

# O Ano da Proteção de Dados no Brasil

Idec

## Reprodução do texto encontrado no site do Idec<sup>1</sup>

Lei Geral de Proteção de Dados deve entrar em vigor em agosto. Saiba quais os direitos que ela garante aos consumidores brasileiros e quais os deveres dos setores público e privado

2020 tem tudo para ser um ano especial. Uma lei que transformará profundamente a maneira como dados pessoais são usados e armazenados pelos setores privado e público no Brasil deve começar a vigorar em agosto. A Lei Geral de Proteção de Dados (LGPD), fruto de um debate que remonta ao início da década e que envolveu diversos atores, como governo, parlamentares, empresariado, instituições acadêmicas e organizações da sociedade civil, como o Idec, estabelece uma série de parâmetros para proteger o direito à privacidade dos cidadãos, além de obrigações que empresas e poder público deverão cumprir no tratamento de dados pessoais, ou seja, ao realizar coleta, classificação, armazenamento e compartilhamento.

Mas o que é um dado pessoal? "É qualquer informação relacionada à pessoa identificada ou identificável. É uma informação que, combinada com outras, pode nos individualizar", sintetiza Bruno Bioni, fundador e professor do Data Privacy Brasil, organização que oferece cursos nas áreas de privacidade e proteção de dados. Ele explica que, hoje, essa definição vai muito além dos dados cadastrais como o RG, o CPF ou mesmo nossas características físicas: "Na internet, há vários identificadores eletrônicos, como o número de IP, que é armazenado quando estamos em uma conexão. Esse número é considerado um dado pessoal". A geolocalização obtida por aplicativos de celular ou por redes sociais também pode, se cruzada com outras informações, nos individualizar.

Dados pessoais incluem ainda informações relativas a nossa saúde, como prontuários médicos, que despertam o interesse de operadoras privadas, ou os nossos dados biométricos, como a impressão digital e as características do nosso rosto, gravadas por tecnologias de reconhecimento facial, que vêm levantando, em todo o mundo, discussões sobre os riscos do uso sem controle desses dados para marketing e vigilância em massa.

---

<sup>1</sup>O Ano da Proteção de Dados no Brasil

## **PROTEÇÃO DE DADOS, UM DIREITO FUNDAMENTAL**

A proteção de dados pessoais pode ser reconhecida como um direito fundamental dos cidadãos pela Constituição Federal. É o que pretende a Proposta de Emenda à Constituição (PEC) no 17, aprovada em julho de 2019 no Senado Federal. A PEC, que aguarda aprovação de uma comissão especial da Câmara dos Deputados, é um reforço importante para a LGPD. Contudo, Diogo Moyses, do Idec, defende que a competência exclusiva da União para legislar sobre a proteção e o tratamento de dados pessoais não impeça estados e municípios de implementarem políticas públicas para incentivar a adoção da LGPD, como conselhos locais de proteção de dados e ouvidorias, inclusive para ajudar a Autoridade Nacional de Proteção de Dados.

As informações dos indivíduos valem muito e são compartilhadas a todo o momento. "Uma compra que fazemos ou uma curtida que damos em uma rede social podem dizer muito sobre nossas características psicológicas, interesses e perfil de consumo. E as empresas usam isso visando ao lucro. Por isso, batalhamos por uma lei que dá ao cidadão controle sobre seus dados", ressalta a advogada Bárbara Simão, do programa Telecomunicações e Direitos Digitais do Idec.

A preocupação atual do Instituto é com o prazo para a lei entrar em vigor, que pode ser prorrogado. Tramita na Câmara um projeto de lei de autoria do deputado Carlos Bezerra (MDB-MT) que adia para agosto de 2022 a vigência da LGPD. "Seria lastimável", opina Francisco Cruz, diretor do InternetLab, centro de pesquisa em direito e tecnologia. "Da aprovação da lei até a entrada em vigor terão se passado dois anos, e a impressão é que se deixou a lição de casa para a última hora. Agora, querem adiar o prazo, como se os direitos dos brasileiros já não estivessem sendo descumpridos", ele critica.

## **LONGO PROCESSO**

Embora a LGPD tenha sido aprovada no Congresso em julho de 2018, a primeira consulta pública sobre o tema foi realizada em 2010 pelo Ministério da Justiça. Nos anos seguintes, foram feitas outras consultas, bem como audiências públicas, em um processo para o qual contribuíram muitas organizações da sociedade civil, entre elas o Idec. "Tivemos uma atuação muito forte pela aprovação da lei", conta Simão.

