Lei de proteção de dados vai mudar cotidiano de cidadãos e empresas.

A nova lei geral de proteção de dados pessoais , aprovada terça-feira (10) pelo Senado, colocou o Brasil ao lado de dezenas de países que já têm legislação sobre o tema, como as nações europeias e boa parte da América do Sul. Ao estabelecer direitos e responsabilidades, a lei vai trazer também impactos no cotidiano dos cidadãos, de empresas e dos órgãos públicos. O texto ainda precisa ser sancionado pelo presidente Michel Temer, e as novas regras só vão entrar em vigor daqui a um ano e meio.

O texto define dados pessoais como informações que podem identificar alguém (não apenas um nome, mas uma idade que, cruzada com um endereço, possa revelar que se trata de determinada pessoa). Além disso, disciplina a forma como as informações são coletadas e tratadas em qualquer situação, especialmente em meios digitais. Estão cobertas situações como cadastros ou textos e fotos publicados em redes sociais.

A nova regra também cria o conceito de dados sensíveis, informações sobre origem racial ou étnica, convicções religiosas, opiniões políticas, saúde ou vida sexual. Registros como esses passam a ter nível maior de proteção, para evitar formas de discriminação. Esse tipo de característica não poderá ser considerado, por exemplo, para direcionamento de anúncios publicitários sem que haja um consentimento específico e destacado do titular. Já registros médicos não poderão ser comercializados.

Se sancionada, a lei valerá para atividades e pessoas em território nacional, mas também para coletas feitas fora, desde que estejam relacionadas a bens ou serviços ofertados a brasileiros. Um site que vende pacotes de viagens com conteúdo em português e ofertas para brasileiros teria as mesmas responsabilidades de uma página sediada no país.

Finalidade específica e consentimento

O uso de dados não poderá ser indiscriminado, mas para uma finalidade determinada. Um prédio que solicite nome dos pais de alguém para acesso ao local, por exemplo, pode ser questionado. Os “testes de personalidade”, como o aplicado no Facebook que originou o vazamento de dados de 87 milhões de pessoas, usados pela empesa Cambridge Analytica, inclusive para influenciar eleições, são outro exemplo.

“As empresas vão ter de justificar o tratamento de dadosm o que pode fazer com que, em alguns casos, eles não precisem ser usados. Isso tende a racionalizar a coleta e o uso de dados, seja porque a lei pode proibir ou porque ele não vai valer a pena por gerar risco pouco razoável”, comenta Danilo Doneda, especialista em proteção de dados e consultor que participou ativamente do processo de discussão da lei.

Além de uma finalidade específica, a coleta só pode ocorrer caso preencha requisitos específicos, especialmente mediante autorização do titular (o chamado consentimento). Ou seja, o pedido de permissão (por exemplo, ao baixar aplicativos) passa a ser a regra, não um favor das empresas. “Por um lado, caminhamos, portanto, no sentido de minimizar a produção de dados que podem ser considerados excessivos para a prestação dos serviços. O que, diante dos inúmeros incidentes de vazamento de dados que vemos a cada semana, é também uma forma de segurança”, avalia Joana Varon, da organização de direitos digitais Coding Rights.

Se o titular consentir ao aceitar as “regras” em redes sociais, os chamados “termos e condições” usados por plataformas como Facebook, Twitter e Google, as empresas passam a ter o direito de tratar os dados (respeitada a finalidade específica), desde que não violem a lei. Contudo, a lei lista uma série de responsabilidades. Entre elas estão a garantia da segurança dos dados e a elaboração de relatórios de impacto à proteção de dados, se solicitados pela autoridade regulatória.

A norma permite a reutilização dos dados por empresas ou órgãos públicos, em caso de "legítimo interesse” desses. Estabelece, no entanto, que esse reúso só pode ocorrer em uma situação concreta, em serviços que beneficiem o titular e com dados “estritamente necessários”, respeitando os direitos dele.

“Não é possível prever todas as situações, especialmente quando se trata de tecnologia. Por isso, é fundamental a previsão de uma norma fluida como o legítimo interesse, capaz de se adaptar às evoluções tecnológicas. Esse conceito indeterminado é justamente o que impedirá

que a lei se torne obsoleta diante do usos novos dos dados, inimagináveis hoje", observa Fabiano Barreto, especialista em política e indústria da Confederação Nacional da Indústria (CNI).

