Por Bernardo Gabineski (*)

O *compliance* digital atrelado ao efetivo treinamento de todos os envolvidos com a atividade empresarial é considerado uma parte vital que demonstrará que a sua empresa leva a sério a proteção privada dos dados dos clientes; mais ainda, demonstrará que a empresa está preparada para colaborar com as obrigações éticas e legais perante a sociedade e a justiça.

A sociedade contemporânea teve como um dos seus alicerces a evolução tecnológica. Essa evolução modificou de forma drástica o modo de comunicação entre as pessoas. Hoje a informação trafega por diversas plataformas. O *smartphone* tornou-se uma ferramenta indispensável para o mundo corporativo, pois facilitou a troca de dados, bem como as operações e as transações econômicas.

Muitos dos exemplos vistos recentemente nos escândalos de corrupção, envolvendo as empresas JBS e Odebrecht, tiveram, nos processos judiciais, informações digitais como meio de provas utilizadas pelo poder judiciário para efetuar buscas e apreensões de documentos (físicos e eletrônicos) e até expedições de ordem de prisão temporária.

É nesse cenário tecnológico que entra em tela a lei 12.846/13 e o decreto 8.420/15. O Brasil, por força das convenções assinadas junto à Organização dos Estados Americanos (OEA), à Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e à Organização das Nações Unidas (ONU), aprovou a Lei Anticorrupção e o decreto que entraram em vigor impondo um modelo de governança corporativa que incorpora o programa de integridade com mecanismos de controle capazes de detectar desvios, fraudes e irregularidades.

O decreto de 2015 surgiu com o intuito de regular a Lei Anticorrupção, estabelecendo diretrizes para o Processo Administrativo de Responsabilização (PAR). Nesse azo, a Lei Anticorrupção prescreve que a instauração e o julgamento de processo administrativo (para apuração da responsabilidade de pessoa jurídica) cabem aos órgãos de controle interno da União, dos Estados, do Distrito Federal e dos Municípios, no âmbito de suas competências; de forma isolada ou em conjunto com o Ministério Público ou com a Advocacia Pública; agindo de ofício ou mediante provocação. Ademais, estabeleceu o decreto que, no ato da instauração do PAR, a autoridade designará uma comissão, composta por dois ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará a pessoa jurídica para, no prazo de 30 dias, apresentar defesa escrita e especificar eventuais provas que pretende produzir.

Por outro lado, prescreve o decreto que caso a pessoa jurídica apresente em sua defesa informações e documentos referentes à existência e ao funcionamento de programa de integridade, a comissão processante deverá examiná-lo segundo os parâmetros indicados no capítulo IV para a dosimetria das sanções a serem aplicadas.

Pois bem, o artigo 42 do decreto em análise estabelece os parâmetros nos quais a autoridade competente utilizará para avaliar o programa de integridade. Em particular, o inciso XV tangencia a necessidade das empresas aplicarem um monitoramento contínuo do programa de integridade visando seu aperfeiçoamento na prevenção, detecção e combate à ocorrência dos atos lesivos.

Destarte, nesse novo cenário vivido pelo mundo corporativo, o controle tecnológico mostra-se como uma ferramenta indispensável para um bom programa de *compliance* e para a governança corporativa.

O monitoramento de mensagens via e-mail, celulares corporativos e plataformas eletrônicas utilizadas pelo negócio, bem como as transações eletrônicas financeiras e operações contábeis são alguns dos exemplos que devem ser observados na formatação de um programa de integridade.

Por outro, é importante salientar que não só esses cenários devem estar sob a ótica do *compliance*, mas também situações donde dados podem ser facilmente perdidos e ocasionarem uma grande dor de cabeça para a empresa. Imagine o cenário onde um diretor esquece em uma cafeteria o seu laptop contendo informações privilegiadas da empresa, como dados estratégicos, informações a respeito de um M&A ou dados valiosos sobre tecnologia.

Portanto, o *compliance* digital atrelado ao efetivo treinamento de todos os envolvidos com a atividade empresarial é considerado uma parte vital que demonstrará que a sua empresa leva a sério a proteção privada dos dados dos clientes; mais ainda, demonstrará que a empresa está preparada para colaborar com as obrigações éticas e legais perante a sociedade e a justiça.

(*) **Bernardo Gabineski** é mestre em direito corporativo, especialista em compliance, integrante da Comissão Especial de Seguro e Previdência Complementar da OAB/RS, integrante do Grupo Nacional de Trabalho de Proteção ao Seguro e Compliance e Grupo Nacional de Trabalho de Previdência Complementar aberta e fechada ambos da AIDA BRASIL (Associação Internacional do Direito do Seguro).

Fonte: Migalhas, em 18.09.2017.