REVISTA DE DIREITO COMERCIAL

liber amicorum

# Noções breves sobre a gestão do risco de *compliance*

Roberto Bilro Mendes[1]

## I. Introdução

Princípios, cultura, normas, decisões e condutas: são esses os ingredientes principais do *compliance*

---

[1] Diretor do Departamento de Financial Services Risk & Regulation da PwC.
Escrever um artigo para o *Liber Amicorum* do Professor Pedro Pais de Vasconcelos é para mim, simultaneamente, uma enorme honra e uma grande responsabilidade. Sem o Professor Pedro Pais de Vasconcelos a minha vida ter-se-ia, sem qualquer dúvida, afastado da prática do Direito. Foi no seu escritório, entre a aprendizagem a ver fazer e a fazer, que a natureza das coisas me fez apaixonar pela procura da correlação do ser e do dever ser e pelo ato (*quiçá* arte?) do processo concretizador da interpretação jurídica, primeiro através da subsunção e depois através da sinéptica. Foi no seu escritório, no primeiro ano do meu estágio, que nasceu a minha paixão pelo Direito Comercial e foi a partir dali (sempre demasiado longe, na minha opinião, da *"minha casa",* do *"meu escritório"* e do *"meu Professor"*) que a minha carreira ganhou um sentido e um propósito. Se os meus dias são hoje passados a pensar e a aplicar uma das disciplinas extravagantes do Direito Comercial, devo-o, sobretudo, ao Professor Pedro Pais de Vasconcelos. Não poderia, assim, deixar de aceitar o desafio de participar nesta homenagem tão merecida. Não poderia também deixar de trazer um tema intimamente ligado aos ensinamentos basilares do Professor e à disciplina do Direito Comercial à qual me dedico diariamente (gestão do risco de *compliance* na atividade bancária, de intermediação financeira e de distribuição de seguros). Hoje, como naqueles primeiros anos, espero, no mínimo, não desiludir e, se possível, deixar o Professor orgulhoso deste seu aprendiz!

www.revistadedireitocomercial.com
2020-03-26

Confiança: é esse o ingrediente principal do comércio (e, por inerência, do Direito Comercial).

A falta de cultura (ou a cultura inadequada) e a conduta imprópria (ou a *mis-conduct*) levam ao incumprimento das normas e regras aplicáveis, à quebra de confiança com os vários *stakeholders* das instituições financeiras (clientes, acionistas, credores, fornecedores, colaboradores, entre outros) e à lesão dos bens jurídicos dos clientes, das próprias instituições e, por fim, do próprio mercado.

Por outras palavras, nesses casos o *dever ser* da confiança nunca chega a *ser*.

Sem confiança as partes afastam-se do mercado. Sem partes no mercado não existem atos de comércio e sem esses atos não existe mercado, nem comércio.

Existem várias ferramentas para a criar e proteger a confiança. A gestão adequada do risco de *compliance* é, cada vez mais, uma dessas ferramentas e, *quiçá,* uma das mais importantes para a proteção da confiança nos agentes de mercado e no próprio mercado e, dessa forma, para a proteção do mercado e do comércio. Tem sido e pode ser cada vez mais um elemento-chave para que o *dever ser* da confiança se aproxime mais do *ser*.

Mas o que é o *compliance*? E o que é a gestão adequada do risco de *compliance?*

O dever de conformidade ou o *"duty to comply"* ou, usando o conceito mais em voga, o *compliance*, existe, na verdade, desde o início da civilização, quer para deveres ou regras escritas, quer para deveres ou regras não escritas.

Traduz-se, na verdade, num conceito bastante simples cujo significante deriva do próprio significado: existem regras (legais, regulamentares, naturais, voluntárias ou outras) aplicáveis a determinadas circunstâncias e essas regras devem ser cumpridas. Para assegurar o cumprimento dessas regras, será necessário que a cultura seja adequada e a conduta seja própria (ou orientada) para o cumprimento.

Não obstante, e apesar da sua (aparente) simplicidade, o *full compliance* ou cumprimento total é uma utopia reconhecida enquanto tal pelo próprio legislador e pelas próprias normas, que, antecipando a possibilidade do incumprimento e tentando dissuadir o mesmo, usam da estatuição para identificar, de forma mais ou menos clara (dependendo, sobretudo, da capacidade do legislador), as consequências para o incumprimento das regras previstas.

Reconhecida a utopia e reconhecidas as situações de cultura inadequada e de conduta imprópria que têm acontecido, no nosso ordenamento jurídico e noutros, com mais ou menos relevo e impacto, desde o início da atividade das instituições de crédito, dos intermediários financeiros e dos distribuidores de produtos de seguros e reconhecida a importância da confiança no âmbito do comércio, percebe-se que o legislador, as empresas (comerciantes) e os seus supervisores disponham, cada vez mais, de esforços e de recursos (financeiros, humanos, técnicos e tecnológicos) para gerir o risco do cumprimento ou, na sua formulação anglo-saxónica: o risco de *compliance*.

O reconhecimento da importância do risco de *compliance* enquanto ferramenta para assegurar a confiança dos vários *stakeholders* levou ao surgimento da teoria da gestão do risco de

*compliance* e ao seu aperfeiçoamento, quer na sua vertente mais teórica, quer na sua vertente mais prática.

Quando efetuada no âmbito da atividade bancária, de intermediação financeira e de distribuição de seguros, a gestão do risco de *compliance* não pode, na nossa opinião, deixar de ser considerada enquanto uma disciplina extravagante do Direito Comercial (estando intimamente ligada com a natureza das coisas) à qual se deverá aplicar (sempre) a atividade jurídica da *Prudentia* e não poderá dissociar-se da teoria do governo e do controlo interno (*internal governance*) e da gestão de riscos gerais.

O Direito Comercial é, na sua génese, eminentemente prático (sem partes não existe negócio e sem condutas tomadas pelas partes também não) e ocupa-se, em primeira instância e diretamente, da conduta e, indiretamente, da cultura das partes de um negócio jurídico, visando, sobretudo, a confiança. Assim, a identificação, a avaliação, a monitorização, o controlo e o reporte adequados das situações de incumprimento interessa (e muito) ao Direito Comercial.

Iremos dedicar-nos, no presente texto, à identificação da evolução da legislação e das boas práticas associadas à gestão do risco de *compliance* no âmbito das atividades supramencionadas, à definição e especificação do conceito e à identificação resumida de alguns dos processos fundamentais da gestão do risco de *compliance*, sempre tendo em conta os princípios do Direito Comercial e o estado atual de desenvolvimento da disciplina em cada uma das atividades.

## II. Da evolução da legislação e das boas práticas associadas à gestão do risco de *compliance*[2]

Tal como dissemos acima, apesar de o tema da conformidade acompanhar, desde sempre, o Direito (desde que existe Direito que o mesmo se destina a ser, em última instância, cumprido ou incumprido) e de podermos encontrar lugares comuns ao estudo da conformidade ao longo dos tempos, a gestão do risco de *compliance* no âmbito dos negócios parece ter tido os seus primeiros sinais nos documentos da civilização Mesopotâmica (3600 A.C.). Alguns autores referem ainda o Talmude como um dos pontos de partida. Não estamos em condições de poder confirmar que assim o seja.

Não obstante, parece-nos que o verdadeiro "nascimento" da teoria do controlo interno das empresas (mais tarde, das instituições de crédito) e, indiretamente, da gestão do risco de *compliance* se terá dado durante a revolução industrial, acompanhando as necessidades crescentes de financiamento de capital e a importância de se observar, de forma mais ou menos clara, os resultados e a posição financeira das empresas. É claro para nós que a gestão do risco de *compliance* (ainda sem esse cunho anglo-saxónico) encontrou a sua primeira casa no Código Comercial Napoleónico em 1804, chegando ao ordenamento jurídico português em 1833, após a publicação do nosso Código Comercial (a necessidade de atuar conforme as leis do comércio e os seus usos e costumes é, ainda nos dias de hoje, parte

[2] Não são aqui citados, propositadamente, diplomas específicos de prevenção de branqueamento de capitais ou de financiamento do terrorismo ou de sanções ou prevenção de corrupção e fraude, por se entender que esses serão subriscos de *compliance*.

central da definição de risco de *compliance* e elemento fundamental dessa disciplina extravagante do Direito Comercial).

