sdecoret/Shutterstock

LGPD: uma oportunidade de negócios para as empresas

Nova lei entrará em vigor em agosto de 2020, dois anos depois de ser promulgada

Leandro Augusto, sócio líder de Cyber Security da KPMG no Brasil
Isabella Becker, gerente da área de Cyber Security da KPMG no Brasil

Leandro Augusto

Isabella Becker

Em agosto de 2020, entra em vigor a Lei Geral de Proteção de Dados (LGPD), promulgada em agosto do ano passado.O período concedido pelo legislador para que os entes obrigados a cumpri-la possam se preparar adequadamente será caracterizado por muito trabalho nos departamentos jurídicos e de segurança de informação, e também muitas dúvidas e desconfiança nas diversas áreas de negócio.

Nas organizações, as diretrizes trazidas pela LGPD poderão ser vistas de duas formas: como mais uma série de burocracias com pouco efeito prático e custo de implementação elevado; ou como aquilo que, de fato, elas representam: uma necessidade contemporânea, cujo custo de adequação é investimento período de *vacatio legis*, ou seja, prazo que a Lei tem, após a publicação, para entrar em vigor, pode ser entendido como uma janela de oportunidades.

Vivemos na era do *Big Data* – é inegável. Nesse contexto, a LGPD no Brasil ou o *General Data Protection Regulation*, da União Europeia, vêm tanto para proteger dados pessoais quanto para garantir a livre circulação deles, o que é inclusive princípio norteador da legislação. Devemos partir da premissa de que as empresas, independentemente do nicho de atuação, continuarão coletando dados, traçando perfis e comercializando informações pessoais . Mas todas essas ações deverão ser adequadamente comunicadas às pessoas físicas titulares de dados, que, por sua vez, deverão estar protegidos por recursos tecnológicos realmente eficazes, com uso técnicas de criptografia e anonimização.

Tanto é verdade que a LGPD não tem por objetivo frear ou fechar os olhos para o tratamento de dados pessoais, que o artigo 7º da referida lei abrange dez diferentes possibilidades jurídicas de justificar essa atividade. Não é necessário sair correndo atrás de consentimentos de clientes antes de esmiuçar as nove outras escusas legais que permitem que as empresas continuem exercendo o tratamento de dados e que esses circulem livremente.

Regulamentar essa atividade é fomentá-la, e não ir na contramão da lei. O objetivo da LGPD é somente que uma dessas justificativas legais seja explicitada, de modo que os dados coletados com base nesses fundamentos sejam tratados com segurança. Vale ressaltar que segurança é confiança, um ativo que, literalmente, não há dinheiro no mundo que compre.

De tal modo, as empresas que entenderam esse recado já saíram na frente na corrida para ganhar a confiança dos clientes e do mercado. Não é à toa, portanto, que há cada vez mais *blogs*, índices e portais dedicados a elencar o nível de confiança do consumidor em determinada marca.

Atualmente, já há empresas nos Estados Unidos e na União Europeia que optaram por levantar a bandeira da Lei de Proteção de Dados para enaltecer os princípios mais primordiais de privacidade e segurança. A Apple publicou uma carta na revista *Time Magazine* pedindo a aprovação da legislação de proteção de dados americana e desafiando outras empresas a fazerem o mesmo. Assim, ela se posiciona não apenas como uma empresa que investe e acredita em privacidade e segurança, mas, principalmente, como uma líder no mercado, puxando os demais.

Nesse sentido, podemos pensar que o cliente de um banco, antes de abrir uma conta, leva em consideração o fato de essa instituição ter sido *hackeada* em algum momento e de os dados dos correntistas terem sido expostos. Por que, então, um consumidor não levaria em consideração o mesmo princípio de

> Quando criminosos têm acesso a dados pessoais, a integridade física e a segurança dos cidadãos ficam em xeque

confiabilidade ao hospedar-se em um hotel? Ou ao optar por fazer cadastro e realizar compras em determinado supermercado ou farmácia, em detrimento dos demais?

Não só a questão da privacidade está em jogo quando dados pessoais não são devidamente tratados e acabam expostos. Quando criminosos têm acesso aos dados pessoais fidedignos, a própria integridade física e a segurança dos cidadãos estão em xeque.

Colocar-se como pioneiro em expor as melhores práticas ao público e demonstrar que a empresa está de acordo com a LGPD não somente atenuam eventuais condenações em caso de vazamento de dados como também inspiram valores intangíveis em consumidores.

