A LGPD e a necessidade de adequação emergencial das estruturas empresariais

Passos preliminares e fundamentais para a conformidade

Ana Frazão

Advogada. Professora de Direito Civil e Comercial da UnB. Ex-Conselheira do CADE.

Angelo Prata de Carvalho

Advogado. Mestre e Doutorando pela UnB.

A entrada em vigor da Lei Geral de Proteção de Dados (LGPD), após conturbada sucessão de adiamentos, trouxe consigo uma série de preocupações, mesmo antes da possibilidade de aplicação de sanções administrativas. Isso porque, com a LGPD em vigor, várias das obrigações dos agentes econômicos que tratam dados pessoais já são exigíveis - inclusive por meio de ações judiciais - seja por titulares, seja pelo Ministério Público ou por entidades cujo objeto esteja relacionado à proteção de direitos de privacidade ou dos consumidores como um todo.

Na verdade, considerando que todos os agentes econômicos lidam, em alguma medida, com dados pessoais, todos os modelos de negócio sofreram, em maior ou menor grau, os impactos da entrada em vigor da LGPD. Daí por que é um grave equívoco imaginar que a nova lei afetará apenas os negócios movidos a dados ou aqueles vinculados à chamada economia digital. Mesmo os negócios da economia tradicional ou pequenos negócios terão que lidar com as exigências relacionadas à proteção dos dados pessoais ao menos no que diz respeito aos seus trabalhadores e clientes ou consumidores. A mesma conclusão se aplica a profissionais liberais, como médicos e advogados.

Nesse sentido, tendo em vista a premência da implementação de medidas de adequação que minimamente façam frente às exigências básicas da LGPD, faz-se necessário o desenvolvimento de estratégias básicas de proteção de dados que, na falta de regulamentos nacionais que densifiquem as disposições gerais da lei já em vigor, observem diretrizes e boas práticas que protejam os direitos de titulares e mitiguem os riscos de responsabilização judicial dos agentes de tratamento de dados.

É sabido que a construção de um programa de conformidade tende a ser tarefa árdua, marcada por uma série de custos e um processo de implementação complexo. Isso porque a instituição de um robusto programa de *compliance* de dados exige a contratação de especialistas, a elaboração de um código de ética e de conduta, a avaliação permanente dos riscos, o investimento contínuo no treinamento de empregados, a contratação ou o treinamento de um encarregado de proteção de dados, o investimento em mecanismos de controle interno e de tecnologia da informação, dentre outros investimentos relacionados ao cumprimento da LGPD[1].

Acontece que, diante de um diploma já em vigor e já capaz de levar à responsabilização de agentes de tratamento de dados que não tenham adotado medidas de adequação de suas estruturas, muitas vezes não há tempo hábil para que se aguarde a implementação completa de um programa de *compliance*. Assim, diante do risco iminente de instauração de investigações civis pelo Ministério Público ou mesmo do ajuizamento de ações de responsabilização por titulares de dados ou outros entes legitimados, é de rigor que se estabeleça uma sistemática expedita de adequação da estrutura organizacional do agente de tratamento de dados à LGPD, sob pena inclusive de medidas judiciais que impeçam ou dificultem o funcionamento de determinadas atividades.

É claro que a implementação de uma estratégia expedita de conformidade à LGPD não pode dispensar uma análise individualizada que compreenda os mecanismos internos de funcionamento da organização de maneira concreta e imediata, sem a qual sequer seria possível obter o contexto geral do tratamento de dados por determinado agente.

1 Ver: FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Desafios para a efetividade dos programas de *compliance*. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. *Compliance*: perspectivas e desafios dos programas de *compliance*. Belo Horizonte: Fórum, 2020. p. 80.

Não obstante, seja no cenário de urgência para a implementação de uma política de conformidade, seja nas situações em que há tempo hábil para o desenvolvimento de todos os passos de um programa de *compliance*, é fundamental que se lance mão de estratégia emergencial multi e transdisciplinar para a conformidade com a LGPD. Dessa maneira, para além de se integrar todas as fontes jurídicas potencialmente relacionadas à proteção de dados, pode-se cogitar da implementação conjunta de soluções tecnológicas que, dentre outros elementos, mapeiem os fluxos de dados manejados pelas aplicações do agente de tratamento de dados e verifiquem eventuais brechas de segurança ou de privacidade nas aludidas aplicações.