Noutras paragens, o tema foi crescendo de importância, principalmente nos Estados Unidos da América, durante e após os escândalos financeiros das décadas de 1920 e 1930 (incluindo o *crash* da bolsa de New York de 1929). Era, nessa altura, essencial regular e supervisionar de forma mais eficaz o mercado de capitais, com vista a garantir a adequada proteção dos investidores. O *Securities Act* (de 1933 e de 1934) e a criação, em 1934, da *Securities and Exchange Comission* (SEC) foram momentos importantíssimos para a implementação da teoria do controlo interno (a teoria moderna da auditoria interna conheceu, por exemplo, aí os seus primeiros passos) e, dessa forma, para a prossecução da conformidade enquanto um dos seus elementos fundamentais.

Foi também nos anos 30 que foi, pela primeira vez, apresentada uma definição de controlo interno (pelo *American Institute of Certified Public Accountants*), incluída na SAS n.º 1 e aplicada pela SEC, onde se poderia ler o seguinte: *"Internal control comprises the plan of organization and all of the coordinate methods and measures adopted within a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operacional efficiency and encourage adherence to prescribed managerial policies".*

A importância do controlo interno foi reforçada após os escândalos de *Watergate* e *Lockheed*, já na década de 70, mas foi nos anos 80 que foram dados alguns dos passos mais importantes no âmbito do controlo interno e, por inerência, da gestão do risco de *compliance*, após a criação e estabelecimento da *Treadway Comission* (juntando, entre outras, a American Accounting

Association e o Institute of Internal Auditors), e a criação, em 1985, do *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), bem como após a publicação, em 1987, do relatório *Fraudolent Financial Reporting* onde, pela primeira vez, se colocava o foco na importância dos controlos internos e na necessidade de criar critérios de análise para avaliação detalhada dos mesmos com o objetivo de atingir a conformidade com a legislação aplicável.

O primeiro momento chave acabaria por chegar em 1992, com a publicação pela COSO do documento *Internal Control – Integrated Framework* (primeiro modelo de princípios COSO), onde foi formalizado, pela primeira vez, um modelo de controlo interno com uma perspetiva de gestão de risco de *compliance*, identificando cinco elementos fundamentais para esse efeito: (i) ambiente de controlo; (ii) processo de avaliação de risco; (iii) processo de controlo; (iv) processo de informação e comunicação e (v) processo de monitorização.

A entrada em vigor nos Estados Unidos da América, em 2002, da Lei Sarbanes-Oxley (SOX) reforçou (sobremaneira) a importância do controlo interno e da gestão do risco de *compliance* para o aumento da confiança dos investidores e para a prevenção e combate à fraude (primeira interligação direta entre a conformidade e a prevenção da fraude e da corrupção).

Dois anos depois a COSO publicou o seu novo modelo de Risk *Management - Integrated Framework*, (princípios COSO II), na sequência da evolução dos estudos efetuados pela Treadway Comission, criando formalmente, nesse documento, a teoria da gestão de riscos associada à identificação, avaliação e monitorização

de riscos financeiros e não financeiros. Esse modelo previa oito elementos fundamentais: (i) ambiente de controlo; (ii) processo de definição de objetivos; (iii) processos de identificação de eventos; (iv) processo de avaliação de riscos; (v) processo de resposta aos riscos; (vi) atividades de controlo; (vii) informação e comunicação e (vii) processo de monitorização de riscos.

Nessa altura, em Portugal, já a OROC, na sua Diretriz de Revisão/Auditoria 410, com entrada em vigor em 2000, aplicava os princípios COSO I e, já antes, o Banco de Portugal tinha preparado os primeiros estudos para a criação de um modelo de governo e controlo interno que viria a ser aplicável, logo a partir de 1996, às instituições de crédito sob a sua supervisão direta (Instrução do Banco de Portugal n.º 72/96), aplicando a totalidade dos princípios COSO I e especificando que as Instituições de Crédito e Sociedades Financeiras deveriam dispor de um sistema de controlo interno que abrangesse a definição da estrutura organizativa, os métodos e os procedimentos adequados à minimização dos riscos de fraudes, irregularidades e erros, assegurando a sua prevenção e deteção tempestivas.

Em abril de 2005, o Basel Committee on Banking Supervision e o Bank for International Settlement acabariam por elaborar e publicar um documento absolutamente fundamental para a teoria da gestão de risco de *compliance*: o "Compliance and the compliance function in banks", onde foi definido formalmente e pela primeira vez que se deveria entender o risco de *compliance* enquanto *"the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities"*. Este

documento viria a ficar conhecido como o BCBS 113.

Apesar de não ser aplicável diretamente no ordenamento jurídico português, o BCBS 113 acabou por influenciar (e muito) o Banco de Portugal no âmbito da revisão e revogação da sua Instrução n.º 72/96, efetuada através do Aviso n.º 3/2006, em maio (que já aplicava os princípios COSO II) e na elaboração e publicação, apenas dois anos depois da entrada em vigor desse Aviso (aí revogado), do Aviso n.º 5/2008, de julho, onde foi dado o primeiro grande (enorme, até) salto qualitativo face ao BCBS 113, principalmente no âmbito da identificação formal da definição de risco de *compliance*, dos princípios base para a sua gestão e da necessidade de implementação, por parte das instituições relevantes, de uma função dedicada à gestão de riscos globais e de uma função dedicada à gestão do risco de *compliance*.

Antes disso, em 2007, a CMVM tinha publicado o Regulamento n.º 2/2007, que aflorava, pela primeira vez, o tema do governo e do controlo interno e, dessa forma, da gestão do risco de *compliance*, no âmbito específico da atividade de intermediação financeira, mas que acabaria por ter uma aplicação diluída no texto do Aviso do Banco de Portugal n.º 5/2008, que se sobrepôs a esse Regulamento, principalmente na sua aplicação às instituições de crédito supervisionadas diretamente quer pela CMVM (no âmbito das atividades de intermediação financeira), quer pelo Banco de Portugal (no âmbito das atividades bancárias). Também em 2007 o Banco de Portugal tinha dado resposta à Diretiva n.º 2006/48/CE, do Parlamento Europeu e do Conselho, de 14 de Junho de 2006, que incentivava os supervisores a desenvolver processos de avaliação das instituições focalizados na natureza e magnitude dos riscos e na qualidade dos sistemas de controlo associados, com vista a impor

dotações de fundos próprios em função do perfil de risco assumido por cada instituição.

Essa resposta foi dada através da publicação do Modelo de Avaliação de Riscos (doravante o "MAR"), onde foi estabelecido, pela primeira vez em Portugal, que se deveria entender por risco de *compliance* a

> "*probabilidade de ocorrência de impactos negativos nos resultados ou no capital, decorrentes de violações ou desconformidades relativamente às leis, regulamentos, contratos, códigos de conduta, práticas instituídas ou princípios éticos. Pode traduzir-se em sanções de carácter legal ou regulamentar, na limitação das oportunidades de negócio, na redução do potencial de expansão ou na impossibilidade de exigir o cumprimento de obrigações contratuais*".

