a responsabilização dos mesmos por atos de outrem, quando houver omissão nesta supervisão.

Para os que entendem que entre os membros do Conselho de Administração existe um dever de vigilância, sustentam esta ideia com base na posição de garantidor. A posição de garantidor traz consigo o dever de vigilância, todavia nestes casos, se excluiria do alcance deste dever de vigilância os atos realizados pelos membros do próprio Conselho. Porém, segue sendo exigido dos integrantes deste órgão, que haja uma diligência devida, que se informem suficientemente sobre as decisões e atividades que estão sendo desempenhadas pela própria empresa.

Esta responsabilidade somente será excluída quando não houver conhecimento sobre os atos dos demais, ou quando, havendo este conhecimento, tenham realizado tudo que lhes cabia para evitar o dano. Logo, resta claro que há um dever de vigilância de certa forma abrandado, mas que deve ser efetuado diante de atos indiscutivelmente ilegais.

Importante frisar que este dever de vigilância não faz com que eles sejam penalmente responsáveis por todos os atos delitivos cometidos pelos demais membros do Conselho, pois esta obrigação de supervisão não compreende todas e cada uma das atividades realizadas por aqueles que agirem além do permitido. Entre os conselheiros não há uma posição de superioridade que lhes confira alguma autoridade, portanto, responsabilizá-los por todo e qualquer ato cometido por outrem seria conferir responsabilidade por atividades que sequer teriam conhecimento.

Caso realizem suas condutas de forma correta e se informem do que está sendo realizado dentro da companhia, não há que se falar em responsabilidade entre os membros do Conselho de Administração por atos cometidos por outros integrantes do mesmo, posto que muitas vezes os atos ilícitos são realizados de forma oculta sem que seja possível a percepção do

3 Conforme jurisprudência espanhola. Julgado STS 377/2004, de 25 de março. Disponível em http://supremo.vlex.es/vid/abuso-sexual-agravante-vulnerabilidad-16873512.Acesso 05 de outubro de 2020.

cometimento deles por outrem. Esta supervisão não se enquadraria completamente no dever de vigilância uma vez que não há um dever específico de conferir ao outro conhecimento sobre a maneira de agir dos demais conselheiros.

No entender de Jesús-Maria Sílva Sanchez[4], há entre eles um dever de garantidores recíprocos, porém que não abarca o dever de vigilância. Logo, eles não necessitam verificar as atividades uns dos outros a todo tempo, porém caso alguém tome conhecimento, ainda que de forma provável, da ocorrência de um delito por parte de outro, o mesmo poderá ser responsável por omissão, pois teria a capacidade de evitá-lo e não o fez.

Utilização do Princípio da Confiança como parâmetro

Outro parâmetro possível para ser adotado, capaz de delimitar o grau de responsabilidade dos dirigentes é o Princípio da Confiança. De acordo com este Princípio, em determinadas relações não é necessário se preocupar em efetuar a vigilância após a delegação da função, a não ser que o delegado demonstre indícios de que agirá de forma incorreta, quando então o delegante deverá atuar para evitar o resultado lesivo.

O Princípio da Confiança se aplica aos casos em que há uma relação prévia entre os envolvidos. Ele pressupõe a existência de uma tarefa comum compartida por ambos, em que haja um dever especial recíproco de correção ou de evitar condutas lesivas de outrem, como é o caso de uma equipe médica que opera conjuntamente, por exemplo.

Nestes casos, para que seja possível punir alguém pela infração de outrem, é necessário que haja um conhecimento da situação, que surge quando um adverte o outro de que este está agindo errado. A imputação pelo outro não ter evitado o dano, somente surge se havia conhecimento dos pressupostos por parte daquele que deveria tentar impedir o agir danoso e não o fez.

Portanto, a característica mais importante do Princípio da Confiança é que A tem o dever de evitar os resultados lesivos produzidos na esfera de B, mas também é certo que A não tem o dever de procurar o conhecimento acerca do comportamento de B, se ele está agindo defeituosamente ou não.

Nas relações pautadas pelo Princípio da Confiança não é necessário que se verifique, que se supervisione o agir do outro. O dever de controle ou vigilância existe justamente nas relações regidas pelo *Princípio da Desconfiança*. A desconfiança rege as relações intra empresariais, que ocorrem no interior da companhia, entre os dirigentes e aqueles que foram selecionados cuidadosamente para efetuarem suas funções.

O que fundamenta este dever é o fato da empresa constituir um risco especial através de sua atividade, pela potencialidade criminológica, pela tendência de se orientar unicamente ao lucro, pelas pautas informais de conduta. O dever de vigilância que permeia estas relações pressupõe dois momentos: um anterior à delegação da função – em que se exige o conhecimento do modo que o subordinado exerce a gestão; e outro posterior – que deve corrigir a ação defeituosa ou informar o superior que possa corrigi-lo, de maneira a evitar as consequências lesivas.

Logo, para haver a responsabilização do superior hierárquico, este deve conhecer o atuar antijurídico do subordinado e, podendo fazer, não atua para evitar. O diretor somente deve ser responsabilizado quando possui dados para saber que a

4 SILVA SÁNCHEZ, Jesús-María; *Compliance* y teoria del Derecho Penal. Madri: Marcial Pons, 2013. p. 97.

conduta dos subordinados cria um risco desaprovado, hipótese em que será responsável pela omissão se não atua para impedi-lo ou não exerce atividades de controle.

Não há um dever de vigilância absoluto e vigilância não significa revisão completa de tudo que o subordinado faz, pois caso assim fosse, a delegação da atividade seria inútil. Apesar desta ressalva, também não deve o supervisor aguardar que cheguem até ele indícios da atuação defeituosa, pois isso seria adequado ao Princípio da Confiança, e o dever de vigilância é necessário justamente nos casos regidos pelo Princípio da Desconfiança, que configuram e regem as relações de subordinação existentes dentro da empresa.

As relações regidas pelo Princípio da Desconfiança poderão ser pautadas pelo Princípio da Confiança a partir do momento em que se exerça um procedimento de vigilância. A vigilância pode se dar através inspeções e informes periódicos, e, em havendo este sistema, o superior pode se considerar amparado pelo Princípio da Confiança.

Daí a necessidade de se implementar um programa de *compliance* efetivo dentro da companhia, pois através da gestão de riscos e de todo monitoramento que se realizará de forma rotineira, será possível minimizar as hipóteses de ocorrência de atos ilícitos internamente, e da mesma forma minimizar o grau de vigilância dos superiores sobre as atividades e, consequentemente, sua responsabilização por atos de outrem.

É justamente o controle efetuado pelo programa de *compliance* que funciona como um sistema de vigilância para que as relações da empresa que seriam pautadas pelo Princípio da Desconfiança, necessitando de supervisão, sob pena dos superiores incorrerem em responsabilidades, se tornarão relações pautadas no Princípio da Confiança, sendo desnecessário o dever de vigilância, mas tão somente um auxílio no sentido de transferir o conhecimento de como aquela atividade deve ser realizada dentro das normas legais.

Neste ponto também se mostra relevante o programa de *compliance* efetivo, tendo em vista que um dos seus pilares é a educação dos empregados na cultura da integridade, logo, em um ambiente onde os trabalhadores já possuam esta consciência e sejam frequentemente treinados a pensarem e agirem de acordo com o código de ética da empresa, será mais fácil comprovar que ao delegar determinadas funções, o delegado possuía os meios necessários e adequados para compreender o que poderia ou não realizar, sem a devida supervisão.

Infração ao dever de vigilância

O simples fato de não ter realizado a correta vigilância não acarreta nenhuma responsabilidade por si, esta somente irá decorrer do fato do vigiado ter cometido um ilícito e essa vigilância ter falhado. Este ilícito deve ter, ao menos, sido iniciado, caso seja doloso, ou se tenha consumado, caso seja culposo. Logo, se verifica que a sanção da infração ao dever de supervisão tem caráter acessório.

As sanções decorrentes da infração ao dever de vigilância ainda são objeto de discussão. Para doutrina majoritária na Alemanha, quando ocorre a infração do dever de vigilância e se produz um resultado lesivo, o delegante-vigilante poderá responder como co-autor em comissão por omissão, como é o caso de quem tem competência jurídica para controle e correção direta do risco. Todavia, se não houver esta competência, sua imputação será a título de participação por omissão.

Importante verificar se a própria infração ao dever de vigilância foi dolosa ou culposa, pois isto irá influir na maneira como

o superior responderá. Será dolosa se ele intencionalmente, para não ter acesso às condutas ilícitas perpetradas pelo delegado, se esquiva de realizar a supervisão devida, entendendo que assim não lhe será imputada nenhuma responsabilidade.

Esta conduta se adequa ao que se convencionou chamar de cegueira deliberada. A Teoria da Cegueira Deliberada busca punir o agente que se coloca, intencionalmente, em estado de desconhecimento ou ignorância, para não conhecer detalhadamente as circunstâncias fáticas de uma situação suspeita, no intuito de se eximir da responsabilidade.

Pode ocorrer também das informações referentes à conduta do agente que comete o ilícito não chegarem efetivamente ao seu superior em virtude da própria organização da empresa, que seria a hipótese de infração culposa do dever de vigilância. Por conta do grande volume de situações, aos dirigentes torna-se inviável tomar conhecimento de tudo que se passa no âmbito da companhia pois muitas vezes eles dependem do repasse destas informações.

As medidas que deveriam ser tomadas pelo superior, só poderiam ser de fato realizadas, caso o mesmo tivesse conhecimento da situação defeituosa, todavia, em muitos casos ocorre o bloqueio de informações e em consequência, o conhecimento incompleto das atividades do subordinado. No caso dos superiores serem instrumentalizados, através do conhecimento incompleto da situação, os subordinados poderão responder por autoria mediata por omissão com relação ao ilícito praticado, em virtude de não lhes terem repassado a correta e completa informação.

Vigilância interempresarial

No caso de conglomerados econômicos, as relações entre matriz e filiais não se adequam nem ao Princípio da Confiança, nem ao da Desconfiança, e também não se coadunam com o modelo de separação absoluta de esferas. Em que pese haja uma separação legal posto que elas possuem personalidade jurídicas diferentes, há uma dependência da empresa filial quanto à sua matriz, logo, a relação entre elas deve observar algum grau de supervisão.

A matriz, como sócia única ou majoritária da filial deve interferir na seleção dos administradores desta última, pois estes têm a exata função de alguém que atua como um indivíduo que fora delegado para exercer determinadas atribuições – como ocorre internamente com as pessoas físicas no caso de delegação de funções. Também é dever da matriz intervir toda vez que obtiver informações relativas ao cometimento de ilícitos por parte da filial, ainda que seja de forma suspeita.

Quanto a empresas que não façam parte do mesmo conglomerado societário, sempre vigorou entre elas o Princípio da separação absoluta de esferas, todavia esta questão tem mudado no que tange aos parceiros.

A política do KYC (*know your customer*)[5] passou a vigorar para analisar atividades dos terceiros que são contratados pela empresa, ampliando ainda mais o grau de responsabilidade por atos que não sejam cometidos diretamente pela pessoa, mas por alguém que possua relação com ela, ainda que indiretamente.

Nesta hipótese de subcontratação, segundo Jesús-Maria Silva Sánchez[6], ocorre um modelo misto: deve haver um dever de seleção correta para a entrada, como uma

5 A política de "Know your customer", comumente conhecida como KYC, é uma medida obrigatória para todos os bancos e outras instituições financeiras focadas no processo de identificação do cliente, para cumprir os regulamentos internacionais ao combate à lavagem de dinheiro e financiamento do terrorismo.

6 SILVA SÁNCHEZ, Jesús-María; *Compliance* y teoria del Derecho Penal. Madri: Marcial Pons, 2013. p. 98.

medida de adequação *ex ante*, e a partir de então se opera o Princípio da Confiança, o que significa não ser necessária a supervisão ou vigilância.

Logo, no que se refere a *third parties*, dependendo da relação que possuam, podem ocorrer casos de separação absoluta de esferas, de aplicação do Princípio da Confiança, do dever de seleção aliado ao Princípio da Confiança, e do dever de vigilância em sentido estrito.

Conclusão

Diante de todo o exposto com relação às teorias de supervisão dos atos praticados internamente, das hipóteses de responsabilização de subordinados e superiores hierárquicos, verifica-se a necessidade imperiosa da vigilância do atuar interno dos funcionários da companhia, bem como das empresas que são contratadas. Esta exigência de supervisão e consequente abrandamento das responsabilidades somente conseguirá ser alcançada mediante um programa de *compliance* efetivo, que realize um procedimento de vigilância, através da gestão de riscos.

O *Compliance* Officer não consiste apenas em um funcionário cuja vigilância lhe foi delegada, mas também em um promotor da gestão de formação das pessoas que ali trabalham, para que assim possa agir com base na confiança do bom funcionamento do programa, o que lhe proporcionará indícios da comissão de um ato delitivo.

Sendo assim, é possível pautar a posição de garantidores dentro da estrutura empresarial em três princípios distintos que se aplicam a diferentes relações: o princípio da separação de esferas – em que não há a posição de garantidor e cada um atua respondendo por seus próprios atos, sem que se exija supervisão de ninguém; o princípio da confiança – em que existe a posição de garantidor, porém não se exige um conhecimento sobre situações de risco, mas tão somente de neutralizar riscos que foram advertidos; e por fim, o princípio da desconfiança – em que se exige um dever de vigilância.

Através desta análise é possível vislumbrar quais relações merecem especial atenção e quais responsabilidades podem ser oriundas de determinadas funções, bem como se mostra inequívoca a necessidade de um programa de *compliance* efetivo de forma a auxiliar o dever de vigilância cada vez mais necessário interna e externamente.

O Papel Estratégico da Alta Direção para o *Compliance* Digital na Proteção de Dados e Sistemas Contra Riscos Cibernéticos

The Strategic Role of High Direction for Digital Compliance in The Protection of Data And Systems Against Cyber Risks

CLAUDIA DA COSTA BONARD DE CARVALHO

Advogada Criminal especializada em *Compliance* Criminal Digital, Cybersecurity e Legal advisor em Cybercrime, graduada pela UERJ e Pós- Graduada em Direito Penal e Processo Penal pela Universidade Estácio de Sá, especializada em Criminal *Compliance* pelo IBEF-Rio, premiada como uma das 50 mulheres CYBERSECURITY TOP WOMEN LATAM 2020 pela Womcy (Women in Cybersecurity), membro do CWC-RJ, da AB2L e da Associação Nacional dos Advogados de Direito Digital, autora de artigos sobre *Compliance* Criminal e do livro Direito Penal 4.0.

1 – Introdução

Empresas do mundo todo tem sido alvo de ataques cibernéticos, causando graves transtornos operacionais, prejuízos financeiros e perda reputacional, o que já figura nas manchetes diárias da mídia.

No caso da América Latina, tais ataques tem se concentrado, principalmente, nos setores estratégicos da economia (bancário, energia, petróleo e gás e transporte), conforme relatório da empresa DELOITTE[1], gerando paralisação de serviços, fraudes e diversos transtornos para seus usuários.

Pesquisa recente do Fórum Econômico Mundial[2] aponta que o ataque cibernético já é considerado o quinto maior risco para as empresas em 2020, sendo que, a pandemia covid-19 aumentou potencialmente tal risco na América Latina[3], pela implantação emergencial do home office, sem as devidas cautelas de cybersegurança em

1 DELOITTE, Relatório Cyber Deloitte América Latina e Caribe 2019

2 FÓRUM ECONÔMICO MUNDIAL, Global Risks Report 2020. Disponível em: <http://reports.weforum.org/global-risks-report-2020/wild-wide-web/>. Acesso em: 02.07.2020.

3 OEA, Reporte Ciberseguridad 2020, Ciberseguridad, riesgos, avances y el caminho a seguir en America Latina y el Caribe, Organização dos Estado Americanos, 2020, p.28

redes domésticas, no seu acesso a sistemas corporativos, e pela ausência de orientação suficiente para colaboradores.

Por conta disso, somente no primeiro trimestre de 2020 foram vazadas 12,66 milhões de credenciais de acesso a domínios corporativos, o que facilitou o ataque aos seus sistemas, de acordo com relatório da empresa AXUR[4].

Tais dados são a "porta de entrada" de ataques cibernéticos, os quais vão proporcionar o vazamento de dados pessoais de valor econômico, para que sejam utilizados na prática de diversos delitos, como estelionatos contra clientes ou extorsões digitais contra empresas.

Nesse sentido, a LGPD no Brasil vem reforçar o cuidado com sistemas de informação, exigindo-se a proteção de dados pessoais em seu tratamento, para que sejam evitados vazamentos e demais consequências, como multas, processos e perda de reputação.

No entanto, a prevenção contra ataques cibernéticos e a proteção de dados pessoais, em conformidade à LGPD, não depende somente de bons softwares, profissionais capacitados e de *data mapping*, mas também da atitude da governança da empresa, que deve ser ativa na detecção e mitigação do risco cibernético.

Assim sendo, torna-se necessário o desenvolvimento de uma governança cibernética participativa e integrada com a rotina de segurança da informação, implantando-se um sistema de *Compliance* Digital.

2 – Risco cibernético e desenvolvimento de negócios

O risco está envolvido em qualquer operação realizada no mundo corporativo, ou seja, não existe operação sem risco, sendo que, cada empresa tem seu nível de tolerância de risco, o denominado "apetite de risco". De acordo com GIOVANINI[5]

> No mundo corporativo, riscos estão associados à incerteza do cumprimento de algum objetivo ou na probabilidade de perda de algo material ou intangível. A gestão adequada deles representa condição fundamental para o sucesso da organização e, por isso, passou a ocupar lugar de destaque na própria gestão da empresa. Os riscos de *Compliance* diferem de acordo com as empresas, seus mercados de atuação, tipos de produtos, serviços e soluções, partes com quem se relacionam (clientes, fornecedores, sociedade, força de trabalho, acionistas), etc. Desta maneira, convém à organização estabelecer a melhor forma para identificá-los, e, a partir daí engajar-se na sua mitigação.

O risco cibernético decorre do ambiente digital de operações, variando conforme a atividade da empresa e as vulnerabilidades em seu sistema.

Assim sendo, os riscos cibernéticos estarão presentes em várias situações, como na contratação de novos fornecedores, cuja proteção de dados pessoais em seus sistemas precisa ser eficiente, na compra de softwares para a rotina da empresa, que devem apresentar certificados de segurança reconhecidos no mercado, bem como em operações como M&A, onde o risco cibernético de expansão deverá ser igualmente mensurado e avaliado.

O risco cibernético, então, poderá manifestar de diversas formas nas empresas, como, por exemplo, o vazamento de dados pessoais, a indisponibilidade de sistemas e o crime cibernético.

---

4 AXUR, Relatório atividade criminosa online Brasil, 1º trimestre 2020

5 GIOVANINI, Wagner, Programas de *Compliance* e Anticorrupção: importância e elementos essenciais. In: SOUZA, Jorge Munhós de; QUEIROZ, Ronaldo Pinheiro de (Org.). Lei Anticorrupção e Temas de *Compliance*. 2. ed. Salvador, Juspodivm, 2017, p. 463 e seguintes.

Cabe destacar entre os riscos cibernéticos o cybercrime, uma vez que, estima-se que, os danos causados por ele devem causar um prejuízo de 6 bilhões de dólares em 2021[6], na América Latina, o que equivale ao produto interno bruto de um país, de modo que o risco cibernético não poderá ser negligenciado num programa de *Compliance*.

Além disso, a expansão digital acelerada pela pandemia covid-19 aumentou os riscos cibernéticos a que estão sujeitos os negócios, pela maior superfície de exposição de sua rede na internet.

Um bom exemplo da expansão de negócio que teve o risco cibernético aumentado foi a intensa utilização de aplicativos de alimentação[7], durante a pandemia covid-19, onde houve vazamento de dados pessoais, os quais foram usados por cibercriminosos, os quais acessaram os dados de cartões de crédito de seus clientes.

