1516-8182
10.25059/2527-2594/retratosdeassentamentos/2024.v27i2.621
Retratos de Assentamentos

Recebimento: 05/01/2024
Aceite: 20/02/2024

Meio ambiente virtual: a lei de proteção de dados pessoais da China

Patrícia Guedes Gomide Nascimento Gomes[I]*
Hildebrando Herrmann[I]
Vera Lúcia Silveira Botta Ferrante[I]
Zildo Gallo[I]

Resumo: Escândalos de sérios e grandes vazamentos de dados pessoais ocorridos nos Estados Unidos da América, os casos Cambridge Analytica e Edward Snowden, levaram o mundo a questionar a segurança, proteção e privacidade dos dados pessoais que trafegam no meio ambiente virtual. Esses vazamentos de dados revelaram a necessidade premente de proteger e preservar os dados pessoais existentes nos mais diversos bancos de dados existentes na rede mundial de computadores e fora dela. A União Europeia saiu na frente e promulgou o GDPR. Em seguida veio o CCPA do Estado da Califórnia. Após, veio o Brasil, que, levando em consideração o teor do GDPR, criou a sua legislação de proteção de dados pessoais, a LGPD. Em novembro de 2021 a República Popular da China publicou o PIPL, sua legislação de proteção de dados pessoais. O objetivo do presente artigo é verificar a legislação da China.

Palavras-chave: Direito à privacidade; Vazamentos de dados; Dados pessoais; LGPD; Proteção.

Virtual Environment: China's Personal Data Protection Law

Abstract: Scandals of serious and large leaks of personal data that occurred in the United States of America, the Cambridge Analytica and Edward Snowden cases, led the world to question the security, protection and privacy of personal data that travel in the virtual environment. These data leaks revealed the pressing need to protect and preserve personal data in the most diverse databases on the world wide web and beyond. The European Union took the lead and enacted the GDPR. Next came the CCPA from the State of California. Then came Brazil, which, taking into account the content of the GDPR, created its personal data protection legislation, the LGPD. In November 2021, the People's Republic of China published the PIPL, its personal data protection legislation. The objective of this article is to verify China's legislation.

Keywords: Right to privacy; Data leaks; Personal data; LGPD; Protection.

[I]Universidade de Araraquara- UNIARA, Brasil. *Autora correspondente: patriciagomide@gmail.com

Introdução

O objetivo do presente trabalho é avaliar a legislação de proteção de dados pessoais da República Popular da China, denominado PIPL.

Hoje, os cidadãos vivem numa sociedade vigiada na internet, todos os seus cliques na rede, suas buscas em sites de pesquisa, suas curtidas e compartilhamentos nas redes sociais geram dados no meio ambiente virtual que contém informações valiosas de cada um dos cidadãos, com indicativos de dados da personalidade e características individuais, que, segundo Rodotá (2008), se denomina por sociedade em rede.

Demonstrando a inexistência de segurança na rede, dois escândalos de vazamento de dados havidos entre 2013 e 2015, respectivamente, causados por Edward Snowden e pela Cambridge Analytica, deixaram o mundo em estado de alerta e evidenciaram a necessidade premente de preservar e proteger os dados pessoais constantes nas mais diversas bases de dados existentes, especialmente no ambiente virtual (BBC, 2018).

Em 2013, Edward Snowden divulgou detalhes do programa de interceptação de dados e comunicações eletrônicas em massa da Agência de Segurança Nacional Norte Americana, da qual era funcionário (GREENWALD, 2014). Os documentos e dados por ele divulgados demonstraram o amplo projeto de espionagem eletrônica realizado pelos Estados Unidos da América ao redor do globo (GREENWALD, 2014).

