Proteção de Dados e Direito Digital

Ana Carolina Cagnoni

A futura Lei Geral de Proteção Dados Brasileira

Novidades que já podemos esperar

O ano de 2018 nem bem chegou à metade de seu curso e já podemos dizer que a proteção jurídica concedida a dados pessoais é um dos temas mais debatidos do ano. A privacidade dos indivíduos e a forma como dados pessoais são coletados, utilizados, transferidos e armazenados por empresas e entidades do governo estão na mira de debates acalorados, em inúmeras matérias de jornal, em temas de seminários diversos e, também, em algumas ações judiciais. Muito difícil que o leitor, mais ou menos atento, ainda não tenha se deparado com a frase "dados são o novo petróleo". E bem, se isso é verdade, estamos vivendo no Brasil (e no mundo) uma verdadeira corrida por garantir uma maior proteção, ou ao menos debater como fazer isso.

Razões não faltam, porém, para que o debate se coloque na pauta do dia. No cenário internacional, em março, o escândalo relacionado às atuações da Cambridge Analytica, consultoria contratada para influenciar eleições em diversos países atuando mediante dados de usuários do Facebook (plataforma com aproximadamente 1/3 da população mundial), trouxe à tona quão sensível é o tema e, ao mesmo tempo, quão complexa é a sua regulação. Coincidências a parte, em maio nos deparamos com a entrada em vigor da Regulamentação Europeia para Proteção de Dados Pessoais (mais conhecida como "GDPR – *General Regulation for Data Protection*"), normativa que visa justamente enfrentar o desafio e melhor regular o uso de dados pessoais, protegendo o titular frente a empresas que atuam dentro ou fora da Europa.

No Brasil, o primeiro semestre também está agitado. Mesmo sem nenhuma mudança em nossa legislação, tivemos medidas significativas nesta área. A Comissão de Proteção de Dados Pessoais, do Ministério Público do Distrito Federal e Territórios vem atuando, quase que mensalmente, na instauração de Inquéritos Civis Públicos e Procedimentos Preparatórios para apurar uso não autorizado de dados pessoais e/ou vazamentos e incidentes de segurança. Além disso, a Portaria Normativa 539, editada em abril por este MP, confere à Comissão nova competência para *"promover a defesa dos interesses e direitos difusos, coletivos e individuais homogêneos dos titulares de dados pessoais"*. Além disso, vimos a propositura de duas Ações Civis Públicas que

tocam o tema, uma pelo Ministério Público Federal de São Paulo e outra pelo Ministério Público do Rio de Janeiro. Por fim, o Banco Central emitiu a Resolução 4.658 que trata dos parâmetros para adoção de políticas cibernéticas e requisitos para contratação, por instituições financeiras, de serviços de processamento e armazenamento de dados em nuvem.

No meio legislativo, contudo, temos ainda mais discussões. Encontram-se em tramitação dois projetos de lei com maiores chances de aprovação, cada um proposto por uma das casas do Congresso Nacional. Assim "PLS 330" e "PL 4060/5276" (agora PLC 53) são os identificadores centrais do debate porque, se aprovados, inaugurariam uma nova fase de proteção jurídica para dados pessoais no país, afastando nosso ordenamento do atual modelo de regulamentação setorial e específica. Ou seja, qualquer um deles criaria a "Lei Geral de Proteção de Dados Brasileira".

Para aqueles que acompanham de perto a movimentação legislativa, as diversas emendas e projetos substitutivos que circulam há alguns anos, é inegável perceber como temos evoluído para projetos de lei claramente inspirados em experiências internacionais, especialmente na GDPR e na sua estrutura de *enforcement*. Da mesma forma, a despeito de suas diferenças, também são significativas as semelhanças entre os projetos.

Por esta razão, decidimos elencar **quatro inovações que serão realidade no país** caso qualquer um destes projetos seja aprovado pelo Congresso Nacional.

- **DIFERENCIAÇÃO ENTRE RESPONSÁVEL E OPERADOR EM ATIVIDADES DE PROCESSAMENTO DE DADOS**

Outra novidade a ser introduzida pela nova lei geral será a diferenciação entre agentes que realizam o tratamento de dados pessoais. Da mesma forma que na GDPR, os projetos de lei analisados aqui trazem a diferenciação entre quem é o "responsável" pelo tratamento dos dados e quem é o "operador" que realiza tal tratamento. E mais uma vez, a definição estabelecida nas propostas é igual. Entender-se-á como "responsável" a empresa, entidade ou órgão que **tomar decisões quanto como se dará o tratamento de dados pessoais**. Por outro lado, "operador" será a empresa ou entidade vinculada ao "responsável" encarregada de realizar tais atividades.

Tais distinções serão relevantes no momento de se apurar as responsabilidades frente ao dano causado ao titular dos dados. E é importante ressaltar aqui que os projetos estabelecem a possibilidade de responsabilidade solidária entre agentes e, mesmo que as propostas legislativas não criem tal vínculo de solidariedade exatamente da mesma forma, ambas garantem o direito de regresso àquele que foi obrigado a reparar o dano integralmente. Entende-se que esta seria uma medida de garantir efetiva indenização ao titular dos dados, parte mais vulnerável da relação.

- **NOVAS REGRAS PARA TRANSFERÊNCIA INTERNACIONAL DE DADOS**

A entrada em vigor da GDPR, como não poderia deixar de ser, trouxe grande discussão em torno das regras relacionadas à transferência internacional de dados, ou seja, o envio de dados pessoais coletados em determinado território para ser "tratado" em outra jurisdição. Afinal, esta é uma prática comum de nossos tempos, principalmente em razão da internet e da existência de

empresas atuando globalmente, algumas operando exclusivamente *online*. O problema surge quando há uso não autorizado de dados pessoais ou até incidentes de segurança em outra jurisdição que não aquela onde se encontra o titular dos dados. Além de ser este também um tema caro às discussões relacionadas à defesa nacional e segurança pública.