Assim, a adequação emergencial à LGPD passa essencialmente por quatro pilares: (i) a avaliação preliminar dos fluxos de tratamento de dados e dos riscos associados; (ii) a adequação da estrutura organizacional para comportar uma estratégia de conformidade com a LGPD, notadamente por meio da indicação de encarregado de proteção de dados e da capacitação das diversas áreas existentes na organização em questão; (iii) a implementação de estratégia de comunicação eficiente seja no plano interno, seja no que diz respeito a agentes externos à organização; (iv) a adaptação dos ambientes digital e físico diante das preocupações com a segurança da informação.

A primeira etapa para que se possa iniciar o planejamento de uma estratégia de implementação emergencial das diretrizes contidas na LGPD indubitavelmente é a de avaliação dos fluxos de tratamento de dados e dos riscos associados às atividades do agente de tratamento de dados em questão. É a partir do mapeamento dos fluxos de dados que será possível compreender tanto a magnitude quanto a urgência do processo de implementação, de tal maneira que, apesar de as adaptações organizacionais serem possíveis mesmo antes ou durante essa avaliação preliminar, dificilmente será possível endereçar os problemas concretos da organização sem a adequada compreensão das situações e dos contextos nos quais o tratamento de dados ocorre.

Evidentemente que, para a implementação expedita da LGPD, nem sempre será possível que os fluxos de dados estejam completa e exaustivamente mapeados. Porém, é essencial para a própria construção da estratégia que a organização minimamente: (i) compreenda as situações nas quais se apresenta como agente de tratamento de dados, seja como controlador, seja como

operador; (ii) revise os instrumentos por meio dos quais realiza o tratamento, tendo em vista especificamente as hipóteses legais de obrigatoriedade de consentimento; (iii) esclareça as finalidades pelas quais realiza tratamentos de dados; (iv) verifique quem, e em que medida, pode ter acesso aos dados em questão, com especial atenção a eventuais transferências de dados (incluindo transferências intragrupo, a parceiros comerciais, a entidades de auditoria, a agentes sediados no exterior, dentre outras).

A segunda etapa consiste no estabelecimento de um conjunto consistente de mecanismos de comunicação interna – entre os diversos departamentos e áreas das empresas envolvidas – e externa – com vistas a operacionalizar o diálogo informado com o público a respeito do tratamento de dados pessoais. Por conseguinte, é necessário desde logo introduzir na estrutura organizacional das empresas envolvidas um encarregado pela proteção de dados, bem como alguém ou um comitê interdisciplinar interno que promova a interação entre os diversos departamentos da organização.

Nos termos do inciso VIII do art. 5º da LGPD, o encarregado 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)". O encarregado, nesse sentido, consiste em peça essencial na implementação de uma política de proteção de dados, na medida em que tanto centraliza informações relevantes a respeito do tratamento de dados realizado nas diversas áreas da organização em que se insere quanto toma a dianteira na resolução de eventuais questões que sejam encaminhadas à organização.

Em síntese, o papel do encarregado é o de servir como ponto centralizador de todas as demandas – internas e externas – relacionadas à proteção de dados, razão pela qual deve coordenar e supervisionar os departamentos envolvidos no âmbito da resposta às solicitações recebidas, das atividades de mapeamento e auditoria de tratamento de dados, das atividades de treinamento e formação de pessoal, dentre outros processos e tarefas relacionados à aplicação da LGPD. Daí a razão pela qual a indicação de encarregado pela proteção de dados é um dos mais importantes pontos da adaptação de curto prazo.

No entanto, a indicação do encarregado não é a única providência necessária à adequação da organização às demandas de centralização da comunicação interna e externa, muito embora se trate da obrigação normativa mais premente. Isso porque o encarregado não é fisicamente capaz de ocupar todos os espaços da organização em questão, razão pela qual deve ter interlocutores qualificados para que lhe enderecem adequadamente as informações e solicitações pertinentes ao cumprimento da legislação de proteção de dados. Com vistas a possibilitar o desempenho das funções do encarregado, notadamente quanto à coordenação e à promoção do diálogo entre as áreas das empresas, é aconselhável indicar representantes de cada um dos departamentos envolvidos, de maneira a mitigar interferências e centralizar a comunicação.

Em um segundo momento, a depender da estrutura da empresa, pode-se pensar na indicação de representantes dos departamentos relevantes à proteção de dados para o fim da implementação de comitê interdisciplinar de proteção de dados, voltado a contribuir tanto para informar a tomada de decisão quanto à implementação da LGPD quanto para sensibilizar os integrantes dos diversos departamentos a respeito do tema.