Essa definição acabaria por ser confirmada pelo Aviso do Banco de Portugal n.º 5/2008 que, para a gestão desse risco, prescrevia que deveria ser instituída uma função de *compliance* "independente, permanente e efectiva, para controlar o cumprimento das obrigações legais e dos deveres a que se encontrassem sujeitas, que seja, nomeadamente, responsável: a) Pelo acompanhamento e a avaliação regular da adequação e da eficácia das medidas e procedimentos adotados para detetar qualquer risco de incumprimento das obrigações legais e deveres a que a instituição se encontra sujeita, bem como das medidas tomadas para corrigir eventuais deficiências no respetivo cumprimento; b) Pela prestação de aconselhamento aos órgãos de administração e de gestão, para efeitos do cumprimento das obrigações legais e dos deveres a que a

instituição se encontra sujeita; c) Pelo acompanhamento e avaliação dos procedimentos de controlo interno em matéria de prevenção do branqueamento de capitais e do financiamento do terrorismo, bem como pela centralização da informação e respetiva comunicação às autoridades competentes; d) Pela prestação imediata ao órgão de administração de informação sobre quaisquer indícios de violação de obrigações legais, de regras de conduta e de relacionamento com clientes ou de outros deveres que possam fazer incorrer a instituição ou os seus colaboradores num ilícito de natureza contraordenacional; e) Pela manutenção de um registo dos incumprimentos e das medidas propostas e adotadas nos termos da alínea anterior; f) Pela elaboração e apresentação ao órgão de administração e ao órgão de fiscalização de um relatório, de periodicidade pelo menos anual, identificando os incumprimentos verificados e as medidas adotadas para corrigir eventuais deficiências".

No entretanto, foi publicada, no dia 17 de maio de 2006, a Diretiva n.º 2006/43/CE do Parlamento Europeu e do Conselho, relativa à revisão legal das contas anuais e consolidadas (oitava Diretiva) que, no seu artigo 41.º n.º 2 alínea b), especificava que o Comité de Auditoria "sem prejuízo da responsabilidade dos membros dos órgãos de administração, de direção ou de fiscalização, ou de outros membros designados pela assembleia geral de acionistas da entidade examinada (…)" deveria proceder "(…) Ao controlo da eficácia dos sistemas de controlo interno, da auditoria interna, sempre que aplicável, e da gestão de risco da empresa; (…)".

Não sendo um artigo dedicado à gestão do risco de *compliance*, acabou por ser fundamental para o governo e controlo interno e, por inerência, para a gestão de risco de *compliance*, visto que, em

setembro de 2010, a European Cultural and Creative Industries Alliance (ECIIA) e a Federation of European Risk Management Associations (FERMA) elaboraram e publicaram a sua *Guidance on the article 41.º of the 8th EU Company Law Directive* com o subtítulo *"Monitoring the effectiveness of internal control, internal audit and risk management systems"*, onde preconizaram aquele que viria a ser conhecido como o modelo das três linhas de defesa que é aplicado, hoje, transversalmente pelas instituições de crédito após a sua receção e aplicação por parte do legislador e dos supervisores.

Esse modelo especifica que as áreas de negócio compõem a primeira linha de defesa (que deve gerir os riscos, incluindo de *compliance*, na sua atividade diária), a função de gestão de risco de *compliance* e a função de gestão de riscos enquanto funções de controlo ao nível da segunda linha e a função de auditoria interna enquanto função de controlo de terceira linha, estabelecendo um modelo em que as três linhas de defesa se integram numa coreografia complexa no âmbito da gestão de riscos globais da instituição, que tem o órgão de administração enquanto definidor e executor máximo da estratégia de risco e do apetite ao risco e originador do *tone from the top* e o órgão de fiscalização enquanto primeiro fiscalizador das práticas do órgão de administração e de toda a instituição.

Um pouco antes dessa publicação fundamental, o Committee of European Banking Supervisors (CEBS), que viria em janeiro de 2011 a dar lugar à European Banking Authority (EBA), publicou, em fevereiro de 2010, os *High level principles for risk management*, lançando as bases das Orientações que a EBA viria a emitir em setembro de 2011 (*Guidelines on Internal Governance - GL44*), onde a aplicação do modelo das três linhas de defesa já era preconizado e

onde a função de *compliance* e a gestão do risco de *compliance* acabam por ser tratados com maior pormenor, indo um pouco além do Aviso do Banco de Portugal n.º 5/2008).

Para a GL44 acabaria por ser também importante a publicação, em 2010, pelo Basel Committee on Banking Supervision e pelo Bank for International Settlement, do "Basel Committee October 2010 Principles for enhancing corporate governance", que acabariam por ser revistos, em 2015, pelo "Corporate governance principles for banks" (que viria a ficar conhecido enquanto BCBS 328), que se tornou numa das peças chave para a consolidação dos princípios do modelo das três linhas de defesa.

No âmbito específico da intermediação financeira e do pacote legislativo MiFID, a ESMA publicou, em 2012, as suas primeiras *Guidelines on certain aspects of the MiFID compliance function* requirements, aproveitando o BCBS 113 e as EBA GL44, como influência e definindo responsabilidades e modelos de governo para as funções de *compliance* dos intermediários financeiros à semelhança desses diplomas.

As orientações que a EBA viria a emitir em 2017 (EBA/GL/2017/11) revogando as EBA GL44, viriam a dar provimento ao estabelecido na Diretiva n.º 2013/36/EU (vulgo CRD IV), transposta para Portugal pelo Decreto-Lei n.º 157/2014, bem como ao preconizado no BCBS 328.

Sob a tremenda influência da CRD IV (corolário dos acordos de Basileia II e III, em conjunto com o Regulamento n.º 575/2013/EU – CRR II) e do BCBS 328, as novas orientações da EBA viriam a atribuir maior relevância à gestão de risco de *compliance* e à função de *compliance*, prevendo a sua participação num maior número de

temas fundamentais às instituições (código de conduta, governação de produtos, conflitos de interesses, transações com partes relacionadas, subcontratação, gestão de reclamações, *whistleblowing*, entre outras).

Essas orientações foram, entretanto, revogadas em 31 de dezembro do de 2021, após a publicação pela EBA/GL/2021/05, que tem como objetivo de reforçar as orientações de governo e controlo interno no âmbito específico da prevenção do branqueamento de capitais e do financiamento do terrorismo[3] e das regras relativas à concessão de crédito aos membros dos órgãos de administração e de fiscalização e que manteve as regras e o espírito das anteriores *Guidelines*.

Antes dessa publicação da EBA, já o Banco de Portugal tinha publicado o Aviso n.º 3/2020 e a Instrução n.º 18/2020 (que especifica as matérias de reporte do Aviso), revogando o seu Aviso n.º 5/2008. Também a Lei n.º 35/2018, de 20 de julho, havia transposto para o ordenamento jurídico português a Diretiva MiFID II (âmbito da atividade de intermediação financeira) e a Lei n.º 7/2019), de 16 de janeiro (Regime jurídico da distribuição de seguros e resseguros), tinha transposto a Diretiva IDD, identificando, em ambos os casos, a importância da função de *compliance*.

Para além desses diplomas, a ESMA publicou as *Guidelines on certain aspects of the MiFID II compliance function requirements*, em

[3] Para efeitos do presente texto e tendo em conta os seus objetivos, não consideramos os diplomas dedicados exclusivamente à gestão do risco de *compliance* no âmbito exclusivo da prevenção do branqueamento de capitais e do financiamento do terrorismo.

junho de 2020 (revogando as primeiras orientações, de 2012, sobre o pacote legislativo MiFID) e a CMVM publicou o Regulamento n.º 9/2020, revogando parte do Regulamento da CMVM n.º 2/2007, tendo as novas orientações da ESMA e o Aviso do Banco de Portugal n.º 3/2020 como base e reforçando a importância da função de *compliance* na atividade de intermediação financeira, equiparando-a, quase *ipsis verbis*, aos requisitos aplicáveis à atividade bancária.

O Aviso do Banco de Portugal n.º 3/2020 reforçou, uma vez mais, a importância da gestão do risco de *compliance* (apesar de, ainda assim, apresentar algumas decisões menos felizes nesse âmbito, como veremos *infra*), bem como a relevância, para esse efeito, do órgão de administração, do órgão de fiscalização, da função de *compliance* e dos órgãos de primeira linha de defesa.

