Souza Lopes: LGPD, limiar entre gasto e investimento

Por experiência própria, não são necessárias complexas pesquisas de campo para identificar que a maior parte das empresas não estão adequadas à Lei Geral de Proteção de Dados (LGPD) [1], seja pelos custos envolvidos ou pela sensação de que se trata meramente de uma burocracia legal, sem benefícios palpáveis para a empresa adequada, e em certo ponto devemos dar razão aos empresários, mas não pelos

Quando em vigor (em agosto de 2021), a LGPD causou um alvoroço, especialmente no meio jurídico, com um número considerável de advogados e profissionais da informação buscando qualificações e se preparando para um possível *'boom'* de empresas que, supostamente, estariam ansiosas para atingirem a conformidade com a lei. Na realidade, um cenário bem mais tímido e que, para muitos, causou um certo desconforto.

Um dos motivos e primeiro problema que podemos identificar neste cenário é a ausência de uma cultura de privacidade e proteção de dados e que não se restringe apenas à LGPD, é um padrão para leis com objetivos semelhantes. Mesmo com dezessete meses da vigência, muitos empresários desconhecem a lei e mesmo a necessidade de proteção dos dados pessoais próprios, e aqueles que vislumbraram algum contato com lei, geralmente por meio de fornecedores ou parceiros de grande porte, não compreendem os riscos envolvidos.

Não é incomum ouvirmos de empresários o clássico, e infeliz, bordão "essa lei não vai dar em nada, logo vai ser esquecida", como justificativa para não aplicação. Neste caso não poderia estar mais longe da verdade, havendo, inclusive, a adição de proteção de dados na Constituição Federal como direito fundamental [2]. Entretanto, o principal problema não estava relacionado à memória coletiva ou esquecimento da lei, mas, sim, à falta de conhecimento sobre sua aplicabilidade e benefícios em contraponto aos ônus e consequências da não conformidade, e, aqui, é pertinente um panorama sobre os riscos (efetivos e reais) da não conformidade.

Costumo dizer (e ouvir) que o medo é um dos maiores motivadores, não que seja sempre positivo, mas cumpre seu propósito muito bem, especialmente quando há necessidade de garantir a segurança, coletiva ou individual. E no caso da privacidade e proteção de dados essa motivação tem seu papel de destaque.

Como exemplo prático, em 2016, um cliente teve dados de seus produtos (projetos sigilosos de engenharia) vazados para um concorrente, o que foi descoberto apenas dois anos depois do incidente, gerando um prejuízo significativo nas vendas. O motivo está longe de ser um ataque organizado realizado por um *black hat* (hacker criminoso), mas, sim, falta de políticas básicas de *compliance* e restrição de acesso: um funcionário novo com acesso irrestrito aos servidores. Algo que um advogado diligente poderia ter detectado e resolvido nas primeiras análises de riscos de *compliance* ou de avaliação para aplicação da LGPD, o que não havia na época.

Em 2017, uma indústria sofreu um ataque localizado nos seus servidores, interrompendo a produção por horas e criptografando diversos dados essenciais. Novamente, o mesmo resultado, perdas financeiras. O motivo: uso de *softwares* não originais, sem atualização periódica. Mais uma situação danosa, facilmente resolvida com políticas básicas de segurança e privacidade de dados.

Em 2019, um tabelionato de notas identificou que dados do seu servidor haviam sido copiados, contento desde modelos de escrituras à informações pessoais dos clientes e cópias de documentos oficiais. O computador utilizado não havia registro individualizado de acesso e estava fora do campo de visão das câmeras de vigilância. Dois problemas, duas soluções simples de *compliance* e proteção de dados e um risco potencial gravíssimo.

Apenas três casos, dentre tantos outros, com incidentes da informação à espreita de empresas de qualquer segmento e porte, situações comuns com consequências evitáveis.