A Cambridge Analytica foi a empresa que atuou na campanha do então candidato à presidência dos Estados Unidos da América, Donald Trump. O caso se tratou do vazamento de dados de mais de 50 milhões de usuários do Facebook, e ocorreu devido a um teste criado por um russo, que obteve de forma consentida dados dos usuários da rede que realizaram o teste por ele desenvolvido, obtidos, especificamente, dos usuários cadastrados no site do Facebook, e comercializados à Cambridge Analytica (BBC, 2018). O problema não foi especificamente o teste, mas os dados que foram voluntariamente disponibilizados, posteriormente vendidos, e que foram utilizados no período eleitoral para direcionar ações pontuais de cunho político (PRESSE, 2019).

Esses escândalos demonstraram ao mundo a absoluta vulnerabilidade dos dados pessoais no meio ambiente virtual, levando os países à corrida para a proteção de dados pessoais (MONTEIRO, 2018). A comunidade europeia foi a primeira a promulgar seu regulamento em 2016, denominado GDPR, que entrou em vigor em 25 de maio de 2018.

A Lei do Estado da Califórnia, o CCPA – Califórnia Consumer Privacy Act, em português, Lei de Privacidade do Consumidor da Califórnia, promulgada em 2018 e em vigor desde 1° de janeiro de 2020 (TROJAN, 2019).

Visando adequar-se e estar em conformidade com a comunidade europeia (PINHEIRO, 2019), o Brasil promulgou a sua lei de proteção de dados, deno-

minada por LGPD – Lei geral de proteção de dados pessoais, n° 13.709, de 14 de agosto de 2018, publicada em 15 de agosto de 2018, com dispositivos que entraram em vigor de imediato e outros apenas em 18 de setembro de 2020, com a exceção das sanções previstas na lei, que entraram em vigor em 1° de agosto de 2021 (KUCEK, 2020).

A LGPD está levando empresas públicas e privadas que tratam, armazenam e coletam dados pessoais, a correrem para se adequar às disposições legais, traçando planos para a adequação e implementação, a fim de evitar vazamento de dados e a aplicação das pesadas multas estabelecidas pela legislação, em cada caso específico, e demais sanções estabelecidas pelo legislador (PINHEIRO, 2019).

A China também promulgou sua legislação de proteção de dados pessoais, seguindo os demais países.

A legislação de dados pessoais da China, lei denominada pela tradução do texto para o inglês pela DigiChina da Universidade de Stanford, por PIPL – Personal Information Protection Law, em português, Lei de Proteção de Informações Pessoais, que entrou em vigor em 1° de novembro de 2021, pode ser considerada como uma legislação mais alinhada ao GDPR e a LGPD, por sua abrangência.

Atentos às legislações acima mencionadas o presente artigo se importou em analisar, em linhas gerais, a legislação da China, estabelecendo alguns comparativos a fim de identificar eventuais semelhanças ou discrepâncias, em especial, no que diz respeito à garantia de proteção de dados pessoais.

Importante estabelecer que pelo teor da Declaração Universal dos Direitos Humanos (ONU, 2020), o direito à privacidade é considerado como tutela de direito personalíssimo e assim foi tratado pela maioria das legislações promulgadas.

O PIPL da China

Em 2021, entrou em vigor na China a sua lei de proteção de dados pessoais, denominada pela tradução do texto para o inglês pela DigiChina da Universidade de Stanford. por PIPL – Personal Information Protection Law, em português, Lei de Proteção de Informações Pessoais, que entrou em vigor em 1° de novembro de 2021, e pode ser considerada como uma legislação alinhada ao GDPR e a LGPD, por sua abrangência.

Além do PIPL, a China também dispõe de uma lei específica sobre Cibersegurança (CSL), que trata de todo tipo de dado e não apenas de dado pessoal, e entrou em vigor em 1° de junho de 2017, e de uma lei de segurança de dados (DSL), que entrou em vigor em 1° de setembro de 2021, o Código Civil Chines, e outras (PEÇANHA DE SOUZA, 2021).