Para além das várias prescrições relativas à instituição de uma cultura e de condutas de conformidade por parte, desde logo, do órgão de administração (*tone from the top*), do órgão de fiscalização (nota especial para a introdução de uma obrigação de avaliação periódica, externa e independente sobre a cultura e a conduta da instituição e dos órgãos de administração e de fiscalização), destacamos o reforço das responsabilidades da primeira linha de defesa, tendo sido formalizado, pela primeira vez, no artigo 26.º do Aviso do Banco de Portugal n.º 3/2020 que:

> "*O órgão de administração, coadjuvado pelas funções de controlo interno da instituição, assegura que as unidades geradoras de negócio e demais unidades tomadoras de risco para a instituição:*
>
> *a) Tomam decisões ponderadas pelo risco subjacente e dentro dos limites de tolerância ao risco definidos na política de risco da*

*instituição;*

*b) Implementam os processos e os mecanismos de controlo necessários para assegurar que todos os riscos que assumem são devida e tempestivamente identificados, avaliados, acompanhados e controlados, de modo a garantir que permanecem dentro dos limites de tolerância ao risco definidos nas políticas de risco da instituição;*

*c) Implementam os processos e os mecanismos necessários para assegurar que todos os riscos assumidos são tempestivamente reportados às funções de controlo interno relevantes*."

Com esse artigo, o Banco de Portugal acabou por formalizar aquilo que já se podia interpretar do modelo das três linhas de defesa e se inferia nas várias peças da EBA e, até, do Aviso do Banco de Portugal n.º 5/2008, dando assim uma *machadada final* nalgumas discussões em torno da efetiva obrigação da primeira linha de defesa conhecer os limites de tolerância ao risco, inclusive os de risco de *compliance*, de implementar controlos para identificar, avaliar, acompanhar e controlar os riscos diários (incluindo o de *compliance*) e de assegurar que todos os riscos assumidos são, tempestivamente, reportados às funções de controlo relevantes (no caso do risco de *compliance*, à função de *compliance*). Este artigo, ainda que uma gota de água no oceano do Aviso do Banco de Portugal n.º 3/2020, faz toda a diferença para a gestão adequada do risco de *compliance*.

Destacamos ainda a revisão e o alargamento das principais responsabilidades da função de *compliance*, sendo agora formalmente exigido, nos termos do artigo 28.º do Aviso do Banco de Portugal n.º 3/2020, entre outras coisas, que essa função deve:

- Acompanhar e avaliar regularmente a adequação e a eficácia das medidas e procedimentos adotados para detetar qualquer risco de incumprimento das obrigações legais, regulamentares e outros deveres a que a instituição se encontra sujeita, bem como das medidas tomadas para corrigir eventuais deficiências detetadas;
- Aconselhar os órgãos de administração e de fiscalização, para efeitos do cumprimento das obrigações legais, regulamentares e outros deveres a que a instituição está ou estará sujeita;
- Participar na definição das políticas, procedimentos e dos normativos internos da instituição, nomeadamente em matéria de código de conduta, conflitos de interesses e transações com partes relacionadas e acompanhar a sua implementação e aplicação efetiva;
- Prestar imediatamente aos órgãos de administração e de fiscalização toda a informação de que dispõe sobre quaisquer indícios de violação de obrigações legais e regulamentares a que a instituição se encontra sujeita, de regras de conduta e de relacionamento com clientes ou de outros deveres que possam fazer incorrer a instituição ou os seus colaboradores num ilícito de natureza contraordenacional ou causar impacto reputacional negativo;
- Participar no processo de aprovação de novos produtos e serviços, quer em momento prévio à sua aprovação, quer posteriormente à sua introdução de modo a assegurar que os mesmos cumprem com a legislação e regulamentação em vigor;

- Acompanhar e monitorizar a aplicação dos procedimentos de governação sobre a comercialização de produtos, mediante o desenvolvimento de análises periódicas a esses procedimentos e a elaboração de propostas dirigidas ao órgão de administração e demais membros da direção de topo com vista à alteração de procedimentos instituídos, caso se verifiquem riscos atuais ou potenciais de incumprimentos legais ou regulamentares;
- Efetuar testes de conformidade com as disposições legais e regulamentares, através de um programa próprio e estruturado de verificação do cumprimento, regularmente revisto e adaptado aos processos com maior risco de conformidade.

São, pois, vários os diplomas relevantes que se encontram em vigor em Portugal, com impacto direto na gestão do risco de *compliance*[4].

[4] Não são aqui referidos os diplomas de aplicação transversal (i.e. pacote legislativo de prevenção do branqueamento de capitais e do financiamento do terrorismo, pacote legislativo de gestão de dados pessoais, requisitos contabilísticos e de relato financeiro, entre outros) nem os diplomas setoriais aplicáveis às atividades bancária, de intermediação financeira e de distribuição de seguros.
- RGICSF, publicado no DR 1.ª Série-A, 6.º Suplemento, n.º 301/1992 de 31-12-1992, disponível em https://dre.pt/dre/legislacao-consolidada/decreto-lei/1992-70072322;
- CVM, publicado no DR 1.ª Série-A, n.º 265/1999 de 13-11-1999, disponível em https://dre.pt/dre/legislacao-consolidada/decreto-lei/1999-34575175;

Em contraciclo face ao aditamento de responsabilidades no âmbito do risco de *conformidade* face ao elencar das responsabilidades da primeira linha de defesa, do reforço das responsabilidades da função de *compliance* e dos seus responsáveis e da nova necessidade de, para instituições de crédito categorizadas como outras instituições de importância sistémica (O-SII), o responsável pela função de *compliance* dever ser objeto de

---

- Regime jurídico da distribuição de seguros e resseguros, publicado no DR 1.ª Série, n.º 11/2019 de 16-01-2019, disponível em https://dre.pt/dre/detalhe/lei/7-2019-117821873;
- EBA/GL/2021/05, disponíveis em https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/1016721/Final%20report%20on%20Guidelines%20on%20internal%20governance%20under%20CRD.pdf;
- ESMA Guidelines on certain aspects of the MiFID II compliance function requirements, disponível em https://www.esma.europa.eu/sites/default/files/library/guidelines_on_certain_aspects_of_mifid_ii_compliance_function_requirements.pdf;
- Aviso do Banco de Portugal n.º 3/2020, publicado no DR 2.ª Série, n.º 136/2020 de 15.07.2020, disponível em https://dre.pt/dre/detalhe/aviso-banco-portugal/3-2020-137954757;
- Instrução do Banco de Portugal n.º 18/2020, publicada no Boletim Oficial n.º 7/2020 de 15.07.2020, disponível em https://www.bportugal.pt/instrucao/182020;
- Regulamento da CMVM n.º 9/2020, publicado no DR 2.ª Série, n.º 243/2020 de 16.12.2020, disponível em https://dre.pt/dre/detalhe/regulamento-cmvm/9-2020-151322797;
- BCBS 113, disponível em https://www.bis.org/publ/bcbs113.pdf;
- BCBS 328, disponível em https://www.bis.org/bcbs/publ/d328.pdf;
- MAR, disponível em https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/consulta_bp_2_07_mar.pdf

autorização para o exercício de funções por parte do Banco de Portugal, no âmbito do exercício de *fit & proper* especificado no artigo 33-A do RGICSF, o novo Aviso acaba por não especificar um conceito de risco de *compliance* e por incluir o mesmo numa categoria menor de "Outros riscos", como veremos no próximo capítulo

## III. Da noção de risco de *compliance*

A opção de não incluir um conceito de risco de *compliance* no Aviso do Banco de Portugal n.º 3/2020 criou, estranha e desnecessariamente, um problema ao intérprete jurídico, que terá agora de recorrer ao conceito especificado no BCBS 113[5] ou ao conceito previso no MAR[6], visto que o Aviso n.º 5/2008, fonte de Direito hierarquicamente superior ao BCBS 113 e ao MAR (que, apesar de aplicado pelo mercado, não passou de uma consulta pública), foi revogado e, dessa forma, o conceito de risco de *compliance* deixa de estar previsto em Aviso do Banco de Portugal.

[5] "The risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities."

[6] "Probabilidade de ocorrência de impactos negativos nos resultados ou no capital, decorrentes de violações ou da não conformidade relativamente a leis, regulamentos, determinações específicas, contratos, regras de conduta e de relacionamento com clientes, práticas instituídas ou princípios éticos, que se materializem em sanções de carácter legal, na limitação das oportunidades de negócio, na redução do potencial de expansão ou na impossibilidade de exigir o cumprimento de obrigações contratuais."

