

Por Filipe Ribeiro Duarte (*)



A adequação à LGPD (Lei Geral de Proteção de Dados) é uma das pautas prioritárias das empresas neste ano de 2022, ao lado de temas como a implementação da agenda ESG. A LGPD ganha ainda mais destaque com a divulgação, por parte da ANPD (Autoridade Nacional de Proteção de Dados), agora no início do ano, das regras para a aplicação das penalidades determinadas na lei. Conforme previsto nas normas da ANPD, estas penalidades podem ter efeito retroativo a agosto do ano passado, época do início da aplicação das sanções.

Descumprir a LGPD pode provocar duras punições, tais como bloqueio dos dados pessoais objeto da infração, além das multas, que podem chegar a 2% do faturamento da empresa ou até R\$ 50 milhões por infração, sendo estas sanções bem impactantes. O risco de infringir a lei, muitas das vezes, pode estar associado a outro prejuízo sofrido pelas empresas: os ataques cibernéticos.

Apenas em 2021, segundo levantamento da Psafe, uma das principais empresas de segurança digital da América Latina, mais de 600 milhões de dados foram vazados em três grandes ataques cibernéticos que ocorreram em janeiro, fevereiro e setembro. Além disso, de acordo com o estudo, foram 44,5 milhões de tentativas de estelionato virtual e 41 milhões de bloqueios de arquivos programados para invadir redes das empresas e roubar ou sequestrar dados.

Com tantas ameaças, riscos e possibilidades de sanções, é necessário que haja uma maior conscientização por parte das corporações e de seu alto comando em relação à importância de se proteger os dados, garantir a segurança das informações e cumprir a LGPD.

E isso já está ocorrendo, segundo a Global Digital Trust Insights Survey 2022, da consultoria PwC, realizada com 3,6 mil executivos de negócios, tecnologia e segurança, sendo 124 deles no Brasil, entre julho e agosto de 2021. A pesquisa constatou que investimentos em segurança cibernética continuam em alta, sendo que 83% das organizações no Brasil e 69% no mundo preveem elevar os gastos cibernéticos em 2022. Em 2020, estas porcentagens foram de 55% e 57%, respectivamente. E para 45% dos executivos brasileiros ouvidos (26% no mundo), esse aumento de gastos será acima de 10%.

A grande maioria dos executivos já percebeu que as organizações se tornaram muito complexas e que protegê-las passou a ser uma tarefa árdua, porém cada vez mais necessária para evitar exposição a riscos cibernéticos e de privacidade.

O sequestro de dados é o crime mais comum que atormenta as organizações, no qual os hackers roubam os dados, criptografam e exigem uma espécie de pagamento de resgate para que os dados voltem aos sistemas das empresas. Os criminosos muitas vezes também exigem um valor extra em troca da não divulgação dos dados capturados. Enquanto isso, as operações podem estar sendo afetadas total ou parcialmente, por dias e até semanas.

Diante deste cenário, o trabalho de adequação à LGPD deve ser iniciado e perenizado nas organizações. Inexiste saída diferente, pois a dinâmica das relações empresariais, surgimento de novos produtos ou serviços, parcerias criadas e o que é feito com as informações nesse contexto mudam o tempo todo, exigindo um acompanhamento de perto pelas empresas.

Por isso, destaca-se a importância de gerir os riscos relativos à LGPD, seja mediante a identificação deles, a escolha cuidadosa dos parceiros comerciais que já estejam adequados ou em processo de adequação e, naturalmente, o ajuste contratual das relações, empresariais ou trabalhistas. Muitos têm buscado proteção nos seguros, como forma de prevenir o caixa diante de eventuais condenações. É importante ter à vista que as seguradoras também exigirão maturidade dos segurados na hora da celebração dos contratos de seguro. Logo, não resta saída senão a adequação contínua à LGPD.

Um plano de ação atualizado para tratar as crises decorrentes de violação de dados é outro fator relevante neste universo, para que as corporações consigam dar respostas rápidas em ataques cibernéticos, sem comprometer sua operação e imagem. Este plano vai dar agilidade e direcionamentos para a empresa agir em caso de vazamentos. Essa velocidade de resposta,

inclusive, é exigência da própria LGPD e da ANPD. É importante lembrar que, a depender da gravidade do incidente, a situação precisa ser comunicada aos titulares e à ANPD.

Diante de um risco que pode acarretar muitos problemas, o cumprimento da LGPD e o aumento dos riscos cibernéticos entraram definitivamente na pauta de discussões prioritárias das diretorias das organizações como temas necessários aos negócios.

(*) **Filipe Ribeiro Duarte** é Mestre em Direito Empresarial pela UERJ, advogado especializado em direito digital do Martinelli Advogados em Joinville (SC).

19.01.2022