OpiniÃ£o: ProteÃ§Ã£o de dados europeia pode afetar empresas brasileiras

O Parlamento Europeu e o Conselho da União Europeia aprovaram, há pouco mais de um ano, o Regulamento Geral sobre Proteção de Dados (GDPR, na sigla em inglês para *General Data Protection Regulation*), que pode ser apontado como a mais importante alteração na legislação de proteção de dados desde o início deste século.

Projetado para padronizar as normas de proteção de dados entre os países da União Europeia, o GDPR entrará em vigor em 25 de maio de 2018. Até lá, pessoas físicas e jurídicas que de alguma forma façam operações de tratamento de dados pessoais deverão adequar as suas práticas e os respectivos contratos para não correrem o risco de serem apenadas com severas sanções.

O âmbito de aplicação material do GDPR é bastante extenso, abrangendo praticamente toda e qualquer operação de "tratamento" de "dados pessoais" — ambos os termos dotados de definição ampla na norma. Isso inclui a coleta, o registro, a organização, a conservação, a utilização, a divulgação e destruição de qualquer informação relativa a uma pessoa física identificada ou identificável.

Norma estrangeira com possíveis impactos sobre empresas brasileiras
Embora em um primeiro momento possam parecer distantes da realidade brasileira, as normas impostas ao tratamento de dados pessoais previstas no GDPR serão aplicáveis não apenas a empresas fisicamente presentes nos países que integram a União Europeia, mas também a pessoas físicas e jurídicas estabelecidas inteiramente fora daquele território.

Para exemplificar, se uma empresa brasileira faz o tratamento de dados pessoais de um indivíduo que está no território da União Europeia, de forma relacionada à oferta de bens ou serviços, ainda que fornecidos gratuitamente, ela estará sujeita às normas do GDPR e potencialmente obrigada a designar um representante no respectivo Estado-Membro — sob pena de arcar com sanções que podem incluir multas e até a proibição do tratamento de dados.

No contexto de uma economia globalizada e digital, esse não é um cenário raro: pode significar a realização de vendas online por meio de uma plataforma de *e-commerce*, o direcionamento de anúncios publicitários veiculados em uma rede social, a prestação de serviço de *cloud computing* e uma infinidade de atividades proporcionadas, sobretudo, por aplicações de Internet.

Direitos para os titulares dos dados; obrigações para os agentes de tratamento
O GDPR estabelece uma série de direitos para os titulares de dados pessoais e impõe diversas obrigações aos agentes de tratamento, sejam eles controladores — que determinam as finalidades e os meios do tratamento —, ou processadores — que façam as operações de tratamento por conta dos controladores.

O tratamento de dados pessoais pode ser feito por esses agentes não apenas mediante o consentimento do titular, mas também quando necessário para a execução de um contrato do qual o titular dos dados seja parte, para o cumprimento de obrigação jurídica a que o agente do tratamento esteja sujeito, para a

defesa de interesses vitais do titular ou de outra pessoa física, além de outras hipóteses.

Quando fundado no consentimento, este deve corresponder a uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular aceita, mediante declaração ou ato positivo inequívoco, que os seus dados pessoais sejam objeto de tratamento. O titular tem o direito de retirar o seu consentimento a qualquer momento, com a mesma facilidade com que o tenha dado.

Outros direitos relevantes previstos no GDPR, assegurados ao titular dos dados pessoais independentemente de o tratamento ser realizado com base no seu consentimento ou sob outra circunstância prevista na norma, são:

— o direito de acesso, pelo qual o titular pode pleitear e obter do agente a confirmação de que os seus dados pessoais são ou não objeto de tratamento e, em caso positivo, pode acessar esses dados e receber informações como as categorias de dados pessoais tratados, as finalidades do tratamento, os terceiros para os quais foram ou serão divulgados e a existência de decisões automatizadas, incluindo para a criação de perfis;

— o direito de retificação, pelo qual o titular pode pleitear e obter do agente de tratamento, sem demora injustificada, a correção dos dados pessoais inexatos que lhe digam respeito;

— o direito de apagamento, pelo qual o titular pode pleitear e obter do agente o apagamento dos seus dados pessoais quando deixarem de ser necessários para a finalidade que motivou sua coleta ou tratamento, bem como (sendo o caso) se o titular retirar o seu consentimento, entre outras circunstâncias;

— o direito de restrição do tratamento, que pode ocorrer, por exemplo, quando o tratamento for ilícito e o titular se opuser ao apagamento dos seus dados pessoais, solicitando ao agente, em vez disso, a limitação da sua utilização – direito este até então não previsto na legislação da União Europeia; e

— o direito de portabilidade dos dados, pelo qual o titular pode pleitear e receber do agente de tratamento os dados pessoais que lhe tenha fornecido, em formato estruturado, de uso corrente e de leitura automática, bem como transmiti-los livremente a outro agente – direito este que também representa uma inovação na legislação da União Europeia.

Além do dever de observância dos direitos assegurados aos titulares de dados pessoais, o GDPR impõe aos agentes de tratamento diferentes obrigações, tais como:

— a manutenção de registro de todas as atividades de tratamento sob a sua responsabilidade, com informações como o nome e os contatos do agente de tratamento, as finalidades do tratamento, as categorias de destinatários a quem os dados pessoais foram ou serão divulgados etc.;

— a adoção de medidas técnicas e organizativas para assegurar um nível de segurança adequado ao risco decorrente da atividade de tratamento; e

— a notificação da autoridade de controle competente e/ou dos próprios titulares em caso de

violação de dados pessoais, a depender da gravidade do risco resultante do evento.

As autoridades de controle têm amplos poderes de investigação sobre os agentes de tratamento de dados pessoais, incluindo as prerrogativas de requisitar informações, obter acesso às suas instalações, ordenar a adoção de medidas para o cumprimento dos deveres e obrigações previstos no GDPR, impor limitação temporária ou definitiva e até a proibição do tratamento de dados, bem como aplicar multas em valores que podem chegar a 20 milhões de euros ou, no caso de empresas, a 4% do seu faturamento anual em nível mundial — o que for maior.

Não é o fim do mundo

O rol de direitos assegurado pelo GDPR aos titulares de dados pessoais e de obrigações impostas aos agentes de tratamento não se limita aos exemplos destacados acima. Há, ainda, muitas outras regras a serem observadas por pessoas físicas e jurídicas que realizem operações de tratamento de dados pessoais abrangidas pelo campo de incidência do GDPR, incluindo condições específicas para a transferência internacional dessas informações.

Se para os próprios países da União Europeia o GDPR implica inovações consideráveis, sob a ótica do ordenamento jurídico brasileiro, que ainda não dispõe de uma lei geral de proteção de dados, os impactos serão significativamente mais drásticos para os agentes de tratamento de dados pessoais.

Até a entrada em vigor do GDPR, em 25 de maio de 2018, não serão poucos os ajustes de procedimentos e de contratos que deverão ser implementados pelas empresas brasileiras que realizem o tratamento de dados pessoais de indivíduos localizados no território da União Europeia, de forma relacionada à oferta de produtos ou serviços, ainda que na condição de processadores subcontratados pelos efetivos fornecedores desses produtos ou serviços.

A mudança é complexa, mas o próprio texto do GDPR fornece subsídios para a identificação e implementação dos ajustes necessários aos agentes de tratamento de dados pessoais ao detalhar a forma pela qual devem cumprir os deveres e obrigações previstos, assim como ao descrever medidas de organização e procedimentos internos a serem observados para o atendimento da norma.

As empresas que se anteciparem nesse processo de mudança certamente terão maior facilidade na adequação de suas práticas ao GDPR.