BLUEPAPER pg law
www.pglaw.com.br

A Nova Lei Geral de Proteção de Dados brasileira

Carlos Portugal Gouvêa, Eduardo Fucci e Gabriela Forti

Em 15 de agosto de 2018 foi publicada a Lei Geral de Proteção de Dados do Brasil, Lei nº 13.709 de 14 de agosto de 2018 ("LGPD"). A LGPD entrará em vigor após completados os 18 (dezoito) meses de sua publicação, ou seja, em fevereiro de 2020. A partir dela, o Brasil moderniza a sua legislação interna, até então esparsa e incompleta sobre o assunto, e dá um importante passo para tornar-se um país que oferece um nível adequado de proteção de dados, alinhando-se aos patamares internacionais lançados pela OCDE (Organização para a Cooperação e Desenvolvimento Económico) e, mais recentemente, pela União Europeia, por meio da sua *General Data Protection Regulation* ("GDPR").

A LGPD é o resultado de um projeto cuja tramitação legislativa perdurou por mais de 8 (oito) anos, e contou com 11 (onze) consultas públicas até chegar ao seu texto final. Seguindo os objetivos almejados pela GDPR, ela também ambiciona ser um marco regulatório no cenário atual, promover a gestão responsável dos dados pessoais por parte das entidades e pessoas que tratam e processam esses dados, e dar maior segurança jurídica aos agentes econômicos atuando em mercados que fazem uso desses dados.

O projeto de Lei da LGPD apresenta um texto bastante próximo ao da GDPR (como será melhor explorado abaixo), o que poderia fazer com que o Brasil fosse incluído pela Comissão da União Europeia na lista dos países que apresentam padrões elevados de proteção de dados. Tal inclusão permitiria, por exemplo, que transferências internacionais de dados pessoais para o Brasil ocorressem sem a necessidade das chamadas *appropriate safeguards* (art. 46 da GDPR), como a obrigação de manter contratos suficientemente protetivos (e que contenham cláusulas padronizadas) entre as entidades envolvidas nas referidas transferências.

Quanto mais elevados os padrões de proteção de dados do país destinatário dos dados pessoais protegidos pela GDPR – na perspectiva da União Europeia –, tanto menores são as obrigações, custos e burocracias necessários à transferência desses dados a países de fora da União Europeia. Não é demais considerar, portanto, que a LGPD consiste em uma iniciativa que permite que o Brasil seja visto, interna e

externamente, como um ambiente seguro para o tratamento e a transferência dos dados pessoais, considerados pilares da economia digital.

Mas o que é a GDPR?

A GDPR é o novo Regulamento Europeu, vigente a partir de 25 de maio de 2018, que dispõe sobre a proteção de dados pessoais de indivíduos que, à época do tratamento de seus dados, estavam localizados em algum país da União Europeia (critério de conexão territorial). Ao atentar para novos paradigmas de relações no ambiente digital e de atuação das empresas de tecnologia, a GDPR revolucionou os padrões de proteção de dados até então praticados, buscando difundir um novo padrão para o tratamento dos dados pessoais, inspirado nos princípios da legalidade, transparência, privacidade e *accountability*. Nos termos do novo regramento europeu, os dados pessoais só podem ser tratados de forma justa, responsável e fundada, a partir do (i) consentimento do indivíduo; ou (ii) se houver legítimo interesse de quem os coleta.

Justamente pela amplitude de seu escopo de aplicação, bem como de conceitos positivados como "tratamento", que abrangem desde o armazenamento dos dados pessoais até a sua utilização e transferência, não é demais pensar que a GDPR deverá alterar – como já vem alterando –, a perspectiva econômica e de risco sobre o tratamento de dados pessoais.

Em que medida o texto da LGPD foi influenciado pela GDPR?

A coincidência material entre os conceitos trazidos por ambas as legislações, bem como a organização lógica dos capítulos e artigos, evidencia a inspiração do texto original do projeto de lei da LGPD na GDPR. As duas legislações, por exemplo, apresentam âmbitos de aplicação quase idênticos (com exceção das diferenças territoriais). O mesmo se pode dizer quanto ao conceito de "dado pessoal", à categorização dos responsáveis pelo tratamento dessa modalidade de dados (*controller* e *processor*) e à eleição dos deveres e obrigações desses agentes.

As principais diferenças entre ambos os regramentos são ocasionadas (i) pela organização jurídica das entidades de direito público envolvidas (no caso da GDPR,

Av. Nove de Julho, 3.452, Conjunto 132, São Paulo, SP 01406-000, Brasil T: +55 11 3085 0089 E: info@pglaw.com.br

abre-se a possibilidade para os países da União Europeia regulamentarem, por exemplo, os procedimentos relacionados à aplicação das regras dispostas na legislação); (ii) pela técnica legislativa; e (iii) pela amplitude de determinados conceitos, ampliando ou restringindo o âmbito de incidência da norma.

Após os vetos presidenciais ao texto do projeto de lei da LGPD, algumas dessas diferenças ficaram mais claras, especialmente no tocante ao tratamento de dados pessoais pelo Poder Público. Com efeito, foram vetados dispositivos que continham restrições e vedações ao compartilhamento de dados pessoais entre entidades do Poder Público, sob a justificativa de que essas barreiras poderiam comprometer o regular exercício de diversas atividades e políticas públicas.