Já a integração do risco de *compliance* na categoria de "Outros Riscos", no Anexo I da Instrução n.º 18/2020, acaba por não confirmar a importância que é dada à gestão do risco de *compliance* quer nas orientações da EBA, quer pelo BCBS 113 e 328, quer pelo próprio Banco de Portugal, especialmente no corpo do Aviso do Banco de Portugal n.º 3/2020.

É uma decisão estranha do Banco de Portugal, que não deverá, ainda assim, tendo em conta a natureza das coisas e o próprio objetivo do legislador e do supervisor, retirar importância ao tema e ao conceito.

Assim, por forma a garantir um adequado posicionamento da gestão do risco de *compliance* nas instituições, consideramos que as instituições deverão utilizar o conceito especificado no MAR, apesar de não passar de *soft law*, por ser o conceito mais completo e, dessa forma, enquadrar o risco de *compliance* na sua gestão de riscos globais enquanto uma categoria de risco autónomo, a par com os riscos de modelo de negócio, de governo interno, de crédito, de mercado, de taxa de juro de carteira bancária, operacional e de liquidez e de financiamento.

Dessa forma, consideramos que o risco de *compliance* deverá ser considerado, tal qual como o mesmo é identificado no MAR[7], enquanto "*probabilidade de ocorrência de impactos negativos nos resultados ou no capital, decorrentes de violações ou desconformidades relativamente às leis, regulamentos, contratos,*

[7] Consulta pública do Banco de Portugal n.º 2/2007 – Modelo de Avaliação de Riscos (MAR)

*códigos de conduta, práticas instituídas ou princípios éticos. Pode traduzir-se em sanções de carácter legal ou regulamentar, na limitação das oportunidades de negócio, na redução do potencial de expansão ou na impossibilidade de exigir o cumprimento de obrigações contratuais*".

Muito mais do que assegurar a conformidade das práticas de negócio à totalidade da legislação aplicável a cada instituição (dependendo da atividade da mesma: bancária, de intermediação financeira e/ou de distribuição de seguros), deve ser assegurado que não existem violações quanto a:

- Determinações específicas dos supervisores (dependendo da instituição, do BCE, da EBA, da ESMA, da EIOPA, do Banco de Portugal, da CMVM, da ASF, entre outros);
- Regras de conduta e de relacionamento com os clientes, previstas nos códigos de conduta e demais normativo interno das instituições;
- Contratos e práticas instituídas na indústria e de princípios éticos (cabendo aqui os usos e costumes, conforme a natureza das coisas e, até, o Direito Natural).

Mas não basta que essas violações ocorram para que o risco de *compliance* se materialize, efetivamente.

Para esse efeito, será necessário que essas violações se materializem em sanções de caráter legal, na limitação das oportunidades de negócio, na redução do potencial de expansão ou na impossibilidade de exigir o cumprimento de obrigações contratuais e que dessas situações resulte, ainda, a probabilidade de ocorrerem impactos negativos nos resultados ou no capital da

instituição.

Tendo em conta o referido acima, é notório que as instituições são, efetivamente, uma das fontes mais relevantes, a par da legislação, do seu próprio risco de *compliance*, visto este risco decorrer, também, das regras escritas por si que vão para além da legislação e ainda dos contratos que celebram (com clientes e com fornecedores) e, dessa forma, o risco decorrer da sua própria cultura. Não são raras as vezes que temos identificado situações de materialização de risco de *compliance*, com enormes prejuízos para as instituições, até ao nível reputacional, devido ao incumprimento reiterado das suas próprias regras ou contratos, cujos requisitos não encontravam paralelo nem na legislação aplicável, nem nos usos e costumes da indústria.

A importância do órgão de administração e da função de *compliance* na gestão do risco de *compliance* começa exatamente aí: no momento da definição das *regras do jogo* que vão para além da legislação aplicável e dos usos e costumes. Na maioria das vezes, ser *mais papista que o papa* pode não dar bom resultado.

A aplicação do conceito de risco de *compliance* pelas instituições é efetuado, na prática, tendo em conta as suas atividades. A verificação dos requisitos legais a cumprir começa aí:

- Se a instituição se encontra registada para receber depósitos e proceder a prática de atividades bancárias, terá de garantir, em primeira instância, que as condutas da instituição garantem a conformidade de toda a legislação aplicável, quer ao nível prudencial, quer ao nível comportamental, incluindo o CRR II, o RGICSF, o Decreto Lei n.º 133/2009, de 2 de junho (crédito ao consumo), o

Decreto-Lei n.º 74-A/2017, de 23 de junho (crédito hipotecário), a Lei n.º 21/2018, de 8 de maio (serviços mínimos bancários), a panóplia de Avisos e Instruções do Banco de Portugal no âmbito da abertura de contas, do crédito e de outras matérias, o Anexo I da Lei n.º 35/2018, de 20 de julho (Regime jurídico da conceção, comercialização e prestação de serviços de consultoria relativamente a depósitos estruturados), as várias orientações da EBA (quando assim for especificado pelo Banco de Portugal através de Carta-Circular), entre muitos outros diplomas que regulam tantos outros temas da atividade bancária;

- Se a instituição se encontra registada enquanto intermediário financeiro junto da CMVM (dependendo sempre dos serviços principais e auxiliares para os quais for autorizado), terá de garantir que as que as condutas da instituição garantem a conformidade de toda a legislação aplicável ao nível comportamental, incluindo o pacote legislativo MiFID II/MiFIR (mercados e instrumentos financeiros), o pacote legislativo PRIIPs (instrumentos financeiros complexos), o pacote legislativo MAD/MAR (abuso de mercado), os vários Regulamentos e Instruções da CMVM, as orientações da ESMA (quando adotadas pela CMVM), entre muitos outros (incluindo os requisitos vertidos no Código dos Valores Mobiliários); e
- Se a instituição se encontra registada enquanto agente de seguros junto da ASF, terá de garantir que as que as condutas da instituição garantem a conformidade de toda a legislação aplicável ao nível comportamental, incluindo

> o pacote legislativo IDD (distribuição de seguros), as várias Normas Regulamentares e Circulares da ASF, as orientações da EIOPA (quando adotadas pela ASF) entre outros.

É aqui que, normalmente, o operador da gestão do risco de *compliance* começa a sentir as dificuldades da operacionalização da gestão desse risco, esteja ele inserido no órgão de administração, de fiscalização, na função de *compliance* ou num órgão de primeira linha de defesa. Afinal, estamos a falar, na melhor das hipóteses, de assegurar o cumprimento de centenas de milhares de páginas de requisitos (só o pacote legislativo MiFID II, segundo o Financial Times, tem mais de 33 mil páginas e mais de 1,5 milhões de parágrafos), às quais acrescem ainda (i) legislações de caráter transversal (bons exemplos são o pacote legislativo de prevenção do branqueamento de capitais e do financiamento do terrorismo, o pacote legislativo de gestão de dados pessoais – RGPD, a legislação fiscal, a legislação de práticas anti concorrenciais e as IFRS – requisitos contabilísticos e de relato financeiro); (ii) as regras e práticas internas que vão além da legislação e (iii) os usos e costumes da indústria.

Na nossa opinião, as instituições deverão refletir se estão a dedicar tempo e esforço suficiente a este momento, até porque apenas através desta identificação de fontes poderá ser executado, posteriormente, o exercício de identificação do risco de *compliance*, que é um dos cinco processos principais da gestão desse risco, nos termos e para os efeitos do Aviso do Banco de Portugal n.º 3/2020 e dos demais diplomas referidos *supra*.

