

Ramos e Navarro: A LGPD e o direito à autodeterminação informativa

07/04/2020



Depois da prorrogação [aprovada](#) pelo Congresso, deve

entrar em vigor no começo de 2021 a Lei Geral de Proteção de Dados Pessoais — LGPD (Lei nº 13.709/18). Referida legislação, fortemente inspirada no Regulamento Geral sobre Proteção de Dados da União Europeia, é revolucionária em vários aspectos.

Em essência, ela vem assegurar ao cidadão o *direito à autodeterminação informativa* em relação a dados pessoais fornecidos a terceiros, sejam eles empresas, órgãos governamentais, partidos políticos, associações, sindicatos e até mesmo pessoas naturais.

Um primeiro e importante passo já havia sido dado no Brasil na direção da afirmação desse importante direito, fortemente vinculado aos direitos fundamentais à privacidade, à intimidade, à honra, à imagem e à liberdade (de expressão, de informação e de opinião), mediante a edição da Lei nº 12.965/14, chamada de Marco Civil da Internet.

Tal lei estabeleceu princípios, direitos e deveres relacionados ao uso da internet no Brasil, com menção explícita, por exemplo, à necessidade do prévio consentimento do titular para a coleta, uso, armazenamento e tratamento de informações pessoais.

Com a vigência da LGPD, porém, o ganho de escopo na proteção aos dados pessoais, inclusive digitais, será significativo. Isso porque a LGPD tem como destinatário todo aquele que demandar algum dado pessoal de alguém, independentemente do fim almejado.

Seguindo os mesmos vetores do Marco Civil da Internet e da LGPD, que acarretam, em essência, o *empoderamento digital* do cidadão no que se refere à coleta, manipulação e transferência de seus dados pessoais (digitais, biológicos, laboratoriais, associativos, financeiros, biométricos, parentais, relativos a doenças, judiciais, entre outros), já tramita no Congresso Nacional proposta de emenda constitucional que visa a incluir a proteção de dados pessoais entre os direitos fundamentais no Brasil (PEC nº 17/2019).

É certo que a intensificação do fluxo de dados vem transformando radicalmente a sociedade e a forma como se pensa, se comunica e se trabalha. Isso constitui a atual *era digital*, fruto dos avanços tecnológicos e científicos em todo o mundo. É notório que estamos cercados de informações por todos os lados, ao mesmo tempo em que nossos dados pessoais estão cada vez mais sendo utilizados para fins comerciais sem o nosso próprio conhecimento. Daí porque uma das pedras de toque da LGPD é o consentimento do titular para a coleta e o tratamento de dados pessoais para uma finalidade determinada e que deve, necessariamente, ser limitada no tempo.

Além disso, entre os princípios relacionados à proteção de dados, a LGPD destaca o princípio do livre acesso, segundo o qual se deve garantir ao titular acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de modo claro acerca: I — da finalidade específica do tratamento; II — da forma e da duração do tratamento, observados os segredos comercial e industrial; III — da identificação do controlador; IV — de informações de contato do controlador e do uso compartilhado de dados com terceiros; V — de responsabilidades dos agentes que realizarão o tratamento.

O escândalo envolvendo as empresas *Facebook* e *Cambridge Analytica* jogou luzes sobre os impactos que a colheita, o repasse e o tratamento de dados de forma desconhecida podem ter, inclusive na democracia.

Naquele caso, revelou-se ter havido repasse e tratamento de dados de perfil de mais de 50 milhões de pessoas com a finalidade de influenciar comportamentos em processos eleitorais (o que ocorreu nas eleições americanas de 2016 e no plebiscito que decidiu pela saída do Reino Unido da União Europeia — Brexit, além de fortes indícios de que também ocorreu nas últimas eleições brasileiras).

A partir daí, surgiram discussões mais profundas sobre o tema em todo o mundo, inclusive considerando a coleta, o tratamento e a transmissão a terceiros, por parte de empresas, de informações básicas ou até mesmo de dados pessoais sensíveis de funcionários e clientes, com fins comerciais.

Hoje em dia já se compreende com clareza que, a bem da efetivação do direito à privacidade, considerado o elevado volume de informações que circulam na sociedade — especialmente em ambiente virtual —, deve-se impor obrigações e limites a quem delas tome conhecimento, no interesse do seu titular.

