Weiss: Paralelo entre LGPD, CCPA e o GDPR europeu

Em setembro de 2020, a Lei Geral de Proteção de Dados (LGPD), 13.709/18, finalmente entrou em vigor. Antes dela, as relações entre empresas e usuários estavam regidas pelo Lei nº 12.965/14, o

Essa lei já protegia os dados dos usuários, exigindo consentimento expresso para coleta e armazenamento e garantindo a exclusão de dados por requerimento, em seu artigo 7º, incisos IX e X, o que foi ratificado na LGPD.

Ambas, assim como as similares da Europa e Califórnia, tentam resolver o maior problema criado pela internet: proteger dados sem turbar a atividade econômica além do estritamente necessário.

O conflito de mais difícil solução ocorre entre as empresas que coletam e tratam dados em escala global, como Google, Apple, Facebook, Instagram, WhatsApp e Twitter, e os usuários localizados em outros países. A maioria das grandes empresas tem sede na Califórnia (salvo a Amazon), sendo regidas pelo CCPA [1] (que é uma alteração do Código Civil da Califórnia) em relação aos usuários lá residentes.

Aos demais usuários, o que inclui os brasileiros, aplica-se, em princípio, à legislação local, o que será o primeiro tópico desse trabalho.

1)Legislação aplicável e abrangência
A definição da legislação aplicável em matéria de relações internacionais, quando não existe uma cláusula expressa, depende dos elementos de conexão, que são os aspectos do fato escolhidos pela lei para definir a competência.

O artigo 3º da LGPD estabeleceu uma ampla abrangência, incluindo qualquer operação de coleta ou tratamento de dados, feita por pessoa natural ou jurídica, que preencha algum dos seguintes requisitos: o titular se encontre em território nacional no momento da coleta (sendo residente ou não no Brasil); o tratamento ocorra em território nacional; a atividade de tratamento vise ao oferecimento de serviços a indivíduos localizados no Brasil.

Em resumo, a LGPD aplica-se a quase toda situação que envolva pessoa física ou jurídica localizada no Brasil, com exceção da mera coleta de dados, por empresa brasileira, de usuários localizados no exterior, com imediato repasse a empresa também localizada no exterior, sem qualquer espécie de tratamento no Brasil (hipótese de difícil configuração).

As três leis protegem os dados apenas das pessoas físicas. O GDPR e a LGPD se aplicam às que estejam no território europeu ou brasileiro, residentes ou não (artigos 1º e 5º, inciso I). O CCPA é mais restritivo e versa apenas sobre os dados das pessoas físicas residentes na Califórnia (artigo 1.798.140, "g").

No Brasil, as pessoas jurídicas que se sentirem lesadas podem recorrer ao Código de Defesa do Consumidor, que expressamente as inclui em seu artigo 2º. O marco civil já previa essa aplicação subsidiária, não afastada pela LGPD.

O CCPA também restringiu o universo de empresas submetidas à lei. Apenas aquelas com finalidade lucrativa (artigo 1.798.140, "c", 1) e que atendam a pelo menos um dos seguintes três requisitos: receita bruta anual superior a 25 milhões de dólares; tratem dados de mais de 50 mil pessoas; obtenham mais da metade de sua receita anual da venda de dados pessoais.

Em respeito ao federalismo, o CCPA deixou claro que não se aplica quando todas as etapas de coleta de dados, tratamento e comercialização ocorrerem fora do Estado. Ou seja, quando o residente da Califórnia estiver fora dos limites e as empresas também (artigo 1.798.140, "a").

O CCPA ainda incluiu um dispositivo antifraude, voltado a evitar que as empresas escapem da sua aplicação por meio de subterfúgios. O artigo 1.798.190 prevê a figura ilícita da *serie of steps* (construção gradual de uma relação jurídica artificial) para escapar à aplicação da lei, semelhante às normas sobre fraudes tributárias.

O GDPR [2] define sua abrangência territorial no artigo 3º, de forma ainda mais ampla que a LGPD. Inclui o tratamento de dados controlado ou executado por empresas localizadas na União Europeia, mesmo que gerido por empresas situadas em outros países. Também vincula empresas localizadas em países signatários de tratados que admitam a aplicação da legislação de algum país da União Europeia.