Se o risco informacional não for motivo suficiente para avaliar os benefícios da lei, ainda existe o temido risco reputacional. O relatório global *"Consumer appetite versus action: the state of data privacy amid growing digital dependency"* [3], publicado em 2021, destaca que cerca de 50% dos brasileiros evitaria contratar serviços de empresas que sofreram violações de dados. Não se trata de atrasos ou gastos com recuperação de arquivos, mas, sim, um dano que pode ser permanente, a confiança dos clientes.

Apenas para termos uma mínima noção do quão suscetíveis estamos no ambiente digital, em 2021, segundo a Kaspersky [4], os ciberataques no Brasil cresceram 23%, somando cerca de 481 milhões de tentativas de infecção de janeiro a agosto. A falta de cultura e educação digital apenas agravaram as consequências, garantindo que o país tenha se tornado o preferido na América Latina pelos cibercriminosos.

A conscientização não deve, preferencialmente, iniciar no cliente, mas sim no profissional, especialmente no advogado, com sua obrigação ética de instruir corretamente seus clientes a cerca das leis, instruindo-os sobre os riscos potenciais, os benefícios e a necessidade legal, e ainda oferecendo soluções para prevenção. E nesse sentido cabe uma fuga ao tema, mas perfeitamente justificável: existe uma urgência em deixarmos as rivalidades e o concorrencialismo de lado e olharmos nossos colegas de classe como parceiros e não como competidores. Firmar parcerias para oferecer o melhor disponível não é entregar o cliente, mas demonstrar zelo. Ainda na fuga ao tema, um clichê profissional é bem aplicado aqui, *"aquele que é especialista em tudo, não é especialista em coisa alguma"*, é necessária a consciência de que precisamos garantir a melhor conformidade dos clientes e isso implica em não sermos os responsáveis em algumas situações. Conscientização, necessariamente, depende de conhecimento, para transmitir a informação corretamente e da melhor maneira, imprimindo a seriedade necessária que o tema requer.

Por experiência, quase a totalidade das empresas que buscaram a conformidade com a LGPD até agora se dividiam em dois grupos bastante distintos: as que precisavam se adequar por exigência de negócios e aquelas que tiveram contato com os riscos. Nos dois casos, a percepção sobre o tema é a única coisa que as diferencia, pois os riscos são os mesmos e suas consequências também.

Não é difícil estabelecer um limiar entre aquilo que é considerado um gasto e outro que pode ser considerado um investimento, os riscos e benefícios falam por si. Quando não se sabe que existe um risco ou um benefício, todo dinheiro despendido é mal usado.

O limiar entre o gasto e o investimento é a conscientização.

[1] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018.* Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 3 mar. 2022.

[2] REVISTA CONSULTOR JURÍDICO. Proteção de dados pessoais passa a ser direito constitucional. *Consultor Jurídico,* [*s. l.*], 11 fev. 2022. Disponível em: https://www.conjur.com.br/2022-fev-10/protecao-dados-pessoais-passa-direito-constitucional. Acesso em: 3 mar. 2022.

[3] KASPERSKY. Kaspersky Consumer IT Security Risks Report 2021. In: KASPERSKY. *Consumer appetite versus action: the state of data privacy amid growing digital dependency.* [S. l.], 2021. Disponível em: https://media.kasperskydaily.com/wp-content/uploads/sites/92/2021/03/16090300/consumer-appetite-versus-action-report.pdf. Acesso em: 3 mar. 2022. Acessado em 03 de março de 2022.

[4]

KASPERSKY TEAM. *Ciberataques crescem 23% no Brasil em 2021: Home office* (acesso remoto) e pirataria são os principais problemas para consumidores individuais e empresas. Kaspersky Daily, [s. l.], 1 set. 2021. Disponível em: https://www.kaspersky.com.br/blog/panorama-ciberameacas-brasil-2021-pesquisa/18020/. Acesso em: 3 mar. 2022.