Direitos

De outro lado, o titular ganhou uma série de direitos. Ele poderá, por exemplo, solicitar os dados que a empresa tem sobre ele, a quem foram repassados (em situações como a de reutilização por "legítimo interesse") e para qual finalidade. Caso os registros estejam incorretos, poderá cobrar a correção. Em determinados casos, o titular terá o direito de se opor a um tratamento.

O titular terá ainda direito à portabilidade de suas informações, assim como ocorre com número de telefone. A autoridade regulatória, se criada, deve definir no futuro como isso será feito. Mas a possibilidade de levar os dados consigo é importante para que uma pessoa possa trocar de aplicativo sem perder seus contatos, fotos ou publicações.

Outra garantia importante é a relativa à segurança das informações. Os casos de vazamento têm se multiplicado pelo mundo, atingindo inclusive grandes empresas, como a Uber. Além de assegurar a integridade dos dados e sua proteção contra vazamentos e roubos, as empresas são obrigadas a informar ao titular se houve um incidente de segurança. No caso envolvendo o Facebook e a empresa Cambridge Analytica, por exemplo, a empresa norte-americana teve conhecimento há anos do repasse maciço de informações, mas foi comunicar aos afetados somente meses atrás.

A lei entra em uma seara importante, na decisão por processos automatizados (como as notas de crédito). "Há também o direito à revisão de decisões tomadas com base no tratamento automatizado de dados pessoais que definam o perfil pessoal, de consumo ou de crédito. A Autoridade Nacional de Proteção de Dados também terá o papel de realizar auditorias para verificação de possíveis aspectos discriminatórios nesse tipo de tratamento", destaca Rafael Zanatta, do Instituto de Defesa do Consumidor (Idec).

O texto listou garantias específicas para crianças e pessoas com idade até 12 anos. A coleta fica sujeita a uma série de restrições, deve ser informada de maneira acessível para esse

público e fica condicionada à autorização de pelo menos um dos pais. “Para as famílias, isso significa ter, finalmente, uma forma de garantir que não estão usando dados de seus filhos de forma não autorizada. Isso é fundamental. Afinal, as crianças estão em um processo peculiar de desenvolvimento e, por isso, são mais vulneráveis”, afirma Pedro Hartung, do Instituto Alana, organização voltada à defesa dos direitos de crianças e adolescentes.

Negócios

Ao estabelecer garantias e responsabilidades às empresas, a lei vai ter impacto importante nos negócios realizados no Brasil e com parceiras estrangeiras. A primeira mudança é que, com sua aprovação, o país passa a atender a exigências de outros países e regiões, como a União Europeia. Sem isso, as empresas nativas poderiam ter dificuldades para fechar negócios.

Na avaliação do coordenador da área de direito digital da firma Kasznar Leonardos Advogados, Pedro Vilhena, as empresas deverão passar por um processo de adaptação. Elas tendem a racionalizar a coleta, uma vez que passarão a estar suscetíveis a sanções por parte da autoridade regulatória. De acordo com o texto, as penalidades poderão chegar a R$ 50 milhões.

“O valor de R$ 50 milhões é considerável para algumas, mas, para outras, é irrisório. A principal sanção é a proibição de tratamento de dados. Algumas empresas podem ter que deixar de operar porque não cumpriram obrigações da lei”, destaca Vilhena.

Autoridade regulatória

O detalhamento de boa parte dessas regras, direitos e responsabilidades depende da autoridade regulatória prevista no texto. Ela poderá definir parâmetros (como as exigências mínimas de segurança), realizar auditorias, solicitar relatórios de impacto à proteção de dados e será a responsável por fiscalizar e definir possíveis punições.

Contudo, sua criação vem sendo alvo de polêmica. Segundo o professor de direito da Universidade Mackenzie e fundador da organizaçao Data Privacy Brasil Renato Leite, há

questionamentos no Executivo tanto de caráter jurídico quanto político e orçamentário. Mas a não criação da autoridade, alerta o especialista, pode afetar duramente a efetividade da lei. “Termos a regra sem uma autoridade que faça a sua aplicação é abrir espaço para uma grande chance de insucesso. É o risco de ser uma lei que na prática ´não pegue´”.

Fonte: Agência Brasil, em 12.07.2018.