Além de obterem o reconhecimento pelo seu pioneirismo, as empresas que iniciarem esse processo, puxando o barco dos mercados em que se inserem, estarão contribuindo para garantir uma sociedade na qual direitos e garantias individuais, sejam perseguidos, exigidos e resguardados por todos.

A nova lei de proteção de dados e o recebimento de currículos

Esqueça o tempo em que inglês fluente, MBA e experiência profissional eram os principais pontos a serem analisados em um currículo. De onde veio esse currículo? Como o dono do documento fará para atualizar os dados quando necessário? Por quanto tempo – e onde – eles serão armazenados?

A Lei Geral de Proteção de Dados (LGPD, trouxe, além do necessário panorama de privacidade no contexto brasileiro, uma nova perspectiva sobre a relação das empresas com os dados das pessoas físicas a que elas têm acesso.

Engana-se quem pensa que os dados pessoais tratados pelas empresas são apenas aqueles referentes aos clientes. Uma das fontes de coleta de dados pessoais de quase toda organização é justamente o recebimento de currículos de candidatos. Nome, endereço, e-mail e telefone são alguns exemplos de dados pessoais (conforme definição do artigo 5º, inciso I da LGPD) informados nesse tipo de documento. Receber currículos, portanto, é tratar conteúdo privado, ou seja, é incumbir-se do dever de fornecer uma abordagem jurídica e de segurança adequada.

chainarong06/Shutterstock

Em linhas gerais, a LGPD exige que todas as atividades que envolvam dados de pessoas físicas (coleta, produção, utilização, transmissão e outros) recebam dois tipos de atenção: o primeiro diz respeito à segurança da informação. Esses dados deverão trafegar por ambientes seguros, ser acessados apenas por colaboradores autorizados e ter um fluxo validado por profissionais de tecnologia. Em segundo lugar, os fluxos que envolvem o tratamento de dados de pessoas físicas deverão ter uma justificativa legal – baseada nas dez possibilidades elencadas pelo artigo 7º da Lei n° 13.709.

Assim, sob o aspecto jurídico, espera-se que os Departamentos de Recursos Humanos entendam que o recebimento de currículos é uma coleta de dados pessoais sujeita à regulação e que informem sobre esse procedimento a todos que desejem candidatar-se às vagas disponíveis.

Em linhas gerais, no momento da recepção de um currículo, independentemente da escolha pelo enquadramento legal, é importante que sejam destacados os seguintes pontos aos candidatos (e, portanto, titulares de dados pessoais): em primeiro lugar, com relação aos princípios da LGPD, é preciso informar aos candidatos o propósito específico da coleta, ou seja, se o currículo será simplesmente salvo e consultado para fins de recrutamento ou se outras áreas da empresa (ex. marketing) também farão uso das informações lá dispostas. O segundo ponto refere-se ao fluxo do tratamento, ou seja, por quanto tempo o currículo permanecerá salvo no banco de talentos. Nesse caso, ser transparente com o titular de dados pessoais, além de configurar uma obrigação legal, é também um valor com o qual muitas empresas querem construir um posicionamento. Já sobre os direitos do usuário, o 18º artigo da LGPD confere ao titular de dados pessoais nove tipos de direitos. Assim, vale informar aos candidatos o que e como será preservado informações. Por fim, sobre as transferências de dados para terceiros, o mais importante é se eles serão enviados para fora do Brasil (ponto especial de atenção para empresas multinacionais). Caso positivo, também é interessante chamar a atenção do candidato para essas questões.

Uma forma relevante de agregar todos os pontos acima pode ser o envio pela empresa (ou departamento) de uma mensagem de confirmação, após o recebimento do currículo de um candidato, que explique como ele deve agir para retificar e atualizar os dados, como fazer caso queira que o currículo seja apagado do Banco de Talentos e que também aponte, de forma simples e didática, o fim específico da coleta e se existe a intenção de compartilhar esses dados com terceiros.

Por fim, vale lembrar que a LGPD é uma oportunidade para as empresas fazerem uma grande faxina nos dados que tratam. Arquivar currículos que não estão atualizados não é apenas ineficiente como também apresenta um alto risco de exposição e de sanções pela Autoridade Nacional de Proteção de Dados. Lembre-se de que o princípio de minimização significa coletar a menor quantidade possível de dados, para um fim específico, e evoca a necessidade de armazenar, igualmente, o menor volume de informações necessárias. ■