## IV. Dos processos fundamentais da gestão do risco de *compliance*

Sabemos que o elencar de responsabilidades fundamentais dos vários intervenientes identificado *supra* tem um enorme potencial para aborrecer o leitor, mas considerámos que os *prós* da sua inclusão no presente artigo superavam os *contras*, especialmente porque (i) nos permite identificar claramente que a gestão do risco de *compliance* não é um tema da responsabilidade exclusiva da função de *compliance* (este é um dos mitos mais ouvidos na nossa prática, proferidos, por vezes, por que tem responsabilidades na gestão do risco de *compliance* que, ou desconhece, ou descura) e porque (ii) nos permite melhor enquadrar o leitor para a leitura da informação que pretendemos expor de seguida sobre algumas das práticas da função de *compliance* e a forma como as mesmas, na nossa opinião, podem (e devem) ser conduzidas para obter um adequado grau de eficácia e de eficiência.

A função de *compliance* deverá assegurar uma adequada governação e organização, deverá estabelecer os meios e metodologias mais adequados face às suas responsabilidades e à atividade geradora de risco de *compliance* e estabelecer os processos e procedimentos mais adequados para atingir os seus objetivos.

Para esse efeito, a função de *compliance* deverá garantir:

(i) que a sua estrutura normativa se encontra corretamente estabelecida;

(ii) que o seu posicionamento e autoridade e que a sua independência são inatacáveis;

(iii) que acompanha adequadamente a legislação e

regulamentação em vigor e a nova legislação que impacte ou venha a impactar a instituição e a sua atividade;

(iv) que identifica corretamente o risco de *compliance* nos seus vários elementos (recordamos o conceito de risco de *compliance*); (v) que tem a capacidade para avaliar e avalia efetivamente esse risco tendo em conta a probabilidade de ocorrência e a magnitude do impacto e que o consegue classificar numa hierarquia de importância ou relevância do risco;

(v) que monitoriza o risco de *compliance* numa perspetiva de *risk based approach* através de um programa próprio e estruturado de verificação do cumprimento;

(vi) que controla o apetite ao risco de *compliance* nos fatores estabelecidos pelo órgão de administração e tendo em conta os limites e as quebras definidas para esses fatores;

(vii) que reporta adequadamente os resultados da sua monitorização e controlo ao órgão de administração, ao órgão de fiscalização e, quando legalmente exigido, ao supervisor relevante;

(viii) que aconselha adequadamente os órgãos de administração e de fiscalização;

(ix) que promove a elaboração, a aprovação, a aplicação, a atualização e a verificação do cumprimento do código de conduta e participa na definição das políticas e procedimentos adequados à implementação das regras nele contidas;

(x) que participa na definição das políticas, procedimentos e normativos internos da instituição em matéria de conflitos de interesses e transações com partes relacionada;

(xi) que participa no processo de aprovação de novos produtos e produz relatórios sobre a aplicação dos processos de governação de produtos após a efetivação de análises periódicas aos mesmos;

(xii) que analisa previamente as transações com partes relacionadas;

(xiii) que mantém um registo dos incumprimentos identificados e comunicados ao órgão de administração e de fiscalização contendo as medidas de mitigação relevantes;

(xiv) que mantém um registo permanentemente atualizado das reclamações dos clientes e que procede à gestão dessas reclamações ou à verificação do cumprimento nesse âmbito caso a instituição tenha uma área dedicada a essa gestão, e

(xv) que elabora os relatórios relevantes (periódicos ou *ad hoc*) ao órgão de administração e ao órgão de fiscalização.

Para efeitos do presente artigo dedicar-nos-emos, assim, a identificar, ainda que sumariamente, algumas das práticas relevantes ligadas diretamente com o cumprimento dos processos de identificação e de avaliação do risco de *compliance*, deixando para um segundo artigo a identificação e análise de outros processos fundamentais, tais como o processo de monitorização e o processo de reporte do risco de *compliance*.

Antes disso, será relevante identificar, grosso modo, os elementos mais relevantes para o adequado posicionamento, autoridade e independência da função de *compliance*. Grosso modo, a função de *compliance* deverá:

- Ser estabelecida numa unidade de estrutura organicamente segregada das atividades que monitoriza e controla;
- Dispor de estatuto e autoridade suficiente para desempenhar as suas competências de forma objetiva e independente e de regulamento próprio aprovado pelo órgão de administração, depois de obtido o parecer prévio do órgão de fiscalização;
- Dispor de um plano de atividades aprovado pelo órgão de administração, depois de obtido parecer prévio do órgão de fiscalização;
- Desempenhar de forma independente as suas responsabilidades, não podendo os resultados das avaliações que desenvolve ser condicionados ou limitados, por exemplo, através da existência de disposições ou orientações internas quanto ao número máximo de deficiências identificadas ou do estabelecimento de qualquer relação, implícita ou explícita, entre as deficiências identificadas e a avaliação de desempenho dos colaboradores afetos à função, incluindo o seu responsável;
- Dispor de um responsável pela função e de um número suficiente de colaboradores permanentemente

qualificados, bem como de recursos materiais e técnicos adequados para o desempenho eficaz das suas responsabilidades;

- Dispor de sistemas de informação adequados, com acesso às informações internas e externas necessárias para cumprir as suas responsabilidades, incluindo informações respeitantes às filiais e sucursais da instituição (se existentes);
- Dispor de acesso total, livre e incondicionado a todas as funções, atividades, incluindo funções, processos e atividades subcontratadas, instalações próprias ou dos prestadores de serviços, bens e colaboradores, informações, registos contabilísticos, sistemas, ficheiros informáticos e dados da instituição;
- Dispor de acesso direto aos órgãos de administração e de fiscalização e aos comités de apoio àqueles órgãos, quando constituídos, por sua iniciativa ou por iniciativa de qualquer membro destes órgãos;
- Dispor do poder de, por sua iniciativa, transmitir qualquer informação ou remeter ao órgão de fiscalização diretamente, qualquer documento que considerem relevante, sem necessidade de pedido ou comunicação prévia ao órgão de administração e sem que este órgão possa obstar ao acesso direto à informação ou documento em causa pelo órgão de fiscalização.

Identificados os elementos fundamentais para esse efeito, é tempo de "mergulhar" nos seus processos fundamentais:

**(i) Identificação do risco de *compliance***

O processo de identificação do risco de *compliance* apresenta diferentes níveis de complexidade e de dificuldade consoante se está perante o primeiro exercício desse tipo por parte da função (novas funções ou funções que sofreram transformações relevantes para efeitos do cumprimento da legislação e regulamentação aplicável e que irão executar o exercício pela primeira vez) ou se se está perante uma atualização anual do exercício.

O exercício de identificação deve ser efetuado pelo menos uma vez por ano. Não obstante, não basta marcar uma reunião anual e, num par de horas, identificar o risco (mesmo para os exercícios de atualização anuais partindo de exercícios prévios).

Para que esse processo seja cumprido, a função deverá identificar toda a legislação e regulamentação aplicável num determinado momento (momento zero) e estabelecer processos diários de acompanhamento de nova legislação com impacto direto ou indireto na própria função de *compliance* ou na atividade da instituição. Para esse efeito, a função terá de garantir que "lança uma rede com a malha suficientemente apertada" para identificar toda a legislação e regulamentação relevante e, tão ou mais importante, que tem recursos humanos afetos a essa atividade qualificados para interpretar os diplomas que "ficaram na rede"[8]. Para esse efeito,

[8] A título meramente exemplificativo, poderão surgir diplomas potencial impacto direto ou indireto nas instituições com atividade bancária, de intermediação financeira e de distribuição de seguros são as seguintes: Assembleia da República; Assembleia Legislativa da Região Autónoma da Madeira; Governo; Governo da

esses recursos humanos deverão ter a capacidade de executar uma adequada interpretação jurídica dos diplomas e dos seus requisitos. Verifica-se que nem sempre os colaboradores afetos à função de *compliance* têm formação jurídica, o que poderá dificultar essa interpretação, mas isso não significará que não o possam fazer, desde que tenham acesso a formação adequada para o efeito.