Importante elucidar antes de adentrar à análise, que a intenção de proteção do PIPL não é necessariamente a proteção de direitos individuais, mas sim a segurança nacional e o controle do estado sobre os dados.

Pois bem, um detalhe bastante importante da legislação chinesa é a de que ela protege o titular do dado contra empresas privadas, mas o governo e empresas públicas podem ter acesso a todos os bancos de dados existentes. A esse respeito, é importante esclarecer que o governo chinês tem o direito de verificar tudo o que o cidadão chinês publica e sua interação na rede, com finalidade de garantir a segurança nacional (GOGONI, 2021). Não significa que as empresas públicas não devam se adequar e aplicar a legislação, significa apenas que não responderão por eventual violação de dados.

Segundo Gogoni (2021), a promulgação do PIPL, levou à saída de várias empresas estrangeiras da República Popular da China, diante das exigências do governo chinês no que diz respeito aos dados dos cidadãos chineses. As exigências impostas pelo PIPL geram elevados custos às empresas, o que as espantou da China, a exemplo da Microsoft e do Yahoo que encerraram suas atividades no país.

O PIPL tem aplicação extraterritorial, ou seja, não se restringe à República Popular da China, pois se aplica a atividades de tratamento de dados dentro do país e fora dele, no que concerne a residentes na China (artigo 3° do PIPL, 2021). O tratamento transfronteiriço de dados deve obedecer ao estabelecido no respectivo tópico da legislação, do qual destacamos os artigos 38 e 39.

A legislação protege os dados pessoais da pessoa física identificada ou identificável, excluindo, como ocorre na LGPD, o dado anônimo (artigo 4° do PIPL, 2021).

Define dados pessoais como qualquer tipo de informação relativa a uma pessoa natural identificada ou identificável, seja eletronicamente ou de outra forma registrada e também aborda o que denomina por dado pessoal confidencial, no qual estão incluídos os dados biométricos, religião, informações de saúde, contas financeiras, informações de localização e informações de menores.

Os princípios aplicáveis na legislação no que concerne ao tratamento de dados são os da transparência, legalidade, necessidade e boa-fé, sendo certo que para o tratamento de dados pessoais deve haver um propósito claro e razoável, caso contrário não é aceita a realização do tratamento, sendo certo, inclusive, que a coleta excessiva de dados é proibida pela lei (artigos 5°, 6° e 7° do PIPL, 2021).

Não é aceita a coleta coercitiva de dados pessoais, havendo expressa vedação na lei nesse sentido.

Logo, para que uma empresa possa tratar dados pessoais deve observar estritamente o teor da lei, agir com transparência, indicando ao titular o que será tratado e com qual finalidade, informando ainda a necessidade para o dado ser tratado. Desta forma, não é possível exagerar na coleta de dados pessoais, prevalecendo o mínimo possível de coleta para o específico propósito de tratamento.

É vedado o uso e tratamento de informações irrelevantes à finalidade principal do tratamento do dado pessoal (art. 6° PIPL, 2021). É certo que a gestão de dados pessoais precisa assegurar a integridade dessas informações, a fim de

prevenir efeitos adversos nos direitos e interesses dos indivíduos que possam resultar de imprecisões ou lacunas nos dados pessoais (art. 8° do PIPL, 2021).

As organizações que lidam com o tratamento de dados pessoais são responsáveis por suas operações de processamento e devem adotar as providências necessárias para assegurar a proteção das informações pessoais manipuladas (art. 9° do PIPL, 2021).

Além disso, ninguém pode manipular informações pessoais infringindo leis e normas administrativas, e não é permitido se envolver em atividades de tratamento de dados que possam comprometer interesses púbicos ou a segurança do país (art. 10 do PIPL, 2021).

