PRIVACIDADE

Em vigor a partir de agosto, implementação da Lei Geral de Proteção de Dados ainda enfrenta desafios

Foto: Pixabay

Sancionada em agosto de 2018, LGPD tem ritmo lento de implementação no Brasil

Faz pelo menos duas décadas que dados pessoais vêm sendo usados por diversas indústrias e empreendimentos no Brasil. No entanto, como já aconteceu antes, a esfera jurídica demorou para iniciar as discussões sobre a regulamentação do uso e tratamento de informações pessoais por empresas. O tema entrou em pauta no Congresso em 2010 e, depois de muitas idas e vindas, com forte influência da sociedade civil, da academia e do setor privado, em agosto de 2018 foi aprovada a Lei 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD). O texto é bastante inspirado no Regulamento Geral sobre a Proteção de Dados da União Europeia, implementado em 2018, com foco na padronização do tratamento de dados e na proteção dos dados dos titulares. Junto à Lei de Acesso à Informação (Lei 12.527/2011) e ao Marco Civil da Internet (Lei 12.965/2014), a LGPD busca regulamentar o tratamento dos dados pessoais, digitais e não-digitais, de modo a garantir o respeito à privacidade do indivíduo e oferecer segurança jurídica a agentes que operam tratando dados. O ritmo lento de implementação, tanto pelas empresas quanto pelo governo federal, mostra que os atores não estavam preparados para se adequar à lei.

De acordo com o texto da LGPD, "tratamento" de dados refere-se a qualquer operação feita com eles, como coleta, processamento, transmissão, modificação e armazenamento, entre outras. Já dados pessoais são as informações sobre a pessoa identificada ou identificável – ou seja, são tanto dados referentes à pessoa (nome, número de RG ou do passaporte, dados biométricos) quanto os dados que permitem identificá-la (rotas percorridas pela pessoa diariamente, nome dos pais etc.). O que muda com a lei é que, a partir de agosto de 2020, os usuários deverão dar seu consentimento explícito (por escrito ou de outra maneira) para que seus dados sejam utilizados. Eles também poderão pedir aos agentes de tratamento a confirmação de seus dados, o acesso a eles, sua correção, anonimização, bloqueio, eliminação e portabilidade. Usuários deverão ainda ser corretamente informados sobre o tipo de operação a que seus dados são submetidos (respeitando-se o segredo comercial e industrial dos tratadores) e se eles são

compartilhados. Caso queiram, poderão revogar o consentimento de uso dado anteriormente. A lei não se aplica ao tratamento de dados pessoais com fins não-econômicos (jornalísticos, acadêmicos, artísticos), com finalidade de garantir a segurança pública e atividades de investigação, e aos dados que tiverem origem fora do país, sem que sejam compartilhados com agentes de tratamento brasileiros.

AGENTES TRATADORES DE DADOS

A LGDP menciona dois agentes responsáveis pelo tratamento de dados: o controlador e o operador. O controlador é a pessoa física ou jurídica, de direito público ou privado, responsável pelas decisões tomadas sobre o tratamento dos dados. Já o operador seria o responsável pelo tratamento de dados pessoais em nome do controlador. A lei menciona um terceiro agente: o encarregado. Também chamado de DPO (*data protection officer*), ele é indicado pelo operador e controlador para atuar na comunicação entre controlador, titular dos dados e a autoridade nacional de proteção de dados (ANPD), além de garantir a proteção dos dados em posse do controlador. Consideremos um caso hipotético em que um usuário fica em dúvida sobre o tipo de tratamento dos dados que um aplicativo de entrega de comida adota. Esse usuário pode pedir essa informação gratuitamente ao encarregado do controlador, cujo contato deve ser divulgado publicamente. O encarregado tem um prazo de 15 dias para entregar a informação. Caso um operador externo tenha sido o responsável pelo tratamento dos dados (por exemplo, uma empresa subcontratada pelo aplicativo para realizar o tratamento), o encarregado continua sendo o responsável por fazer a comunicação ao titular.

Além de garantir um acesso facilitado ao titular e de reformular suas bases de dados para facilitar o compartilhamento, a lei estabelece que os tratadores devem reforçar os mecanismos de segurança e proteção dos dados, ser capazes de produzir relatórios de impacto à proteção de dados pessoais com detalhes sobre o fluxo e transformação sofrida pelos dados e manter um registro das operações realizadas com os mesmos.