Para a LGPD, os dados pessoais sensíveis, cujo acesso só é admitido em hipóteses bastante restritas previstas na lei e para finalidades específicas, são aqueles que, diferentemente do nome e do e-mail, por exemplo, são capazes de levar a uma possível discriminação, como 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.

A esse respeito, vale mencionar que investigações vêm sendo realizadas pelo Ministério Público no Brasil com o objetivo de apurar se farmácias estão vendendo informações de clientes sobre o uso de medicamentos para empresas de planos de saúde. Órgãos governamentais também estão

sendo questionados, como o Ministério da Economia e seu “Clube de Descontos”, por expor indevidamente dados de servidores públicos a empresas de *marketing* de produtos e serviços.

Com base no Regulamento da União Europeia (RGPD), em vigor desde 25 de maio de 2018, condenações de empresas em valores significativos estão sendo estabelecidas naquele continente^[1]. As 10 maiores somaram mais de 400 milhões de euros. As três maiores até agora recaíram sobre a *British Airways* (204,6 milhões de euros), por não se proteger adequadamente de *hackers* que roubaram dados de pagamentos de cerca de 500 mil pessoas; *Marriott Internacional* (110,4 milhões de euros), por permitir que 339 milhões de registros de hospedagem fossem expostos; e Google (50 milhões de euros), por falta de transparência na política de uso de dados. Empresas como a Vodafone também já foram condenadas em razão do envio de mensagens de texto e da realização de ligações para fins de *marketing* e propaganda, e ainda por manter dados de quem solicitou sua exclusão.

Na mesma linha, já foram multadas empresas pelo uso de câmeras de vídeo com transmissão de imagens pela internet sem o consentimento de empregados, locadoras de veículo que rastreiam automóveis por GPS sem anterior informação ao cliente, imobiliárias pela falta de adoção de medidas de segurança quanto a dados sensíveis como certidões de divórcio e fotos nos *sites* ou por armazenarem dados por tempo excessivo sem justificativa. Seguradoras, bancos, hospitais, provedores de internet, empresas de publicidade também vêm sendo pesadamente multados e tendo sua imagem severamente abalada. Nesse contexto, parece-nos temerária a opção pela implementação meramente cosmética de *compliance* a esse respeito.

No Brasil, apesar de a LGPD ainda estar em período de vacância, com entrada em vigor prevista para agosto deste ano, em dezembro de 2019, o Departamento de Proteção e Defesa do Consumidor, vinculado ao Ministério da Justiça e Segurança Pública, condenou o *Facebook* ao pagamento de multa de R\$ 6,6 milhões por violações ao Código de Defesa do Consumidor e ao Marco Civil da Internet, fundamentando-se em razões semelhantes ao que a LGPD busca evitar, como o compartilhamento de dados de usuários com terceiros sem que houvesse o consentimento explícito e consciente dos titulares.

Além do mais, a Constituição de 1988 considera invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. Portanto, buscar proteger os dados pessoais a que se tem acesso já é obrigação de todos, independentemente da plena vigência da LGPD ou da atividade da Autoridade Nacional de Proteção de Dados a que se refere a lei em questão, ainda que alguns pontos demandem melhor detalhamento. Recomenda-se tal postura até mesmo porque o itinerário de *compliance* envolvendo a LGPD é complexo e exige investimentos em segurança digital, além da modificação de processos, de contratos e, sobretudo, de perspectivas individuais ancoradas em noções incorretas acerca da importância do lidar com dados pessoais de outrem.

Buscar conformidade à LGPD demandará uma mudança cultural ampla de toda a sociedade no tocante à proteção de dados pessoais. Daí seu caráter disruptivo. Será preciso aprender, fundamentalmente, que não se deve solicitar, tratar ou repassar algum dado pessoal sem uma justificativa específica e sem o livre consentimento do seu titular, a quem deverá ser facultado amplo e transparente acesso, alterações no conteúdo registrado ou até mesmo sua eliminação.



E mais: será preciso a conscientização de que, uma vez na posse do dado pessoal de alguém, tal informação está sob sua responsabilidade, devendo ser muito bem protegida, por meios tecnológicos e com ações juridicamente bem orientadas, sob pena de severas sanções legais, com reflexos materiais e imateriais. Mais adiante, porém, será possível constatar que a plena adequação à LGPD terá tornado as organizações socialmente melhores e mais prósperas, porque confiáveis.

Fonte: <https://conjur.jumps.com.br/2020-abr-07/entrada-vigor-lgpd-brasil-direito-autodeterminacao-informativa-digital/>