No cenário internacional, episódios de mal uso de dados pessoais por governos e empresas revelaram a urgência dessa discussão e dinamizaram a aprovação da LGPD. Um exemplo foi a eleição de Donald Trump à presidência dos Estados Unidos, em 2016, na esteira da divulgação de um escândalo de vazamento de dados de usuários do Facebook à empresa de consultoria Cambridge Analytica - que usou esses dados para construir estratégias de comunicação com a finalidade de influenciar as eleições em favor do candidato republicano.

A aprovação da lei não significou o fim da discussão. A LGPD teve alguns artigos vetados pelo então presidente Michel Temer, entre eles o que criava a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pela sua regulamentação e fiscalização. A justificativa foi a de que caberia ao Executivo criar a autoridade, o que foi feito por meio da apresentação de uma medida provisória (MP) no final de 2018 e aprovada pelo Congresso em julho de 2019. Depois de aprovada, a MP foi transformada na Lei no 13.853, que também foi sancionada com vetos, dessa vez pelo presidente Jair Bolsonaro. Parte desses vetos foi derrubada pelo Congresso em setembro do ano passado.

Nesse processo, a lei acabou fragilizada, de acordo com Diogo Moyses, coordenador do programa Telecomunicações e Direitos Digitais do Idec. A primeira perda diz respeito ao perfil administrativo da ANPD. "Nós defendemos um modelo que tenha autonomia e independência em relação ao Executivo. Mas, infelizmente, ela acabou sendo vinculada de forma direta à Presidência da República, o que é um problema, considerando que a Autoridade precisa fiscalizar também o poder público", ele avalia. Moyses critica ainda a morosidade do Executivo para nomear os integrantes da ANPD. A reportagem entrou em contato com a assessoria de imprensa da Presidência, mas não obteve resposta até o fechamento desta edição.

Bioni destaca outro ponto vetado por Bolsonaro e que por um voto acabou não sendo derrubado pelo Congresso, que diz respeito ao direito de revisão de decisões automatizadas. Ele dá um exemplo: suponha alguém que tem um crédito pré-aprovado de R\$ 2 mil no banco, mas pede um empréstimo de R\$ 4 mil. O banco vai ter um sistema para avaliar o histórico financeiro da pessoa, e um algoritmo vai calcular o potencial de risco de não cumprir com aquele empréstimo. E, então, ele pode negar. O cidadão pode pedir para que esse processo seja revisto. Contudo, do jeito como está na lei, o gerente do banco não precisa revisar isso, basta passar por outro processo automatizado, com base em algoritmos diferentes. O texto original previa que essa revisão deveria ser realizada por uma pessoa e não por outra máquina.

## O QUE MUDA?

Os avanços trazidos pela LGPD à legislação brasileira sobre dados pessoais são muitos. O primeiro deles diz respeito à titularidade dos dados. "A LGPD afirma de maneira categórica que os dados são do cidadão, do consumidor. Isso é o mais relevante", destaca Moyses. Já Cruz, do InternetLab, informa que a coleta, o uso e o compartilhamento de dados pessoais só pode se dar a partir do consentimento do titular. "A pessoa tem que dizer que é ok aquele dado ser tratado daquela forma e com aquela finalidade".

A lei ainda cria a categoria "dados pessoais sensíveis", que terá um controle mais rígido. Dados biométricos, sobre origem racial ou étnica, convicção religiosa, opinião política e dados referentes à saúde são alguns exemplos. Nesses casos, é preciso um consentimento especial. Cruz explica que, para os dados sensíveis, a autorização tem de ser dada pelo titular para cada uma das finalidades para as quais a empresa ou a instituição pública pretende utilizá-los.

Bioni lembra que a partir de agosto não vão ser mais permitidos termos de uso ou políticas de privacidade vagos, comuns nas redes sociais ou aplicativos de celular. "Não vale mais coisas do tipo 'eu vou utilizar esse dado para melhorar a sua experiência'. Ele tem de justificar porque quer aquela informação", reforça. O professor acrescenta que dessa forma a LGPD consagra o que ele chama de "princípio da minimização" no uso e tratamento dos dados pessoais. "Hoje, se você instala qualquer aplicativo, mesmo do governo, ele pede um monte de informações que não fazem sentido. Por que ele quer a minha lista de contatos ou a minha geolocalização se não vai me entregar nada atrelado a isso?", questiona o fundador do Data Privacy Brasil. Quando a LGPD entrar em vigor isso deve mudar.