2) Competência regulamentar e fiscalizatória

A diferença de formato entre o federalismo americano e o brasileiro gera competências distintas para regular o tratamento de dados. Nos Estados Unidos, compete aos Estados tudo o que não for atribuído ao governo federal. Em consequência, a CCPA pôde regular inteiramente a matéria, já que não há menção na Constituição americana a essa atribuição. A competência regulamentar é do *attorney general*, nos termos do artigo 1.798.185.

No Brasil, as competências concorrentes entre União e Estados são listadas no artigo 24, da Constituição, cabendo à União as normas gerais e aos Estados, as específicas.

O tratamento de dados das pessoas físicas por empresas, que é o conteúdo essencial da LGPD, inclui-se nos incisos V, "produção e consumo", VIII, "responsabilidade por dano ao consumidor", e XV, "proteção à infância e à juventude". A leitura dos quatro parágrafos do artigo 24 permite concluir que leis estaduais poderão prever multas, procedimentos administrativos de apuração de irregularidades e de mediação, mas sempre respeitando os conceitos, as listagens dos direitos, as exclusões de incidência e as vedações previstas na lei federal.

A LGPD, por meio dos artigos 55-A e seguintes, criou a Agência Nacional de Proteção de Dados (ANPD), com competência regulamentar e fiscalizatória. Os artigos 58-A e seguintes instituíram o Conselho Nacional de Proteção de Dados (CNPD), com funções apenas consultivas. Ambos ainda em fase de implantação.

A GDPR prevê o estabelecimento de penalidades por normas dos países-membros da União Europeia, em seus artigos 83 (limites) e 84. A aplicação das multas depende da instituição de autoridades supervisoras independentes, criadas por cada país, o que está previsto nos artigos 51 a 59. Essas autoridades devem zelar para que as penalidades sejam efetivas, proporcionais e dissuasivas (artigo 83).

O CCPA e a LGPD criaram fundos orçamentários para receber uma parte ou até a totalidade das multas, por meio dos artigos 1.798.160, a, e 52, §5º.

3) Consentimento dos usuários
Outra distinção relevante entre as três leis é quanto ao direito ao uso de dados. O artigo 7º da LGPD exige o consentimento expresso do usuário para que as empresas utilizem seus dados. O artigo 7º do GDPR deixa espaço para cada país decidir se o processamento de dados depende do consentimento expresso, sempre garantido o direito do usuário a revogar a autorização a qualquer momento.

A LGPD, em seus artigos 5º, II, e 11, instituiu a figura dos dados pessoais sensíveis (religião, etnia, opinião política, entre outros), cuja utilização exige consentimento "de forma específica e destacada". Os dados das crianças e adolescentes receberam semelhante tratamento, no artigo 14, §1º. O GDPR prevê a necessidade de consentimento explícito para propósitos específicos, no artigo 9º e item 1, que inclui aspectos raciais, étnicos, religiosos e até convicções filosóficas.

Em sentido oposto, mais preocupado com a agilidade empresarial, o CCPA presume a autorização desde que o usuário tenha mais de 16 anos e tenha havido um claro aviso por parte da empresa. Ao consumidor é sempre garantido o direito de solicitar a retirada dos dados, o chamado *opt out.* Consumidores entre 13 e 16 anos precisam autorizar expressamente a coleta de dados. Caso tenham menos de 13 anos, a autorização deve partir dos pais ou responsáveis (artigo 1.798.120, "d").

Apesar da presunção de autorização, o CCPA não permite que os usuários californianos renunciem aos direitos nela previstos, o que constitui uma garantia contra a venda ou renúncia por engano, mas limita a negociação de direitos (artigo 1.798.192). A LGPD e o GDPR não possuem vedações semelhantes, o que proporciona mais riscos aos usuários, mas, também, mais liberdade de negociação.

As três leis excluem de sua incidência os dados desidentificados, que a lei brasileira denominou anonimizados, bem como os dados de utilidade pública, como os necessários à segurança nacional e aos processos judiciais (LGPD artigo 7º, II a X, 11, II, e 12, CCPA artigo 1.798.145, e GDPR artigo 23).