Cabe destacar também a intensa utilização do ataque ransomware contra empresas, conhecido como extorsão digital, no qual se invade um sistema, quebrando-se sua criptografia, para bloquear o acesso aos seus dados, em troca do pagamento de um resgate em criptomoedas, o que tem vitimado diversas empresas brasileiras[8].

Verifica-se, então, que **não houve a devida** adoção de maiores medidas para proteção do maior tráfego de informações corporativas e de clientes, o que causou inúmero vazamento de dados[9].

Assim sendo, é fundamental a identificação e o monitoramento do risco cibernético de negócios, em qualquer circunstância. A norma ABNT ISO 27005[10], que traz diretrizes para gestão do risco de segurança da informação, destaca a importância da sua identificação, em seu item 8.2.1.1

O propósito da identificação de riscos é determinar eventos que possam causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer.

Logo, há necessidade de classificação de níveis de risco, sua descrição e definição de estratégias para sua melhor mitigação, o que caracteriza o *Compliance* Digital, de acordo com as características da atividade desempenhada pela empresa.

Por fim, cabe destacar que a gestão de risco cibernético se perfaz no mesmo sistema de linhas de defesa de auditoria de *Compliance*. O IBGC[11] assim as define:

> A primeira linha de defesa tem responsabilidade direta em relação às práticas de gestão de riscos e controles internos. Nela estão os gestores das unidades e os responsáveis diretos pelos processos.
>
> A segunda linha de defesa é responsável por monitorar a visão integrada de riscos, desenvolver políticas e metodologias, dar suporte, supervisionar e monitorar o desempenho da gestão de risco feita pela primeira linha de defesa (áreas operacionais), realizando também testes de controle e simulações.
>
> A terceira linha de defesa é realizada pela auditoria interna. É recomendável que esta área tenha profissional especializado em segurança da informação.

6 OEA, Reporte Ciberseguridad 2020, Ciberseguridad, riesgos, avances y el caminho a seguir en America Latina y el Caribe, Organização dos Estados Americanos, 2020, p.29

7 OLHAR DIGITAL. Disponível em: <https://olhardigital.com.br/noticia/ifood-admite-falha-que-expos-dados-de-clientes-nesta-sexta-feira/102381>. Acesso em 15.08.2020.

8 KASPERSKY. Disponível em: <https://www.kaspersky.com.br/blog/empresa-brasil-ransomware-pandemia/15527/>. Acesso em: 20.06.2020.

9 OLHAR DIGITAL. Disponível em: <https://olhardigital.com.br/noticia/dados-de-usuarios-do-uber-eats-vazam-na-dark-web/104842#:~:text=%C3%89%20importante%20ressaltar%20que%20o,aplicativos%20ou%20plataformas%20de%20terceiros.> Acesso em 15.08.2020.

10 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, NBR ISO 27005: 2008, p.10

11 IBGC, Papéis e Responsabilidades do Conselho na Gestão de Riscos Cibernéticos, Instituto Brasileiro de Governança Corporativa, IBGC Orienta, São Paulo, 2019, p 21-22

3 – Gestão do risco cibernético em conformidade às normas reguladoras

O gerenciamento dos riscos cibernéticos e sua avaliação são realizados dentro dos seguintes parâmetros, de acordo com o item 05 da norma ABNT ISO 27005[12]:

Convém que a gestão de riscos de segurança da informação contribua para:

- Identificação de riscos
- Análise/avaliação de riscos em função das consequências aos negócios e probabilidade de sua ocorrência
- Comunicação e entendimento da probabilidade e das consequências destes riscos
- Estabelecimento de ordem prioritária para tratamento destes riscos
- Priorização das ações para reduzir a ocorrência dos riscos
- Envolvimento das partes interessadas quando as decisões de gestão de risco são tomadas e mantidas informadas sobre a situação de gestão de risco
- Eficácia do monitoramento do tratamento do risco
- Monitoramento e a análise crítica regular de riscos e do processo de gestão dos mesmos
- Coleta de informações de forma a melhorar a abordagem, da gestão de riscos
- Treinamento de gestores e pessoal a respeito dos riscos e das ações para mitiga-los

Importa mencionar que, na avaliação do risco é bastante comum realizar-se um *score* de cybersegurança feito por machine learning[13], baseado em diversas situações que descrevem prováveis vulnerabilidades que podem afetar o sistema da empresa, para que seja calculado o nível de risco de que seja sofrido um cyber ataque.

Verifica-se, então, que a gestão do risco cibernético funciona de forma bastante semelhante à gestão de qualquer risco em programa de *Compliance*, ou seja, com necessidade de *risk assessment*, avaliação e monitoramento constante, bem como de engajamento de seus gestores para definição das melhores estratégias.

Sobre o monitoramento do risco cibernético em nível operacional, **é importante ressaltar** que ele depende de diversos profissionais, que estarão na sua linha de frente, garantindo a sua funcionalidade e alto desempenho.

Em muitas empresas, o profissional que atuará no dia a dia do funcionamento do sistema de segurança da informação será o CISO (CHIEF INFORMATION SECURITY OFFICER), que receberá os reportes do monitoramento de fluxo de dados e de vulnerabilidades detectadas, bem como de falhas de softwares ou equipamentos da empresa.

Ao lado dele estará o CFO (CHIEF FINANCIAL OFFICER) que será o avaliador do desempenho e dos custos da estrutura montada para segurança de dados e sistemas, o que será objeto de reporte aos investidores e conselho de administração.

Como canal de comunicação entre a segurança da informação corporativa e sua governança teremos ainda o CIO (CHIEF INFORMATION OFFICER), que trará os resultados e as novas demandas de risco cibernético e proteção de dados pessoais para a alta administração, que precisará estar

12 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, NBR ISO 27005:2018, p.4

13 TECNOBLOG, Machine learning o que é e porque é tão importante. Disponível em: <https://tecnoblog.net/247820/machine-learning-ia-o-que-e/>. Acesso em 14.06.2020.

devidamente cientificada do quadro atual do funcionamento da arquitetura da informação da empresa, para desenvolvimento de novas estratégias de mitigação.

Não podemos deixar de incluir neste time o DPO (Data Protection Officer), o qual será responsável pelo controle da qualidade do tratamento de dados, o qual deverá ser imediatamente reportado sobre qualquer possível vazamento que possa acontecer, colocando em risco o sistema.

4 – Proteção de dados pessoais e *compliance* digital

A proteção de dados sempre foi algo bastante importante para as empresas, devido às consequências desastrosas decorrentes de seu vazamento, sendo tais acontecimentos ora denominados como incidentes de segurança.

A norma ISO 27001[14], que disciplina os sistemas de gestão de segurança da informação, define em seu item 3.6 os incidentes de segurança da informação como "um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação".

Nesse sentido, um vazamento de dados pessoais pode ser considerado um incidente de segurança, diante das suas graves consequências, de acordo com a normativa supra citada.

Frise-se que, a maioria das empresas de porte já utilizava *frameworks*[15] para proteção de sistemas, como, por exemplo, o **COBIT**[16], criado em 1996 pelo **ISACA**[17], que estabelece diretrizes internacionais essenciais para governança de TI, como políticas de planejamento, gerenciamento e monitoramento de risco cibernético.

Importa salientar que a norma brasileira **ABNT ISO 27001**[18] destaca questões importantes ligadas ao vazamento de dados na letra **e** do item 4.2.1:

e) Analisar e avaliar os riscos.

1) Avaliar os impactos para o negócio da organização que podem resultar de falhas de segurança, levando em consideração as conseqüências de uma perda de confidencialidade, integridade ou disponibilidade dos ativos.

2) Avaliar a probabilidade real da ocorrência de falhas de segurança à luz de ameaças e vulnerabilidades prevalecentes, e impactos associados a estes ativos e os controles atualmente implementados.

3) Estimar os níveis de riscos.

4) Determinar se os riscos são aceitáveis ou se requerem tratamento utilizando os critérios para aceitação de riscos estabelecidos em 4.2.1c)2).

f) Identificar e avaliar as opções para o tratamento de riscos.

Ocorre que, as referidas diretrizes seriam apenas orientações gerais de gestão de segurança da informação, sem enfrentar especificamente determinados temas, como a proteção de dados pessoais, pelo que, havia lacuna legal sobre o assunto.

A questão da proteção de dados pessoais e risco cibernético ganhou especial relevância, mais tarde, pela edição do **Regulamento Europeu de Proteção de Dados (GDPR)**, que entrou em vigor em maio

14 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, NBR ISO 27001: 2006, p.2.
15 FRAMEWORK - estrutura básica de gerenciamento de projetos.
16 COBIT - objetivos de controle da informação e tecnologia relacionada.
17 ISACA - Associação de Auditoria e Controle de Sistemas de Informação.
18 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, NBR ISO 27001:2006, p.5.

de 2018 e trouxe medidas de observância obrigatória para empresas que possuem em seu sistema dados de pessoas domiciliadas na União Européia, impondo políticas de concordância efetiva sobre teor de dados, a necessidade de retirada de informações do sistema, após determinado prazo, e até mesmo aplicação de multa, caso haja negligência sobre o tratamento daqueles dados.

No Brasil tivemos, a princípio, a edição do **Marco Civil da Internet (Lei 12.965/14),** que trouxe regramento para o uso da internet no país, estabelecendo direitos e garantias ao usuário, mas não disciplinou especificamente a proteção da privacidade.

Posteriormente, foi promulgada a **LGPD (Lei Geral de Proteção de Dados – Lei 13.709/18)**, que, inspirada na legislação europeia, traz uma série de medidas justamente para proteção da informação, no momento do tratamento dos dados de qualquer pessoa no Brasil, para preservá-los, prevenindo os danos decorrentes de sua circulação descontrolada na rede mundial de computadores.

Vale destacar que a LGPD também determina que sejam implantadas políticas de governança e boas práticas na gestão de sistemas de informação, para fins de mitigação de riscos, conforme o texto do seu artigo 50:

> **Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.**
>
> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
>
> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
>
> I – implementar programa de governança em privacidade que, no mínimo:
>
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
>
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
>
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
>
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
>
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
>
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
>
> g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

No entanto, a LGPD é mais específica que a norma ISO 27001, pelo fato de disciplinar prioritariamente a proteção dos dados pessoais e não somente a proteção do sistema contra riscos cibernéticos e demais dados.

Assim, a LGPD trouxe medidas relevantes, como a necessidade do consentimento do titular das informações para tratamento, o destaque para a proteção de dados sensíveis (dados de cunho étnico, religioso, político e etc., que possam identificar uma pessoa), prazo para o seu tratamento e a obrigatoriedade de sua eliminação, ao término do tratamento, conforme as normas dos artigos 7, inciso I, 11, 15 e 16 da LGPD:

Art. 7º - O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I – mediante o fornecimento de consentimento pelo titular;

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II – fim do período de tratamento;

III – comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV – determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I – cumprimento de obrigação legal ou regulatória pelo controlador;

II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Vale destacar dois documentos fundamentais para a eficaz proteção de dados no *Compliance* Digital: o **ROPA** (Record of Processing Activities), que é um demonstrativo do tratamento de dados que descreve o fluxo de dados pessoais, a sua finalidade, local de armazenamento etc.. e o **DPIA (**Data Protection Impact Assessment), que é o relatório de impacto de ameaças cibernéticas, que aponta os riscos do sistema, bem como suas medidas de proteção e mitigação, os quais devem ser constantemente revisados pelos gestores, conforme a expansão dos negócios da empresa.

Percebe-se que a LGPD trouxe, então, diversas diretrizes de proteção de dados, que devem ser incorporadas ao dia a dia da governança cibernética da empresa, para que ela seja realizada de forma segura e satisfatória.

5- A interlocução entre a governança de SI (segurança da informação) e a alta direção das empresas

Diante desse quadro de necessidade de proteção de sistemas e dados pessoais, conforme a LGPD e demais normas que incidem sobre o tema, a sua gestão nas empresas precisará estar integrada com a sua governança, para que possa ser eficiente, de forma a existir um verdadeiro *Compliance* Digital corporativo.

Logo, o conselho de administração de uma empresa precisa entender a estrutura da proteção de dados pessoais e sistemas da empresa e não associar o assunto somente ao setor de TI, ou seja, incorporar a questão realmente ao gerenciamento do risco de processos da sua atividade.

A OEA[19] recomenda o engajamento da alta direção sobre risco cibernético, sendo algo que deve fazer parte da realidade da governança corporativa.

À medida que a ameaça cibernética tem crescido, a responsabilidade (e expectativas) dos membros do conselho tem crescido. Os diretores precisam fazer mais do que simplesmente entender que as ameaças existem e receber relatórios da administração. Eles precisam empregar os mesmos princípios de investigação e desafio construtivo que são características padrão nas discussões de gestão do conselho sobre estratégia e desempenho da empresa.

Assim sendo, não se trata de um mero recebimento de relatórios de segurança da informação e consequente autorização de despesas por parte do setor operacional de proteção de dados e sim de efetiva participação na tomada de decisões sobre diretrizes de cumprimento de normas como a LGPD.

Com isso, **é fundamental o estabelecimento de** uma governança cibernética integrada na governança corporativa já estabelecida, a qual será responsável, inclusive, pela definição do apetite de risco cibernético que será tolerado ou não pela empresa.

6 – A atuação da alta direção na governança cibernética do *compliance* digital

A atuação estratégica de um conselho de administração é fundamental no sucesso da governança cibernética da empresa, diante de todas as necessidades que envolvem a gestão do risco cibernético.

19 OEA, Manual de suporte sobre risco cibernético para o conselho administrativo, Organização dos Estados Americanos, 2020, p.18.

Assim sendo, há que se inteirar a alta direção da empresa sobre os pontos mais importantes do planejamento da segurança da informação, facilitando-se o seu entendimento relativo aos pilares de proteção de sistemas e dados pessoais, com consulta a especialistas externos sobre segurança cibernética, sempre que for necessário.

Fundamental ainda que o assunto segurança cibernética seja pauta constante das reuniões de governança da empresa, pois o tema, caso seja mal conduzido, pode afetar contratos e gerar má reputação para a empresa, tendo em vista que um empreendimento que se vê envolvido em constantes vazamentos de dados pessoais ou sofre frequentes ataques cibernéticos não oferece ambiente seguro de negócios.

Frise-se que muitas ações de empresas foram desvalorizadas no mercado por conta de vazamentos de dados, como ocorreu com o Facebook[20] e o Banco Inter[21], pelo que, a gestão deficiente do risco cibernético pode afetar seriamente a situação de uma empresa e prejudicar o seu crescimento.

Com isso, um conselho de administração que realiza a gestão de risco com excelência, deve estar atento à diversas questões, como o custo de manter o sistema protegido na superfície de exposição necessária à operação de novos negócios da empresa, o esboço de um plano de contingência para socorrer sistemas, caso fossem atacados, a avaliação do dano causado por ataques cibernéticos em vulnerabilidades descobertas na sua rede, por conta do limite da cobertura do seguro cibernético, bem como a análise de segurança de softwares que são oferecidos para proteção de sistemas, de acordo com os certificados exigidos no mercado.

Importante também será a alta direção definir a periodicidade de auditorias externas de sistemas, com a realização de testes de segurança (*pen test*) para detecção de eventuais vulnerabilidades, com revisão de budgets de investimento neste setor.

A alta direção da empresa ainda será responsável pelo engajamento dos colaboradores nas políticas de prevenção ao risco cibernético, definindo as melhores práticas para proteção de dados e de rotinas de serviço padrão e participando de treinamentos específicos sobre o tema, de modo a dar o exemplo para os seus colaboradores, demonstrando o seu engajamento.

Outra preocupação que deve ser relevante para conselho de administração é o roubo interno de dados de empresa, conforme pesquisa realizada pela KROLL[22], o que reforça a necessidade de definir-se um monitoramento diferenciado sobre o tema:

> A pesquisa da Kroll aponta que são os funcionários da empresa, mais do que qualquer outra entidade, os principais responsáveis por fraudes e vazamentos de informações internas. O que não chega a surpreender. De acordo com a Kroll, a pesquisa revela que esse grupo é responsável pela maior parte do roubo de dados e de fraudes internas nas empresas (44% e 45% dos incidentes citados são, respectivamente, perpetrados por funcionários). Além disso, os funcionários são uma fonte significativa de danos à reputação e a principal fonte de incidentes de suborno e corrupção. Para a consultoria, esse último ponto serve como um lembrete: embora as regulamentações contra suborno e corrupção geralmente se concentrem em terceiros, em geral, esses incidentes exigem um participante de dentro da organização. "Apenas 13% dos vários tipos de incidentes

20 EXAME. Disponível em: <https://exame.com/mercados/facebook-derrete-na-bolsa-em-meio-ao-escandalo-de-vazamento-de-dados/. Acesso em 12.06.2020.

21 TUDO CELULAR. Disponível em: <https://www.tudocelular.com/seguranca/noticias/n138074/banco-inter-vazamento-dados.html>. Acesso em 12.06.2020.

22 LEC, Revista Digital, ano 8, nº 28, abril-2020, p.61

abordados nessa pesquisa foram cometidos por atores desconhecidos.

Um outro ponto que deve estar no radar da alta administração é a cadeia de suprimentos da empresa, pois as pequenas e médias empresas tem sofrido muitos ataques cibernéticos[23], por não possuírem recursos suficientes para proteção de dados pessoais, sendo elas usadas como atalhos de acesso ao sistema das grandes corporações.

Logo, é importante que a governança cibernética seja cientificada sobre estas vulnerabilidades e defina controles internos sobre o tema, uma vez que o risco cibernético nela pode ser aumentado, caso não haja monitoramento periódico, atingindo-se o sistema da empresa.

Mesmo assim, apesar de todas estas questões complexas, a pesquisa da DELOITTE[24] de 2019 sobre segurança cibernética na América Latina e Caribe aponta que:

70% das organizações afirmam não ter certeza da eficácia de seu processo de resposta diante desses incidentes, enquanto apenas 3% realizam simulações para testar suas capacidades efetivas de resposta diante de um evento cibernético.

Apenas 31% das empresas colocam em prática medidas de inteligência para detectar riscos e compartilham ameaças com outras organizações.

Tal conclusão acima é bastante preocupante e demonstra que o risco cibernético precisa ser uma preocupação real no *Compliance* Digital, pelo que, a maturidade organizacional sobre o tema em muitas empresas precisa ser melhorada.

7 – Considerações finais

Diante disso tudo, a alta direção das empresas terá um novo desafio pela frente, que será o gerenciamento do risco cibernético**,** assumindo-se novas responsabilidades impostas agora pela expansão de negócios no meio digital, pelas exigências de proteção de dados pessoais, definidas pela LGPD e pelo mercado.

Assim sendo, os deveres de governança corporativa incluirão o acompanhamento das questões de proteção de dados pessoais e de segurança da informação das empresas, através do desenvolvimento de estratégias de seu implemento e de políticas de mitigação de danos causados por eventuais ataques cibernéticos que possam atingir suas operações e negócios.

Tais práticas trarão um novo tom da liderança, que estará alinhada com a natureza do negócio, pelo conhecimento dos principais riscos nele envolvidos, o que é essencial para o sucesso do *Compliance* Digital de qualquer empresa.

Referências bibliográficas

Normativas

Associação Brasileira de Normas Técnicas, NBR ISO 27001:2006

Associação Brasileira de Normas Técnicas, NBR ISO 27005:

LGPD (Lei Geral de Proteção de Dados – Lei nº 13.709/18)

Bibliográficas

AXUR, *Relatório Atividade Criminosa Online Brasil*, 1º trimestre 2020

DELOITTE, *Relatório Cyber América Latina e Caribe*, 2019

GIOVANINI, Wagner. *Programas de Compliance e Anticorrupção: Importância e Elementos Essenciais*. In: SOUZA, Jorge Munhós de; QUEIROZ, Ronaldo Pinheiro de (Org.). Lei Anticorrupção e Temas de *Compliance*. 2. Ed. Salvador: Juspodivm, 2017.