Além disso, foram vetados os dispositivos atinentes à criação de uma Autoridade Nacional de Proteção de Dados, o que comprometeu a manutenção de normas visando ao reforço e aplicação da LGPD, bem como à relação entre tal autoridade e outros agentes como o "encarregado" pelo tratamento de dados pessoais (*data Protection officer*, na linguagem da GDPR).

Finalmente, foram retiradas do texto final da LGPD algumas sanções que seriam aplicadas após a apuração do descumprimento de determinados preceitos legais por parte dos responsáveis pelo tratamento de dados pessoais, a exemplo da suspensão parcial ou total do funcionamento do banco de dados a que se referia a infração e a proibição parcial ou total do exercício de determinadas atividades relacionadas ao tratamento de dados pessoais.

Por outro lado, a GDPR contém provisões detalhadas quanto à atuação das chamadas *supervisory authorities*, responsáveis, dentre outras atribuições, pela fiscalização e aplicação da GDPR, conferindo maior seriedade aos mecanismos de *enforcement* da legislação e não deixando dúvidas quanto ao reforço dos direitos dos *data subjects* mesmo ante o tratamento de dados pessoais realizado pelo Poder Público. Nesse sentido, coloca-se em dúvida a efetividade de alguns dispositivos contidos na LGPD, especialmente no tocante aos direitos dos indivíduos cujos dados pessoais foram objeto de tratamento.

LGPD: como os entes privados deverão se preparar

Av. Nove de Julho, 3.452, Conjunto 132, São Paulo, SP 01406-000, Brasil T: +55 11 3085 0089 E: info@pglaw.com.br

Após a entrada em vigor da LGPD, os titulares cujos dados pessoais foram tratados enquanto se encontravam no Brasil poderão exigir uma série de informações dos responsáveis pelo tratamento desses dados, tais como a natureza dos dados que estão sendo tratados, a forma como se dá esse tratamento e com quem foram compartilhados seus dados pessoais. Os responsáveis que não observarem os prazos dispostos na legislação (com destaque para o prazo de resposta de 15 (quinze) dias após requisição de acesso e confirmação de existência pelo titular) poderão se sujeitar a sanções até o limite de R$ 50.000.000,00 (cinquenta milhões de reais) ou 2% (dois por cento) de seu faturamento no último exercício, descontados os tributos, – o que for maior.

Todos os entes privados sujeitos à aplicação da LGPD deverão se preparar para atender às requisições dos titulares com organização e celeridade, sendo recomendável a criação de procedimentos padronizados de resposta aos titulares e de acesso aos dados pessoais deles armazenados, o que poderá gerar a necessidade de alterar a forma como tais dados são armazenados nas bases de dados utilizadas por tais entes. Possivelmente, surgirá a necessidade de criar novas bases de dados contendo o registro de determinadas operações, especialmente as relacionadas à transferência de dados dos titulares para terceiros, o que deverá ampliar consideravelmente o custo de armazenamento de determinadas empresas.

Para determinadas atividades em que não resta claro o interesse legítimo ou, mais especificamente, a base contratual a permitir o tratamento de dados pessoais dos titulares, será necessário obter destes o consentimento por escrito ou por outro meio que demonstre de forma inequívoca a sua vontade, acarretando na necessidade de se realizar uma série de mudanças, em especial, nos meios de contratações digitais que regulam a relação jurídica entre determinadas empresas e os usuários de suas aplicações na Internet.

Os entes privados deverão se posicionar contratualmente, em relação aos indivíduos e/ou entidades com quem compartilharem dados pessoais dos titulares, como responsáveis ou operadores de tais dados. Os entes privados devem também atentar para as diversas obrigações conferidas pela LGPD para cada um desses agentes, bem como para a responsabilidade resultante de eventuais danos causados aos titulares dos dados tratados em descumprimento à LGPD. No caso específico da transferência

Av. Nove de Julho, 3.452, Conjunto 132, São Paulo, SP 01406-000, Brasil T: +55 11 3085 0089 E: info@pglaw.com.br

internacional dos referidos dados, exige-se dos agentes envolvidos na operação um rigor ainda maior na proteção dos direitos dos titulares.

A LGPD, na esteira do regramento europeu, contém dispositivos que descrevem as práticas de tratamento de dados recomendáveis para o Poder Público e os entes privados, que poderão servir de guia, inclusive, para a implementação de procedimentos internos e gerenciais que garantem o cumprimento da legislação no que se refere, inclusive, aos colaboradores e funcionários que fazem parte do dia-a-dia dos responsáveis e operadores.

Exsurge, portanto, a necessidade premente de revisar procedimentos internos e externos de tratamento de dados pessoais, no âmbito dos entes privados. Tendo em vista o potencial de extensão dos mercados consumidores de produtos e serviços oferecidos em meio digital, é possível que algumas empresas tenham que se adaptar aos mais diversos regramentos de proteção de dados pessoais, incluindo a GDPR. Por ser de interesse de muitas empresas brasileiras atingir o mercado europeu, pode ser igualmente importante para elas atentarem-se para a aplicação do regramento europeu por meio das *supervisory authorities* e judiciários dos países pertencentes à União Europeia, o que deverá servir de referencial para a medição dos riscos aos quais estarão sujeitas, inclusive, do ponto de vista das autoridades brasileiras.

Av. Nove de Julho, 3.452, Conjunto 132, São Paulo, SP 01406-000, Brasil T: +55 11 3085 0089 E: info@pglaw.com.br