Opinião: As investigações corporativas e a proteção de dados

As empresas têm o dever de prevenir, detectar e apurar qualquer atividade ou processo que não esteja de acordo com as suas políticas internas e determinações legais, combatendo, assim, fraudes, corrupção ou até mesmo condutas antiéticas de sua equipe. Nesse contexto, visando a mitigar riscos, entram em cena as.

As investigações corporativas internas podem começar de diferentes maneiras, sendo os meios mais populares o canal de denúncia e as auditorias internas.

Inicialmente, um ponto de atenção a se considerar é o dever de manter *sigilo* sobre o levantamento primário a fim de apurar os fatos denunciados e obter a respectiva documentação probatória. Nesse momento, o acesso a informações, incluindo dados pessoais, deve estar restrito aos gestores desse processo. Finda a fase inicial, tanto investigados como outras partes envolvidas poderão ser informadas e trazidas ao processo.

Após a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD), a questão do tratamento de dados pessoais passou a ser objeto de discussão. Como a transparência é um dos princípios norteadores da LGPD, como tratar os dados em procedimentos de investigações corporativas sem comprometer o sigilo das apurações?

Considerando a natureza das investigações e as potenciais consequências danosas à empresa e à sociedade por eventual desconformidade jurídica, incluindo atos de corrupção realizados um de seus prepostos, manter o sigilo sobre os fatos é essencial para não colocar em risco todo o processo investigatório, ainda que o titular tenha solicitado informações sobre o tratamento de seus dados pessoais.

Assim, passemos a entender as exigências legais.

A LGPD, em seu artigo 4º, traz uma suposta vedação em realizar investigações preliminares às empresas, permitindo somente aquelas feitas pelo poder público.

No entanto, há de se considerar a obrigação legal da empresa em agir em cumprimento à Lei Anticorrupção, pois se assim não o fizer poderá ser responsabilizada administrativa e civilmente.

Em seu artigo 7º, a Lei Anticorrupção indica quais serão os pontos de análise para aplicação de eventual sanção. A *"cooperação da pessoa jurídica para a apuração das infrações"* e *"a existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica"* são dois deles.

Já a Lei do Combate à Lavagem de Dinheiro, em seus artigos 9 e 10, entre outros, também traz a necessidade de criar mecanismos internos para controle do caminho do dinheiro.

Considerando o Direito Comparado, é importante a análise do Regulamento Europeu de Proteção de Dados (GDPR) sobre o tema. O GDPR consolida o entendimento de que investigações corporativas entram no escopo da finalidade de interesse legítimo dos empregadores, desde que o tratamento dos dados pessoais do investigado seja apenas para satisfazer a essa necessidade e respeite os princípios do regulamento.

Portanto, de acordo com a interpretação doutrinaria e o entendimento europeu sobre o tema, não há restrição para o tratamento sigiloso de dados pessoais em procedimentos investigação interna corporativa. Mas há a necessidade de determinar a finalidade e a base legal adequada para fundamentar o referido tratamento.

A respeito da base legal de tratamento nos casos do canal de denúncia e investigações corporativas pode-se concluir que a LGPD traz como base mais adequada o cumprimento de obrigação legal ou regulatória pelo controlador.

É imprescindível informar referida finalidade de tratamento aos colaboradores e demais partes relacionadas, seja pela publicação de políticas de tratamento de dados pessoais, seja por meio de termo de ciência. Diante desse cenário, recomenda-se ao controlador de dados:

1) Utilizar somente os dados estritamente necessário para a investigação;

2) Adotar medidas para garantir a transparência em relação ao titular dos dados, sem que comprometa o necessário sigilo do procedimento investigatório, em atenção ao *princípio da razoabilidade*;

3) Incluir o canal de denúncias em seu mapeamento de fluxos de tratamento de dados pessoais e no relatório de impacto à proteção de dados pessoais;

4) Possuir o registro das operações de tratamento de dados pessoais que realizarem, conforme artigo 37 da LGPD;

5) Cumprir todas as boas condutas trazidas pelos princípios fundamentais da LGPD, a fim de mitigar riscos.

Dessa forma, ressalta-se a importância dos princípios da proteção de dados pessoais, mas errado seria dizer que se aplicam indiscriminadamente a todos os fluxos de tratamento de dados, independentemente da situação. É necessário ponderar as obrigações legais da empresa, como organização que poderá ser responsabilizada por atos daqueles que lhe representam.