## EXCEÇÕES QUE PREOCUPAM

O Idec está preocupado com as exceções previstas na LGPD com relação à necessidade de consentimento do cidadão para uso e tratamento de dados pessoais em alguns casos específicos. Um exemplo são os birôs de crédito, como SPC e Serasa. A situação se agrava com a Lei do Cadastro Positivo, aprovada no Congresso logo depois da LGPD para regulamentar o mercado de avaliação de risco de

crédito. Ela prevê a inclusão automática dos dados financeiros de todos os consumidores numa base de dados relativa à proteção do crédito. Ou seja, essas empresas terão acesso aos dados pessoais de todos os brasileiros independentemente de sua autorização. Para Moyses, há uma brecha para que os birôs façam o tratamento de dados pessoais que não tenham relação com o risco de crédito. "Há elementos que indicam que as empresas estão coletando dados além daqueles relacionados ao risco financeiro oferecido por consumidores, como os ligados à navegação em redes sociais e à geolocalização", alerta. Ainda que a LGPD tenha aberto uma exceção aos birôs de crédito, a lei garante aos consumidores alguns direitos, como o de exigir que eles informem os dados a que têm acesso e de pedir a correção de eventuais equívocos.

## DE OLHO NOS DADOS DA SAÚDE

Sobre dados de saúde, a lei diz que a partir de agosto de 2020 as operadoras de planos privados ficam explicitamente proibidas de tratá-los a fim de cobrar mais caro ou recusar clientes que possuam determinadas doenças. Ainda que isso seja proibido pela Lei de Planos de Saúde e pelo Código de Defesa do Consumidor, há indícios de que essa prática exista, como apontou a reportagem "Seus dados valem mais do que ouro", publicada na edição no 226 da Revista do Idec. A matéria cita a empresa Dr. Consulta, cujo fundador afirmou em entrevista que pretendia oferecer aos planos de saúde uma ferramenta para medir o grau de risco dos pacientes a partir de dados coletados em consultas feitas em suas clínicas. O Idec acionou a Agência Nacional de Saúde Suplementar (ANS) pedindo que a lei fosse cumprida. "A ANS disse que essa prática é proibida, e o Dr. Consulta recuou. Mas é preciso ficar atento", declara Diogo Moyses.

Dados usados para segurança pública também não requerem permissão. "A LGPD mostrou que é preciso construir uma legislação específica sobre segurança pública e dados pessoais. Essa construção precisa ser muito cuidadosa, porque pode haver um impacto negativo para o cidadão se não forem observados riscos de vigilância excessiva", adverte Moyses, citando a China, que tem coletado dados dos seus cidadãos de forma massiva. "Não podemos cair na tentação de construir uma sociedade vigilante", ele diz. No final de novembro, o presidente da Câmara dos Deputados, Rodrigo Maia (DEM-RJ), instalou uma comissão para discutir a criação de uma lei que trate do uso de dados para fins de segurança pública.

Raquel Saraiva, advogada e presidente do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), comenta que o uso de dados para combater fraudes também não requer consentimento. "A gente brigou muito no Congresso contra isso, mas não conseguimos mudar", lamenta. Segundo Saraiva, a implantação, por empresas de ônibus, de câmeras para o reconhecimento facial, para combater fraudes nos bilhetes eletrônicos da capital pernambucana, ilustra potenciais riscos dessa exceção. "Estão alegando que é combate à fraude, o que nos deixa de mãos um pouco atadas", declara. Segundo a advogada, a empresa não informou como ou onde esses dados estão sendo armazenados nem as medidas de segurança adotadas. "Eles têm de cumprir os critérios de transparência e publicidade. Contudo, apenas depois que a LGPD entrar em vigor".

Camila Marques, coordenadora do Centro de Referência Legal da Artigo 19, relata situação similar no Metrô de São Paulo, que abriu licitação para instalar câmeras de reconhecimento facial nas estações. "Elas vão coletar informações sensíveis que podem ser usadas de forma perigosa se não houver controle. O que chamou nossa atenção foi a falta de transparência", afirma Marques, que teme que os dados sejam utilizados de forma a gerar preconceitos. "Será que esses algoritmos não reproduzirão o racismo institucional do Estado brasileiro? Essa é uma questão que nos vem à mente e para a qual os termos da licitação não dão resposta", assinala.

## O IDEC E A LGPD

A LGPD não implica mudanças apenas de empresas e do poder público. Como uma organização da sociedade civil que lida com dados pessoais de seus associados, funcionários e pessoas que acessam seu portal, o Idec também está sujeito à lei. Por isso, formou um comitê executivo para desenvolver um programa de adequação a ela. "Nosso papel é cobrar as empresas em relação ao cumprimento da lei. Então, o mínimo que precisamos fazer é estar em conformidade", comenta Simão, uma das integrantes do comitê.

O grupo iniciou o trabalho em novembro de 2019, e a previsão é de que o processo se estenda até abril deste ano. "Por enquanto, estamos informando nossos colaboradores sobre a lei - sua importância, como ela impacta as atividades do Idec e o que as equipes têm de fazer para respeitá-la", explica Simão. Uma das mudanças será no modo de solicitar, a quem acessa o site, permissão para envio de e-mails e comunicações institucionais.