Gabriel Fortes: Capacitação profissional e desafios da LGPD

Publicada em 2018, a Lei Geral de Proteção de Dados (Lei nº 13.709) [1] consolidou uma nova regulação sobre o modo como as empresas podem, ou melhor, devem tratar as informações pessoais de todo cidadão. Contudo, embora já conte quatro aniversários, a lei infelizmente é pouco conhecida nas suas entranhas pelos advogados, e parcamente ensinada nas faculdades, o que acaba gerando riscos para

Afinal, a LGPD já está em vigor, mas quase não há profissionais preparados para enfrentá-la. E, claro, sequer as próprias empresas estão adaptadas para esta nova realidade. Então, já que não estávamos tão prontos, por que publicamos uma lei como essa?

A lei era, na prática, inevitável, enquanto a digitalização da economia acontece ao passo que aumenta a conectividade e a troca de dados entre as pessoas. Por reflexo, o mercado vai se reestruturando a partir de estratégias orientadas por dados (*data driven*, como se diz), principalmente por dados pessoais. Alguma regulação sobre essa nova realidade era inadiável.

Partindo do pressuposto de que a manipulação de suas informações pessoais pode gerar riscos para o indivíduo, a LGPD veio com o objetivo de *"proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"* (artigo 1º). É certo que já existiam regras que protegiam a intimidade, a imagem e a identidade das pessoas, mas a lei é um divisor de águas neste tema.

De todo modo, embora seja comum imaginar que ela deve afetar apenas os grandes negócios digitais, suas normas, na verdade, são aplicáveis ao tratamento de dados realizado por qualquer tipo de organização (artigo 3º). Aliás, sobre isso há uma questão perigosa que precisa ser resolvida, pois ainda muitos empreendedores não compreenderam o que significa "tratar dados" de acordo com a nova legislação.

É que, pela definição legal, o tratamento de dados abrangeria basicamente todo tipo de ação realizada com informações relativas a pessoas (artigo 5º, X). Isto é, praticamente qualquer tipo de dado que permita individualizar alguém — ainda que de maneira indireta, ou mediante combinação de informações complementares — é considerado "dado pessoal", e, por conseguinte, o seu tratamento fica submetido às normas da LGPD.

Portanto, não parece viável delimitar quais atividades poderiam ou não estar enquadradas na previsão legal. Tudo vai depender do caso concreto. Mas, de regra, se há dados pessoais em jogo, aplica-se a lei. Acontece que provavelmente toda organização trata dados de indivíduos (sejam consumidores, empregados, sócios, fornecedores, parceiros, acionistas, representantes, associados, entre outros). E, ao lidar com dados pessoais, atrai para si a responsabilidade legal.

Assim, se toda empresa acaba realizando alguma forma de tratamento de informações pessoais (seja de empregados, seja de clientes), a relevância de compreender a LGPD e o seu impacto no mercado torna-se alarmante. Até porque a lei estabelece punições para quem cometer qualquer infração às suas normas. As penas vão desde uma advertência formal, até a proibição de atividades relacionadas a tratamento de dados, passando pela aplicação de multas, dentre outras (artigo 52).

Além disso, as empresas que, durante o tratamento de dados, ou em razão de realizá-lo, causarem algum tipo de dano à pessoa, seja patrimonial ou extrapatrimonial, deverão repará-lo integralmente (artigo 42). Ou seja, o impacto da nova regulação tende a ser extremamente sensível no mercado, até porque toda empresa agora deve adotar, por força da lei, medidas oficiais de segurança da informação e proteção de dados (artigos 46 e 47).

Afinal, como lidam com dados de pessoas em seus sistemas, diretórios e documentos, todas estão submetidas à LGPD — ainda que não saibam. Por consequência, encontram-se sujeitas às sanções administrativas e à responsabilidade por danos, ainda que seus administradores não tenham muita noção do risco. E, para piorar a situação, o número de ameaças e de incidentes informacionais aumenta a cada ano, o que tem gerado consequências significativas para organizações públicas e privadas, aumentando os custos financeiros do mercado, principalmente por causa de vazamento de dados [2].

Diante desse quadro, inúmeras normas estão surgindo mundo afora, com intuito de cobrar mais segurança e privacidade, não só para os usuários dos serviços digitais, mas em toda situação em que dados pessoais estejam envolvidos. Porém, à medida em que os governos criam regulamentos para garantir às pessoas a proteção de suas informações, as próprias empresas também precisam assumir o protagonismo, cada vez maior, e ter a iniciativa de liderar a adoção de novos padrões de privacidade e de gerenciamento de dados que possam acompanhar as novas demandas e necessidades [3].

E quem conseguir compreender — e implementar — isso primeiro, parte na frente, até porque se torna uma expectativa crescente no mercado. A privacidade tende a ser uma característica-chave do futuro, dos serviços, produtos e sistemas a serem disponibilizados no mercado daqui para frente.

Lá fora, as próprias empresas de tecnologia da informação e comunicação (TIC) passam a investir em modelos de negócio que, desde a concepção, protejam dados pessoais (*privacy by design*). Essa remodelagem será cada vez mais necessária à medida que a robótica e a inteligência artificial (AI) tornam-se mais comuns nos espaços públicos e privados [4].

Então, é neste contexto de novas regras, responsabilidades e expectativas, que, no Brasil, as organizações precisam reciclar seus modelos de negócio e suas práticas de gestão, para inserir métodos de gerenciamento de riscos de modo a atuar, de maneira preventiva, sob orientação da LGPD. É importante destacar que incidentes de segurança digital podem afetar uma empresa em várias dimensões, causando danos à imagem, ineficiência operacional, baixas financeiras, interrupção de serviço, entre outros. Ou seja, a baixa segurança de dados pode diminuir a competitividade, atrasar a capacidade de inovação e afetar a sua posição de mercado – fatores que destroem qualquer negócio, por mais promissor que seja.

É necessário incorporar ao vocabulário empresarial o adequado gerenciamento de riscos (*Enterprise Risk Management*), de modo a minimizar a frequência e o impacto negativo dos incidentes e, ao mesmo tempo, explorar, de maneira segura, as vantagens e possibilidades da transformação digital [5].

Investir em segurança e privacidade pode se tornar a maneira mais fácil de agregar valor à marca, neste novo ambiente normativo, que pode se mostrar muito seguro para a inovação, desde que haja adequação à LGPD.

Notas

[1] Ver em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[2] Disponível em: https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

[3] Disponível em: https://www.sciencefocus.com/future-technology/new-technology-trends-2020s/

[4] Disponível em: https://www.accenture.com/_acnmedia/Thought-Leadership-Assets/PDF-2/Accenture-Technology-Vision-2020-Full-Report.pdf

[5] Measuring digital security risk management practices in businesses | READ online (oecd-ilibrary.org)

Date Created
27/11/2022