Fábio Canton Filho: Barreiras legais contra o vazamento de dados

Em 2013, a ONU aprovou resolução para reafirmar o direito à privacidade, previsto no artigo 12 da Declaração Universal dos Direitos Humanos, segundo o qual "ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataques"[1].

A resolução propunha que os Estados-membros revisassem suas leis e práticas para coleta, armazenamento e uso da dados e sedimentassem o respeito à privacidade dos cidadãos no universo digital. Nesse contexto, a União Europeia elaborou a Regulação Geral de Proteção de Dados (*General Data Protection Regulation – GDPR*), uma legislação moderna e consistente, que entrará em vigor em maio.

O Brasil, sem a mesma diligência da UE, ainda não possui legislação sobre proteção de dados, embora esteja tramitando no Senado Federal, desde 2013, o Marco Regulatório da Proteção de Dados do Brasil, substitutivo ao PLS 330/13, do senador Antonio Carlos Valadares (PSB-SE). A proposta surgiu em decorrência das denúncias de que agências de inteligência dos Estados Unidos estariam monitorando informações (e-mails e telefonemas) de empresas e cidadãos brasileiros.

O texto em tramitação contempla um detalhamento sobre uso, proteção, tratamento e armazenamento de dados pessoais e dispõe sobre a segurança dos dados, infrações e penalidades. Aprovado na Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática, agora tramita na Comissão de Assuntos Econômicos.

Também tramita em regime de prioridade na Câmara dos Deputados o PL 5.276/2016, de autoria do Executivo, sobre a mesma matéria. Vale lembrar que o Marco Civil da Internet foi aprovado após três anos de tramitação, mas o Marco de Proteção dos Dados já chega aos cinco anos, sem perspectiva de votação em Plenário em curto prazo.

No vácuo de uma legislação que proteja os dados privados dos brasileiros na internet, o Planalto está avaliando de forma emergencial criar um órgão federal nesse sentido, como forma de credenciar o Brasil para obter uma cadeira na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que exige dos países-membros um marco legal para proteger seus cidadãos contra vazamentos de dados privados.

De acordo com a nova legislação europeia, "qualquer tipo de informação pode ser considerada dado pessoal, desde que seja relativa a uma pessoa". Além das pessoas singulares, a proteção de dados é expandida a pessoas coletivas e inclui categorias, como os chamados dados sensíveis (origem étnica, posições políticas, convicções religiosas, orientação sexual etc.), cabendo ao legislador nacional da UE definir penalidades, no caso de violação de tais dados.

O crescimento das novas tecnologias e a capacidade de captar e utilizar dados pessoais por parte das "gigantes de tecnologia" torna fundamental o debate sobre políticas de proteção de dados e a sua regulação, assim como sobre a privacidade do usuário, que está diretamente ligada aos direitos da personalidade. As plataformas tecnológicas ampliaram a possibilidade de coleta, processamento e

vazamento massivo desses dados pessoais, com notórios danos aos direitos dos usuários.

O caso Facebook/Cambridge Analytica acendeu o alerta sobre as chamadas tecnologias invasivas das grandes corporações digitais sobre a vida do cidadão, colocando como principal desafio a construção de barreiras legais. Calcula-se que 87 milhões de pessoas foram atingidas, incluindo, nesse universo, 443 mil usuários brasileiros. Tudo começou com um teste de personalidade sobre a vida digital aplicado aos usuários que concordaram com o teste. A Cambridge Analytica, contudo, coletou os dados dos amigos desses usuários para montar perfis voltados a influenciar eleitores (durante a última eleição americana) e para formar opinião (na campanha pela saída do Reino Unido da UE), em flagrante afronta ao direito à privacidade. A ferramenta propicia indevido e indesejável "controle social", muito ao gosto dos regimes totalitários.

A persuasão argumentativa em muito difere do domínio digital que molda a opinião pública e que constitui uma negação da liberdade de escolha, do interesse público da comunicação e do direito à privacidade nas sociedades democráticas.