23 SIMPLIFIQUETI. Disponível em: <https://simplifiqueti.com.br/site/pequenas-medias-empresas-ataques-ciberneticos/>. Acesso em 10.05.2020.

24 DELOITTE, Relatório cyber América Latina e Caribe, 2019.

IBGC, *Papéis e Responsabilidades do Conselho na Gestão de Riscos Cibernéticos*, IBGC Orienta, São Paulo, Instituto Brasileiro de Governança Corporativa, 2019.

LEC, *Revista Digital*, ano 8, nº 28, abril/2020.

OEA, *Manual de Suporte Sobre Risco Cibernético Para o Conselho Administrativo*, Organização dos Estados Americanos, 2020.

Eletrônicas

EXAME. Disponível em: <https://exame.com/mercados/facebook-derrete-na-bolsa-em-meio-ao-escandalo-de-vazamento-de-dados/>. Acesso em 12.06.2020.

FÓRUM ECONÔMICO MUNDIAL, *Global Risks Report*, 2020. Disponível em: <http://reports.weforum.org/global-risks-report-2020/wild-wide-web/>. Acesso em: 02.07.2020

KASPERSKY. Disponível em: <https://www.kaspersky.com.br/blog/empresa-brasil-ransomware-pandemia/15527/>.Acesso em 20.06.2020.

OLHAR DIGITAL. Disponível em: <https://olhardigital.com.br/noticia/ifood-admite-falha-que-expos-dados-de-clientes-nesta-sexta-feira/102381>. Acesso em 15.08.2020.

OLHAR DIGITAL. Disponível em: <https://olhardigital.com.br/noticia/dados-de-usuarios-do-uber-eats-vazam-na-dark-web/104842#:~:text=%C3%89%20importante%20ressaltar%20que%20o,aplicativos%20ou%20plataformas%20de%20terceiros.>. Acesso em 15.08.2020.

SIMPLIFIQUETI. Disponível em: <https://simplifiqueti.com.br/site/pequenas-medias-empresas-ataques-ciberneticos/>. Acesso em: 10.05.2020.

TECNOBLOG, *Machine Learning o que é e porque é tão importante*. Disponível em: <https://tecnoblog.net/247820/machine-learning-ia-o-que-e/>. Acesso em 14.06.2020.

TUDO CELULAR. Disponível em: <https://www.tudocelular.com/seguranca/noticias/n138074/banco-inter-vazamento-dados.html>. Acesso em 12.06.2020.

Compliance, Governança Corporativa e Ética

EDMO COLNAGHI NEVES

Diretor Jurídico e *Compliance* ABB Asea Brown Boveri e GE General Electric durante dez anos, trabalhou também em Trench, Rossi & Watanabe Advogados. Professor em Mackenzie, PUCSP, PUCRS, autor dos livros "*Compliance* Empresarial, o tom da liderança" e "Doing *Compliance* in Brazil. Doutor e Mestre em Direito do Estado, PUC/SP,cursou Business for Foreign lawyers, Michigan, Estados Unidos; Business Program, em Lausanne, Suíça, no IIMD – International Institute for Management Development e Direito e *Compliance* na Universidade de Coimbra, Portugal; Gestão de Riscos, COSO ERM,IIA -International Institute for Auditors, pós em administração de empresas, FIA – Fundação Instituto de Administração e curso de Conselheiro de Administração no IBGC. É Presidente do IBDEE – Instituto de Direito e Ética Empresaria, fluente em inglês, espanhol e italiano e atualmente é Sócio fundador de Colnaghi Neves Consultoria Empresarial.

A Ética tem sido cada vez mais considerada nas boas práticas de Governança Corporativa e *Compliance* na última década no Brasil, o que não significa necessariamente que esta consideração tenha resultado em incorporação de valores éticos nas condutas dos membros das organizações. E aqui cabe a ressalva de que buscamos pensar sempre em pessoas que conduzem as organizações, eis que estas últimas são ficções jurídicas. Quem pratica atos antiéticos são as pessoas, não as organizações.

Esta consideração embora óbvia é particularmente importante eis que há uma tendência de se generalizar indevidamente quando se trata do assunto, criando-se situações injustas em que culpados não são punidos e inocentes muitas vezes passam por situações injustas ou pouco apropriadas, para se dizer o mínimo.

Veja-se, por exemplo, a situação de funcionários que trabalham honestamente para organizações envolvidas em grandes escândalos de corrupção que são veiculados pela grande mídia. Tais funcionários não participaram das práticas ilícitas, mas sempre fica uma associação indevida da pessoa com a organização, sempre uma suspeita de que a pessoa é desonesta ou, pelo menos, não confiável

Há situações ainda piores em que diretores de *compliance* foram acusados indevidamente por autoridades públicas por algo que não fizeram e nem deixaram de fazer. O dever do diretor de *compliance* é conduzir o programa de *compliance* e integridade continuamente de modo diligente, com lealdade e com prática documentada de informação, sem conflitos de interesse, assim como administradores em geral tem tais deveres, como bem estabelecido pela legislação correspondente.

Se, no entanto, ainda assim vier a ocorrer a corrupção na organização, não se pode imputar a responsabilidade ao diretor de *compliance*, que não é a pessoa que toma as decisões de negócios. Não existe o dever de garantia, dever de garante, de que tais ilícios não irão ocorrer. Organizações são compostas de indivíduos, com livre arbítrio, que muitas vezes decidem pela fraude por questões de necessidade ou desejo, controles fracos e processo de racionalização, como nos ensina o conhecimento do triângulo da fraude e posteriores alterações.

De outro lado, atrás da ficção jurídica das organizações, há indivíduos que não são alcançados, remanescendo a punição para a pessoa jurídica que, com a piora dos resultados em virtude do pagamento das penalidades e perdas de negócios, acaba por implementar processos de demissão em massa, uma vez mais punindo os economicamente hipossuficientes

O Memorando Yates exemplifica isto de maneira contundente. A procuradora geral do DOJ – Department of Justice dos Estados Unidos da América do Norte, que emitiu e empresta o sobrenome a este Memorando, antes da eleição do atual presidente daquele país, redirecionou as negociações de acordos com aquele órgão justamente considerando este aspecto pessoal do cometimento dos ilícitos.

Em linhas gerais ,orientou a Procuradora que novos acordos com o DOJ somente seriam assinados se todos os executivos da empresa envolvidos no ato de corrupção fossem indicados de modo transparente, esclarecendo e comprovando quais foram suas práticas, independente de sua estatura ou importância para a organização.

Determinou também que os indivíduos seriam punidos com penalidades independentes das penalidades aplicadas às pessoas jurídicas e que os procuradores do DOJ, tanto da área civil quanto da área penal tivessem em conta as particularidades de tais indivíduos para que as penas fossem efetivas. Além disto, as penas pecuniárias já não mais poderiam ser pagas pelas organizações, mas sim diretamente pelos indivíduos, dentre outras coisas.

Isto nos dá mais um exemplo da importância de sempre se considerar a individualidade das práticas ilícitas e antiéticas, seja para não prejulgar ou condenar pessoas inocentes, seja para não deixar de aplicar penalidades às pessoas efetivamente culpadas, evitando-se assim causar injustiça em ambas as situações.

A história nos traz grandes pensadores que elaboraram profundamente sobre a Ética como, por exemplo, Spinoza, Immanuel Kant e Aristóteles. Este último escreveu Ética a Nicômaco, seu filho, em que parte da premissa que toda empreitada humana inicia buscando um bem , que pode ser fama, fortuna ou alguma outra coisa. Pondera que todos estes bens na verdade levam a algo mais, que no final das coisas é a busca pela felicidade, o bem final, "Eudaimonia", num sentido diferente do que se tem hoje em dia .

Para Aristóteles isto implica em viver uma vida de acordo com virtudes, sobre os quais passa a discorrer em sua obra. Tais virtudes incluem a moderação, a prudência, a justiça, a generosidade, a amizade e o prazer, mas dentre todas elas, considera a justiça como a mais importante.

Tais valores éticos, citados a título de referência, para dar um conteúdo mais consistente à sua menção, devem informar as iniciativas de *Compliance* e Governança Corporativa. *Compliance* não abrange Integridade, mas antes o contrário, quem age com Integridade certamente criará uma situação em que há *Compliance*, embora vá além.

Certa organização, em determinada época, após desenvolver seu Programa de *Compliance* por vários anos, decidiu que referido Programa deixaria de ser "de *Compliance*" e passaria a ser "de Integridade" e ante aqueles que duvidaram da real diferença entre ambos, explicou que em *Compliance* há uma adequação das condutas às normas e as pessoas procuram se conformar ao programa eis que visam preservar seus empregos e suas funções.

No entanto, em Integridade, vai-se mais a fundo, o foco deixa de ser o mero cumprimento de normas e passa a ser a efetiva crença em valores, que passam a integrar a cultura e o agir das pessoas que formam a organização. Agir com honestidade é a melhor forma de conduzir os negócios.

Portanto, passa-se de *Compliance* à Integridade e naturalmente isto deve levar à longevidade e à prosperidade, ou seja, à sustentabilidade em sentido amplo. Sustentabilidade da organização que dá suporte, consequentemente, à sustentabilidade das pessoas que a formam, todos os seus "stakeholders".

Compliance, naturalmente, aqui se vê também, muito mais do que ajustamento, adequação ou conformidade. Vê-se como uma estratégia que leva a organização a atingir seus objetivos, estratégia esta que ora se volta para o passado, ao detectar violações e aplicar medidas disciplinares, ora se volta para o futuro ao, preventivamente, tomar medidas criando códigos, dando treinamentos, fazendo comunicações e ainda faz parte do presente, recebendo denúncias de violações, fazendo auditorias de fornecedores e parceiros de negócios e aprovando controles sobre doações, patrocínios, presentes e entretenimento.

Este conjunto de atividades apresenta-se, do ponto de vista pragmático, como medidas para evitar que os riscos da organização se concretizem, o que poderia impedi-la de alcançar seus objetivos, que naturalmente não se restringem a alcançar a lucratividade, trazendo dividendos aos sócios e acionistas, mas vai além, incluindo a reponsabilidade social, a satisfação dos clientes, a responsabilidade ambiental, segurança para os administradores, salário e emprego aos trabalhadores e cumprimento das normas em geral.

Sob esta ótica, *Compliance* e seu programa seria uma forma de mitigar os riscos, uma das possíveis respostas aos riscos, detectada num processo de gestão de riscos, que pode apontar também mais alternativas, como: eliminação pura e simples dos riscos, transferí-los a terceiros, assumir os riscos ou ainda explorar os riscos.

Mitigando o risco por meio de um Programa de *Compliance* ou adotando outras modalidades de respostas aos riscos, aqueles que são responsáveis pelos riscos da organização e aqueles que são responsáveis pelas respostas aos riscos (que não se confundem uns com os outros) devem seguir princípios éticos e morais que, em certa medida, já devem estar esclarecidos e registrados, quando a organização define sua missão, visão e valores e a divulga aos quatro ventos. De nada adianta definir missão, visão e valores e guardá-los na gaveta.

Esta decisão, esta atividade e estes valores devem ter respaldo em uma instância mais elevada da organização, que tenha poder de decisão, que tenha respaldo naqueles que criaram a organização e que investem capital na organização, os sócios e acionistas, bem como nos seus mandatários diretos, conselheiros de administração e

diretores e outros órgãos de alta hierarquia dentro da estrutura administrativa como o conselho fiscal, o conselho consultivo, o conselho de família e o comitê de auditoria.

Tais pessoas avaliando situações e emanando decisões, conforme rotinas e práticas reiteradas e muitas vezes pré-determinadas, governam a corporação, fazem a governança corporativa, igualmente buscando dar sua contribuição como autoridades da organização na consecução dos objetivos do negócio.

Seu poder é grande, no entanto não é ilimitado, vez que devem observar as leis do país que se aplicam à organização, com todas as suas peculiaridades que abrangem e muitas vezes, regulamentações específicas, como costuma acontecer em mercados específicos em que há agências governamentais. Sendo exemplos disto as agências federais ANVISA, ANS, ANATEL, ANEEL, ANP, ANAC, ANCINE, AMN, ANA, ANTT e ANTAQ.

E esta governança das corporações, com suas práticas, que visam atingir os objetivos dos negócios, além de observar a legislação e as regulamentações, devem ter também em conta a Ética e os princípios aplicáveis à boa governança corporativa: equidade, transparência e prestação de contas.

Tais princípios implicam que devem ser tratados de modo igualitário acionistas majoritários e minoritários tanto quanto possível, para que haja o valor justiça, bem como os demais "stakeholders", na medida em que são interessantes e interessados na organização e em certa medida também concorrem para a consecução dos seus objetivos e representam o atual estágio de evolução da governança corporativa. A injustiça, ou pelo menos o sentimento de injustiça, pode levar ao contencioso judicial, que prejudica a organização por um longo período, tendo se expandido nas últimas décadas as práticas de mediação e de arbirtragem.

Deve haver também transparência de tal forma que as práticas e informações sejam reveladas às instâncias apropriadas, não somente na medida das obrigações legais, mas também na proporção em que sejam efetivamente necessárias.

Devem os administradores prestar contas de suas ações e nesta medida serão responsabilizados se não forem leais à organização, diligentes e se agirem com conflitos de interesse.

Tudo isto compõe a Ética que deve permear a comunicação e as boas práticas da governança corporativa, desde as tarefas mais operacionais de *Compliance* e Gestão de Riscos até as mais importantes e estratégicas decisões do Conselho e aqui se pensa no Conselho em sentido amplo, como utilizado mundialmente, não somente o Conselho de Administração, mas outros Conselhos que a organização possa vir a ter ou adotar como o Conselho Fiscal, o Conselho Consultivo e o Conselho de Família.

Documentos podem servir de esteio para esta atividade de Governança Corporativa, Gestão de Riscos e *Compliance* para que não se perca no caminho entre as decisões urgentes do dia a dia, ou nas decisões estratégicas da alta liderança, envolvendo questões importantes que podem mudar o rumo da organização como uma incorporação, uma fusão, a emissão de debêntures, o caminho IPO, a abertura de filiais, a sucessão do sócio fundador que venha a falecer ou outros temas desta grandeza.

Tais documentos vão além do estatuto social, contrato social, acordos de acionistas, passando também pelo código de conduta, políticas de *compliance*, bem como procedimentos. Todos estes documentos naturalmente devem estar inspirados pela Ética e refletir valores como o respeito às pessoas dos funcionários, dos funcionários de fornecedores, dos funcionários de clientes e de parceiros e de funcionários públicos, à não discriminação e a proibição

enérgica de pagamentos indevidos, daí logicamente com destaque à proibição a pagamentos indevidos a qualquer autoridade pública, que representa o interesse comum, o interesse de toda a nação, a coisa pública.

Assim, a Ética deve se espraiar por todas as relações entre *Compliance* e Governança Corporativa, como efetivamente tem sido cada vez mais presente na última década no país. Há certamente um longo caminho a percorrer, se compararmos a realidade nacional com a realidade de nações mais evoluídas neste aspecto, mas o caminho foi iniciado e deve continuar.

O profissional de Governança Corporativa e de *Compliance* ao tomar suas decisões e exercitar suas práticas deve manter sempre presente a indagação interna: isto é ético? Deve fazer diferente do protagonista da história do anel de Giges, que ao obter o poder da invisibilidade, passou a cometer atrocidades. Vale lembrar, por fim, que ser ético deve ser a qualquer momento, mesmo quando ninguém está vendo.

Open Banking e a Proteção de Dados

GABRIELA DE ÁVILA MACHADO

Líder no Marcos Martins Advogados, LLM em Direito Societário pela University of Cambridge, LLM em Direito Comercial Internacional pela University of California – Davis, Bacharel em Direito pela Fundação Armando Alvares Penteado, Capacitação em Proteção de Dados pela PrivacyID e pela Antebellum, Capacitação em *Compliance* pela Via Ética e pela LEC, Data Protection Officer certificada pelo Exin, Coautora do "Manual de Implementação da Lei Geral de Proteção de Dados", Editora Via Ética, São Paulo, 2019 e outros artigos sobre o tema.

Open banking, também conhecido como "open bank data", é a prática bancária por meio da qual instituições financeiras abrem o acesso a dados bancários, de transação e outros dados financeiros, do consumidor por meio de interface de programação de aplicativos (ou em inglês *application programming interfaces* (APIs)). Pelo open banking, instituições financeiras darão acesso a dados pessoais e financeiros do consumidor, com o consentimento deste, a terceiros prestadores de serviço – normalmente fintechs.

A proposta do Open Banking é a descentralização das informações financeiras, que atualmente estão em posse das grandes operadoras. Com isso, o consumidor poderá escolher a solução que quer usar. Outra vantagem para o consumidor é a possibilidade de portabilidade. Com o open banking, consumidor que decidir pela mudança de instituição não perderá seu histórico financeiro, podendo levar suas informações de forma automatizada para outra instituição.

Segundo especialistas, o Open Banking forçará grandes bancos a serem mais competitivos com bancos menores e mais novos, o que resultará em taxas menos abusivas e custos mais baixos aos consumidores, sem contar na melhoria do atendimento ao

consumidor e da tecnologia usada. Além disso, os provedores de crédito também teriam uma noção mais detalhada do perfil de crédito do solicitante.

Na Europa, a PSD2 (revised Payment Services Directive, diretiva revisada sobre os serviços de pagamento) é a regulação que rege o Open Banking e o prazo para a implementação do modelo Open Banking era setembro de 2019 – de forma que as instituições financeiras europeias já devem operar em conformidade com o tema.

A versão brasileira passou por audiência pública em novembro de 2019 e a Resolução Conjunta 01/2020, que dispõe sobre o escopo de dados e serviços do Sistema Financeiro Aberto (Open Banking) foi publicada em 4 de maio de 2020. Em conjunto com a Resolução foi publicada também a Circular nº 4.015.

A Resolução obriga os grandes e médios bancos (classificados como S1 e S2) a participarem do Sistema, enquanto os fintechs, dentre outras instituições poderão escolher e ainda determina que o Sistema deverá ser implementado em quatro fases com fim previsto para outubro de 2021.

Segundo uma reportagem da Veja[1], a preocupação dos grandes bancos seria maior do que a das fintechs, já que estes grandes bancos (Itaú, Banco do Brasil, Bradesco, Santander e Caixa –possuem 80% do mercado) carregam muitos sistemas legados de suas aquisições ao longo dos anos e sua tecnologia poderia se mostrar em desvantagem àquela das fintechs.

No geral, a Resolução Conjunta 01/2020, no seu artigo 3º expõe quatro objetivos do Open Banking: incentivo à inovação, promoção da concorrência, aumento da eficiência do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro e a promoção da cidadania financeira. E logo em seguida, o artigo 4º apresenta os seis princípios que devem ser observados:

1. Transparência;
2. Segurança e privacidade de dados
3. Qualidade dos dados;
4. Tratamento não discriminatório;
5. Reciprocidade;
6. Interoperabilidade.

De pronto podemos ver que quatro desses princípios estão diretamente ligados aos princípios previstos na Lei Geral de Proteção de Dados. Abordaremos isso mais a frente.

A primeira fase do Open Banking, com início previsto para 30 de novembro de 2020, envolve a divulgação, pelos participantes, de produtos e serviços oferecidos. O Diretor de Regulação do Banco Central explica que com as informações sobre custos e preços dos produtos e serviços, terceiros poderão tratar as informações para oferecer consultoria para clientes.

Na segunda fase, prevista para terminar em maio de 2021, os participantes deverão abrir os dados cadastrais e de operações financeiras dos clientes. O intuito dessa fase é permitir a ampliação do leque de produtos e serviços oferecidos aos clientes. O agente terceiro, munido dessas informações, poderão oferecer produtos financeiros personalizados à cada cliente.

A terceira fase, prevista para terminar em agosto de 2021, traz a adesão aos serviços, o início das transações.