Ao contrário da LGPD, o CCPA define conceitos como agregação, desidentificação e pseudonimização de dados, no artigo 1.798.140. O GDPR também o faz em seu artigo 4º, embora de forma menos extensa que o CCPA.

4) Execução das leis
A LGPD determinou que todas as entidades e empresas que controlem e operem dados pessoais (artigo 5, VI e VII) instituam um encarregado pelo tratamento de dados pessoais, que zelará pela proteção dos dados dos usuários (artigo 41, §2º, I a IV, e 46, entre outros).

O GDPR impôs às empresas que coletem e processem dados a elaboração de avaliações e relatórios das medidas de proteção de dados. O Recital 84 os denominou *risk evaluation* e *impact assessment*, o que foi ratificado no artigo 35, que formalmente criou os chamados *data protection impact assessment* (DPIA). Também criou o *data protection officer* (DPO), em seus artigos 37 e 38, figura adotada na LGPD por meio dos referidos encarregados.

A principal diferença para a LGPD é que no GDPR a realização do DPIA decorre diretamente da verificação de um alto risco em relação à privacidade dos dados. É dever da empresa constatar esse nível de risco, sem prejuízo da imposição pela autoridade supervisora local. A LGPD menciona esse relatório nos artigos 5º, XVII, 10, §3º, e 38, mas não é clara ao determinar as situações em que ele deve ser instituído pelas empresas, deixando margem de discricionariedade para a ANPD.

O CCPA não cria figuras como o encarregado de tratamento de dados, mas, no artigo 1.798.130, estabelece os requisitos mínimos para o cumprimento da norma: pelo menos dois meios de contato, um telefone e um website, responder em 45 dias e por meios transmissíveis, entre outros.

Uma questão em aberto é sobre a possibilidade de usuários domiciliados em um país moverem ações contra as empresas na sede delas, mas escolhendo a lei que mais lhes convier.

A LGPD e o GDPR não tratam dessa opção. O CCPA exclui a possibilidade de sua aplicação por pessoas não abrangidas por ela, como os residentes em outros estados americanos ou no exterior (artigo 1.798.150, 3, "c"). O CCPA veda, ainda, sua própria aplicação mesclada com fundamentos de outra norma (artigo 1.798.150, "c").

Por outro lado, o mesmo dispositivo, em sua parte final, também deixa claro que o CCPA não pode ser usado para excluir qualquer direito de usuários com base em outra lei. Em complemento, o artigo 1.798.175 garante a prevalência da lei mais favorável aos consumidores (*"but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control"*).

A LGPD e o GDPR não limitam o valor das indenizações para casos de invasão e roubo de dados (hackeamento). Os usuários lesados podem acionar as empresas responsáveis pelos dados vazados nos países em que residirem (desde que elas tenham algum escritório ou filial), pleiteando indenizações proporcionais à lesão sofrida.

O CCPA, por aplicar-se às empresas californianas que coletam dados de bilhões de usuários do mundo todo, estabeleceu, em seu artigo 1.798.150, "a", 1, limites mínimo e máximo de indenização, entre 100 e 750 dólares por invasão ou por efetivo dano. Tais limites só se aplicam aos usuários residentes na Califórnia.

O mesmo dispositivo criou uma linha de defesa para as empresas ao definir a falha em proteger os dados dos usuários como *"violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information"*.

Ou seja, as empresas receberam da própria lei que limitou a indenização um argumento de defesa pautado na razoabilidade dos procedimentos de segurança adotados, que, uma vez comprovada, pode excluir o direito ao ressarcimento de danos por parte dos usuários que tiveram seus dados vazados.

[1] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
A CCPA entrou amplamente em vigor no último dia 1º de julho.

[2] https://gdpr-info.eu/art-4-gdpr/ O GDPR foi aprovado pelo Conselho Europeu em 2016 e entrou em vigor em maio de 2018. Consiste em 173 *recitals* (considerandos) e 99 artigos, devendo ser completado pelas normas de cada país componente da União Europeia.

Date Created
28/10/2020