Segundo o artigo 13 do PIPL, a base legal primordial para o tratamento é o consentimento, expresso e informado, que deve ser prévio. Há necessidade de consentimento específico para o tratamento de dados confidenciais, assim como a transferência de dados para outro país ou no caso de realização de marketing direto, divulgação pública de dados, transferência de dados a outro controlador. A intenção do legislador é de que haja total transparência quando da solicitação do consentimento, a fim de que o consentimento seja fornecido, ou não, de forma livre, em especial, que o titular tenha total conhecimento prévio de modo preciso, e ainda com as razões para o tratamento de seus dados (LEE, CHI, CHEN, *et al.*, 2021).

Outras bases legais também existem, a exemplo do GDPR e da LGPD, que são: necessidade de tratamento para o cumprimento de contratos, inclusive de trabalho, para o cumprimento de obrigações estatutárias ou legais, em casos de incidentes de saúde pública ou para a proteção da vida e saúde das pessoas, para a segurança pessoal e patrimonial, para fins jornalísticos e de interesse público e outros (artigos 13 e 14 do PIPL, 2021).

Para processar informações pessoais de menores de 14 anos a entidade deverá obter o expresso consentimento dos pais ou responsáveis (art. 15, do PIPL, 2021).

Além das bases legais, há necessidade de informar o titular sobre o tratamento que será realizado e para qual razão os dados serão tratados, de forma que o titular possa adequadamente consentir com o tratamento (artigos 16 e 17 do PIPL, 2021). Se houver mudança no tratamento do dado, mudança de finalidade do tratamento o indivíduo deverá ser comunicado da alteração e autorizar, ou não, o novo tratamento (artigos 18 e 24 do PIPL, 2021).

A legislação não estabelece um período de tempo para o tratamento do dado pessoal, no entanto dispõe no artigo 20 que o período de retenção da informação deve ser o menor necessário ao atingimento da necessidade de tratamento.

Segundo o artigo 21 do PIPL é possível a mais de uma entidade, em conjunto, processar e tratar dados pessoais de indivíduos chineses desde que observadas as bases de dados legais existentes, o que leva à solidariedade entre elas em caso de violação da lei.

O artigo 27 do PIPL traz um dispositivo específico acerca da coleta da biometria facial, através de câmeras de segurança espalhadas pelas ruas do país, para fins de segurança pública. Essas imagens não podem ser utilizadas para qualquer outra finalidade, salvo com autorização expressa do titular. Não há dispositivo semelhante no GDPR, LGPD ou CCPA.

Para o tratamento de informações sensíveis deve ser obtido um consentimento específico. São dados considerados sensíveis pelo PIPL, a teor do artigo 29, a biometria, credo, saúde, informações financeiras, geolocalização, dentre outras não especificadas na lei.

As empresas são obrigadas a manter protegidas informações pessoais e confidenciais, criando e implantando sistemas de gerenciamento de segurança de dados, o que inclui a aplicação de medidas técnicas adequadas contra o processamento ilegal dos dados, além de proteção contra o vazamento de dados, estando, ainda, obrigadas a comunicar a autoridade no caso de ocorrência de vazamento de dados. Essas medidas de segurança devem ser implantadas com base nas legislações existentes (CSL, DSL, PIPL) na República Popular da China.

A lei também estabelece o regramento adequado para o tratamento de dados a ser realizado por agências estatais, a teor dos artigos 33 a 37 do PIPL.

O titular do dado pessoal tem o direito de solicitar a adequação ou a correção do dado (art. 46 do PIPL, 2021), a exclusão (art. 47 do PIPL, 2021), a anonimização, e pode também cancelar o consentimento antes concedido, e pedir explicações sobre as regras de usadas pela entidade para o tratamento do dado pessoal (art. 48 do PIPL, 2021).

A legislação ainda estabelece que as entidades devem adotar regras de prevenção de vazamento, roubo, alteração ou eliminação de dados pessoais, determinando que de acordo com a finalidade e método do processamento, o tipo de informação pessoal, o impacto nos indivíduos, os possíveis riscos de segurança, as entidades de tratamento devem implementar as ações necessárias para assegurar que as operações de processamento de informações pessoais estejam em conformidade com as leis e normas administrativas (art. 51 do PIPL, 2021).

