

Bruna da Rocha: A LGPD e os acordos de leniência

A identificação de envolvidos em atos infracionais contra a Administração Pública e a obtenção célere de informações e documentos comprobatórios das práticas ilícitas são condições fundamentais para o êxito dos acordos de leniência, consoante estabelecem os artigos 16, II, da Lei nº 12.846/2013 (Lei nº 12.846/2015).



Para que isso seja possível, a empresa colaboradora inicia

uma fase de investigação interna após a celebração do acordo de leniência que visa à coleta de informações e provas por meio de diligências cujo alcance é o mais amplo acesso a dados e informações.

Ocorre que as medidas de busca adotadas nessa fase — como o acesso à máquinas, e-mails institucionais, banco de dados da corporação, documentos internos, perícias, entre outros — com frequência esbarram em dados pessoais de executivos, colaboradores e terceiros, o que, à luz da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados — LGPD), requer tratamento adequado e em consonância com a novel legislação.

O conceito de dado pessoal trazido na norma brasileira adota uma concepção expansionista, isso é, determina que qualquer informação que identifique ou que possa identificar uma pessoa física é um dado pessoal (artigo 5º, I).

Estão submetidas ao cumprimento da nova legislação as pessoas físicas que tratam dados pessoais para fins econômicos e todas as pessoas jurídicas. Não se enquadram na lei o tratamento de dados realizados por pessoas físicas para fins particulares e não econômicos e o tratamento de dados pessoais realizados para fins exclusivamente jornalísticos e artísticos, acadêmicos, de segurança pública, defesa nacional, segurança do Estado ou de investigação e repressão de infrações penais (artigos 3º e 4º).

A lei traz ainda um rol exemplificativo sobre as atividades consideradas como "tratamento de dados pessoais", sendo toda operação de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados (artigo 5º, X).



São quatro os personagens principais referenciados na LGPD: o titular dos dados, que é a pessoa física ao qual o dado se refere; o controlador, que é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; o operador, que é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; e o encarregado, que é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (artigo 5º, V ao VIII).

A ANPD, por sua vez, é o órgão vinculado à Administração Pública federal direta responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional (artigo 5º XIX e 55-A).

O tratamento de dados pessoais conforme os ditames da LGPD deve observar a boa-fé e os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (artigo 6º).

Ademais, quaisquer atividades de tratamento de dados pessoais somente podem ser realizadas se enquadradas em uma das dez bases legais previstas no artigo 7º da lei, consistentes: 1) no consentimento; 2) no cumprimento de obrigação legal ou regulatória pelo controlador; 3) na execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; 4) nos estudos por órgãos de pesquisa; 5) no cumprimento de contrato do qual o titular seja parte; 6) no exercício regular de direitos em processo judicial, administrativo ou arbitral; 7) na proteção da vida ou incolumidade física do titular ou de terceiros; 8) na tutela da saúde; 9) nos interesses legítimos do controlador ou de terceiro; e 10) na proteção ao crédito [\[1\]](#).

O não cumprimento das normas de proteção de dados pessoais sujeita os agentes às sanções administrativas a serem aplicadas pela autoridade nacional, de forma gradativa, isolada ou cumulativa, que consistem em advertência, multas de até R\$ 50 milhões, publicização da infração, bloqueio e eliminação de dados pessoais, suspensão de banco de dados e proibição do exercício de atividades de tratamento de dados (artigo 52).

No caso dos acordos de leniência, uma vez celebrado o acordo entre o poder público e a pessoa jurídica infratora, é inaugurada pela empresa a fase de investigação interna visando identificar agentes infratores e coletar as provas das condutas ilícitas necessárias para dar cumprimento ao acordo.

Nesse momento, verifica-se um intenso fluxo de dados e informações oriundos do acesso a equipamentos eletrônicos, bancos de dados internos, ferramentas de trabalho, caixas de e-mail institucionais, perícias, entre outros, condutas que, como se pode supor, frequentemente esbarram em dados pessoais de executivos, colaboradores e terceiros, que acabam sendo tratados e posteriormente compartilhados com o poder público.