A doutrina do *right to privacy* começou a tomar corpo a partir de um artigo de 1890, dos juristas americanos Samuel Warren e Louis Brandeis, publicado no *Harvard Law Review*, no qual defenderam o direito à intimidade da filha de Warren, que teve divulgados fatos constrangedores ligados ao seu casamento. Hoje, o direito à privacidade está mais voltado ao controle informacional do titular do direito, que precisa ser resguardado contra intromissões indesejadas.

A exemplo da lei anticorrupção americana (*FCPA – Foreign Corrupt Practices Act*), que tem caráter transnacional — e pode alcançar empresas brasileiras com ações na Bolsa de Valor americana ou que receberam investimentos americanos —, o novo diploma legal europeu pode atingir empresas fora da UE, desde que lidem com dados de cidadãos europeus, o que pode ocorrer a partir de uma simples transação de *e-commerce*. O Google, principal empresa tecnológica do mundo e que há muito deixou de ser apenas uma plataforma de busca, já disponibilizou na internet uma tela para remoção de conteúdos indexados em suas pesquisas para usuários europeus, em conformidade com o novo diploma legal. No Brasil, o esforço da empresa se concentra em contendas jurídicas objetivando a não remoção de conteúdos da internet.

A Regulação Geral da União Europeia constitui um avanço no sentido de proteger o titular dos dados, estabelecer controles e prevenir a ocorrência desse tipo de violação de segurança em outros países. O prazo para as empresas notificarem o vazamento às autoridades e aos cidadãos afetados, assim como as medidas adotadas, é de 72 horas. Também proíbe a transferência de informações de europeus para países onde a legislação não proteja seus dados.

O prazo tem grande relevância para as vítimas. O Facebook, por exemplo, levou quase um mês para enviar notificações aos usuários, avisando que tiveram seus dados utilizados ilegalmente pela consultoria Cambridge Analytica, contando da publicação de matéria nos jornais *The New York Times* e *The Observer* e na edição dominical do *The Guardian*, em 17 de março. Pela legislação europeia, o consentimento para o uso dos dados pessoais captados precisa ser inequívoco. O fundador e presidentedo Facebook, Mark Zuckerberg, fez um *mea culpa* no Senado americano e aceitou uma possívelregulação e garantiu medidas para assegurar a integridade das eleições pelo mundo, incluindo abrasileira.

As informações pessoais na UE devem estar protegidas por técnica de encriptação e não podem ser disponibilizadas a terceiros de forma automática. O usuário tem direito à portabilidade de dados, com a transmissão de dados entre empresas, direito de acesso, de retificação, de esquecimento, de bloqueio, de restrição e de oposição à automatização, como acontece, por exemplo, na classificação do risco de crédito.

O direito à privacidade está previsto na Constituição brasileira, mas a comercialização indevida de dados é prática reiterada. O Ministério Público investiga gigante de telefonia móvel pelo uso indevido dos dados de seus milhões de usuários para fins publicitários.

Não há mais como viver sem disponibilizar nossos dados na rede, seja pelo uso do cartão do banco, *posts* em redes sociais e até pelo uso de um *app* de mobilidade. As grandes corporações digitais sabem quanto gastamos e com que tipo de produtos e serviços, para onde vamos, filtram nossas preferências etc. Com a internet das coisas (TV, geladeira, máquina de lavar), isso será ampliado ainda mais.

Diante dessa realidade, o novo regulamento europeu pode servir de inspiração para o Brasil e demais países interessados em regular de forma efetiva o uso e gestão de dados pessoais e o direito à privacidade, inclusive o de crianças. O GDPR usa um trunfo que tem surtido efeito para todo tipo de violação de diplomas legais: o estabelecimento de multa robusta para as empresas que vazarem de forma ilegal dados pessoais, atingindo 4% de seu faturamento global ou 20 milhões de euros (o que for maior).

[1] DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS. Assembleia Geral das Nações Unidas em Paris. 10.dez.1948. Disponível em: http://www.onu.org.br/img/2014/09/DUDH.pdf

Date Created
24/04/2018