Em terceiro lugar, é fundamental capacitar tais agentes a responder a eventuais solicitações encaminhadas especialmente por agentes externos à organização que procurem compreender de maneira aprofundada a política de proteção de dados e/ou as finalidades do tratamento de dados ocorrido no interior da organização. É necessário, nesse sentido, esclarecer que o único sujeito competente para a resolução de eventuais questões atinentes à proteção de dados pessoais é o encarregado, razão pela qual os eventuais representantes de área devem ser imediatamente capacitados a encaminhar-lhe eventuais solicitações caso as recebam. O encarregado, por sua vez, deve estar capacitado para respondê-las da maneira mais completa possível, sempre ressaltando o estado atual de implementação da LGPD em que a organização se encontra, porém esclarecendo que já conta com estrutura adequada à gestão dos fluxos de dados e à resolução de eventuais solicitações que possam vir a surgir.

Nesse sentido, a resposta do encarregado deve ser informada por dados e eventualmente documentos encaminhados pelo representante da área competente, de maneira a oferecer argumentos coesos no sentido de demonstrar

o compromisso da organização com a proteção de dados, ainda que fazendo referência ao processo de implementação de uma estratégia abrangente de revisão das políticas de proteção de dados. Dessa maneira, pode-se construir uma estratégia de resposta a solicitações eficiente e expedita, notadamente com vistas a atender aos direitos de titulares de dados constantes do art. 19 da LGPD, que exige maior agilidade do agente de tratamento de dados, bem como outras solicitações como, por exemplo, de alteração de dados ou de encerramento do tratamento.

Em quarto lugar, é importante também tomar-se algumas medidas no sentido de (i) estabelecer respostas emergenciais a fragilidades eventualmente identificadas no processo preliminar de mapeamento de riscos e (ii) promover alterações na conduta dos integrantes da organização no sentido de incrementar a segurança da informação e mitigar riscos relacionados à proteção de dados.

No que se refere ao fornecimento de respostas a fragilidades identificadas no mapeamento de riscos, deve-se endereçar a questão à área competente, verificando-se especialmente se há algum dano, concreto ou potencial, que tenha sido produzido sobre titulares de dados. Ademais, deve-se lançar mão dos recursos necessários para a superação da fragilidade em questão (por exemplo, na hipótese de se ter identificado evento de segurança recente, deve-se proceder à correção da fragilidade detectada e da notificação dos sujeitos potencialmente afetados).

De outro lado, para além da postura reativa a ser desencadeada após o mapeamento ou após uma solicitação, pode-se lançar mãos medidas de segurança voltadas a mitigar riscos de maneira preventiva, como, por exemplo: (i) a implementação de procedimentos de controle de acesso; (ii) a proibição de acesso a dados que não são necessários para a execução das atividades do profissional em questão; (iii) a conscientização, mesmo na fase preliminar de implementação da política de conformidade, dos integrantes da organização a respeito da importância da proteção de dados; (iv) a análise constante a respeito da necessidade de continuidade do tratamento de dados, buscando-se especialmente eventos que conduzem necessariamente ao término do tratamento (como a morte do titular ou o encerramento do vínculo contratual); (v) a utilização exclusiva de servidores de e-mail validados pela organização

para envio de informações ou documentos atinentes às atividades profissionais, sendo obrigatória a utilização de e-mail institucional; (vi) a vedação a comportamentos que impliquem riscos de segurança ou de privacidade da organização, com especial atenção a acessos remotos (elemento relevante sobretudo no momento pandêmico, com a intensificação de atividades de *home office*).

Em síntese, pode-se afirmar que a implementação da LPGD certamente ainda produz uma série de desafios aos agentes de tratamento de dados, embora muito já se tenha produzido no sentido de construir uma melhor compreensão da proteção de dados no contexto brasileiro e já existam diversas diretrizes e guias de melhores práticas emitidos inclusive por órgãos oficiais de outras jurisdições, como é o caso da União Europeia.

No entanto, mesmo na ausência de regulamentação da LGPD pela ANPD, é fundamental que os agentes adequem sua estrutura à proteção de dados tanto para mitigar riscos de responsabilização quanto para a prestação de serviços que verdadeiramente estejam comprometidos com o respeito à privacidade de seus usuários.

Somente assim os agentes econômicos poderão estar preparados e capacitados para a produção de respostas a essas solicitações e, em última análise, para agir no sentido da preservação de seus modelos de negócios a partir do momento em que estejam em conformidade com a LGPD.

Link: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/a-lgpd-e-a-necessidade-de-adequacao-emergencial-das-estruturas-empresariais-03022021

Publicado em 03/02/2021