USO DE DADOS NO SETOR PÚBLICO

Sob a LGPD, os dados de todas as pessoas de posse do governo continuam sendo tratados como dados pessoais e submetidos aos demais artigos da lei. Os órgãos do poder público também devem estar prontos a fornecer acesso e outras informações sobre o tratamento dos dados pessoais aos titulares e, por isso, as bases de dados de tais órgãos devem ser organizadas em formato interoperável, ou seja, adequadas para uso compartilhado. Dados podem ser compartilhados entre órgãos do poder público, respeitados os princípios dessa mesma lei, e com pessoas físicas, de acordo com a Lei de Acesso à Informação. Esse é um dos pontos polêmicos da versão final da LGPD, porque o requerente da Lei de Acesso à Informação passa a ser registrado, sendo ele próprio passível de reconhecimento. Entidades públicas são proibidas de compartilhar dados com entidades privadas, a não ser em situações específicas – por exemplo, quando há previsão legal respaldada em contratos e instrumentos, nos casos em que a finalidade do compartilhamento seja a prevenção de fraudes e irregularidades, e na proteção da segurança e integridade do titular. Marina Pita, coordenadora do coletivo de comunicação social Intervozes, ressalta que, pela nova lei, esse compartilhamento deve ter como finalidade a execução de políticas públicas para benefício dos cidadãos, ao contrário do que aconteceu no polêmico acordo entre o Tribunal Superior Eleitoral e a Serasa, em 2013. Nele, dados de 141 milhões de eleitores foram fornecidos à Serasa (uma empresa

privada controlada pela britânica Experian) em troca de serviços de certificação digital para uso do Tribunal. Tal convênio foi suspenso ainda em 2013.

A nova lei criou a ANPD, órgão público federal vinculado à Presidência da República e de natureza jurídica transitória (ou seja, que pode no futuro ser transformada em um órgão mais independente, como uma autarquia), com autonomia técnica e decisória. Uma das críticas a esse formato refere-se justamente a esse vínculo com o poder executivo, que também deveria ser fiscalizado pela ANPD. Tal órgão ficará responsável pela criação de normas para a política nacional de proteção de dados pessoais e da privacidade; pela implementação das mesmas, pela fiscalização e aplicação de sanções quando necessário e pela elaboração de estudos sobre práticas nacionais e internacionais de uso de dados, dentre diversas outras funções.

A ANPD será comandada por um conselho diretor, formado por cinco diretores apontados pelo presidente da República e aprovados pelo Senado Federal, com mandato de quatro anos. Ela ainda contará com o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, composto por 23 representantes dos três poderes e de diversos órgãos públicos e privados do setor produtivo e da sociedade civil.

IMPLICAÇÕES E DESAFIOS Embora a lei tenha sido sancionada em agosto de 2018, seu ritmo de implementação em empresas parece estar muito aquém do esperado. Um relatório de novembro de 2019, da consultoria ICTS Protiviti, apontou que, até então, 84% das empresas não estavam preparadas para a nova regulação. Rafael Zanatta, coordenador da Data Privacy Brasil e estudioso do tema, acredita que provavelmente esta é a realidade da maior parte dos pequenos e médios negócios no país, para os quais a adequação à lei não é prioridade. As exceções, para ele, estariam nos ramos bem regulamentados, como o da comunicação, finanças e energia, que já dispunham de práticas e rotinas para lidar com dados.

Outro ponto delicado concerne a decisões sendo tomadas por algoritmos. Uma versão anterior dessa lei previa que o titular dos dados teria direito a pedir a revisão humana de decisões automatizadas que afetassem seus interesses. Tal versão foi vetada e substituída por outro texto em que titulares ainda têm direito a uma revisão, porém não fica claro como isso aconteceria. Marina Pita ressalta que a nova versão é problemática, já que deixa a interpretação da lei a cargo de decisões judiciais ou de diretrizes da ANPD que podem não ir ao encontro aos interesses dos titulares.

Mas talvez mais preocupante seja o atraso na criação da ANPD. Caso este órgão não seja criado e esteja operando em tempo hábil, uma parte de suas funções seria forçosamente exercida por outros órgãos públicos, conforme aponta Zanatta. Ele explica que, nesse contexto, o Ministério Público teria um papel importante, ao representar direitos coletivos dos titulares de dados perante os tribunais. No entanto, a ocupação do vácuo de poder por diferentes instâncias e a multiplicidade de ações civis públicas levaria a uma pulverização decisória e à instabilidade de interpretação jurídica da lei.

Ele calcula que, quando a ANPD eventualmente surgisse, a harmonização da jurisprudência e das instâncias decisórias seria uma tarefa muito mais trabalhosa.

A demora na adaptação à lei e na criação da ANPD já gerou reações no Congresso. Um Projeto de Lei (5762/19) foi elaborado pelo deputado Carlos Bezerra (MDB-MT) propondo o adiamento da entrada em vigor da LGPD para agosto de 2022. Se ele tiver sucesso, empresas e o setor público terão mais tempo para se adaptar às mudanças.

Raphaela Velho