Surge a necessidade, portanto, de se estabelecerem normas para regular o trânsito de informações pessoais. E ambas propostas legislativas não se furtam em estabelecer tais regras. **Os dois textos, portanto, determinam critérios muito semelhantes para que empresas no Brasil transfiram dados ao exterior legalmente.** Dentre estes cabe frisar (a) a possibilidade de transferência lícita para "país ou organização internacionais com grau de proteção adequado", a ser declarado por autoridade competente; (b) a possibilidade de transferência mediante consentimento específico, livre e informado do titular dos dados e (c) a possibilidade de transferência quando o responsável oferecer garantias ao titular do cumprimento dos direitos, princípios e regime de proteção da lei brasileira na jurisdição de destino. Cada uma destas hipóteses traz desafios diferentes, a serem avaliados cuidadosamente, às empresas que transferem dados ao exterior, a depender do país de destino, do tipo dos dados e/ou da estrutura da corporação.

- **APLICAÇÃO DA LEI PARA ENTIDADES PÚBLICAS E PRIVADAS**

Por diversas vezes, ao lermos artigos ou participarmos de discussões relacionadas à privacidade, proteção de dados, big data ou internet das coisas, verificamos que o enfoque dado ao debate é restrito ao tratamento e uso de dados pessoais por empresas do setor privado, dos mais diversos mercados, das mais distintas áreas de atuação. Isso pode levar o leitor a concluir que os projetos de lei em debate não seriam aplicáveis a entidades governamentais, órgãos estatais ou até empresas públicas ou de economia mista.

Da mesma forma, sabemos que entes públicos em todas as esferas (bancos públicos, hospitais e postos de saúde, órgãos de controle fiscal e tributário, bases de dados de serviços assistenciais, judiciais e penitenciários, escolares, para citar alguns), inegavelmente, têm acesso, utilizam e armazenam dados pessoais de todos os cidadãos brasileiros. Razoável, portanto, que uma lei que visa a proteção do titular dos dados pessoais possa garantir tal proteção também contra entidades públicas de forma mais concreta e eficiente do que a legislação atual.

Felizmente, é o caso. Ambos os projetos, em maior ou menor grau, trazem capítulos específicos que detalham quais as **normas e responsabilidades dos órgãos do setor público** frente à proteção dos dados pessoais que dispõem e, sabidamente, se utilizam. Serão, portanto, impostas a tais entes públicos deveres e responsabilidades quanto ao uso dos dados pessoais dos brasileiros, cujos direitos estarão assegurados da mesma forma.

- **BOAS PRÁTICAS COMO CRITÉRIO DE PONDERAÇÃO NA APLICAÇÃO DE MULTAS E SANÇÕES**

Por fim, é importante mencionar que ambos projetos trazem um rol de sanções a serem aplicadas àqueles que violarem os termos da futura lei. Tais sanções são apresentadas em lista que se inicia pelo menos gravoso (advertência) e evolui para o mais gravoso ao infrator (proibição parcial ou

total do exercício das atividades de tratamento de dados). Cumpre observar que este modelo e estas sanções são as mesmas hoje em vigor no Marco Civil da Internet.

Quanto à multa estabelecida, **ambas propostas legislativas trazem o valor de 2% do faturamento** da empresa ou grupo econômico no Brasil, no último exercício. Contudo, enquanto que o PLS 330 determina que a multa deve ser aplicada apenas em caso de reincidência de infração já sancionada, o PL 4060/5276 não impõe essa condição e ainda prevê a possibilidade de aplicação diária, mas limita seu valor a 50 milhões de reais por infração.

Ressalte-se que as duas propostas também incluem parâmetros e critérios a serem observados pela autoridade na calibragem das sanções a serem aplicadas, das quais destacamos **(a) a implementação de boas práticas e políticas internas e (b) a adoção de medidas e mecanismos capazes de minimizar o dano ao titular dos dados em caso de infração**. Portanto, resta evidente que a futura lei privilegiará empresas que entendam a responsabilidade de sua atuação no tratamento de dados pessoais e implementem medidas concretas para gerir e devidamente resguardar os dados pessoais dos quais dispõe.

Conclui-se, portanto, que a despeito da existência de dois projetos de lei e das incertezas sobre quando será sua aprovação (com a Copa do Mundo e eleições disputando atenção dos membros do Congresso) é fato, como demonstrado aqui, que as propostas têm diversos pontos de convergência.

E por isso é fundamental notar também que os **prazos estabelecidos nestes projetos para entrada em vigor são extremamente enxutos**, considerando o impacto da nova lei nas atividades de, virtualmente, todas as empresas e órgãos públicos do país. Para adequação, empresas e órgãos estatais teriam apenas 12 meses (no caso do PLS 330) ou 18 meses (no caso do PL 4060/5276). Em termos comparativos, a própria GDPR contou com 24 meses de *vaccatio legis* e, frise-se, ela não foi a primeira normativa europeia sobre o tema que já é debatido no continente há mais de 20 anos.

Desta forma, se é certo que o país caminha para a edição de uma nova Lei Geral de Proteção de Dados, resta imperativo às empresas e entidades afetadas pela nova legislação, seja pelas semelhanças entre os projetos, seja pelo curto prazo disponível após a sua sanção, **tomar medidas imediatas de conscientização** sobre como dados pessoais são coletados, utilizados, transferidos e armazenados no desempenho de suas atividades e **buscar se preparar às mudanças**. Não há, pois, tempo a perder.