Por Humberto de Sá Garay (*)

Muito se tem falado sobre a nova Lei Geral de Proteção de Dados brasileira – LGPD (n. 13.709/2018) e sua relação com a necessidade de instituir medidas de compliance em organizações públicas e privadas, para que todos possam estar em conformidade com as novas regras legais. Entretanto, também não se pode perder de vista a Lei Anticorrupção (n. 12.846/2013), de extrema importância para todas as corporações.

É por força dessa lei que qualquer corporação pode se ver envolvida em alguma investigação tão somente porque alguns de seus colaboradores internos ou parceiros externos estejam protagonizando ou participando de atos fraudulentos, notadamente em organizações públicas.

No que se refere à atividade de inteligência, o tema se relaciona com duas áreas importantes: o compliance de dados, no qual a doutrina e a metodologia de inteligência e de contrainteligência se prestam para a produção de informações e a sua consequente proteção; e aquelas inerentes às práticas comerciais, pelas quais a inteligência pode ser empregada para o monitoramento do time comercial, por exemplo, se de fato os contratos estão sendo realizados de acordo com as normas de compliance instituídas.

Quanto ao *due diligence*, vincula-se a investigações internas e externas contra eventuais práticas fraudulentas, além de produzir conhecimento para o desenvolvimento de negócios. Importante ressaltar que essas investigações não se limitam ao ambiente da própria empresa ou de suas atividades, mas alcançam também terceiros que atuem em conjunto com ela, em decorrência de parcerias, fusões ou aquisições.

Isso posto, na medida em que há a necessidade de reunir dados para a produção de informação ou conhecimento, há também a imperativa obrigação de proteção de todo esse manancial informacional, passos diferentes mas que integram o mesmo ciclo.

Tanto por força da LGPD, como da Lei Anticorrupção, é de se concluir que tantos os dados internos, como os de parceiros comerciais precisam de eficiente proteção, uma vez que a ingerência e a violação das regras legais protetivas de dados podem trazer riscos à empresa e às pessoas, os quais podem se manifestar principalmente na forma de responsabilidade civil ou outra consequência jurídica negativa.

Hoje existe o famoso ‘eu digital’, que nada mais é que comportamento do usuário na internet, observado via netnografia, diferente do monitoramento usado em investigação policial.

A netnografia é uma metodologia etnográfica que dá a ciência ou traduz o comportamento do usuário na internet. Busca-se saber o que ele curte, onde dá check-in, o que compartilha e os relacionamentos que estabelece com terceiros. Ao abastecer as redes, criamos o ‘eu digital’, analisado no *due diligence*.

O uso da tecnologia, neste ponto, é fundamental. Softwares que fazem busca em redes sociais e outras páginas públicas na internet, para traçar o perfil público das pessoas envolvidas no negócio, estão sendo cada vez mais utilizados.

Contextualizando com o ambiente corporativo, a partir do momento em que é estabelecida uma parceria, é importante pesquisar o que eventuais parceiros de negócios fazem, se estão envolvidos em escândalos, se estão sendo julgados, além das informações fornecidas em contrato. Isso tudo constitui uma fonte importante para o *due diligence* que, quando analisadas, diminuem possíveis riscos ao negócio.

Medidas para instituir compliance de dados e *due diligence* — é fundamental dispor de profissionais e recursos como tecnologia para executar tanto o compliance de dados quanto o *due*

diligence de forma adequada e eficiente, em conformidade com a LGPD e a Lei Anticorrupção. Nesse contexto, três medidas são importantes a serem empregadas: 1) a criação de um canal de denúncia; 2) o desenvolvimento de códigos de conduta; e 3) a instituição de um comitê.

Cada vez mais é comum a presença de **canais de denúncia** nas organizações. São utilizados para receber denúncias internas ou externas. Servem para expor um ato incomum e buscar transparência. Já existem softwares com foco nessa ação — acoplados a PABX, por exemplo — pelo qual um colaborador atende ligações telefônicas e pode, inclusive, gravar as chamadas. Sobre o conteúdo, é possível produzir inteligência e análise das informações.

Os **códigos de conduta** constituem uma ferramenta importante do *due diligence* para estabelecer as regras de compliance na empresa. Tratam-se de documentos que descrevem os princípios éticos e as normas de conduta para orientar as relações internas e externas de todos os colaboradores, fornecedores e parceiros.

As relações comerciais devem obedecer aos preceitos que darão reputação e credibilidade à empresa. Esses dois últimos fatores passam a ser um ativo da organização, cuja tangibilidade é difícil, mas precisam ser monitorados. Quais os valores cultivados? Excelência no cuidado ao cliente, atitude inovadora, responsabilidade socioambiental, ética e transparência, são alguns deles.

Descrever esses procedimentos em cada área é um desafio, porém é necessário criar uma estrutura para regulamentação interna, olhando a parte externa, para que os colaboradores tenham em mente as condutas estabelecidas em termos de atitudes, além dos procedimentos praticados em suas atividades. Demanda tempo, mas depois de realizado, oferece uma grande contribuição para a marca e o controle das informações.

Por fim, e não menos importante, é essencial construir um **comitê de conduta**. Caso haja alguma ação que não estava de acordo com as condutas previstas pela empresa, pode ser criado um comitê para fazer a gestão das denúncias coletadas.

Também será responsável por fazer a leitura sobre o resultado de um eventual *due diligence*.

Esse comitê geralmente possui membros permanentes — que fazem a assessoria jurídica, além de auditores internos — e volantes — que podem ser superintendentes, gerentes ou outros colaboradores eleitos. São eles que farão uma votação para dar transparência e justiça ao processo.

Essas medidas garantem a realização de um compliance de dados e de um *due diligence* eficazes, em conformidade com a legislação vigente, agindo em benefício dos negócios e do público envolvido, seja ele interno ou externo.

(*) **Humberto de Sá Garay**, consultor sênior em investigação e inteligência para segurança pública na **Dígitro Tecnologia**.

Fonte: **Fausto Macedo – O Estado de S. Paulo**, em 20.04.2019.