Se as organizações que processam informações pessoais detectarem um vazamento de dados pessoais, devem agir prontamente, informando os departamentos e pessoas que exercem funções de proteção de informações pessoais (art. 56, do PIPL, 2021).

À semelhança da LGPD e do GDPR, o PIPL também obriga que as empresas mantenham um encarregado de dados, que é o executivo responsável dentro da empresa por supervisionar o tratamento de dados, e que será responsável por tratar com o governo chinês no que diz respeito a prestar esclarecimentos e auxiliar o governo em investigações (GOGONI, 2021). Esse encarregado, deverá

ter seus dados registrados como pessoa responsável junto a autoridade de proteção de dados do país (artigo 52 do PIPL, 2021).

As empresas que não estão estabelecidas na China estão obrigadas a manter no país um encarregado de dados e um departamento de proteção e segurança de dados. A lei também determina que as empresas tornem públicas as informações de contato para o recebimento de reclamações e relatórios.

Em conformidade com o disposto no art. 54 do PIPL, a entidade responsável pelo tratamento de dados pessoais deverá realizar auditorias regulares, a fim de que suas atividades estejam em conformidade com a lei e regulamentos administrativos.

A autoridade pode aplicar sanções às empresas em caso de violação da legislação, a teor dos artigos 65 a 71 da lei, que estabelece multas de mais de um milhão de Yuans. A autoridade de dados da República Popular da China é o CAC – Administração do Ciberespaço da China que através do Departamento estadual de Ciberespaço e Informatização é a principal responsável pelas ações de planejamento e proteção de informações pessoais dentro do território chinês, e, pois, responsável pela verificação de conformidade das empresas ao PIPL, a teor do artigo 40 (LEE, CHI, CHEN, *et al.*, 2021). No entanto, além do CAC outros também podem monitorar a aplicação da legislação, como o Banco Popular da China ou a Comissão Reguladora de Seguros e Bancários da China.

O CAC, será responsável pela verificação de conformidade e juntamente com outros órgãos de proteção locais, pela aplicação das penalidades impostas na legislação (LEE, CHI, CHEN, *et al.*, 2021).

As sanções pela violação à lei podem ir de um milhão de Yuans ou 50 milhões de Yuans ou corresponder a 5% da receita anual do ano anterior ao da violação (art. 65 do PIPL, 2021). Além da multa a autoridade de dados da China também poderá determinar a suspensão de atividades ou a paralisação dos negócios para a retificação e emissão de relatório ao departamento responsável.

Há também sanção para as pessoas físicas diretamente responsáveis pela violação da legislação, sendo que nesses casos a multa será no valor de 10 mil Yuans até 100 mil Yuans.

É importante esclarecer que a legislação não se aplica a dados pessoais processados por indivíduos que processam informações pessoais para questões pessoais ou para propósitos domésticos.

Conclusão

As legislações de proteção de dados pessoais se mostram indispensáveis para a proteção das pessoas, diante do quanto narrado no presente trabalho, em especial diante dos vazamentos de dados reportados.

Muitos países promulgaram suas legislações de proteção de dados pessoais, tal qual ocorreu na União Europeia que saiu na frente, criando o GDPR, seguida pela legislação da Califórnia e posteriormente a legislação brasileira, a LGPD.

Logo após veio a China com sua legislação de proteção de dados pessoais que além de visar a proteção da segurança nacional privilegia também a pessoas. Nesse aspecto e também em outros a legislação chinesa se aproxima muito do Regulamento da União Europeia e da LGPD do Brasil.

A toda evidência, após a leitura de todo o acima relatado, que não representa um estudo exaustivo da legislação chinesa, vemos que o PIPL é bastante rígido e impõe pesados ônus para as empresas que realizam tratamento de dados pessoais na República Popular da China.