A quarta fase, por fim, teremos a expansão de dados e serviços disponibilizados, como investimentos, seguros, dentre outros.

As promessas do Open Banking são infinitas, mas até que ponto elas são vantajosas para os consumidores?

Segundo a pesquisa Ipsos feita com entrevistados de 15 países, as principais

1 https://veja.abril.com.br/economia/cade-se-antecipa-a-open-banking-e-enquadra-bradesco/ Acesso em 09/10/2020

preocupações dos usuários em relação ao Open Banking são "achar que haverá falta de proteção aos seus dados pessoais; o risco de que seus dados financeiros sejam obtidos por partes mal-intencionadas; e não saber quem, afinal, guardará seus dados financeiros"[2].

De fato, é de se imaginar que o open banking apresenta sérios riscos à privacidade financeira de consumidores bem como à segurança de suas finanças e isso traz também um risco de responsabilização das instituições financeiras.

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – "LGPD") entrou em vigor[3] no Brasil em setembro, após diversas discussões e prorrogações.

Nesse sentido, a proteção da privacidade foi prevista pelo Banco Central quando do desenvolvimento da norma. Inclusive, quatro dos princípios listados no artigo 4º da Resolução do Open Banking estão também previstos na LGPD: transparência, segurança e privacidade de dados, qualidade dos dados e tratamento não discriminatório.

A transparência objetiva garantir aos titulares fácil acesso a informações claras e precisas sobre a realização do tratamento de dados pessoais. O princípio da segurança e privacidade de dados objetiva garantir a segurança dos dados, por meio de medidas (sejam elas técnicas, de gestão ou outras) para proteção dos dados pessoais, bem como proteção contra a acessos não autorizados e incidentes de segurança. O princípio da qualidade dos dados visa garantir que os dados permaneçam exatos, claros, tenham a relevância preservada e sejam atualizados. E, por fim, a não discriminação visa garantir que o tratamento dos dados pessoais não seja realizado com fins discriminatórios, ilícitos ou abusivos.

Ainda, segundo o Banco Central, dentre os requisitos fundamentais para a implantação do Open Banking está o consentimento do titular, que, inclusive é uma das bases legais para o tratamento de dados pessoais prevista no inciso I do artigo 7º da LGPD.

É importante, no entanto, notarmos que consentimento, segundo o artigo 5º da LGPD, é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Dessa forma, a exemplo do que os reguladores determinaram no Reino Unido, o consentimento, pelos clientes, somente deve ser válido se baseado em informações completas sobre o tratamento de seus dados.

O próprio artigo 10º da Resolução determina as regras para obtenção deste consentimento: ele deve ser "solicitado por meio de linguagem clara, objetiva e adequada", fazendo referência a um fim determinado e que os dados ou serviços que serão objeto de compartilhamento, sejam discriminados, sendo que o consentimento deve conter a identificação do cliente. Esses requisitos se comunicam diretamente com aqueles previstos na LGPD.

Mas a Resolução vai além. Ela determina que o consentimento seja obtido com prazo de validade compatível com as finalidades, limitado a doze meses e que a instituição transmissora de dados ou detentora de conta, seja identificada. Por fim, a Resolução vai além, para esclarecer que o consentimento deverá ser obtido após a data de entrada em vigor da Resolução.

A Resolução visa ainda proteger os direitos do cliente, bem como sua hipossuficiência. O consentimento obtido por meio de contrato de adesão, por formulário com opção de aceite previamente preenchida ou de

2 https://www.gazetadopovo.com.br/gazz-conecta/open-banking-no-brasil-tera-que-superar-clima-de-desconfianca-e-risco-financeiro/. Acesso em 04/10/2020

3 Exceção feita aos artigos 52, 53 e 54, referente às sanções administrativas, que entrarão em vigor apenas em agosto de 2021.

forma presumida, sem manifestação ativa pelo cliente não será válido.

O artigo 14 da Resolução indica ainda que, além das informações sobre o consentimento, os clientes têm o direito de receber algumas informações sobre os consentimentos relativos aos compartilhamentos nos quais estejam envolvidos.

Ocorre que, inobstante o consentimento seja obtido de forma adequada à Resolução e à LGPD, as duas normativas trazem que o consentimento é revogável. Ou seja, o consentimento dado poderá ser retirado a qualquer momento, bastando uma manifestação expressa, por procedimento gratuito e facilitado, "por meio de procedimento seguro, ágil, preciso e conveniente"[4].

A Resolução prevê que a opção da revogação de consentimento deve estar disponível ao menos pelo mesmo canal de atendimento no qual o consentimento foi concedido.

Por isso costumamos dizer que o consentimento é a base legal mais frágil. Após a revogação, o controlador deverá cessar o tratamento dos dados imediatamente (exceto no caso de obrigação legal que permita a continuidade do tratamento).

Ainda, é importante ressaltar que mesmo que o tratamento seja feito com fundamento em uma das bases legais previstas na LGPD, neste caso o consentimento, isso não exime o controlador ou o operador de cuidar da proteção dos dados disponibilizados nestas plataformas unificadas, conforme princípio da segurança e proteção de dados. Existe uma preocupação quanto a tecnologia que será utilizada para manter as informações protegidas contra invasores. Estas deverão ser eficientes e robustas com regras de acesso robustas.

O próprio Banco Central entendeu os participantes do open banking deverão propor "padrão tecnológico para as interfaces e para os certificados de segurança, a padronização do leiaute de dados, os canais de encaminhamento de demandas e de resolução de disputas e os valores de ressarcimento"[5].

Neste sentido, a LGPD determina que a tecnologia utilizada na proteção deve observar algumas regras de segurança (a exemplo da ISSO 27.001). Os bancos e APIs deverão ter em vigor medidas de segurança para criptografar e proteger informações confidenciais.

Há também que se falar em regras de acesso.

Outro ponto muito importante a ser observado pelas instituições financeiras é a sua responsabilização por incidentes de segurança causados por ação ou omissão do "parceiro contratado".

A Resolução, no artigo 36, permite que as instituições contratem com entidades não autorizadas a funcionar pelo Banco Central do Brasil com o objetivo de compartilhar os dados. Poderíamos então, numa análise simplificada, colocar o parceiro como operador, no conceito previsto na LGPD[6]. Não há que se falar em co-controladores, já que o parceiro realiza o tratamento conforme determinado pela instituição, que é a controladora, nos termos da LGPD[7].

Sendo assim, apesar de a responsabilidade perante os titulares ser do controlador, pela confiabilidade, pela disponibilidade, pela segurança e pelo sigilo do compartilhamento, bem como pelo cumprimento

4 Artigo 15 da Resolução Conjunta 01/2020. https://www.in.gov.br/web/dou/-/resolucao-conjunta-n-1-de-4-de-maio-de-2020-255165055

5 Diretor do BC explica funcionamento da regulação e autorregulação do Open Banking. https://fintechlab.com.br/index.php/2020/05/25/diretor-do-bc-explica-funcionamento-da-regulacao-e-autorregulacao-do-open-banking/, Acesso em 27/05/2020.

6 Artigo 5º, VI, da LGPD "controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

7 Artigo 5º, VII, da LGPD "operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"

da legislação e da regulamentação em vigor (artigo 39 da Resolução), a LGPD prevê que o operador poderá ser solidariamente responsável quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador e que o controlador diretamente envolvido no tratamento do qual decorreram danos ao titular dos dados responderá também solidariamente.

Assim, questões de responsabilidade e indenização por danos, bem como condução de defesa, são itens fundamentais que deverão estar previstos no contrato entre instituição, como controladora, e contratados parceiros, como operadores.

A LGPD ainda, assim como o Código do Consumidor, concede permissão ao juiz para inverter o ônus da prova a favor do titular dos dados.

Então, entramos nos direitos previstos no artigo 18 da LGPD, que devem ser observados a todo tempo pelo controlador e operador: (a) confirmação da existência de tratamento; (b) acesso aos dados tratados; (c) correção de dados incompletos, inexatos ou desatualizados; (d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD; (e) portabilidade dos dados; (f) eliminação dos dados pessoais tratados com o consentimento do titular; (g) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; (i) revogação do consentimento.

Ainda há que se discutir e regular a transferência internacional de dados dentro do sistema open banking, não podemos falar em transações bancárias sem chegar a esse tema. A LGPD apenas permite a transferência de dados pessoais nos casos descritos no artigo 33: (i) para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; ou (ii) quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei; ou (iii) quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução (iv) quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; ou (v) quando a autoridade nacional autorizar a transferência; (vi) quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; (vii) quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, (viii) quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou (ix) quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º da LGPD.

A transferência internacional de dados é um tema de muita importância que depende ainda da Autoridade Nacional de Proteção de Dados para maiores esclarecimentos, principalmente no que se refere ao item (ii) acima.

Por fim, a necessidade e importância do *compliance* se faz imediata. A Resolução BACEN nº 4.595/2017, que "dispõe sobre a política de conformidade (*compliance*) das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil" determina que instituições financeiras (mencionadas no artigo 1º) "devem implementar e manter política de conformidade compatível com a natureza, o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio da instituição, de forma a assegurar o efetivo

gerenciamento do seu risco de conformidade". Então um programa de integridade dentros destas instituições não é mais opcional.

Pela leitura do artigo 48 da Resolução Conjunta, as instituições participantes do Open Banking devem ter políticas para gerenciamento de riscos, conforme previsto na regulamentação em vigor. E, nesse sentido, determina que essas políticas tenham previsão de procedimentos relacionados ao tratamento de incidentes relacionados com a violação da segurança dos dados relacionados ao compartilhamento e as medidas tomadas para a sua prevenção e solução. Esse requisito anda, também, ao lado da LGPD, que, prevê a inclusão de regras de boas práticas de tratamento de dados (que não são obrigatórias, porém podem contar para mitigar eventuais sanções).

Segundo a LGPD, este programa de governança e proteção de dados pessoais, no mínimo, deverá demonstrar o comprometimento em adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas, estabelecendo políticas e salvaguardas adequadas e que este programa esteja integrado a estrutura geral de governança – ou seja, adequar o Programa de Integridade da instituição às regras previstas na LGPD e na Resolução Conjunta é de necessidade imediata. Além de estar em conformidade com as regras, a instituição poderá melhorar sua imagem perante titulares/clientes, e se beneficiar em eventual processo judicial ou administrativo[8].

Como verificamos, a adequação das instituições participantes do Open Banking à LGPD se mostra essencial para a segurança dos consumidores titulares. É necessário que as plataformas tenham área de acesso fácil ao encarregado do controlador, como determina a própria LGPD e que as instituições criem procedimentos de atendimento e solução de problemas simplificado e transparente para fins de evitar ainda mais litígios, congestionando o Poder Judiciário.

Também, não são apenas os juristas que estão ansiosos com o início das atividades da Autoridade Nacional de Proteção de Dados. Espera-se que, como aquelas autoridades europeias, a nossa venha para regulamentar as lacunas deixadas pela LGPD, seja no que se refere à transferência internacional de dados, seja no que se refere a proteção de dados dentro do PIX e do sistema open banking, ou ainda no que se refere à medidas tecnológicas de proteção de dados e segurança da informação.

8 Artigo, 52, § 1º: "As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: (...) VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança."

Como o coronavírus deve afetar os sistemas de *compliance*?

MARIANA DE ALMADA JEVEAUX

Advogada especializada em *Compliance*, Lei Anticorrupção Empresarial e Controle da Administração Pública pela Faculdades Integradas de Vitória (FDV), com mais de 3 anos de experiência em *compliance*. Secretária da Comissão Anticorrupção e *Compliance* – CAC OAB/SP Pinheiros. Atualmente trabalha como consultora na KPMG Brasil. Obteve o Certificado Pro-Ética para o escritório de advocacia VLM em 2019.

Introdução

Assim que a pandemia do coronavírus foi declarada pela Organização Mundial da Saúde (OMS), em 11 de março de 2020, as empresas tiveram que ser rápidas para se ajustarem à nova realidade. A pandemia afetou o governo, as empresas, o comércio e a própria vida das pessoas. Fomos pegos de surpresa e estamos aprendendo no caminho quais são as melhores soluções para os novos problemas que a pandemia nos apresentou.

Nos primeiros meses de pandemia estávamos todos nos adaptando à nova situação: o governo estabeleceu novas leis e/ou leis foram flexibilizadas; empresas se esforçavam para fornecer seus serviços de novas maneiras para sobreviverem financeiramente; funcionários e membros da alta administração empresarial passaram a trabalhar de home office – não só isso, mas autoridades reguladoras também adotaram o trabalho remoto.

A preocupação com a conformidade pode ter caído na lista de prioridades de várias empresas, pois, em situações de crise, é tentador pensar que as regras normais não se aplicam mais – isto é um erro. Impostos ainda serão devidos, reportes às autoridades públicas ainda terão que ser realizados, obrigações contratuais ou trabalhistas ainda serão devidas, dentre outras obrigações que

podem até ser flexibilizadas, mas não serão extintas em decorrência da pandemia.

A situação mudou e, portanto, a resposta do *compliance* deve mudar também – sempre levando em consideração que as obrigações e necessidade de conformidade não mudaram.

I. O que mudou

De maneira geral, a orientação dos órgãos de saúde com maior impacto para as empresas foi a paralisação dos serviços não essenciais e a orientação que as pessoas ficassem em casa – o que levou as empresas a adotarem o home office. Embora seja uma tendência há muitos anos, o home office ainda não é uma prática disseminada de forma uniforme no ambiente corporativo brasileiro, por diversos motivos.

Mesmo nas empresas que adotavam o home office antes da pandemia, as duas maiores dificuldades tecnológicas foram que nem todos os colaboradores trabalhavam em notebooks e nem todas as empresas tinham a estrutura tecnológica para suportar o acesso aos sistemas centrais por todos colaboradores ao mesmo tempo. Sem contar que o home office não é solução unânime a todas as indústrias.

A crise colocou em evidência a importância de ter um plano de gestão de crise, que pode incluir um Comitê de Crise, um Plano de Contingência / Continuidade de Negócios (define as ações a serem tomadas pela empresa para continuarem atuando num momento de crise, sinistro, perdas); um Plano de Resposta (estabelece os cenários de crise que podem ocorrer -por exemplo pandemia, desastres naturais, interrupção ou roubo de dados, desordem social, etc- e estabelecer as respostas para tais cenários). As empresas que já tinham governança corporativa robusta em voga antes da pandemia economizaram muito tempo após o primeiro baque da pandemia.

A falta de governança corporativa dificultou a retomada de atuação de empresas durante a pandemia, pois tiveram que estabelecer o plano de contingência durante o momento de crise, mas "entre mortos e feridos salvaram-se (quase) todos".

Além da falta de práticas robustas de governança corporativa na realidade empresarial brasileira, uma dificuldade que afetou *compliance officers* globalmente na pandemia foi o não envolvimento do *compliance* na gestão de crise.

Tendo em vista a necessidade de focar os esforços e recursos para manter o negócio funcionando, pode parecer razoável desacelerar as atividades de *compliance* até que a situação melhore. Entretanto, esse tipo de situação crítica é justamente quando a função de *compliance* pode mostrar seu verdadeiro valor, pois as pressões éticas não param durante uma crise de saúde global.

Na verdade, geralmente esses são os momentos em que os valores e a cultura de uma empresa são mais testados. O compromisso da alta e média gerências com o *compliance* durante este período de crise será testado caso, no futuro, a empresa seja investigada por algum ato corrupto.

II. O que é possível fazer agora

Antes de abordar algumas das mitigações de riscos possíveis dentro deste novo contexto social, é importante pensar como o fraudador pensa e como a fraude frequentemente inicia. Cressey criou a teoria do Triangulo de Fraude[1], que são as três dimensões do comportamento de quem

1 MACHADO, Michele Rílany Rodrigues e GARTNER Ivan Ricardo. A hipótese de Cressey (1953) e a investigação da ocorrência de fraudes corporativas: uma análise empírica em instituições bancárias brasileiras. Scielo, 2017. Disponível em: <https://www.scielo.br/scielo.php?pid=S1519-70772018000100060&script=sci_arttext&tlng=pt>. Acesso em: 26, outubro 2020

pratica a fraude e é dividido em três pilares: oportunidade; pressão; e a racionalização.

O primeiro pilar, da oportunidade, ocorre em emergências ou quando os problemas precisam ser solucionados rapidamente e, geralmente traz como consequência a negligência ou flexibilização de controles internos. Este é um risco em potencial facilmente identificado em situações de contratações públicas, por exemplo, quando o procedimento licitatório é flexibilizado – o que ocorreu na pandemia com a Medida Provisória 926/10. Para evitar a concretização desta situação, as empresas que têm relações comerciais com entidades públicas devem avaliar a correta caracterização de situação emergencial, a razoabilidade do preço oferecido, registrar todas as aprovações internas e reuniões com representantes da entidade pública, por exemplo.

O pilar da pressão ocorre em situações de crise, principalmente as que impactem de forma econômica e pessoal o indivíduo, que "forçam" o fraudador a violar regras internas e/ou leis para potencialmente reverter este impacto econômico e pessoal – em outras palavras, aumenta o apetite de risco dos colaboradores. É possível mitigar este aumento do apetite de risco em situações de pressão relembrando os colaboradores dos princípios éticos da empresa, das políticas internas, a forma de contato em caso de dúvida.

A racionalização é a justificação do fraudador de que é preciso violar as regras internas e/ou leis para sobreviver ou então para diminuir a importância de seus atos. Infelizmente, se o colaborador decidir ir em frente com a fraude, não tem treinamento ou monitoramento que irá impedi-lo – as empresas têm pouca influência neste pilar.

Como explicado no pilar da pressão, a comunicação com os colaboradores para lembra-los dos valores, a cultura da empresa e do comportamento que a empresa espera de seus funcionários é muito importante. O *compliance* deve relembrar (mesmo com a distância física do *home office*) do Código de Conduta da empresa, das formas de acessar o canal de denúncia e os pontos mais críticos para o seu negócio. A comunicação constante com a empresa e, principalmente, com a média gerência é fundamental para que todos saibam que o *compliance* continua funcionando de forma remota.

De acordo com o Relatório da ACFE[2], o coronavírus está afetando a habilidade das empresas enfrentarem fraude. Respondentes indicaram que as atividades de prevenção, detecção e investigação de fraudes estão mais difíceis agora em comparação com o período pré-pandemia.

Mas como o *compliance* pode ajudar a solucionar problemas empresariais complexos, dilemas empresariais, que eventualmente surgem em decorrência da situação de crise pandêmica (ou qualquer outra situação difícil, até mesmo pós pandemia)? Existem duas formas: com o uso dos valores ou por regras. Os valores empresariais ajudam para facilitar a tomada de decisão de problemas que não podem ser facilmente previstas (como é o caso da pandemia). Por outro lado, a rigidez das regras internas pode auxiliar se a cultura da empresa for mais voltada a ganhos e oportunidades e os funcionários frequentemente se envolverem em comportamentos de riscos (para bater metas ou para ganhar o bônus do final do ano, por exemplo). As regras, nesse caso, podem ajudar a corrigir o apetite de risco dos funcionários e o *compliance* também pode ajudar lembrando sempre que possível as regras relevantes para os desafios atuais da empresa que já constam no Código de Conduta e políticas internas.

2 Association of Certified Fraud Examiners (ACFE), Fraud in the Wake of COVID-19: Benchmarking Report, September 2020 Edition. Disponível em: < https://www.acfe.com/covidreport.aspx>. Acesso em: 26, outubro 2020

Outra medida importante que deve ser tomada é a reavaliação dos riscos da empresa. A realidade não é mais a mesma, atividades previstas para mitigar possíveis riscos futuros talvez tenham que ser adiadas para dar espaço a ações relacionadas a riscos mais imediatos. Novas prioridades devem ser estabelecidas – como, por exemplo, saúde, segurança, questões de *cyber security*, tributário e questões regulatórias, dentre outros.