No tocante à empresa, o tratamento dos dados pessoais que estejam no âmbito da investigação interna encontra respaldo na base legal prevista no artigo 7º, II da LGPD, o qual prevê o tratamento de dados pessoais para fins de cumprimento de obrigação legal ou regulatória pelo controlador. Para o fim de cumprir o acordo e, por conseguinte, os artigos 16, II, da Lei nº 12.846/2013 e 28, II, do Decreto nº 8.420/2015, a empresa colaboradora necessariamente precisa ter acesso às informações e dados que invariavelmente identificarão pessoas naturais, executivos, colaboradores e/ou terceiros, visando especificamente à coleta de informações e provas das condutas ilícitas que fundamentam o acordo de leniência.

Por sua vez, ao receber as informações e provas das condutas ilícitas contendo dados pessoais, o poder público deve tratá-los com base no artigo 7º, III, da LGPD, que autoriza o tratamento de dados pessoais pelo poder público para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Além disso, é necessário que todo o processo observe os princípios constantes no artigo 6º da lei, em especial a finalidade e adequação do tratamento, a real necessidade de uso de determinados dados, a segurança de que tais informações não serão utilizadas de forma inadequada ou ilícita de modo a causar prejuízos ao titular dos dados, a prevenção da ocorrência de violações e a responsabilização e prestação de contas quanto ao tratamento dos dados.

Nesse sentido, a empresa deve elaborar relatórios das operações de tratamento de dados pessoais contendo especialmente informações relacionadas a quais dados estão sendo tratados, a finalidade do tratamento, a forma de coleta, o plano utilizado para a segurança da informação e quem é o operador, conforme determinam os artigos 37 a 39 da LGPD [2], tudo a cumprir com o dever de *accountability*. Ademais, a atualização das políticas de privacidade e proteção de dados também são instrumentos que compõem a transparência e a prestação de contas.

Outra questão relevante é que a empresa colaboradora, na qualidade de controlador, deve proceder com a nomeação do encarregado para coordenar o tratamento dos dados pessoais coletados junto aos operadores (escritórios de advocacia ou empresas de auditoria que possam estar envolvidos na etapa de investigação interna) e ser o canal de comunicação junto aos titulares e a ANPD.

Acresce-se, por fim, que eventuais diligências de investigação internas realizadas em momento anterior à celebração do acordo de leniência também podem encontrar respaldo na base legal do legítimo interesse constante no artigo 7º, IX, da LGPD.

Isso porque, em tese, a empresa possui interesse legítimo de investigar desvios de condutas que possam configurar práticas ilícitas e gerar prejuízos financeiros e reputacionais à companhia.

Em casos assim, sendo compatível com a legítima expectativa do titular e os direitos e liberdades fundamentais, a investigação pode se dar consubstanciada no legítimo interesse, desde que observados todos os princípios da lei, especialmente a boa-fé, a finalidade, a adequação, a necessidade do tratamento e a segurança da informação.



A etapa de investigação interna dos acordo de leniência deve seguir em conformidade com as regras de proteção de dados pessoais, afastando novas penalizações e conferindo maior segurança jurídica ao processo de coleta de informações e provas.

No mais, a adequação da etapa de investigação interna dos acordos de leniência à LGPD certamente conferirá maior segurança jurídica à empresa colaboradora na medida em que ela terá certeza sobre quais dados devem ser coletados, tratados e compartilhados com o poder público, baseado nos princípios da finalidade e adequação. A diretriz quanto à segurança da informação também determina que os dados sejam devidamente gerenciados a fim de que não ocorram vazamentos, mitigando riscos reputacionais ligados à empresa e às pessoas físicas envolvidas na investigação.

[1] Para o tratamento de dados sensíveis, que são dados relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referentes à saúde ou à vida sexual, genéticos e biométricos, assim como nos casos de dados de crianças e adolescentes e dados tratados pelo poder público, o regime de bases legais e procedimentos de tratamento diferem da regra comum.

[2] Destaca-se, nesse ponto, que a doutrina é incipiente quanto à definição de uma responsabilidade solidária entre controladores e operadores em caso de incidentes envolvendo dados pessoais. Se a aplicação da norma brasileira seguir a prática da União Europeia, o controlador sempre será responsável por qualquer ilícito envolvendo o tratamento de dados; já o operador somente será responsabilizado em caso de falha na segurança da informação.