Alexander Coelho: Proteção de dados em processos de due diligence

Quando falamos dos cuidados que uma empresa direciona para a *proteção de dados*, estamos falando de uma implementação de *compliance*. É interessante refletir sobre a pertinência desse tipo de mecanismo de governança corporativa nas empresas, uma vez que o *compliance* visa a criar as condições para que ilícitos não ocorram, implementando um sistema de prevenção de reponsabilidade, bem como de cumprimento da legislação. Em outras palavras, trata-se de fomentar uma cultura de integridade, que

correto, independentemente de regulamentos específicos.

Algumas normas jurídicas possuem um nítido viés preventivo e, por isso, são mais relacionadas a *compliance*. É o caso, por exemplo, da Lei de Lavagem de Dinheiro (Lei nº 9.613/98), da Lei Anticorrupção (Lei nº 12.846/2013) e da *Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).* Além de possuírem imperativos de condutas diretos — presentes em todas as normas jurídicas — essas leis contemplam orientações indiretas de conduta, que são posteriormente internacionalizadas em estruturas de incentivo. Essas estruturas envolvem a criação de cargos específicos (exemplo: "encarregado de dados" na LGPD), padrões de conduta, reponsabilidades, sistemas de monitoramento, dentre outros.

Nesse sentido, quando falamos em processos de M&A (fusões e aquisições de empresas), analisar se a documentação de uma empresa está em *compliance* com a legislação vigente é de suma importância e zelo para o sucesso do negócio. Além disso, especificamente sobre o "valuation" das empresas, não é de hoje que o nível de maturidade de uma empresa em relação ao tratamento dos dados dos seus clientes/consumidores, bem como a ausência de incidentes de vazamento de dados ou a existência de um plano efetivo de resposta a eventuais incidentes, reflete diretamente no seu valor de mercado.

Exatamente nesse ponto que entra em cena o processo de *due diligence*, um processo analítico e investigativo sobre o grau de conformidade da empresa-alvo, com audição técnica sobre a saúde financeira e contábil, questões jurídicas e, inclusive, sobre o grau de adequação para *proteção de dados* , bem como uma análise antecipada sobre os riscos.

A entrada em vigor da LGPD, trouxe aumento significativo de importância dos dados pessoais com relação às transações de M&A. Em particular, o processo de *due diligence* de uma empresa está sujeito a novos requisitos e padrões, na medida em que se as atividades de tratamento de dados da empresa em avaliação não estiverem de acordo com a LGPD há um aumento de riscos significativos que poderão impactar tanto a saúde financeira da empresa, quanto a sua reputação.

Nessa seara, podemos destacar como um grande aliado no processo de *Due Diligence* o *Relatório de Impacto de Proteção de Dados (RIPD)*, por ser de um dos instrumentos mais essenciais em qualquer programa de governança em privacidade, ele nos possibilita averiguar os registros de regularidade e legalidade das operações de tratamento de dados pessoais realizadas por uma empresa.

Pois bem, nas operações de M&A é importante considerar que as práticas de privacidade e proteção de dados não são mais opcionais. A conformidade com a Lei Geral de Proteção de Dados coloca-se como uma obrigação legal, uma forma de diminuir riscos, garantir a integridade da organização pós-fusão ou aquisição e um definidor quanto à confiança que clientes e parceiros estão dispostos a depositar nela. Incorporar a análise quanto às práticas envolvendo dados pessoais no processo de *due diligence* melhora significativamente as chances de um negócio bem-sucedido.

De forma prática, na análise quanto às práticas envolvendo dados pessoais, alguns itens se tornam imprescindíveis para confirmar se a empresa-alvo respeita a lei no que tange ao nível de regularidade em proteção de dados, tais como: 1) verificar no Relatório de Impacto à Proteção de Dados (RIPD) quais foram as medidas técnicas e organizacionais adotadas nas atividades de tratamento de dados; 2) verificar a estrutura de privacidade existente, se há um Encarregado de Proteção de Dados (DPO) nomeado e um Comitê de Privacidade atuante; 3) consultar o histórico de incidentes com dados pessoais e as comunicações relacionadas à Autoridade Nacional de Proteção de Dados e outros órgãos setoriais, e aos titulares dos dados, bem como a existência de um plano de respostas à incidentes; 4) realizar ou consultar o assessment de dados pessoais. Por meio deste levantamento será possível dimensionar o volume de dados tratados e a quantidade de titulares envolvidos; 5) acessar todos os documentos de proteção de dados relevantes, como políticas e procedimentos, diretrizes, contratos e termos firmados; 6) verificar quem são os Operadores e Cooperadores envolvidos nas operações e os termos em que foram estabelecidas as atividades de tratamento de dados pessoais; 7) elencar todos os sistemas utilizados nas atividades de tratamento de dados; 8) relacionar as informações sobre quaisquer processos judiciais ou administrativos relacionados a LGPD; 9) levantar o fluxo de atendimento às demandas de titulares existentes e as áreas envolvidas no atendimento e 10) verificar se há necessidade de cumprimento de outras legislações sobre proteção de dados, nos casos em que há operações envolvendo transferência internacional de dados.

Desta forma, assim como outros aspectos contribuem diretamente para avaliação de uma empresa, influenciando o *valuation* de forma positiva ou negativamente, sem dúvidas, a análise do nível de adequação da empresa-alvo à LGPD, ou a outras legislações setoriais aplicáveis, será determinante para a fixação do valor de mercado após a diligência, merecendo especial atenção de todas as partes envolvidas no processo.

Date Created
24/01/2023