Tal reavaliação de riscos não pode deixar de considerar as ações e comportamentos de terceiros. Afinal, nem todas as empresas poderão (ou darão prioridade) à conformidade durante a crise. Mesmo que os terceiros e a sua empresa não tenham a mesma consciência ética (ou a mesma tomada de decisão em situação de crise), é importante lembrar que a sua empresa ainda pode ser responsabilizada por atos dos terceiros, pois a lei não mudou em decorrência da pandemia.

Como explicado, novas prioridades devem ser estabelecidas, entretanto, a crise não pode atrapalhar a visão a longo prazo da empresa e do *compliance*. A prevenção não pode ser abandonada durante a pandemia. As necessidades emergenciais devem ser endereçadas primeiro, por outro lado, as atividades diárias de *compliance* não devem cessar por completo. É um equilíbrio difícil, mas comunicações precisam continuar, funcionários precisam ser treinados, políticas e procedimentos internos devem ser atualizados, dentre outras funções mais rotineiras do *compliance* que não podem parar.

Após a reavaliação dos riscos da empresa será crucial comunicar as novas diretrizes. Quais serão as regras para acesso remoto, quais contratos serão mantidos ou suspensos, quais serão as novas regras para doações, como a comunicação com o cliente será afetada, dentre outros assuntos.

Uma atitude crucial durante crises que não precisa ser encabeçado por *compliance* mas que vale a pena lembrar é a necessidade de anotar nos balanços todos os eventuais prejuízos apurados durante e decorrente da pandemia.

A investigação interna foi uma das atividades de *compliance* mais afetadas durante a pandemia, pois entrevistas e coleta de informações e documentos nem sempre são possíveis remotamente – principalmente se a investigação for muito sensível. Ainda que exista dificuldade, entrevistas podem ser feitas à distância por sistemas online com uso de câmeras e é possível organizar tomando todas as medidas de prevenção à saúde para que alguém da equipe faça a coleta de documentos *in loco*. Afinal, as investigações devem seguir.

De acordo com *Compliance* Survey realizado pela KPMG Brasil[3] realizado com 40 Chief *Compliance* Officers de diversos setores, 22% dos quais afirmaram que as investigações foram uma das atividades mais impactadas na pandemia e 39% dos respondentes afirmam que a capacidade de investigar fraude, corrupção e desvios de conduta foram prejudicadas neste período.

Com relação à proteção de dados, não existe uma resposta certa para solucionar todas as dificuldades que a pandemia trouxe. Na verdade, a proteção de dados pessoais já era desafiadora antes da pandemia, a situação atual só aumentou o nível de dificuldade.

Faz-se necessário agora mais do que nunca o mapeamento dos tipos de dados mantidos pela empresa, entender como eles circulam e quem tem acesso. É preciso documentar tudo e estabelecer regras de acesso e utilização destes dados.

Além disso, existem os riscos relacionados ao *home office*, que muitas vezes são acessados de computadores pessoais, em redes

3 KPMG BRASIL. Covid-19: *Compliance* Survey. Disponível em: <https://home.kpmg/br/pt/home/insights/2020/06/covid-19-*compliance*-survey.html>. Acesso em: 26, outubro 2020

domésticas e dispositivos móveis pessoais, possivelmente deixados sem vigilância ou com sérias falhas de segurança. Tal situação representa consequente aumento de risco de exposição de dados que, combinado com a dificuldade de responder efetivamente a incidentes, podem ter resultados catastróficos para empresas.

Existem tecnologias como criptografias, conexões de rede privada virtual e ferramentas de proteção contra perda de dados que podem ser bastante efetivos se a empresa tem como implantar tais ferramentas de forma rápida e combinado com treinamentos para não criarem novas vulnerabilidades.

Para finalizar, seguem abaixo recomendações gerais que o *compliance* deveria tomar neste momento de pandemia:

- Tome as medidas necessárias para detectar quais processos foram afetados, quais situações de risco tem mais probabilidade de ocorrer e estabeleça um plano de ação para combatê-los;
- Verifique se as políticas e procedimentos da empresa ainda representam a nova realidade, atualize-os se necessário (não esqueça de comunicar e treinar sobre as atualizações!);
- Verifique se a frequência e temas dos treinamentos atendem a nova realidade;
- Reflita em conjunto com a alta administração e o RH se a mudança em algumas funções e responsabilidades suas ou de colegas na empresa seria a solução de alguma dificuldade interna;
- Não suspenda a comunicação, esse é o momento de expandir a presença do *compliance*;
- Considere ser avaliado por terceiros para verificar a efetividade e ética do sistema de *compliance* e/ou do plano de gestão de crise.

III. Conclusão – como será no futuro?

Da mesma forma que a humanidade já superou outras pandemias, esta também passará. E quando isso acontecer o ideal é que as empresas vejam o momento pós pandemia como uma oportunidade para reconsiderar como fazem negócios, incluindo o sistema de *compliance*, que auxiliará a estabelecer uma cultura forte e ética.

A integridade e a governança serão reforçadas no mercado como vantagem competitiva. As empresas que puderem se adaptar ao novo normal serão reconhecidas por terem abordagens baseada em risco e compromisso com a sustentabilidade e ética do negócio. Empresas com sistemas de *compliance* bem projetados e maduros provavelmente assumirão a liderança no mercado. Se tudo der certo, estas empresas ajudarão a implementar a conformidade em toda a cadeia de produção, de tal forma que outras empresas serão estimuladas a terem o mesmo padrão de *compliance*.

O *compliance* (e suas atividades) não poderá ser bem-sucedido sem orquestrar-se em cooperação com diversas áreas da empresa. A situação atual pressiona todos a encontrarem maneiras virtuais e mais eficientes de exercer suas atividades – principalmente quando consideramos que, em caso de alguma investigação, o órgão investigador poderá exigir documentos e explicações relacionadas às atividades que daremos prioridade nesta situação de crise.

A melhor maneira de proteger a empresa em que trabalha, os acionistas e a si mesmo de futuros riscos de conformidade é fazer agora, durante a pandemia, tudo o que for possível para garantir que o *compliance* permaneça ativo, visível e assertivo e que se mantenha desta forma para enfrentar o pós-quarentena.

Programas de Estímulo ao *Compliance* Tributário e Benefícios Empresariais

RAFAEL SGODA TOMAZETI

Advogado, sócio da Moreno Moro Advogados. Bacharel em Direito pelo UniBrasil, tendo sido laureado com o título de melhor aluno do Curso de Direito. Especialista em *Compliance* e Integridade Corporativa pela PUC Minas. Membro da Comissão de *Compliance* e Governança Corporativa (Curitiba/PR) da ABA – Associação Brasileira de Advogados. Membro do Comitê Público da Associação Nacional dos Profissionais de Privacidade de Dados. Membro da Comissão de Inovação e Gestão da OAB Paraná. Possui formação em propriedade intelectual pela WIPO e em proteção de dados pelo ITS Rio.

RHAIZA DE SOUZA

Graduada em Direito pelo UniBrasil – Centro Universitário Autônomo do Brasil (antiga FACBRASIL – Faculdades Integradas do Brasil). Pós-graduanda em Advocacia Empresarial pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas). Tem experiência profissional nas áreas de direito civil e empresarial (consultiva e contenciosa) e controladoria jurídica. Atualmente é advogada cível/corporativa no escritório De Paola & Panasolo Sociedade de Advogados.

ANA CAROLINE FERREIRA

Advogada associada na Domingues Sociedade de Advogados. Graduada em Direito pelo UniBrasil – Centro Universitário Autônomo do Brasil. Pós-graduanda em Direito Tributário e Processo Tributário pelo Instituto Brasileiro de Estudos Tributários – IBET. Atuação no consultivo tributário. É pesquisadora no grupo de estudos de Direito Tributário da Escola de Direito da PUCPR (Taxpuc).

1. Introdução

Muito discutida no debate de efetivação de políticas públicas para cumprimento de direitos sociais, a escassez dos recursos públicos também desafia o Poder Público no exercício de atividades de fiscalização.[1]

Com efeito, a complexidade da sociedade contemporânea, com seus velozes avanços tecnológicos e inovações em produtos, serviços, projetos e outras iniciativas, não apenas dificulta trabalho do legislador em acompanhar os avanços sociais[2], como também desafia a capacidade estatal de fiscalizar os jurisdicionados ante a limitação dos recursos públicos.

Reflexo direto desse cenário, são as legislações contemporâneas, que tendem a imputar aos seus destinatários uma maior responsabilidade, com o estabelecimento de cada vez mais elevadas sanções pelo seu descumprimento.

Exemplificativamente, a Lei Anticorrupção brasileira (Lei nº 12.846/13) traz como uma das principais inovações no ordenamento jurídico pátrio a imputação de responsabilidade objetiva (ou seja, independentemente de comprovação de culpa) às pessoas jurídicas pela prática de atos lesivos à Administração Pública (art. 1º).

Do mesmo modo, mais recentemente, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18), que tutela o tratamento de informações relativas às pessoas naturais identificadas ou identificáveis, prevê a possibilidade de inversão do ônus da prova em favor do titular (art. 42, §2º), de modo que caberá aos agentes de tratamento comprovar que as operações por si realizadas cumprem as determinações legais.

Outra característica marcante dessas legislações contemporâneas, é o fomento para que o próprio jurisdicionado passe a se fiscalizar, comprometendo-se com uma cultura de conformidade legal.

Enquanto a Lei Anticorrupção brasileira fomenta que as organizações implementem e mantenham um programa de integridade (*compliance* anticorrupção) (art. 7º, inc. VIII), com o objetivo prevenir, detectar e remediar os atos proibidos pela legislação[3], a Lei Geral de Proteção de Dados Pessoais estimula a adoção de um programa de governança em privacidade (*compliance* em proteção de dados pessoais), que contemplem políticas e outras ferramentas para gerenciar riscos de proteção de dados pessoais (art. 50, §2º, inc. I).

Em ambos os casos, a existência efetiva desses programas poderá ser utilizada para abrandar as penas legais, servindo como prova da boa-fé do infrator.[4]

Especificamente na área tributária e em que pese os avanços tecnológicos dos últimos anos, o complexo sistema tributário nacional ainda desafia o Fisco no exercício

1 Veja-se: Não apenas a efetivação de direitos sociais demanda recursos públicos. Em verdade, qualquer poder-dever estatal exige recursos, inclusive para efetivação de direitos de liberdade negativa, pois mesmos nesses casos há atuações estatais, exemplificativamente, com a manutenção de instituições governamentais. HOLMES, Stephen; SUNSTEIN, Cass R.; The cost of rights: Why liberty depends on taxes. Nova Iorque; Londres: W. W. Norton & Company, 1948, p. 29.

2 Desde o direito romano, fixou-se o brocardo ex factor oritur jus (o direito nasce do fato), no entanto, contemporaneamente, há uma capacidade menor da legislação acompanhar a realidade social, considerando que as transformações acontecem cada vez mais rápido. PECK, Patricia. Quando a sociedade muda, o Direito também deve mudar. Conjur, 2002. Disponível em: <https://www.conjur.com.br/2002-nov-28/quando_sociedade_muda_direito_tambem_mudar>. Acesso em: 05 set. 2020.

3 CONTROLADORIA-GERAL DA UNIÃO. Programa de integridade: Diretrizes para empresas privadas. Disponível em: <https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf>. Data de acesso: 05 set. 2020.

4 Em relação ao descumprimento da LGPD, a professora Patricia Peck PINHEIRO destaca: "um programa de gestão de dados pessoais bem implementado pode ajudar na redução das penas, na hipótese de ocorrência de um tipo de infração que enseje a aplicação de alguma penalidade". PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020, p. 37-38.

do poder de polícia e na identificação e repreensão de atos ilícitos.

Ilustrativamente, a instituição do Sistema Público de Escrituração Digital (Sped) pelo Decreto nº 6.022/07 representou um grande avanço às administrações fazendárias, permitindo o compartilhamento de informações contábeis e fiscais dos contribuintes e facilitando as atividades de fiscalização, mas o novo sistema não elimina riscos de sonegação fiscal e outros ilícitos tributários.

Não por outra razão, há mais de dez anos a Receita Federal adota planos anuais de fiscalização, que, dentre outros objetivos, visam promover a conformidade tributária e garantir a arrecadação necessária ao funcionamento da máquina estatal, estabelecendo focos de atuação de acordo com os recursos (humanos, tecnológicos, financeiro e outros) disponíveis.[5]

A busca por uma maior eficiência na fiscalização das obrigações tributárias e na criação de uma cultura de *compliance*[6] tributário também tem ganhado atenção com uma iniciativa mais atual: a instituição de programas estatais de estímulo à conformidade tributária, em que o Fisco passa a recompensar os contribuintes com maior índice de adimplência das obrigações legais, sejam elas principais ou acessórias.

Como melhor detalhado a seguir, no Estado de São Paulo, a Lei Complementar nº 1.320/18, instituiu o "Programa de Estímulo à Conformidade Tributária 'Nos Conformes'", que classifica contribuintes de ICMS (Imposto sobre Operações Relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual e Intermunicipal e de Comunicação) de acordo com o cumprimento das obrigações pecuniárias, a aderência de sua escrituração com os documentos fiscais emitidos ou recebidos e o perfil de seus fornecedores.

A depender da classificação atribuída, o contribuinte passa a ter direito a "contrapartidas" do Fisco. Exemplificativamente, na categoria de maior nível de *compliance* tributário ("A+"), o contribuinte tem acesso a procedimento de análise fiscal prévia, antes da lavratura de auto de infração e imposição de multa, e renovação por procedimentos simplificados de regimes especiais de tributação – benefícios não previstos a todos os contribuintes.

De maneira similar, a Lei nº 17.087/19 do Estado do Ceará instituiu o "Programa de Conformidade Tributária Contribuinte Pai D'Égua", ainda pendente de regulamentação, que também classificará os contribuintes estaduais "de acordo com condições e critérios objetivos avaliativos e níveis de conformidade tributária" (art. 3º) assegurando contraprestações àqueles com maior grau de *compliance* tributário.

Não obstante as iniciativas estaduais, a Receita Federal também estuda a possibilidade de criação de um programa de fomento ao *compliance* tributário.

A Consulta Pública RFB nº 04/2018[7], já encerrada, submeteu à avaliação popular minuta de portaria a ser publicada pelo Fisco federal que objetiva instituir o "Programa de Estímulo à Conformidade Tributária Pró-Conformidade".

---

5 Por exemplo, o plano de ação de 2020 da Receita Federal prevê uma atuação especial na fiscalização de planejamentos tributários vinculados a eventos de reorganização societária com geração de ativos amortizáveis e em evasões nos setores de cigarros, bebidas e combustíveis. RECEITA FEDERAL DO BRASIL. Relatório anual de fiscalização: Resultados de 2019 e plano de ação para 2020. Disponível em: <https://receita.economia.gov.br/dados/resultados/fiscalizacao/arquivos-e-imagens/plano-anual-de-fiscalizacao-resultados-de-2019-e-plano-para-2020.pdf/view>. Data de acesso: 29 ago. 2020.

6 O termo "*compliance*" aqui empregado remete à ideia de conformidade, de cumprimento de um comando, de uma determinação legal. CRUZ, Marco. Fazendo certo a coisa certa: Como criar, implementar e monitorar programas de efetivos de *compliance*. S.l.: Simplíssimo, 2017. n. p.

7 RECEITA FEDERAL DO BRASIL. Consulta Pública RFB nº 04/2018. Disponível em: <https://receita.economia.gov.br/sobre/consultas-publicas-e-editoriais/consulta-publica/arquivos-e-imagens/consulta-publica-rfb-no-04-2018.pdf>. Data de acesso: 03 set. 2020.

2. O pioneiro programa de *compliance* tributário do Estado de São Paulo

Nesta esteira de evolução de políticas que incentivem o contribuinte a fiscalizar-se no cumprimento de suas obrigações tributárias, o Estado de São Paulo foi o precursor no Brasil ao publicar a Lei Complementar nº 1.320, de 06/04/2018, por meio da qual foi instituído o "Programa de Estímulo à Conformidade Tributária 'Nos Conformes'", que tem como principal objetivo criar um ambiente de confiança mútua e boa-fé entre os contribuintes e a Administração Tributária.

Trilhando o Princípio da Isonomia, consagrado no artigo 5º da Constituição Federal, o programa "Nos Conformes" apresenta critérios para classificar os contribuintes de ICMS (Imposto sobre Operações Relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual e Intermunicipal e de Comunicação) de acordo com as suas obrigações tributárias, ranqueando-os entre "A+", "A", "B", "C", "D" e "E", bem como "NC" (Não Classificados).

As classificações são traçadas utilizando-se dos seguintes pilares: obrigações vencidas e não pagas (artigo 7º); aderência (artigo 8º); e, perfil dos fornecedores do contribuinte (artigo 9º). Com ressalva ao último critério aqui citado, os demais estão regulamentados através do Decreto nº 64.453, de 06/09/2019, o qual apresenta diretrizes para a classificação dos contribuintes.

O critério das obrigações vencidas e não pagas, previsto no artigo 7º da Lei Estadual Complementar, observa o tempo de atraso de pagamento da obrigação pecuniária, sendo que os classificados na categoria "A+", não poderão ter obrigações vencidas há mais de 02 (dois) meses. Por sua vez, os classificados na categoria "D", piores ranqueados, são aqueles com obrigações vencidas há mais de 06 (seis) meses.

O pilar da aderência, previsto no artigo 8º da Lei Complementar nº 1.320 de 06/04/2018, tem como intuito averiguar se os valores indicados nos documentos fiscais emitidos e lançados pelo contribuinte estão de acordo com aqueles constantes na declaração na escrituração contábil, sendo que o contribuinte melhor classificado ("A+") é aquele que possui 98% (noventa e oito por cento) de concordância entre as declarações, e o menor classificado (categoria "D") é aquele com menos de 90% (noventa por cento) de adesividade.

Por fim, o juízo mais polêmico da lei, disciplinado no artigo 9º, diz respeito ao perfil dos fornecedores do contribuinte, porquanto este critério é traçado a partir da análise de terceiros e não do próprio contribuinte.

Os contribuintes mais bem classificados (categoria "A+") são aqueles com, no mínimo, 70% (setenta por cento) de suas entradas provenientes de fornecedores classificados nas categorias "A+" ou "A". Por sua vez, os contribuintes com menos pontuação (categoria "D") são aqueles com receita inferior a 40% (quarenta por cento) provenientes de fornecedores classificados nas categorias "A+", "A" ou "B", ou com receita maior de 30% (trinta por cento) proveniente de fornecedores da categoria "D".

Mas e como ficam os contribuintes com boa parte dos fornecedores de outros estados? É por este motivo que este critério não está regulamentado pelo Decreto nº 64.453/2019 e, consequentemente, ainda não sendo aplicado.

Uma vez traçadas as diretrizes e determinada a classificação dos contribuintes, a lei, por óbvio, estabelece os incentivos/benefícios que cada categoria poderá usufruir.

Aqueles classificados na categoria "A+" gozarão, em especial, da faculdade de transferência de crédito não acumulado para empresa não interdependente.

Por sua vez, os contribuintes das categorias "A+", "A" e "B" usufruirão da (i) autorização para pagamento do ICMS relativo à importação de mercadoria oriunda do exterior, mediante compensação em conta gráfica (artigo 16, inciso I, alínea "e", inciso II, alínea "e" e inciso III, alínea "b"); e; (ii) inscrição de novos estabelecimentos do mesmo titular no cadastro de contribuintes de que trata o artigo 16 da Lei nº 6.374, de 1º de março de 1989, observando-se procedimentos simplificados, na forma e condições estabelecidas em regulamento (artigo 16, inciso I, alínea "g", inciso II, alínea "g" e inciso III, alínea "c").

