

Por Enio Klein (*)



2020 é o ano da privacidade no Brasil. 16 de agosto próximo é o “dia D”, quando entraremos para

o grupo de países que passam a possuir regras claras para o uso de dados pessoais de seus cidadãos.

Falta pouco mais do que 180 dias para que a Lei Geral de Proteção de Dados, a LGPD, entre em vigor, e o que vemos é um ambiente confuso. Grande parte dos empresários, empreendedores ou executivos de organizações de todos os tamanhos ainda não têm a clareza do que precisam fazer em relação ao tema.

Aqueles que não desejam regras sobre o uso dos dados pessoais falam em adiamento, abrandamento ou outras formas de procrastinação, para que possam continuar a fazer o que estão fazendo, sem restrições ou formas de controle. Muitos de nós, a quem a lei protege, sequer sabe de que se trata a legislação. O governo, cuja responsabilidade é mediar a aplicação da lei, não cumpre a sua parte, e a “Autoridade Nacional de Proteção de Dados”, a quem caberá a regulamentação e a interpretação dos procedimentos estabelecidos pela legislação, não saiu do papel.

Sempre que o cenário é confuso e as diretrizes não são claras, prospera o ambiente ideal para as interpretações e para os oportunistas de plantão. Quanto mais perto do “dia D”, mais cuidado as organizações precisam ter, no sentido de encaminhar uma jornada de conformidade que lhes permitam cumprir, de uma forma mínima, a nova legislação neste primeiro momento, dentro das possibilidades e realidades de cada negócio.

Embora seja uma lei, a adequação à LGPD não é uma questão só para advogados. Da mesma forma, só porque uma das disciplinas envolvidas aqui seja segurança da informação ou tratamento de dados, também não significa que seja um assunto de TI. Nas organizações grandes, particularmente expostas e, supostamente, bem organizadas, o conflito parece resolvido, pois a cultura da governança e conformidade já é praticada e exigida. E quanto as outras, as médias e pequenas? Como sair desta encruzilhada?

Nos projetos em que tenho tido oportunidade de participar, vejo a frequente polarização entre o jurídico e a tecnologia da informação. Se, por um lado, a preocupação jurídica é se ater a interpretação da lei na organização, a TI se preocupa com os orçamentos e a possível necessidade de adquirir novas ferramentas, para fazer frente às necessidades que a lei venha a impor para a segurança da informação. Não existe razão única em nenhum dos polos. Não se trata de interpretar a lei para ter certeza de que todos os artigos e parágrafos estejam sendo cumpridos ou não, assim como não são as ferramentas tecnológicas que farão que as organizações atendam às práticas que a lei endereça. A LGPD se baseia em práticas de privacidade e proteção de dados, já há muito tempo estabelecidas e usadas em diversas regiões do mundo, assim como a europeia GDPR. Se essas forem cumpridas, provavelmente a legislação também o será.

O desafio a ser vencido é descobrir como o negócio irá se adequar para que as práticas de privacidade e proteção de dados sejam seguidas. Não se trata do direito e nem da tecnologia. Trata-se de um modelo de governança que estabeleça, da melhor forma possível, formas de como as práticas necessárias para a garantia da privacidade e proteção de dados sejam adotadas e executadas no dia a dia nos processos de negócio.

O papel do direito é validar o modelo de governança à luz da legislação para certificar de que será suficiente. O da tecnologia, de garantir que infraestrutura, processos e ferramentas irão suportar os recursos necessários e suficientes para que os mecanismos de governança estabelecidos possam ser respeitados. Entre um e outro existe a continuidade do negócio, que é o verdadeiro objeto da adequação.

Sob o ponto de vista do negócio, é importante entender a razão da importância sobre o uso dos dados pessoais e como eles são usados na organização. Como falar em lei de proteção de dados sem entender a razão de negócio que leva uma organização a precisar usar dados pessoais? Como discutir finalidades e bases legais, sem levantar quais os ciclos das informações dentro da empresa e onde elas são usadas? Como proteger dados sem saber quais precisam ou não ser protegidos? Qual o intuito de proteger dados se não soubermos quais são realmente necessários ao negócio e

quais não são?

Entendemos que a jornada da conformidade começa com o negócio, e não com a lei. Entender a necessidade do negócio em relação ao uso de dados pessoais irá determinar como cada um deles precisará desenvolver seus modelos de governança para torná-los conformes às melhores práticas e, conseqüentemente, aptos a atender a legislação. É o que a adequação significa. Começar pela lei e aplica-la simplesmente sobre o que a empresa está fazendo não é adequação. É preparar defesa em caso de problemas. Comprar ferramentas pelas funcionalidades e não para respaldar necessidades reais e identificadas, tampouco é adequar-se. É gastar dinheiro possivelmente à toa.

Ainda temos um longo caminho a percorrer até que a sociedade como um todo entenda a importância desse assunto. Ainda falta um pouco para que se entenda que a proteção de dados e privacidade não é uma disciplina do direito ou da tecnologia. Envolve o direito, envolve a TI, mas é uma disciplina de negócios que precisa permear as organizações em todos os seus níveis. Do mais alto executivo a cada um de seus funcionários. Adequar-se não é um fardo, mas um movimento rumo ao futuro e a competitividade.

(*) **Enio Klein** é CEO da Doxa Advisers, professor de Pós-Graduação na Business School SP, especialista em Transformação Digital, em vendas, experiência do cliente e ambientes colaborativos.