Por Humberto de Sá Garay (*)

Com a publicação da Lei nº 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), o Brasil passou a integrar o rol formado por mais de 100 países que podem ser considerados capazes de proteger satisfatoriamente a privacidade dos dados pessoais em larga escala. Embora a LGPD somente entre em vigor após 18 meses de *vacatio legis* (precisamente em 16 de fevereiro de 2020), desde já as organizações públicas e privadas precisam se preparar para adequarem suas atividades aos ditames da nova lei. E qual o melhor caminho para que as organizações empresariais encaixem suas práticas e rotinas nessas novas regras legais? Ter no compliance um aliado.

Assim como o compliance é adotado em outras esferas da cultura organizacional, notadamente na prevenção à lavagem de capitais, também pode ser um importante apoio na implementação de boas práticas da organização, seus colaboradores e fornecedores, na aplicação das diretrizes que regem a LGPD e nos cuidados com os dados pessoais daqueles que lhes fornecem informações. Portanto, a elaboração de um plano de governança de dados e a adoção de medidas de compliance devem ser elaborados e adotados desde agora, para evitar consequências jurídicas negativas num futuro próximo. E como delimitar esse conjunto de disciplinas internas? Seguindo os parâmetros previstos na própria LGPD, elencamos seis passos básicos que irão promover uma política eficiente de governança e compliance.

1. **Definição de um encarregado interno**

Deve-se designar um profissional, de preferência um especialista em proteção de dados pessoais ou de inteligência, para servir como elo comunicacional entre os titulares dos dados pessoais e a futura autoridade nacional, que irá regular e fiscalizar a aplicação da lei. Esse agente será responsável — internamente, na própria organização — por elaborar pareceres, avaliando riscos à segurança da informação e sugerindo medidas para eliminar vulnerabilidades, além de produzir relatórios de impacto à proteção de dados pessoais (entre outras tarefas, como prevê o artigo 41, da LGPD).

2. **Obtenção de consentimento para tratamento de dados**

O consentimento do titular é um dos principais aspectos da LGPD, sendo verdadeira decorrência lógica da privacidade e da autodeterminação informativa (dois dos fundamentos da LGPD). É também o primeiro requisito autorizador para o tratamento de dados (art. 7º, I). Portanto, é necessário que se colha a manifestação livre, informada e inequívoca do titular concordando com o tratamento de seus dados pessoais para uma finalidade determinada – sempre por escrito e constante em cláusula destacada. Além disso, nos casos de comunicação ou compartilhamento de dados com outros controladores, é preciso consentimento específico para tanto.

3. **Revisão das políticas de segurança da informação**

É preciso rever as medidas de segurança adotadas pela organização para prevenir, detectar ou corrigir possíveis violações a dados pessoais. Essa medida é importante, já que serve de atenuante em caso de eventual penalização administrativa.

4. **Elaboração de relatórios de impacto à proteção de dados pessoais**

Nesse documento devem constar todas as atividades de tratamento de dados, mencionando quais dados são processados, por quais motivos, quais medidas de segurança adotadas, identificação dos agentes de tratamento, etc.

5. **Reavaliação os dados pessoais e transparência**

Os dados já coletados e processados deverão ser reavaliados, verificando o objetivo de sua coleta e o correspondente fundamento jurídico. Também será necessário informar aos titulares sempre que houver a coleta de seus dados pessoais.

6. **Revisão de contratos com fornecedores**

Especialmente para aqueles que mantêm contratos com fornecedores, os quais possuem direta ou indiretamente acesso às informações, é prudente revisar os contratos firmados. No novo contrato, é preciso estabelecer novas cláusulas contratuais, prevendo a conformidade legal no tratamento dos dados pessoais, sob pena de responsabilização solidária.

(*) **Humberto de Sá Garay** é consultor sênior em Inteligência de Segurança Pública e Corporativa da Dígitro Tecnologia.

Fonte: Canaltech, em 05.10.2018.