Além dos incentivos elencados acima, os contribuintes classificados nas categorias "A+" e "A" usufruirão das seguintes contrapartidas: (i) acesso ao procedimento de Análise Prévia, consistente na faculdade de, antes da lavratura do Auto de Infração, sanar irregularidades apontadas pelo Auditor Fiscal; (ii) autorização para apropriação e transferência de crédito acumulado; (iii) efetivação da restituição de ICMS/ST pagos antecipadamente em razão da substituição tributária, valendo-se de procedimentos simplificados; (iv) autorização para pagamento do ICMS relativo à substituição tributária de mercadoria oriunda de outra unidade federada, cujo valor do imposto não tenha sido anteriormente retido, mediante compensação em conta gráfica, ou recolhimento por guia especial até o dia 15 do mês subsequente (artigo 16, inciso I, alínea "d" E inciso II, alínea "d") e; (v) renovação de regimes especiais concedidos com fundamento no artigo 71 da Lei nº 6.374, de 1º de março de 1989, observando-se procedimentos simplificados, na forma e condições estabelecidas em regulamento (artigo 16, inciso I, alínea "f" e inciso II, alínea "f").

Diferente dos contribuintes classificados no *ranking* "A+" e "A", os contribuintes da categoria B gozarão da autorização de apropriação de apenas 50% (cinquenta por cento) do crédito acumulado.

Por fim, os contribuintes relacionados na categoria "C" somente desfrutarão da possibilidade de inscrição de novos estabelecimentos do mesmo titular no cadastro de contribuintes de que trata o artigo 16 da Lei nº 6.374, de 1º de março de 1989 (artigo 16, inciso IV).

Os demais contribuintes, classificados nas categorias "D", "E" e "NC" (Não Classificado) não fruirão de nenhum benefício da lei. No entanto, vale lembrar que a Lei Complementar prevê a revisão periódica da classificação, de modo que, nada impede que o contribuinte suba de posição no *ranking* e usufrua dos incentivos legais.

Embora o programa "Nos Conformes" tenha sido implementado recentemente, os resultados iniciais são bastante promissores. Citam-se como exemplos, o expressivo número de contribuintes orientados em relação a pendências fiscais, maior engajamento dos Auditores Fiscais e, em especial, o aumento de mais de R$ 3 milhões no total do caixa gerado, sem que tenha ocorrido aumento na carga tributária[8].

3. Benefícios empresariais para além das contraprestações legais

É cediço que a legislação tributária atual no Brasil impõe às empresas diariamente desafios quanto à análise da atividade tributária de suas operações, uma vez que o volume de tributos e obrigações acessórias exigidos dos contribuintes no país é muito elevado[9]. Mesmo assim, toda empresa pre-

8 SECRETARIA DA FAZENDA E PLANEJAMENTO DO ESTADO DE SÃO PAULO. Relatório do Programa "Nos Conformes". Disponível em: https://portal.fazenda.sp.gov.br/servicos/nosconformes/Paginas/Resultados-Programa.aspx>. Data de acesso: 14 set. 2020.

9 Um estudo do Instituto Brasileiro de Planejamento e Tributação (IBPT) aponta que, em 2017, cada empresa gastou, em média, 1958 (um mil, novecentos e cinquenta e oito) horas para cumprimento das obrigações

cisa estudar, escolher um regime tributário mais adequado aos seus negócios, de modo a cumprir todas as obrigações legais de recolher e administrar seus tributos tempestivamente, preservando sua capacidade empresarial.

Nesse ponto que se observa a importância da implementação dos programas de estimulo à conformidade tributária, patrocinados pelas Secretarias das Fazendas dos Estados, cujo o objetivo nada mais é que harmonizar a relação dos contribuintes com o Fisco, reduzindo o número de autuações que levam a diversos processos administrativos fiscais, bem como valorizando os contribuintes que cumprem com a legislação tributária.

Além dos diversos benefícios que todos esses programas de incentivo a autorregulação fornecem aos contribuintes, como visto na análise da legislação paulista, existem outros benefícios com a implementação adequada do *compliance* tributário nas empresas, como por exemplo, redução de custos e levantamento das contingências tributárias.

O *compliance* tributário faz com que o empresário obtenha controle total de todos os processos do departamento fiscal de seu negócio, possibilitando a identificação das contingências tributárias da empresa (identificação de passivos ocultos, análise de riscos de autuação fiscal e estimar a razoabilidade de quitações de passivos).

Além da organização do departamento fiscal da empresa, os proveitos proporcionados pelo *compliance* também alcançam o cumprimento regular das obrigações acessórias (SPED Fiscal, EFD Contribuições, EFD ICMS, ECF, etc.), pois com todas as obrigações transmitidas da maneira correta e no prazo, a empresa passa a diminuir a incidência de multas e juros, bem como não corre o risco de ficar sem certidão negativa de débitos (CND).

Portanto, a conformidade tributária traz inúmeros benefícios aos contribuintes, posto que se trata de um trabalho preventivo, focado na implementação das melhores práticas na gestão fiscal de uma corporação, utilizando-se de ferramentas que garantirão aos empresários maior segurança jurídica tributária em suas operações. Além disso, auxilia na implementação de um planejamento tributário adequado, evitando sempre que a empresa responda por eventuais autuações.

4. Conclusões

Os programas de estímulo à conformidade tributária, capitaneado no Brasil pelo Estado de São Paulo, seguem o movimento contemporâneo de reconhecer a limitação dos recursos públicos, a impossibilidade de fiscalização detalhada de todos os jurisdicionados e de transferência ao particular do dever de fiscalização.

A autofiscalização já é conhecida pelos estudiosos de *compliance*. Com efeito, sistemas corporativos de gestão em *compliance* têm entre suas premissas a necessidade de autofiscalização, levantando pontos de alerta e identificando desvios de conduta. Esse dever é ainda maior quando a legislação passa a transferir maiores responsabilidades aos jurisdicionados – como ocorre na Lei Anticorrupção brasileira (Lei nº 13.846/13) e na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18).

No campo tributário, a ideia de autofiscalização também não é anômala. As altas sanções pelo descumprimento de obrigações legais e os avanços no sistema de

tributárias. ALVARENGA, Darlan. Empresas gastam 1.958 horas e R$ 60 bilhões por ano para vencer burocracia tributária, apontam pesquisas. G1. Disponível em: < https://g1.globo.com/economia/noticia/empresas-gastam-1958-horas-e-r-60-bilhoes-por-ano-para-vencer-burocracia-tributaria-apontam-pesquisas.ghtml>. Data de acesso: 14 set. 2020.

fiscalização, principalmente com a adoção de novas tecnologias pelo Fisco, também impõem um maior cuidado do contribuinte.

Nesta conjuntura, os programas de estímulo ao *compliance* tributário parecem conjugar com a realidade posta, incentivando a adoção de uma cultura de conformidade legal.

Independentemente dos benefícios previstos na Lei Complementar nº 1.320/18 do Estado de São Paulo e daqueles que serão instituídos em programas análogos, alhures apresentados, um alto nível de *compliance* tributário é capaz de trazer inúmeros outros benefícios às organizações. Em outras palavras, para além da submissão a procedimentos especiais de fiscalização ou facilitação para obtenção de incentivos fiscais, o *compliance* tributário proporciona uma maior governança tributária, facilitando o controle das obrigações a serem cumpridas, a emissão de relatórios, a identificação de desvios/incorreções e a estruturação de planejamentos tributários.

Veja-se que os benefícios do *compliance* tributário são inegavelmente tangíveis e, uma vez enraizado na área contábil/fiscal, é capaz de fazer com que essa cultura de agir de acordo com as regras irradie para as demais áreas da organização e, com sorte, para toda a sociedade.

Referências bibliográficas

ALVARENGA, Darlan. Empresas gastam 1.958 horas e R$ 60 bilhões por ano para vencer burocracia tributária, apontam pesquisas. **G1**. Disponível em: < https://g1.globo.com/economia/noticia/empresas-gastam-1958-horas-e-r-60-bilhoes-por-ano-para-vencer-burocracia-tributaria-apontam-pesquisas.ghtml>. Data de acesso: 14 set. 2020.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União**. Brasília, 05 out. 1998.

_____. Decreto nº 6.022, de 22 de janeiro de 2007. Institui o Sistema Público de Escrituração Digital – Sped. **Diário Oficial da União**. Brasília, 22 jan. 2007.

_____. Lei nº 12.846, de 01º 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. **Diário Oficial da União**. Brasília, 02 ago. 2013.

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**. Brasília, 15 ago. 2018.

CONTROLADORIA-GERAL DA UNIÃO. **Programa de integridade**: Diretrizes para empresas privadas. Disponível em: <https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf>. Data de acesso: 05 set. 2020.

CRUZ, Marco. **Fazendo certo a coisa certa**: Como criar, implementar e monitorar programas de efetivos de *compliance*. S.l.: Simplíssimo, 2017.

ESTADO DE SÃO PAULO. Decreto nº 64.453, de 06 de setembro de 2019. Regulamenta a classificação de contribuintes do Imposto sobre Operações Relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual e Intermunicipal e de Comunicação – ICMS – prevista na Lei Complementar nº 1.320, de 06-04-2018, que institui o Programa de Estímulo à Conformidade Tributária – "Nos Conformes". **Diário Oficial do Estado**. São Paulo, 07 set. 2018.

_____. Lei Complementar nº 1.320, de 06 de abril de 2018. Institui o Programa de Estímulo à Conformidade Tributária – "Nos Conformes", define princípios para o relacionamento entre os contribuintes e o Estado de São Paulo e estabelece regras de conformidade tributária. **Diário Oficial do Estado**. São Paulo, 07 abr. 2018.

ESTADO DO CEARÁ. Lei nº 17.087, de 29 de outubro de 2019. Institui o Programa de Conformidade Tributária denominado Contribuinte Pai D'Égua no âmbito da administração tributária do Estado do Ceará. **Diário Oficial do Estado**. Fortaleza, 29 out. 2019.

HOLMES, Stephen; SUNSTEIN, Cass R.; **The cost of rights**: Why liberty depends on taxes. Nova Iorque; Londres: W. W. Norton & Company, 1948, p. 29.

PECK, Patricia. Quando a sociedade muda, o Direito também deve mudar. **Conjur**, 2002. Disponível em: <https://www.conjur.com.br/2002-nov-28/quando_sociedade_muda_direito_tambem_mudar>. Acesso em: 05 set. 2020.

PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020

RECEITA FEDERAL DO BRASIL. **Consulta Pública RFB nº 04/2018**. Disponível em: <https://receita.economia.gov.br/sobre/consultas-publicas-e-editoriais/consulta-publica/arquivos-e-imagens/consulta-publica-rfb-no-04-2018.pdf>. Data de acesso: 03 set. 2020.

_____. **Relatório anual de fiscalização**: Resultados de 2019 e plano de ação para 2020. Disponível em: <https://receita.economia.gov.br/dados/resultados/fiscalizacao/arquivos-e-imagens/plano-anual-de-fiscalizacao-resultados-de-2019-e-plano-para-2020.pdf/view>. Data de acesso: 29 ago. 2020.

SECRETARIA DA FAZENDA E PLANEJAMENTO DO ESTADO DE SÃO PAULO. **Relatório do Programa "Nos Conformes"**. Disponível em: https://portal.fazenda.sp.gov.br/servicos/nosconformes/Paginas/Resultados-Programa.aspx>. Data de acesso: 14 set. 2020.

Comunicação Interna como Instrumento de Efetividade dos Programas de *Compliance*

ISABELLA ZAMPINI VENEROSO

Advogada. Graduada em Direito pela Universidade Presbiteriana Mackenzie. Pós-Graduanda em *Compliance* pela Universidade Presbiteriana Mackenzie. Analista de *Compliance* em empresa do setor Alimentício. Atua na elaboração e monitoramento de Programa de *Compliance*, com a estruturação de matriz de risco, produção e gestão de políticas internas, elaboração e desenvolvimento de plano de comunicação, acompanhamento de canal de denúncias, treinamentos e due diligence de terceiros. Possuí experiência, também, em investigações corporativas de grande porte.

1. Introdução

Nos últimos anos os Programas de *Compliance* têm se tornado elemento cada vez mais atuante e necessário dentro das organizações, tanto públicas quanto privadas e, como consequência, muito se fala na imprescindibilidade da manutenção de controles internos atuais e precisos para o equilíbrio e mitigação de riscos de uma grande companhia.

A análise clara e contemporânea dos riscos aos quais a atividade de uma companhia está exposta, bem como a estruturação de mecanismos e processos para sua mitigação realmente fazem parte de um Programa de *Compliance* bem-sucedido e exitoso.

Porém, não são raros os casos em que o discurso da companhia e Alta Administração não está alinhado com a cultura e práticas de seus colaboradores por falha na comunicação interna da empresa e consequente falta de alcance da mensagem a ser transmitida aos demais colaboradores da companhia, tornando a prática de atos fraudulentos e corruptos mais comum e suscetível.

Por essa razão o presente artigo busca explorar a relevância da estruturação de um canal de comunicação interna nas organizações e compreender seu

respectivo papel para promoção da eficácia dos Programas de Integridade dentro da cadeia de valor de cada negócio, não apenas auxiliando no combate à prática de atos corruptos e fraudulentos mas também assegurando a manutenção de uma cultura corporativa proba e íntegra.

2. Programas de *Compliance*

Após o advento do chamado *Foreign Corrupt Practices Act* (FCPA), lei norte americana promulgada em 1977 que busca o combate à corrupção internacional, os programas de integridade passaram a ser instrumento cada vez mais presente na cadeia de negócios das empresas ao redor do mundo.

Mais especificamente no Brasil, a adesão aos Programas de Integridade começou a ser tornar mais frequente após a promulgação da Lei Anticorrupção nº12.846/13 e do Decreto nº 8.420/2015 que regulamenta a lei, ambos responsáveis por apontar a necessidade e urgência da implementação de programas de *compliance* suficientemente capazes de prevenir a prática de atos fraudulentos contra a administração pública por meio da implementação de uma série de controles internos nas organizações.

Nesse contexto os programas de *compliance* vêm passando por uma evolução e aprimoramento contínuos, ao passo em que os elementos para sua efetividade vêm sendo constantemente debatidos tendo em vista a observância de uma série de programas de integridade de "fachada" que foram expostos pelos sérios casos de corrupção que tomaram a atenção da mídia nos últimos anos.

A eficácia dos programas de integridade passa a ser o ponto fulcral para uma análise clara de sua aplicação e é o fator determinante para que leis como FCPA e a Lei Anticorrupção possam considerar o programa como elemento suficientemente capaz de prevenir atos ilícitos e, assim, ser considerado para abatimento de eventuais multas e penalidades.

Nesse tocante, alguns pilares têm sido identificados como essenciais para garantia da eficácia de um programa de *compliance* pela doutrina moderna, sendo eles: i. Compromisso da Alta Administração; ii. Avaliação de Riscos; iii. Políticas de *Compliance*; iv. Controles Internos; v. Treinamento e Comunicação; vi. Canal de Denúncias; vii. Investigações Internas; viii. *Due Diligence* de Terceiros; e ix. Monitoramento.

Todos esses elementos reunidos são a base para um programa de integridade de sucesso, não sendo estes, no entanto, elementos exaustivos, mas sim parâmetros e diretrizes gerais que devem ser adaptadas à cadeia de valor de cada modelo de negócio.

Mesmo estes conceitos sendo amplamente defendidos no âmbito teórico, não é incomum que ao observar os Programas de *Compliance* de grandes organizações, o pilar referente à Comunicação Interna tende a ser subestimado e passa desapercebido em relação aos demais requisitos basilares para o sucesso da prevenção de fraudes corporativas.

A Comunicação Interna, elemento extremamente relevante para o fomento da cultura de integridade entre os colaboradores de uma companhia, não costuma ter a visibilidade e atenção necessária dos Programas de Integridade o que, por muitas vezes, afasta a discussão do tema e cria barreiras instransponíveis para um diálogo aberto que sustente a cultura da ética e integridade das organizações entre seus colaboradores.

3. Eficácia da Comunicação Interna

A comunicação interna de uma organização é a principal responsável pela externalização das diretrizes e valores do negócio e, por isso, deve alcançar a todos os colaboradores sem distinção.

Os Programas de Integridade não devem ser exceção a isto, uma vez que é por meio dos canais de comunicação da companhia que o *compliance* passa a fazer parte da cultura da empresa, transmitindo, por meio de suas comunicações, os objetivos, regras, postura esperada, bem como a clara adesão da alta administração e suporte da diretoria executiva para todos os seus colaboradores.

Infelizmente casos em que a comunicação interna não se adequa para transmissão da mensagem com seu público alvo são comuns queixas com relação ao uso recorrente de termos técnicos, extensão demasiada de textos, comunicações repetitivas e cansativas vêm afastando o interesse do telespectador para temas relacionados ao *compliance* e minando a relação do mesmo com a área.

A comunicação interna desempenha papel fundamental na criação de identidade e imagem do Programa de Integridade, sendo responsável por desenvolver recursos lúdicos e objetivos suficientes para que todas as mensagens vinculadas ao campo da ética e integridade sejam efetivamente transmitidas e tenham adesão do público, se tornando verdadeira guardiã da reputação organizacional do negócio[1].

A aceitação positiva e criação de uma cultura de importância e relevância de conteúdo relativo ao *compliance*, tornando aspecto legais e formais em um tema de fácil aceitação não pode ou deve ser aquém à comunicação de uma corporação, sendo seu dever manter o tema perene através do tempo, fomentar o número de adeptos e incentivar os colaboradores a praticarem e respeitarem as diretrizes de integridade da companhia.

Os colaboradores que devem ser atingidos pela comunicação, no entanto, raramente são compostos por um público homogêneo. Por essa razão, é necessário que, além do cuidado com a identidade visual, linguagem coerente e meios para transmissão da mensagem, a comunicação se preocupe com o público alvo das mensagens transmitidas.

Esse é o grande desafio da comunicação interna: encontrar o mecanismo ideal para que as mensagens alcancem de forma igualitária todos os públicos, desde público administrativo até o público operacional, se esse for o caso, entendendo que há limitações nos dois campos de atuação, que devem ser superadas com esforço e criatividade.

3.1 Plano de Comunicação Estratégico

Para a promoção do conhecimento das normas aplicáveis às atividades desempenhadas no ambiente corporativo, bem como a conduta esperada de cada colaborador, é fundamental a definição de estratégia do plano de comunicação da companhia. Com isso é possível identificar o público alvo que será abrangido, bem como fundamentar a abordagem, frequência e temática da comunicação.

Por isso a elaboração de um plano de comunicação especificamente voltado para fomentar a adoção de postura ética e a inclusão de um profissional responsável pela área de integridade nas discussões do planejamento anual de capacitação da empresa são essenciais, assim como compreender a dinâmica da empresa para ações de comunicação e harmonizar com o plano corporativo, definindo ações que tragam resultados de conhecimento e de informação reais.

1 KUNSCH; PARAVENTI, 2016, p.116

Além disso, o orçamento destinado a uma comunicação coordenada e programada também é fator decisivo para o sucesso dessas comunicações.

Como já mencionado no presente artigo, a Alta Administração da organização desempenha um papel fundamental para a efetividade de um Programa de Integridade. Isso significa que a Alta Administração não deve apenas compreender e fomentar a importância dos Programas de Integridade, mas também disponibilizar os recursos necessários para que a cultura seja disseminada a todos os funcionários. Isso envolve a previsão de um orçamento específico para que área de *Compliance* seja capaz de estruturar um canal de comunicação capaz de alcançar os diversos públicos com que se comunica, assim como fomentar a cultura de integridade por meio de ações especificas, produção de materiais como calendários, folders, adesivos corporativos, eventos da área, divulgação de políticas e normas internas, mailing personalizado, treinamentos customizados, entre tantos outros artifícios necessários para prenderem a atenção do público alvo e transmitirem a mensagem desejada.

Outro ponto que deve constar no planejamento estratégico da comunicação dos Programas de *Compliance* é trazer atenção à linguagem que está sendo utilizada para cada discurso. A escolha por uma linguagem clara, sem artifícios jurídicos ou técnicos, inserindo as situações no contexto cotidiano de cada um com exemplos práticos oferece leveza às comunicações e permitem que as mesmas tenham grande aderência dos leitores.

