Por Livia Cunha Fabor*

Em vigor a partir de 2020, a Lei Geral de Proteção de Dados (LGPD) estabelece que dados anonimizados não fazem parte de seu escopo. Essa definição é positiva em muitos aspectos, mas ainda pode gerar questionamentos sobre qual é o limite entre uma informação anônima e aquela que permite a identificação de uma pessoa.

Para ilustrar o conceito de informação anônima, imagine que dados coletados sobre um indivíduo o descrevam como homem, moreno, solteiro e de 35 anos – ou em uma segunda hipótese, o revelem como brasileiro, caucasiano, jovem e casado. É impossível revelar a identidade da pessoa com base apenas nesses dados. Essa capacidade de se referir a alguém e ainda assim garantir o anonimato de um cidadão é o que define o termo anonimizado.

Inspirada em legislação europeia pioneira no tema, a LGPD tem como premissa a proteção de dados pessoais e a garantia de tratamento diferenciado para informações sensíveis de um indivíduo. A própria redação da lei (art. 5, II) explicita quais dados são considerados sensíveis: “sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico”. O texto também resguarda os direitos de crianças e adolescentes.

A aprovação da LGPD pelo Congresso e a posterior sanção presidencial indicam que a classe política compreendeu a realidade atual, na qual a sociedade depende cada vez mais de ferramentais digitais e em que avanços na área de inteligência artificial permitem análise de uma grande massa de dados em pouco tempo. Nessa conjuntura, permanecer inerte representaria elevado risco para a privacidade dos cidadãos, enquanto interesses coletivos ficariam em segundo plano diante da constante inovação tecnológica.

Criada com a intenção de colocar o cidadão e os seus direitos à privacidade, à intimidade e à liberdade individual, a lei manifesta disposição em coibir o uso inadequado e a monetarização de dados pessoais por empresas, sem que os titulares tenham o direito de escolha. As companhias passam a ser responsabilizadas por eventuais quebras de segurança na base de dados pessoais e devem comunicar clientes e agências regulatórias em caso de vazamentos.

Assim, a LGPD cria desde já uma preocupação para todas as empresas que adotem mecanismos e boas práticas para a proteção de dados pessoais identificados ou identificáveis. O contexto indica que chegou a hora de planejar e implementar programas de compliance digital.

Uma vez garantida a segurança sobre as bases de dados, devem ser consideradas e analisadas alternativas para usá-las com fins legítimos e alinhados à legislação. As informações levantadas podem ser estratégicas ao auxiliar as companhias a compreender preferências pessoais e traçar diferentes perfis de clientes. Em setores como a indústria de bens de consumo de massa e o varejo, conhecer os desejos do consumidor é determinante para o sucesso ou fracasso de uma iniciativa.

Muitas dúvidas ainda giram em torno da LGPD e a falta de parâmetros dificulta a projeção de cenários e desdobramentos. O risco do mau uso de dados anonimizados, com o objetivo de transformá-los em informações pessoais, não pode ser descartado. Basta imaginar uma situação em que há o cruzamento de duas ou mais bases de dados, ou em que informações conhecidas são associadas. Para exemplificar, imagine uma pesquisa de opinião sobre o conteúdo de uma aula em que todos os alunos são brasileiros, com a exceção de um estudante estrangeiro. Mesmo sem o nome e dados de identificação na ficha, se o campo nacionalidade for preenchido com qualquer

resposta que não seja brasileira, a opinião e preferências do aluno estrangeiro serão identificadas. Dessa forma, passariam a ser consideradas dados pessoais protegidos, portanto dentro do escopo da LGPD. Além disso, não há como prever a adequação, sob o ponto de vista tecnológico, de recursos disponíveis para assegurar o alcance à anonimização, já que o texto deixa a questão em aberto e cita “meios técnicos razoáveis e disponíveis”.

Mesmo diante da incerteza sobre a aplicação da lei, as empresas devem saudar a chegada do marco regulatório e investir em estudos sobre os dados anonimizados. Tal postura representaria mais do que uma boa prática de governança em compliance digital e em privacidade do consumidor, áreas importantes no que se prevê no cenário de negócios pós-LGPD. Significaria uma oportunidade de se beneficiar dos bancos de informações a serem criados, sem estar exposta a risco e contingências decorrentes de eventual violação aos direitos e garantias constitucionais previstas pela legislação.

*Livia Cunha Fabor é head da área de compliance de Martinelli Advogados