Mas não bastará uma interpretação jurídica "feita pela rama". Consideramos que, por forma a garantir que se identificam os requisitos relevantes dos quais decorrerão risco de *compliance* para a instituição, os colaboradores afetos a essa atividade deverão ser capazes de executar uma atividade jurídica cunhada por Martin

---

Região Autónoma dos Açores; Tribunal Constitucional; Ministério das Finanças; Banco de Portugal; Comissão do Mercado de Valores Mobiliários; Autoridade de Supervisão de Seguros e Fundos de Pensões; Conselho Nacional de Supervisores Financeiros; Associação Portuguesa de Bancos; Associação Portuguesa de Fundos de Investimento, Pensões e Patrimónios; Associação Portuguesa de Seguradores; European Parliament and Council; European Commission; European Economic and Social Committee; Court of Justice of the European Union; European Central Bank; European Banking Authority; European Securities and Markets Authority; European Banking Authority/European Securities and Markets Authority; European Central Bank/European Systemic Risk Board; European Insurance and Occupational Pensions Authority; European Supervisory Authorities;
Single Resolution Board; European Payments Council; Euro Banking Association
Association for Financial Markets in Europe; European Fund and Asset Management Association; European Central Securities Depositories Association; Federation of European Securities Exchanges; European Economic Area Joint Committee; Bank for International Settlements; Basel Committee on Banking Supervision; Committee on Payments and Market Infrastructures; International Accounting Standards Board
Financial Stability Board; International Organization of Securities Commissions.

Kriele como *Prudentia.* Não o lemos no seu original alemão, mas ficou-nos marcado na memória pelas lições do Professor Pedro Pais de Vasconcelos durante o estágio. Tivemos a oportunidade de voltar a essas lições no Congresso de Direito Comercial, organizado pela Revista de Direito Comercial e Almedina, nos dias 17 e 18 de novembro de 2017, onde o Professor especificou, uma vez mais, que a *Prudentia* tem por fim a concretização da solução justa e adequada da questão à qual se pede ao Direito uma resposta, por oposição à *Scientia*, que tem como objetivo o conhecimento e a descoberta da verdade. Continuo a subscrever as lições do Professor, reforçadas uma vez mais nesse congresso: o Direito Comercial pende mais para a *Prudentia* do que para a *Sciencia*. E isso é notório logo no artigo 3.º do Código Comercial:

Código Comercial

*Art.º 3.º*

> *Se as questões sobre direitos e obrigações comerciais não puderem ser resolvidas, nem pelo texto da lei comercial, nem pelo seu espírito, nem pelos casos análogos nela prevenidos, serão decididas pelo direito civil.*

Este artigo, sobre o qual ouvimos várias lições do Professor no seu escritório e ao qual voltamos muitas vezes para garantir uma correta interpretação jurídica dos requisitos dos quais possam decorrer risco de *compliance* no âmbito da atividade bancária, de intermediação financeira e de distribuição de seguros, que mais não são, na nossa opinião, do que disciplinas extravagantes do Direito Comercial, é, na nossa opinião, a "chave mestra" para abrir a porta da adequada identificação do risco de *compliance*. Essa chave é a Natureza das

Coisas. Não de qualquer coisa, claro. Mas, certamente, a natureza do comércio e a natureza do Direito Comercial.

As fontes para a concretização da interpretação jurídica por parte do colaborador da função de *compliance* são claras:

Em primeiro lugar, vale a lei comercial (no presente caso de estudo, todos os diplomas identificados pelo colaborador da função de *compliance* como tendo o potencial de impactar a atividade da sua instituição, independentemente do seu tipo);

Em segundo lugar, devemos atender ao espírito da lei comercial (ou ao próprio Direito Comercial);

Em terceiro lugar, teremos de tentar a analogia com a Lei Comercial;

Só esgotados estes recursos, o Direito Civil será chamado a intervir.

Significa isto que, até esgotar a possibilidade de interpretação face à perspetiva mercantil (lei comercial, o seu espírito e a analogia com essa lei), não perderemos de vista a Natureza das Coisas e não entraremos na atividade pura da *Scientia*.

Assim, não podemos deixar de concluir que a interpretação da legislação e da regulamentação aplicável quer à função de *compliance* quer à atividade da instituição terá sempre como barómetro o comércio (mercado ou atividade) em que a instituição se insere. A interpretação jurídica no âmbito da gestão do risco de *compliance* parte do comércio para a conformidade e volta ao comércio para garantir que se encontra conforme. Não se deve sacrificar o negócio pela conformidade, se a única opção for a morte

do negócio e se essa opção não for razoável e justa. O texto da lei não pode ser contrário à Natureza das Coisas e sê-lo-á se não der à questão jurídica (de conformidade) uma solução razoável ou justa. Nos casos de perda de negócio sem lesão efetiva de bens jurídicos, a solução não é nem razoável, nem justa e acabará por, indo contra a Natureza das Coisas, lesar o próprio mercado.

Este parece ser, na nossa opinião, um tema pouco explorado pelos operadores da gestão do risco de *compliance* e pelos Comercialistas. Estranhamos essa situação por sempre nos ter parecido que este é um tema com uma importância única na gestão do risco de *compliance*, visto que indica o caminho para a sua operacionalização no dia a dia. O *compliance* para assegurar o comércio.

Esta parece também ser a separação fundamental entre as disciplinas de auditoria interna e de gestão de risco de *compliance*. Uma das opiniões mais comuns é a de que as duas disciplinas são uma e a mesma coisa, mas com posicionamentos diferentes no modelo das três linhas de defesa. A nós parece-nos claro que são disciplinas completamente diferentes, sendo a auditoria interna ligada diretamente à *Scientia* (enquanto descoberta da verdade e, dessa forma, enquanto disciplina forense sem ligação ao Direito Comercial) e a função de *compliance* ligada diretamente à *Prudentia* (e, dessa forma, à Natureza das Coisas, que é como quem diz ao espírito da lei comercial e, assim, ao Direito Comercial).

Para além da identificação do risco de *compliance* adveniente da legislação e da regulamentação aplicável, a função de *compliance* deverá ainda identificar, no dia a dia, em articulação com a primeira linha de defesa, os fatores, internos e externos em relação ao risco de *compliance* que a instituição está ou pode vir a estar exposta,

devendo para isso identificar todo o risco de *compliance* adveniente do normativo interno, dos princípios éticos e das práticas implementadas para os cumprir, dos contratos celebrados e dos usos e costumes das atividades que executa, na medida em que a sua violação ou não conformidade pode fazer incorrer a instituição ou os seus colaboradores num ilícito de natureza contraordenacional ou limitar as oportunidades de negócio, reduzir o potencial de expansão ou impossibilitar a exigência do cumprimento de obrigações contratuais.

A função de *compliance* deve ainda assegurar que implementa um fluxo de informação adequado com a função de gestão de riscos, no âmbito da gestão de riscos globais da instituição e que se aconselha com essa função para garantir o tratamento adequado da identificação do risco de *compliance*.

São vários os fatores de risco de *compliance* existentes e não existe propriamente uma lista fechada dos mesmos. A título de mero exemplo, poderemos identificar os seguintes:

- Estrutura de governo interno inadequada;
- Comercialização indevida de produtos;
- Ausência de segregação de ativos dos clientes;
- Manipulação de mercado.

Para assegurar um tratamento adequado da identificação do risco de *compliance*, garantida que está a sua adequada interpretação jurídica, consideramos que a função de *compliance* deverá especificar uma taxonomia do risco de *compliance*, identificando categorias de subriscos de *compliance* onde os diferentes fatores

poderão ser "arrumados".

A título de mero exemplo, poderemos identificar os seguintes subriscos, estando, no entanto, na disponibilidade de cada instituição o estabelecimento dos subriscos que considerar mais relevantes:

- Risco de conduta;
- Risco de governo interno;
- Risco de contratação;
- Risco de manipulação de mercado.

As atividades diárias de identificação dos fatores de risco de *compliance*, da sua interpretação jurídica e da sua classificação nos vários subriscos da taxonomia de risco de *compliance* permitem à instituição o cumprimento tempestivo do processo de identificação do risco de *compliance*, ficando a função pronta para passar ao segundo processo fundamental: o processo de avaliação.