As demais legislações, especialmente a brasileira e a da união europeia, estão embasadas na garantia fundamental da tutela da personalidade, tratando o direito à privacidade do dado pessoal como direito personalíssimo do titular, já a legislação chinesa tem como fundamento a segurança nacional.

Referências

BBC News. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades – **Vazamento sem precedentes expôs dados de 50 milhões de usuários e mergulhou empresa em nova crise, pouco tempo depois de comoção sobre disseminação de notícias falsas.** 20/03/2018. Disponível em https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 13 jul. 2024.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. **Lei geral de proteção de dados pessoais.**

BRASIL. **Medida Provisória n° 869, de 27 de dezembro de 2018**. Altera a Lei geral de proteção de dados pessoais.

BRASIL. Lei n° 13.853, de 8 de julho de 2019. Altera a Lei n° 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

CCPA – **Califórnia Consumer Privacy Act**. 2018. Disponível em https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 10 mai. 2024.

DIGICHINA da Universidade de Stanford. Disponível em: https://digichina.stanford.edu/about/. Acesso em 10 de mai. 2024.

GDPR. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 10 mai 2024.

GREENWALD, Glenn. **Sem lugar para se esconder:** Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

GOGONI, R. **Lei de segurança de dados da China pega pesado com big-techs**. 2021. Disponível em: https://meiobit.com/455272/china-lei-privacidade-dados-vs-big-techs/. Acesso em: 16 jul 2024.

KUCEK, G. B. **Lei geral de proteção de dados e sua vigência**. 2020. Disponível em: http://www.agkn.com.br/blog/lei-geral-de-protecao-de-dados-e-sua-vigencia. Acesso em: 11 nov. 2020.

LEE, A.; SHI, M.; CHEN, Q.; HORSLEY, J. P.; SCHAEFER, K.; CREEMERS, R.; WEBSTER, G. Seven Major Changes in China's Finalized Personal Information Protection Law - **Algorithmic discrimination, cross-border data rules, data portability, post-mortem rights, and more**. 2021. Disponível em: https://digichina.stanford.edu/work/seven-major-changes-in-chinas-finalized-personal-information-protection-law/. Acesso em: 11 jul. 2024.

MONTEIRO, R. L. **Lei Geral de Proteção de Dados do Brasil:** análise contextual detalhada - A LGPD terá um impacto na sociedade como poucas leis antes tiveram. Jota, 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018. Acesso em: 10 ago. 2024.

PEÇANHA DE SOUZA, C. **A Lei de proteção de informações pessoais (PIPL) e o papel do direito numa China hiperconectada**. 2021. Disponível em: https://www.observachina.com/post/a-lei-de-prote%C3%A7%C3%A3. Acesso em 10 jan. 2022.

PINHEIRO, P. P. **Palestra proferida no ScaleUp**. Rio de Janeiro, nov. 2019. Disponível em: https://www.youtube.com/watch?v=_H7iz9powFc. Acesso em: 11 jul. 2024.

PIPL- **Personal Information Protection Law**. 2021. Disponível em: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/. Acesso em: 30 jul. 2024.

PRESSE, F. **Cambridge Analytica se declara culpada em caso de uso de dados do Facebook**. 2019. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/01/09/cambridge-analytica-se-declara-culpada-por-uso-de-dados-do-facebook.ghtml. Acesso em: 24 jul. 2024.

RODOTÁ, S. DE MORAES, M. C. B. **A vida na sociedade da vigilância: a privacidade hoje**. São Paulo: Renovar, 2008.

TROJAN, V. A nova lei de privacidade e proteção de dados na Califórnia (CCPA) - **Os principais pontos da nova regulação vista como a 'GDPR da Costa Oeste'**. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-nova-lei-de-privacidade-e-protecao-de-dados-na-california-ccpa-04052019. Acesso em: 12 jul. 2024.