

Lei geral de proteção de dados pessoais para não-advogados: 10 mitos e verdades

Por Filipe Fonteles Cabral

Neste breve artigo selecionamos 10 afirmações recorrentes entre empresários sobre o tema, nem todas verdadeiras. Entre fatos e mitos e verdades, seguem nossos comentários.

A Lei Geral de Proteção de Dados Pessoais (LGPD) entrará em vigor somente no dia 15 de agosto de 2020, mas já causa grande movimentação na comunidade jurídica. No meio corporativo, sobram dúvidas sobre o alcance da nova Lei e desconfianças sobre a real necessidade de conformidade.

Neste breve artigo selecionamos 10 afirmações recorrentes entre empresários sobre o tema, nem todas verdadeiras. Entre fatos e mitos e verdades, seguem nossos comentários.

1 - A Lei não vai pegar. Essa possibilidade é remota, qualquer que seja o ângulo de análise. Para citar três motivos: a) uma lei de proteção de dados efetiva é requisito para que empresas brasileiras continuem recebendo dados de indivíduos estrangeiros sem entraves burocráticos, isto é, por vias reflexas, trata-se de um importante pilar para o desenvolvimento da economia; b) o Brasil possui sólidas instituições de proteção a direitos difusos (como o direito do consumidor e o direito ambiental), sendo pouco provável que o direito à proteção de dados pessoais reste desamparado; c) os deveres previstos em Lei têm o potencial de movimentar uma nova “indústria de indenização”, equiparável ao volume de causas trabalhistas e consumeristas. Com tantos fatores em seu favor, é pouco provável que a lei se torne “letra morta”.

2 - A privacidade “morreu” na sociedade da informação. Não é verdade. Houve, sim, uma proliferação de usos abusivos de dados pessoais, por motivos tecnológicos e sociológicos que fogem ao escopo deste breve texto. Todavia, a confiança do consumidor no uso legítimo dos dados pessoais é força motriz da economia digital. Novas leis de proteção e dados vêm sendo aprovadas ao redor do mundo, com a criação de agências reguladoras e a figura do Data Protection Officer, isto é, novas instituições e profissionais dedicados exclusivamente ao tema. Mais viva do que nunca, a privacidade está em expansão.

3 - Dados disponibilizados na Internet tornam-se de domínio público. O mito da “Internet sem lei” foi debelado desde a década de 2000 pela indústria de conteúdo e algumas icônicas ações de proteção a direitos autorais. O mesmo raciocínio pode ser aplicado à proteção dos dados pessoais. A disponibilização voluntária de dados pessoais não implica na extinção de direitos e tampouco autoriza o uso da informação para finalidades diversas daquelas almejadas por seu titular.

4 - A obtenção de consentimento é imprescindível para a coleta e o tratamento de dados pessoais. Engano comum. A LGPD prevê 10 hipóteses de uso lícito de dados pessoais, sendo que o consentimento do titular é apenas uma das alternativas. Os dados também podem ser coletados e tratados para a execução de um contrato, para o cumprimento de obrigações legais e até mesmo para usos decorrentes de “interesses legítimos”. Recomenda-se que a revisão dos fluxos de dados e os respectivos enquadramentos nas bases legais sejam conduzidos por profissionais especializados.

5 - O dever de conformidade legal está limitado aos processos internos da empresa. Seguramente não. A LGPD é regida pelo princípio da responsabilização (dentre outros). Significa dizer que, além de responder pelos seus processos internos, a empresa também deve tomar precauções e adotar medidas de garantia de conformidade em relação aos seus fornecedores e parceiros comerciais com quem compartilha dados.

6 - Violações à privacidade nem sempre decorrem de vazamento de dados para ambientes externos ou invasões de hackers. Verdade. A LGPD prevê diversos deveres que

devem ser observados por qualquer pessoa física ou jurídica que realize a coleta e/ou o tratamento de dados pessoais. O inadimplemento dos deveres implica na violação das normas da LGPD. Exemplos de violação compreendem o armazenamento de dados pessoais por tempo indeterminado após o término do contrato, bem como o acesso aos dados pessoais por colaboradores que não exercem as funções profissionais que motivaram a coleta dos dados.

7 - A revisão da política de privacidade não é suficiente para a conformidade com a LGPD. Correto. Como visto no item anterior, são diversos os deveres previstos em lei, incluindo questões de natureza técnica (como gerenciamento de dados e segurança da informação) e de natureza jurídica (como a definição da base legal, a revisão de contratos, a elaboração de Relatórios de Impacto à Proteção de Dados, etc.). Portanto, a revisão da política de privacidade é apenas uma das diversas medidas que deverão ser adotadas por empresas que tratam dados pessoais.

8 - A LGPD exigirá uma mudança de cultura empresarial mesmo após a conclusão do projeto de adaptação. Sim, sem dúvida alguma. Os deveres decorrentes da LGPD se estendem por todo o tempo em que a empresa esteja coletando e tratando dados pessoais, ou seja, potencialmente para sempre. Por exemplo, ao gerenciar a proteção aos dados pessoais, a empresa deve ser capaz de responder a demandas de titulares de dados, fornecendo relatórios e excluindo ou anonimizando informações, nas hipóteses previstas em Lei. Além disso, como regra geral, novos produtos ou serviços que utilizem dados pessoais deve passar pelo escrutínio de uma avaliação de impacto aos dados pessoais.

9 - Não é obrigatória a criação de um novo cargo na empresa para a figura do Data Protection Officer. De fato. A LGPD prevê que o papel do DPO pode ser exercido por pessoas físicas ou jurídicas aptas a exercer sua missão. Não há na Lei qualquer obrigação de que o DPO pertença ao quadro de funcionários da empresa. Não há sequer a obrigação de que o Encarregado (DPO) seja um nacional ou uma pessoa sediada no Brasil. A escolha do perfil do DPO deve observar as características de cada empresa e, principalmente, o volume e a complexidade das operações de tratamento de dados.

10 - O armazenamento de dados em servidores de outros países serve para blindar a empresa do alcance da LGPD. Felizmente não. A LGPD, a exemplo de outras leis (como o General Data Protection Regulation – GDPR europeu), possui efeitos “extraterritoriais”. A Lei é aplicável a todos que realizem operações de coleta e/ou tratamento de dados pessoais, desde que a coleta e/ou o tratamento seja realizado no Brasil, que o tratamento vise à oferta de bens ou serviços no território nacional, ou que o tratamento tenha por objeto dados de indivíduos localizados no Brasil. Na prática, até mesmo empresas estrangeiras que não tenham representação no Brasil estarão sujeitas à LGPD.

Conclusão. A lei obriga a adoção de boas práticas de proteção de dados pessoais por parte de empresas que ofertem produtos ou serviços a indivíduos localizados no Brasil. Via de consequência, o marco regulatório dos dados pessoais possibilitará a reconquista da confiança de usuários da internet quanto ao uso responsável das suas informações em troca de produtos ou serviços cada vez mais personalizados e menos onerosos.

Serão mais usuários fornecendo dados pessoais, mais tratamentos realizados, mais algoritmos em desenvolvimento e mais modelos de negócio inovadores e disruptivos. A LGPD chegou para construir as bases de uma economia digital sólida e sustentável. Sairá na frente quem for capaz de entender a nova realidade, transformando o dever de conformidade legal em vantagem competitiva.

(*) **Filipe Fonteles Cabral** é sócio advogado do escritório [Dannemann Siemsen](#).

Fonte: Migalhas, em 16.07.2019.