Na nossa opinião, as instituições deverão dedicar o tempo e os esforços suficientes para identificar se o seu processo de identificação do risco de *compliance* se encontra corretamente implementado e se os recursos afetos às atividades que lhe dão corpo dispõem da formação necessária para assegurar a correta interpretação jurídica dos vários diplomas relevantes e dos restantes elementos de onde podem decorrer risco de *compliance* e se estabeleceram os fluxos de informação necessários e suficientes com a primeira linha de defesa e com a função de gestão de risco.

**(ii) Avaliação do risco de *compliance***

Após o exercício anual de identificação de risco de *compliance*, que, como vimos *supra*, é resultado de um conjunto de tarefas diárias da função de *compliance*, é necessário avaliar o risco de *compliance* para cada fator de *compliance* identificado.

Não existe uma exigência legal de forma para o exercício de avaliação do risco de *compliance*, apenas a necessidade de se assegurar, a final, que os fatores pertencentes a cada subrisco de *compliance* sejam avaliados tendo em conta dois vetores fundamentais: (i) a probabilidade de ocorrência do risco e (ii) a magnitude do impacto desse risco.

São vários os modelos para chegar a esse resultado. Não obstante, da nossa experiência, tendemos a destacar o seguinte modelo, que tem em conta algumas das melhores práticas de avaliação de riscos e que tem sido experimentado e aprimorado, primeiro, pelas funções de gestão de riscos e, nos últimos anos, pelas funções de *compliance*:

O primeiro passo é dado na política de gestão de risco global da instituição, onde deverá ser definida a matriz de avaliação de riscos tendo em conta os dois vetores referidos *supra*, com uma escala de quatro níveis para cada vetor e, dessa forma, com 16 incidências possíveis:

| | | | | | |
|---|---|---|---|---|---|
| **Magnitude do impacto** | **Elevada** | *Risco moderado* | *Risco material* | *Risco elevado* | *Risco elevado* |
| | **Material** | *Risco moderado* | *Risco moderado* | *Risco material* | *Risco elevado* |
| | **Moderada** | *Risco reduzido* | *Risco moderado* | *Risco moderado* | *Risco material* |
| | **Reduzida** | *Risco reduzido* | *Risco Reduzido* | *Risco moderado* | *Risco moderado* |
| | | **Reduzida** | **Moderada** | **Material** | **Elevada** |
| | | **Probabilidade de ocorrência** | | | |

Matriz de avaliação de riscos típica nas políticas de gestão de risco global e de gestão de risco de *compliance*

O segundo passo é dado com a inclusão de uma matriz semelhante na política de gestão de risco de *compliance*, que, dessa forma, respeita os requisitos da política de gestão de risco global (duas peças relevantes do *risk apetite framework* da instituição).

A aplicação do exercício de avaliação do risco tendo em conta as matrizes indicadas *supra* permitirá a hierarquização das subcategorias do risco de *compliance* constantes na taxonomia de risco de *compliance* da instituição e permitirá, desse forma, identificar as subcategorias materiais.

Para esse efeito, será necessária a elaboração e a utilização de uma ferramenta de avaliação de risco de *compliance* que permita recolher dois tipos de avaliação: (i) a avaliação qualitativa do risco de *compliance* da primeira linha de defesa e da segunda linha de defesa, incluindo da função de *compliance* e (ii) a avaliação quantitativa do risco de *compliance*.

A avaliação qualitativa pode fazer-se através a avaliação (ou autoavaliação) dos vários fatores de risco de *compliance* por parte dos responsáveis (Diretores) das unidades de estrutura da instituição que integrem a primeira linha de defesa e dos Diretores da função de gestão de risco e da função de *compliance*. É prática comum elaborar um questionário relativo a cada um dos fatores e obter a resposta desses *stakeholders*. A avaliação é feita tendo em conta os vetores da matriz de avaliação de risco e tendo em conta, dessa forma, uma escala de incidência que vai de 1 a 16.

Os resultados desse exercício qualitativo permitem perceber qual a visão sobre o risco de *compliance* destas linhas de defesa. É comum atribuir uma percentagem mais elevada no algoritmo (que irá permitir chegar a um resultado matemático) à visão da segunda linha de defesa e, por vezes, até um ponderador mais elevado para a função de *compliance*, mesmo face à função de gestão de riscos.

A visão qualitativa sobre o risco de *compliance* é depois confirmada pelos elementos que compõem a avaliação quantitativa, dos quais destacamos os dados históricos relativos ao acompanhamento dos indicadores de risco de *compliance* que integram o *Risk Appetite Statement* e, por vezes, os que não o integrando, são ainda assim acompanhados pela função de *compliance* no âmbito do seu apetite ao risco. As situações de aproximação aos limites de risco definidos ou de quebra desses limites são aqui bastante relevantes e deverão ter um peso também bastante relevante no algoritmo. Outros elementos que podem ser usados são a mudança histórica observada dos recursos humanos afetos à primeira linha de defesa ou à função de *compliance*, o histórico de deficiências ou incumprimentos e a evolução da legislação (volume e impacto). As boas práticas relevam ainda a

importância da inclusão de cenários de *stress* para cada um dos componentes que forem utilizados (os referidos acima e outros) que permitam verificar o impacto no risco de *compliance* nesses cenários stressados.

O mais importante é que no final a ferramenta permita obter uma visão do risco de *compliance* que se encontre alinhado com a Natureza das Coisas. Caso assim não o seja, poderá ficar reservada à função de *compliance* a aplicação do seu *expert judgement* para majorar os resultados por forma a aproximar os mesmos à sua visão, desde que essa visão seja razoável e justa.

A interligação da avaliação com um catálogo de requisitos dos quais decorre risco de *compliance* (alinhado com o conceito que especificámos *supra*), com um catálogo de controlos do risco de *compliance* implementados pela primeira linha de defesa face aos requisitos relevantes e com um catálogo de testes a efetuar pela função de *compliance* face a esses controlos será um passo de gigante para garantir uma monitorização do risco de *compliance* alinhada com uma perspetiva de *risk based approach*.

Na nossa opinião, as instituições deverão verificar se dispõem de uma matriz de risco de *compliance* alinhada com a matriz de riscos globais e que permita a verificação do risco face à probabilidade de ocorrência e à magnitude do impacto, bem como uma ferramenta de avaliação de risco de *compliance* suportada com os componentes relevantes (fatores de risco decorrentes dos subriscos identificados na taxonomia de risco de *compliance*, indicadores para o acompanhamento desses riscos (a título de mero exemplo: número de situações de comercializações indevidas; número de ausência de respostas a reclamações de clientes, entre outros), um algoritmo

capaz de calcular a avaliação de risco de *compliance* qualitativa e quantitativa e maturidade suficiente nas suas linhas de defesa para executar o exercício, bem como capacidade para executar testes de stress aos componentes quantitativos. Por fim, deverão ainda verificar se dispõem de catálogos de requisitos dos quais decorrem risco de *compliance* devidamente trabalhados e atualizados, catálogos de controlos de primeira linha de defesa (bem como processos de primeira linha devidamente mapeados) e catálogos de testes de *compliance* sobre esses controlos que permitam o adequado planeamento da monitorização, numa perspetiva de *risk based approach*. Como vimos acima, a execução eficaz e eficiente do processo de avaliação de risco de *compliance* depende de uma adequada execução do processo de identificação. Cumpridos corretamente os dois processos, a função de *compliance* estará, tendencialmente, capacitada para executar (numa perspetiva de *risk based approach*) a monitorização do risco de *compliance* e, a jusante, o reporte desse risco aos decisores (Órgão de Administração) e aos fiscalizadores (Órgão de Fiscalização). Parece simples… mas, na verdade, não é bem assim.

É por isso que pretendemos, num futuro artigo, complementar o atual através de uma incursão nos restantes processos fundamentais do risco de *compliance,* no seu posicionamento atual e na sua remuneração e incentivos, que nos permitirá refletir sobre a adequação ou inadequação do modelo atual de gestão *compliance*.

Roberto Bilro Mendes