Para que um Programa de *Compliance* seja eficaz, ele deve ser aderido por todos os seus colaboradores sendo o grande desafio do profissional do *Compliance* sair da rigidez técnica inerente à área, inovando em meios de comunicações que possibilitem a transmissão de mensagens claras e coesas que cativem seus funcionários à prática de atitudes éticas que preservem a imagem e reputação da Companhia.

O tamanho dos comunicados e normativos também deve ser levado em consideração. A objetividade deve ser preservada para que os documentos e mensagens não sejam extensos e sejam de fácil leitura, sempre com a utilização de ferramentas visuais que chamam a atenção do leitor e despertem sua curiosidade, como imagens, ilustrações e cores cativantes.

O objetivo dos comunicados é fazer com que temas antes vistos como burocráticos e densos despertem o interesse do leitor para que este passe a se interessar pelo assunto e entenda a relevância daquelas mensagens, aplicando-as em seu dia-a-dia e gravando-a na memória.

Ou seja, com o alinhamento da área de *Compliance* com as comunicações internas busca-se a harmonização e aproximação de todos os colaboradores com as políticas e diretrizes da Companhia, fazendo com que mensagens claras e precisas sejam transmitidas e, assim, gerando maior engajamento e comprometimento do público alvo com práticas íntegras, atitudes éticas e afastando a possibilidade da prática de fraudes corporativas

Por essa razão, a utilização de recursos visuais é muito bem-vinda, bem como a criação de um canal próprio e personagens que facilitam a interação da área com o público alvo, fugindo da linguagem convencional e estrutura rígida comumente adotada pelo mundo corporativo.

3.2 Mecanismos de Monitoramento

Diante da necessidade de atendimento e atenção à tantos requisitos para que haja a efetiva e clara transmissão da mensagem e fomento da cultura ética pretendida pelo Programa de Integridade, a aderência desse plano de comunicação deve ser monitorada pelos agentes responsáveis por sua transmissão, permitindo uma avaliação correta do que está sendo absorvido pelo público alvo ou não.

Para que seja verificada a eficiência do plano de comunicação interna do Programa de *Compliance* é essencial que o alcance das comunicações não apenas seja rastreado, mas que haja previsão de uma segunda via de troca dessa informação, na qual a empresa seja capaz de captar as informações dos colaboradores por meio de *feed backs*, pesquisas e formulários.

Além disso o monitoramento de acesso às plataformas vinculadas nos comunicados, assim como número de visualização de publicações, políticas e documento internos são meios pelos quais o acompanhamento se torna cada vez mais fidedigno e permite o ajuste do plano de comunicação de acordo com a aderência do público.

Outra ferramenta que em muito auxilia esse monitoramento é o canal de denúncias, responsável pelo recebimento de reportes de colaboradores ou terceiros que prestam serviços para a organização acerca das práticas de atos que contrariam as diretrizes da companhia. Por meio do monitoramento deste veículo, é possível verificar se a comunicação está sendo realmente efetiva, o que implica no aumento da utilização do mesmo e, consequentemente maior do número de reportes, ou não, tornando o canal obsoleto e infrutífero.

4. Conclusão

A Comunicação Interna assume um papel fundamental quando se trata da disseminação da cultura da integridade inerente aos Programas de *Compliance*, sendo parte imprescindível dentro da estrutura de *Compliance*.

A corrupção é um tema difícil de ser abordado e causa uma certa desconfiança por parte dos colaboradores, motivo pelo qual a comunicação precisa não apenas atingir pessoas, mas sensibilizá-las e envolvê-las na cultura ética da organização, alinhando o discurso da alta direção e seus objetivos com todos os colaboradores envolvidos em todas as etapas da cadeia de produção.

Afirmar que a Comunicação Interna é capaz de eliminar a corrupção das organizações é temerário. No entanto, ela ganha contornos relevantes quando alinhada ao Programa de Integridade e pode ser responsável pela promoção de uma cultura organizacional baseada na ética e integridade corporativa, fomentando o diálogo, a implementação de novas diretrizes, a aderência às normas e regulações internas, além de incentivar reportes de atitudes não conformes por meio da divulgação do canal de denúncias, prevenindo a prática de futuros atos fraudulentos, corruptos e não conformes com as diretrizes internas.

O Programa de *Compliance* aliado a atuação de uma comunicação forte, robusta e planejada é responsável pela promoção de diálogos que possam criar o entendimento da moral organizacional, a aderência dos colaboradores às políticas e diretrizes internas e possibilita um discurso alinhado entre todas as instâncias da organização.

Referências Bibliográficas

CGU. Programa de Integridade – Diretrizes para Empresas Privadas. 2015. Disponível em:< https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf>. Acesso em 31/07/2020

DUARTE, Jorge (Org); BRANDÃO, Elizabeth. Comunicação Pública: Estado, mercado, sociedade e interesse público. 3 ed. São Paulo: Atlas, 2012.

MARTINS, Marina. Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação. Programas de Integridade e a Comunicação Organizacional em Estatais: Uma Visão de Gestores das Áreas de Comunicação e *Compliance*. 2017. Disponível em: <https://portalintercom.org.br/anais/nacional2017/resumos/R12-1017-1.pdf>. Acesso em 06/08/2020

MORAIS, Wilma. Comunicação e corrupção. Recife: Ed. Universitária da UFPE, 2011.

OBRIGADO!

Gratidão a todos os palestrantes de 2020! Neste ano desafiador, todos mudamos a forma de trabalhar inclusive os encontros da CAC que majoritariamente foram realizados de forma online. Muito obrigada a todos que caminharam conosco e contamos com vocês em 2021!

AKIRA ANO JR.
ALESSANDRA GONSALES
ANTONIO NÓBREGA
ANTONIO JUAN FERREIRO
CUNHA
DANIELA CANESCHI YERASSANI
EDMO C. NEVES
ELDY RIZZO
FABYOLA EN. RODRIGUES
FELIPE FARIA
GUSTAVO DIAS
ISABEL FRANCO
JORGE JUAN SOTO DELGADO
JULIO ANDRADE
LUCIA CASASANTA
LUCIANA SILVEIRA
MARCELO ZENKNER
MARCUS VINICIUS DE CARVALHO
RENATA ANDRADE
SALIM SAUD
WASHINGTON LUIZ BOTELHO SOUZA

Legis Compliance

OAB PINHEIROS
COMISSÃO ANTICORRUPÇÃO E COMPLIANCE

RONCARATI

Fraudes em Licitações e Contratos Públicos

JULIANA FOSALUSA DA SILVA

Advogada, com MBA em Administração Hospitalar e Sistemas de Saúde (CEAHS) pela Fundação Getúlio Vargas (2019), especialista em Direito Administrativo pela Pontifícia Universidade Católica de São Paulo (2012) e Bacharel em Direito pela Universidade Presbiteriana Mackenzie (2008).

JULIO CESAR CHAVES

Graduado em Direito pela Universidade Presbiteriana Mackenzie. Com extensões acadêmicas em "Obras Públicas de Edificação e Saneamento", "Licitações Sustentáveis" pelo Instituto Serzedello Corrêa – Escola Superior do Tribunal de Contas da União. Pós-graduado em Direito Público com ênfase em Gestão Pública e Processo Civil pelo Complexo Educacional Damásio Evangelista de Jesus. Coordenados da área de Direito Público consultivo e contencioso do WFaria Advogados.

PEDRO TEIXEIRA LEITE ACKEL

Advogado, Professor de *Compliance* Financeiro da Legal Ethics & *Compliance* (LEC) e da Associação Brasiliera de Bancos (ABBC), Sócio do WFaria Advogados, graduado em Direito pela PUC-SP. Pós-Graduado em Direito Administrativo pela FGV-SP. Pós-Graduado em Direito Tributário pelo IBEGESP. Diretor jurídico da ABRAPSA – Associação Brasilieira de Empresas Prestadoras de Serviço de Apoio Administrativo.

1 – Breve histórico

O procedimento de licitação, ou seu precursor histórico, nasceu nos Estados Medievais da Europa, onde usava-se o sistema denominado "vela e prego", que consistia em apregoar-se a obra desejada, enquanto uma vela ardia. Ao fim da chama, "adjudicava-se" o certame em favor do concorrente que ofertou ao Estado o menor preço durante a disputa.

Nas terras tupiniquins, o sistema precursor dos certames públicos foi trazido pelo Decreto 2.926/1862, que, editado ainda em eras monárquicas, regulamentava as arrematações dos serviços a cargo do então Ministério da Agricultura, Comércio, e Obras públicas. Esse texto normativo, já externava traços, ainda que precários, do que se tornariam os Princípios da Publicidade, Competitividade e Vantajosidade.

O Decreto 2.926/1862 não foi editado por mero capricho ou predição da autoridade Administrativa, mas para combater as fraudes e desvios de dinheiro público que já ocorriam no recém formado Império do Brasil. Nessa época, histórias de desvios e corrupções já permeavam a construção da Estrada de Ferro Curitiba-Paranaguá e a construção do Ramal Ferroviário de Antonina.

Dificilmente conseguiremos datar o início da corrupção, que, como é notório, acompanha o ser humano desde sua gênese. De toda forma, olhando prospectivamente resta saber por que as fraudes continuam sendo praticadas? O que proporciona o nascimento da figura de um fraudador? Seria a fome de dinheiro e poder? Ou ainda, será que o dito popular está correto, e a ocasião realmente faz o ladrão?

Ao longo do texto e sem pretensão de esgotar o tema, pretendemos explanar a teoria consolidada sobre a origem das fraudes, e apresentar os principais gêneros que ocorrem nas licitações ocorridas no País, e ainda, como elas podem ser evitadas, seja do ponto de vista do empresário, como também do próprio Poder Público contratante.

2 – O pentágono da fraude

Na tentativa de encontrar a raiz da fraude, Donald Cressey, em sua obra *Other people's Money; a study of the social psycholgy of embezzlement*, trouxe a teoria que ele mesmo denominou de Triângulo de Fraudes.

Segundo a hipótese de Cressy, ocupadores de cargos de confiança tornam-se fraudadores, quando sob a **pressão** de um problema financeiro pessoal, buscando alento para sua consciência, **racionalizam** e classificam atitudes ímprobas como aceitáveis ou justificáveis, cometendo a fraude na primeira **oportunidade** que julgarem possível.

Pressão, Racionalização e Oportunidade. Estava determinado o perímetro das circunstâncias que originavam os agentes fraudadores e por consequência, as próprias fraudes.

Em meados de 2004, um novo elemento passou a compor a equação filosófica da concepção da origem das fraudes, David T. Wolfe e Dana R. Hermanson[1] adicionaram a **Capacidade** ao modelo até então, consagrado. Nascia a primeira evolução da teoria, que passou a ser denominada de diamante da fraude.

Com o avançar dos estudos sobre *Compliance* e Governança Corporativa, em 2017 a teoria foi novamente relida, e aperfeiçoada por Renato de Almeida dos Santos[2] que adicionou a **disposição** do agente à teoria.

1 The Fraud Diamond: Considering the Four Elements of Fraud." CPA Journal 74.12 (2004)

2 Modelo Preditivo de Fraude Ocupacional nas Organizações Privadas – Tese apresentada à Banca da Pontifícia

Essa alteração foi amplamente acolhida pelos doutrinadores, e culminou em uma última definição teórica, o pentágono da Fraude.

Com essa concepção mais moderna, chegamos à conclusão que a fraude ocorre quando, sob a **pressão** de um problema financeiro pessoal, buscando alento para sua consciência, um agente, com **capacidade** de conhecer e fraudar um processo interno, **racionalizando** e classificando sua iminente atitude ímproba, como aceitável ou justificável, **disposto** a correr os riscos inerentes à sua atitude, comete a fraude na primeira **oportunidade** que julgar possível.

Pressão, Capacidade, Racionalização, Disposição ao risco e Oportunidade. Está delimitado o pentágono da Fraude.

3 – Tipos de fraude

Muitos são os tipos de fraudes perpetradas nas contratações públicas, e o presente ensaio nem de longe tem a pretensão de abordar todas elas, tampouco esgotar o tema, mas antes demonstrar não apenas a sua existência como conscientizar o leitor acerca das formas de combatê-las. Para tal, muito do presente ensaio se baseia na excelente obra Métodos de Detecção de Fraude e Corrupção em Contratações Públicas (MONDO, Bianca Vaz, produzido e disponibilizado publicamente pela Transparência Brasil em seu portal eletrônico), o qual é extremamente feliz neste viés de combate prático às ocorrências de fraude.

Portanto, ainda que nem todos os tipos de fraude estejam aqui retratados, é de bom tom mencionar seus principais gêneros antes abordar algumas de suas espécies, ainda que muito brevemente:

Projeto mágico – este tipo de fraude, magistralmente batizada na obra supramencionada Métodos de Detecção de Fraude e Corrupção em Contratações Públicas, compreende todo tipo de ilícito que se refira a "erros" ou "inconsistências" do descritivo do objeto no edital de licitação, seja de modo a impedir ou dificultar o processo de formação de preço das licitante não participantes do esquema, seja para inviabilizar a concorrência através de situações na caracterização do objeto, como a promoção de licitação organizada em lote único que poderia ser perfeitamente desmembrada e adjudicada por itens. Aqui também se inserem os fracionamentos indevidos de despesa, as fraudes de precificação e até o conluio entre o projetista e a empresa licitante.

Edital restritivo – Embora este tipo de fraude também resida na redação do edital, sua grande diferença com relação ao projeto mágico é que ela se funda mais em colocar condições excessivas de participação às interessadas do que na descrição do objeto propriamente dito. Nesta seara se encaixam todas as exigências cumulativas que a lei prevê como excludentes (fazendo com que o termo "ou" se torne na prática "e" na redação do edital), exigência de documentos de habilitação e comprovações diversas das legalmente previstas, tais como capacidade financeira, comprovação de profissionais e/ou equipamentos disponíveis antes da assinatura do contrato, excursão técnica, dentre outros.

Publicidade precária – a publicidade dos atos é um dos princípios regentes da

Universidade Católica para obtenção do título de Doutorado em Administração

Administração Pública, consoante ao texto constitucional. Neste tipo de fraude, como o próprio nome sugere, se encontram todas as falhas de publicizar determinados atos da forma e meio apropriados para que atinjam seu propósito.

Julgamento negligente, conivente ou deficiente – este tipo de fraude se concentra em mascarar atos e/ou fatos para garantir determinado resultado ao certame, sempre com vistas a frustrar o caráter competitivo do certame. Aqui também se enquadram admissões dolosas de situações que são evidentes erros grosseiros, e até mesmo algumas situações em que as licitantes fraudadoras se esmeram para criar um aspecto crível ao condutor da licitação, para que incorra em erro face à robustez daquilo que se apresenta "formalmente".

Contratação direta indevida – A licitação com ampla disputa é a regra das contratações públicas, ao passo que as contratações por inexigibilidade ou dispensa de licitação são as notadas exceções. Aqui se inserem portanto todas as hipóteses em que determinadas contratações deveriam ser precedidas de disputa mas que, por razões espúrias, são levadas a cabo diretamente junto às fornecedoras, tais como as situações emergenciais forjadas ou indevidamente prorrogadas, fracionamento da despesa, e a falsa exclusividade de produto ou singularidade de profissional.

Cartelização – Se os cartéis fossem o objeto deste ensaio, as páginas percorridas até aqui pouco bastariam para dar sua introdução; este tipo de fraude, em que há uma pluralidade de agentes, mormente empresas licitantes, além de ser uma fraude em si, ainda permite que se entremostrem praticamente todos os outros tipos de fraudes conjugados, na medida em que os cartéis, com o passar do tempo, adquirem cada vez mais influência e domínio nos mercados em que se inserem, destruindo a concorrência e criando monopólios em ambientes de disputa aparente.

4 – Fraudes em Espécie

Abaixo, citamos e exemplificamos alguns dos tipos de fraudes mais comuns.

4.A – Jogo de Planilhas

O jogo de planilha é uma fraude de todo corriqueira e largamente reconhecida pela jurisprudência atual, especialmente no âmbito dos Tribunais de Contas. Geralmente de formas discretas, mas por vezes descaradas, licitantes honestas se veem prejudicadas nos certames licitatórios, preteridas por empresas que, lançando mão desta prática, acabam por conseguir apresentar uma proposta que aparentemente seria a mais vantajosa à Administração contratante, mas isso é só no papel.

O jogo de planilhas verifica-se mormente em licitações cujo objeto sejam obras e serviços de engenharia em que o critério de adjudicação seja o de preço global por lote, em que a redação do edital não fixa os valores máximos aceitáveis para itens unitários, embora também seja possível em certames de objeto distinto, e até mesmo em atas de registro de preços.

Essa confluência danosa de fatores permite que as licitantes mal-intencionadas zerem ou fixem valores irrisórios em itens que serão pouco demandados quando da execução contratual e, em contrapartida, fixe valores muito mais altos do que o padrão para itens de alta demanda, o que, em termos práticos, efetivamente é capaz de gerar uma proposta de valor global mais vantajoso, mas que, ao longo da execução contratual, acabará sendo muito mais onerosa ao erário do que as propostas das licitantes honestas.

Tentando coibir o aumento desta prática, o E. Tribunal de Contas da União editou a Súmula n. 259, que serve como o primeiro bastião de defesa contra esta malfadada prática:

Nas contratações de obras e serviços de engenharia, a definição do critério de aceitabilidade dos preços unitários e global, **com fixação de preços máximos para ambos, é obrigação e não faculdade do gestor.** (grifa-se)

Com efeito, a mera leitura da súmula supra transcrita deixa claro que **a primeira linha de defesa contra esta prática é a fixação no edital dos preços unitários máximos aceitáveis**. Aliás, destaque-se ainda que, ao determinar que a fixação dos preços máximos aceitáveis é um dever e não uma faculdade do gestor, aquele gestor que não o fizer terá cometido o erro grosseiro e passível de responsabilização previsto no art. 28 da LINDB.

Portanto, a licitante que pretende evitar ser vítima de um jogo de planilhas, ao deparar-se com um instrumento convocatório cuja redação não fixe os valores máximos aceitáveis para os itens contidos nos lotes, deverá apresentar impugnação ao edital, no sentido de requerer tal fixação. Caso esta impugnação não seja acolhida, isto será um indicador de possível conchavo entre alguma empresa licitante e integrantes da Administração, o que inspirará ainda mais cautela no trato deste certame.

4.B – Robôs

A utilização de robôs para a oferta de lances em licitações do tipo pregão não chega a ser exatamente uma fraude em si, mesmo porquê, não há uma vedação literal e decorrente de texto de lei à sua utilização. O que se vê na atualidade é apenas um posicionamento jurisprudencial maciçamente contrário, que é ocasionado mais pelo ferimento da isonomia entre as licitantes do que pela utilização do robô propriamente dito.

Neste sentido, cita-se o trecho emblemático acórdão n. 1.647/10 – Plenário, em que o E. Tribunal de Contas da União enfrentou o tema pela primeira vez detalhadamente:

a) é possível aos usuários de dispositivos de envio automático de lances (robôs) a remessa de lances em frações de segundo após o lance anterior, o que ocorre durante todo o período de iminência do pregão;

b) com a possibilidade de cobrir lances em frações de segundo, o usuário do robô pode ficar à frente do certame na maior parte do tempo, logrando assim probabilidade maior (e real) de ser o licitante com o lance vencedor no momento do encerramento do pregão, que é aleatório;

c) ciente dessa probabilidade, que pode chegar a ser maior que 70%, o licitante usuário do robô pode simplesmente cobrir os lances dos concorrentes por alguns reais ou apenas centavos, não representando, portanto, vantagem de cunho econômico para a administração.

Para o relator, os fatos configurariam a inobservância do princípio constitucional da isonomia, visto que "a utilização de software de lançamento automático de lances (robô) confere vantagem competitiva aos fornecedores que detêm a tecnologia em questão sobre os demais licitantes" [...]

(TCU, Acórdão n. 1647/10 – Plenário)

Deveras, a irregularidade do uso de robôs reside na sua capacidade de ofertar lances muito mais rapidamente do que mãos humanas seriam capazes, e muitas vezes, com descontos irrisórios, descontos estes que, no apagar das luzes, não se revelam como vantagem ao Poder Público contratante, e se prestam apenas para manter a empresa detentora do robô como a primeira colocada quando o sistema do chat do pregão inicia a contagem o tempo randômico. Aliás, o uso de robôs é determinante nestes ambientes virtuais que utilizam o tempo randômico que, embora esteja em declínio com o advento do Decreto Federal n. 10.024/19, ainda existe.

Assim, mesmo sem saber em quanto tempo o *chat* do certame continuará

aberto para a disputa, o robô manterá seu usuário como primeiro colocado, na medida em que é capaz de cobrir qualquer lance registrado no sistema em uma fração de segundo.

Mas muito embora não haja no ordenamento jurídico uma vedação expressa, na prática, muitas são as tentativas de tentar coibir o uso de robôs nos certames licitatórios, tais como a fixação de intervalo mínimo entre lances, fixação de desconto mínimo entre cada lance, e até mesmo a colocação de ferramentas do tipo CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*, que se traduz livremente como Teste de Turing público totalmente automatizado para diferenciar computadores e humanos) podem ser vistos em alguns ambientes de disputas virtuais.

Infelizmente, as medidas de prevenção não são muitas, até mesmo pelo fato de não se conhecerem as licitantes até o final da fase de lances; ou seja, não há como prever se e qual licitante estará ofertando lances via robô antes do certame, desta feita, a principal medida a ser tomada pelas licitantes que desejem se precaver desta prática é a apresentação de pedido de esclarecimento com o intuito de esclarecer se (i) será permitido às licitantes o uso de robôs, (ii) tempo mínimo entre lances e (iii) valor mínimo de desconto em cada lance, e, conforme o caso, eventual pedido de impugnação para que o instrumento convocatório os preveja.

Mas se por um lado há poucas medidas preventivas, o que torna o combate a este tipo de irregularidade uma via mais reativa do que preventiva, por outro, os Tribunais de Contas, em especial o da União, têm se mostrado favoráveis ao acolhimento dos pleitos das empresas que se sentem lesadas pela ferramenta.

De outra banda, os robôs são tremendamente benéficos para que empresas de porte pequeno possam participar de múltiplos pregões simultaneamente mesmo sem ter uma equipe dedicada ao tema, como as grandes empresas. Neste prisma, o robô seria uma ferramenta de inclusão ao invés de uma ferramenta anticompetitiva. Assim, se sob este prisma da isonomia é correto coibir o uso de robôs, seria então correto proibir que empresas que possuem um departamento de licitações disputem contra aquelas que não têm condições para tal?

Assim, se uma licitante desejar utilizar de robôs sem correr o risco de sofrer consequências danosas, deverá estar atenta aos intervalos mínimos de tempo e de descontos, de maneira a parametrizar a máquina de modo a enquadrar-se e, eventualmente, dirigir um pedido de esclarecimentos à Administração antes de tomar parte do certame, rememorando que a resposta da Administração terá tanta força vinculante quanto os comandos editalícios.

4.C – Coelhos

Tal como os coelhos que servem de isca aos cães de corrida em seus páreos, esta fraude ocorrente em pregões eletrônicos consiste na participação de empresas de fachada na disputa, cujo único papel será o de ofertar lances de forma muito agressiva, apenas com vistas a ludibriar licitantes honestas a disputar com estes coelhos, reduzindo assim os seus preços de forma a alcançar até mesmo valores inexequíveis para o contrato em disputa, ou até mesmo desistir de continuar na disputa.

Assim, quando as licitantes sérias terminam de disputar com o "coelho", seu preço geralmente está completamente abaixo da possibilidade – ou interesse – em seguir com aquela contratação, que é quando a mágica do coelho acontece: o coelho geralmente desiste de sua proposta ou, convocado para apresentar os documentos necessários para a contratação, a empresa de fachada que

na verdade é o "coelho" acaba se furtando à sua obrigação, ou cumprindo-a de forma sabidamente deficitária, e que levará à sua consequente inabilitação. Isso permitirá que a licitante "dona do coelho" tome parte da disputa sem ter que se preocupar com as empresas realmente competitivas, que já estarão exauridas em termos de margem de valores em seus preços após terem "perseguido o coelho".

O Decreto n. 10.024/19, que regulamentou a modalidade licitatória Pregão em sua forma eletrônica no âmbito Federal, trouxe em seu bojo a principal forma de se combater este tipo de expediente fraudulento. Com efeito, é que, ao determinar que as licitantes estão obrigadas a enviar os documentos de habilitação conjuntamente com as propostas, o legislador cuidou para que as empresas que fazem as vezes de "coelhos" minimamente possam ser perseguidas pela prática fraudulenta, já que no formato ainda adotado fora do âmbito federal, as empresas que tomam parte da disputa só precisarão se identificar se vencedoras da etapa de lances.

Na prática, da mesma forma que a utilização de robôs, é virtualmente impossível descobrir se em dado pregão eletrônico haverá uma empresa que fará às vezes de coelho, o que torna as medidas combativas desta prática igualmente em medidas reativas do que preventivas. Assim, tão logo o certame se inicie, a licitante bem intencionada deverá manter a calma e não iniciar uma disputa de preços muito agressiva logo de saída, para evitar correr o risco de perder a margem de seu preço disputando com o coelho e, caso este tipo de fraude se verifique, o licitante lesado deverá buscar a penalização do coelho junto tanto à Administração licitante quanto aos Tribunais de Contas.

4.D – Propostas de Cortesia

De acordo com a Organização para Cooperação e Desenvolvimento Econômico – OCDE, as propostas fictícias são a forma mais comum de fraude em licitações no mundo todo, pois se presta geralmente a dar a aparência de legitimidade a uma contratação fraudulenta, como por exemplo, para que não fique tão evidente o direcionamento de uma licitação para dada empresa, de forma que o certame escape ao radar dos órgãos de controle. Assim, a proposta da beneficiada pelo direcionamento costuma estar acompanhada de outras propostas puramente "pró forma", de forma a legitimar uma disputa que na verdade nunca ocorreu.

Assim, é correto afirmar que as propostas de cortesia servem apenas para simular uma concorrência que muitas vezes não teria nem condições de existir.

Deveras, as propostas de cortesia geralmente apresentam (i) valores muito elevados se comparados com o valor da proposta da "dona do edital", ou ainda, (ii) valores mais elevados até do que o próprio valor estimado para a contratação, de maneira a não haver riscos de a empresa fraudadora venha a ser contratada "por um infeliz acidente"; igualmente, para dar um ar de maior verossimilhança à prática, algumas vezes estas propostas possuem valores praticáveis, mas (iii) apresentam condições de habilitação inaceitáveis à Administração licitante.

As condições não são excludentes, ou seja, uma proposta de cortesia poderá ao mesmo tempo ter valor superior ao estimado pela Administração, o que será igualmente superior à proposta "destinada" à vitória, e também apresentar condições inaceitáveis de habilitação.

Aliás, é de todo frequente que empresas idôneas venham a tomar parte de licitações onde apresentam propostas legítimas, mas que acabam por servir como uma proposta de fachada, o que é inclusive o melhor dos mundos para os fraudadores. Com efeito, é que assim os fraudadores sequer precisam

envolver uma empresa "parceira" para que lhes dê cobertura, quando por exemplo uma empresa inocente acode a um certame flagrantemente direcionado, na tentativa de alterar o descritivo do edital ou ainda, de "comover" o pregoeiro com uma proposta comercialmente muito melhor e ainda exequível do que suas adversárias.

Se por um lado esta é a fraude mais comum nos certames licitatórios, de outro, ela deixa evidentes uma série de "coincidências" totalmente impossíveis e que podem ser captadas e interpretadas pelas licitantes que desejem evitar serem suas vítimas, tais como:

1) Documentos sequenciais: ocasionalmente os documentos apresentados por licitantes em conluio para acobertar um certame serão produzidos em série e/ ou em um curto espaço de tempo, o que poderá ser facilmente visto se comparadas informações de impressão ou criação dos arquivos entre si.

2) Linearidade de preços: com vistas a assegurar à empresa "dona do edital" fique em primeiro lugar no certame de forma indisputável, por vezes ela estará acompanhada de empresas que terão um preço tão similar ao seu que ficarão classificadas sequencialmente. Esta precificação "uniformemente díspar" geralmente pode ser vista em toda a composição de preço das empresas conchavadas de maneira totalmente uniforme, ou seja, outra coincidência impossível.

3) Mesmos Erros: por mais cômico que possa parecer em uma primeira análise, muitas vezes as empresas fraudadoras se utilizam de arquivos com erros de digitação, ortográficos, de diagramação, formatação... enfim, a incompetência humana é o limite aqui. E quando estas empresas vêm a se utilizar dos mesmos arquivos e documentos de habilitação em vários certames em que atuam de maneira a simular a competição, basta um olhar atento para se perceber outra rara coincidência a indicar a fraude. Aliás, as empresas que compõem os cartéis por vezes trocam estes documentos entre si, o que torna a fraude ainda mais evidente.

4.E – Empresas de fachada

Hoje em dia, por meio de diversos avanços legislativos criados para desburocratizar e fomentar a economia, é possível de se obter um CNPJ em pouquíssimo tempo e com muito menos formalidades do que no passado recente. Pois se por um lado tal medida é de fato indispensável para que a economia pátria seja alavancada, por outro, ela também facilita a criação de empresas de fachada que se prestam a diversas finalidades espúrias, dentre as quais se encontra a possibilidade de fraudar licitações públicas.

Aliás, esta fraude se encaixa como uma luva em outros tipos de fraude aqui tratadas de maneira a complementá-las, tais como a propostas de cortesia e os coelhos, que não precisam de muito mais do que uma empresa que só exista formalmente para que se operem.

Da mesma forma que as propostas de cortesia, este tipo de fraude se presta a simular a competição e alijar empresas sérias da disputa, pois muitas vezes elas são criadas como aqueles tipos societários beneficiários da lei complementar n. 123/06 (ME e EPP), até mesmo pela facilidade de criação deste tipo de empresa.

Em outra possível vertente deste tipo de fraude é que, muitas vezes, a empresa de fachada de fato pretende não apenas acobertar, mas sim vencer a licitação, inclusive se beneficiando das vantagens da sobredita lei complementar. Só que, no momento de execução contratual, a estrutura a ser utilizada será a de outra empresa de porte maior e com mais capacidade, mas que não faria jus ao benefício da lei.

Não bastante, as empresas de fachada se prestam ainda a albergar as pessoas físicas de empresários fraudadores que tiveram suas outras empresas penalizadas. A lei ainda não alcançou a evolução adequada para tratar disto, mas fato é que se uma empresa denominada "João e Maria LTDA" venha a ser penalizada e impedida de licitar e contratar com o Poder Público, nada impede que seus sócios criem uma nova empresa denominada "Maria e João LTDA" e sigam fraudando os certames de que tomem parte, o que geralmente – mas nem sempre – é feito em nome de "laranjas".

A prevenção deste tipo de ocorrência mais uma vez reside na atenção das licitantes, pois as empresas de fachada possuem algumas características em comum, como por exemplo:

1) Pluralidade de CNAE: as empresas de fachada costumam possuir objeto social bastante amplo e uma vasta gama de CNAE's (Cadastro Nacional de Atividade Econômica) registrados em seu contrato social que não possuem relação entre si, como por exemplo a venda de alimentos *in natura* e construção civil na mesma empresa.
2) Administração por Laranjas: muitas vezes os sócios das empresas de fachada nem sabem que estão a integrar o quadro societário de alguma empresa, pois são pessoas simples e sem instrução que simplesmente um dia "assinaram um papel sem ler", o que lhes rendeu um cargo de sócio. Assim, por muitas vezes será possível de identificar, até mesmo pelas redes sociais, que determinada pessoa não é sócia de uma grande empresa, dado por exemplo à humildade de sua moradia.
3) Procuração com plenos poderes: nenhum empresário de respeito conferiria uma procuração com plenos poderes a terceiros para que conduzam na integralidade seus negócios. A mera existência de um instrumento de mandato que confira totais poderes a pessoa alheia ao quadro societário já é um indicador de que se trata de uma empresa de fachada.
4) Coincidências: as empresas de fachada muitas vezes são registradas no mesmo endereço que outras empresas – de fachada ou não – e com elas compartilham por vezes telefones e prepostos.
5) Evidente falta de estrutura: como dito alhures, a única coisa verdadeiramente necessária a uma empresa de fachada é o número de CNPJ. Assim, por muitas vezes uma busca no endereço informado pela empresa revelará um imóvel vazio, por exemplo.

5 – Primeiro passo de como evitar a fraude?

Não restam dúvidas, de que tão ou mais importante quanto combater as fraudes ocorridas e suas consequências, é prevenir-las. E é impossível nos precavermos de algo que desconhecemos.

Por isso, é importante sabermos a fundo, como, quando e porque as fraudes ocorrem, bem como, quem e em que condições, os agentes as praticam. Sem essas informações é virtualmente impossível traçarmos um planejamento eficaz de prevenção a essas práticas ilícitas.

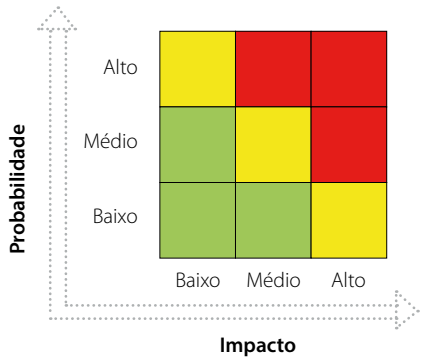
Nesse sentido, existem diversas técnicas para analisarmos e mensurarmos os riscos aos quais uma determinada companhia ou entidade, estão expostas. Dentre todas, a que julgamos mais efetiva e menos custosa é a estruturação de uma matriz de riscos, que deve ser construída a partir de entrevistas com os agentes-chaves da empresa/entidade, a fim de se ter a exata compreensão do mapa (com início, meio e fim) do

processo completo de licitação e contratação pública na empresa/entidade.

A matriz de riscos, também chamada de matriz de probabilidade e impacto, é uma ferramenta gerencial através da qual, o gestor poderá identificar e determinar o tamanho dos riscos ao quais está sujeito, bem como planejar suas ações para impedi-los, mitigá-los ou controlá-los.

Planificando os fluxos de toda a empresa/entidade, o gestor poderá acompanhar os projetos em andamento e mapear e priorizar os processos mais importantes, atuando diretamente neles, seja através de ações repreensivas ou de controle, utilizando, por exemplo, ferramentas de auditoria, ou apenas de conscientização para fomentar uma cultura organizacional proba e retilínea.

Uma das principais vantagens da elaboração da matriz de riscos é que ela não pressupõe a existência de um ambiente 100% (cem por cento) controlado e imutável. Muito pelo contrário, a implantação da matriz de riscos é altamente flexível e aderente às realidades individuais de cada corporação/entidade, bem como de suas variações em decorrência de influências internas ou externas.



A construção da matriz de riscos, **é realizada através do equacionamento de duas principais variáveis: Probabilidade e Impacto.**

A mensuração e escalonamento dessas duas variáveis em cada um dos fluxos de trabalho, nos permite, com um elevado grau de precisão, **diagnosticar** a quais ameaças estamos sujeitos, e quais eventuais prejuízos sofreríamos com a superveniente incidência das referidas ameaças.

Nesse sentido, a probabilidade da incidência de um dano deverá ser mensurada em (0) improvável, (1) Pouco Provável, (2) Possível e (3) Muito Possível; já, o impacto caso o dano sobrevenha, deverá ser classificado em (0) Sem impacto, (1) Baixo Impacto, (2) Médio Impacto ou (3) Alto impacto.

É importante que ao elaborar a matriz de riscos, o gestor tenha em mente algumas características inerentes a área da empresa que pode afetar diretamente o seu grau de risco, como, por exemplo, sua autonomia financeira e decisória e ainda, a quantidade e a qualidade dos mecanismos de controle que incidem sobre ela; via de regra, quanto mais autonomia e menos controle houver sobre a área, maiores são os riscos que ela traz.

Após a realização de um diagnóstico eficiente, o mapa de riscos passar a ser uma importante ferramenta de **controle** para os gestores, que poderão analisar os dados à mesa, alocar recursos e rever os mecanismos de controle que incidem sobre determinada área da operação, priorizando as mais sensíveis de acordo com as estratégias da organização.

Afinal, um dano cuja incidência é improvável e que, caso sobrevenha não impactará as operações da empresa, não deverá ser objeto de preocupação de gestores, ao passo que alocar recursos ali, poderia culminar em um desperdício dos recursos da organização.

Por fim, em sua fase final de implantação, a matriz de riscos passa a ser um importante mecanismo de **monitoramento** das operações da empresa, devendo ser revista de tempos em tempos, para que se garanta sua aderência a realidade.

Não existe "*Compliance* de prateleira". Cada organização possui suas características e

peculiaridades, e todas estão sujeitas às mutações provenientes de fatores internos, externos, ou até mesmo do mero decurso do tempo.

Em síntese, seja para afastar como também para mitigar as fraudes às licitações e contratos públicos, a utilização de matriz de risco como ferramenta de gestão é o primeiro passo para o estabelecimento de uma cultura de conformidade, que deverá seguir com a revisão e reforço dos mecanismos de controles e implementação do monitoramento das práticas para combater as fraudes.

6 – Conclusão

Historicamente, a existência de fraudes em licitações e contratos públicos é uma certeza em nosso País. Em maior ou menor grau, ela se dá em licitações de todo tipo e porte. Existem diversos topos de fraudes em licitações e contratações públicas, dos mais rotineiros como uma proposta fictícia, aos mais engenhosos, como um cartel.

O diagrama do pentágono das fraudes permite compreender bem o porquê as fraudes continuarem a perpetuar: falta de vigilância por parte das empresas/entidades. Só com vigilância é que se consegue (i) pôr fim, mitigar ou controlar o número de oportunidades dos agentes, (ii) reduzir suas capacidades de fraudar um processo interno, (iii) desestimular o agente a ter disposição para o risco e (iv) constranger o agente a ponto de impedir a racionalização da conduta ímproba como aceitável ou justificável.

Assim, o primeiro passo para evitar, ou, ao menos mitigar as fraudes em licitações contratações públicas, consiste na preparação de mapa de riscos dos processos de licitações e contratos públicos. Feito esse diagnóstico, segue-se o fortalecimento dos mecanismos de controle e de monitoramento. Nesse processo, com retroalimentação, certamente a incidência de fraudes será severamente reduzida. Vamos praticar!?

LegisCompliance, o Portal que auxilia na Gestão das Demandas Regulatórias ligadas ao compliance no Brasil

Cadastre-se gratuitamente em:
www.legiscompliance.com.br

- Base de Dados inteligente
- Textos atualizados e consolidados
- Filtros de busca que facilitam a pesquisa
- Legislação e normatização reunidas em um único ambiente
- Ferramenta de suporte para as áreas de compliance, jurídica, controles internos e governança
- Envio de informativos

Legis Compliance

RONCARATI

SUA PRESENÇA É MUITO IMPORTANTE PARA NÓS!

VENHA FAZER
PARTE DA COMISSÃO
ANTICORRUPÇÃO E COMPLIANCE
DA OAB/SP-PINHEIROS!

PARTICIPE DOS ENCONTROS
E MANTENHA-SE INFORMADO
SOBRE TENDÊNCIAS
E PRINCIPAIS NOVIDADES

PARA PARTICIPAR BASTA
ENTRAR EM CONTATO NO E-MAIL

CAC.OABPINHEIROS@GMAIL.COM

OAB PINHEIROS | COMISSÃO ANTICORRUPÇÃO E COMPLIANCE