VULNERABILIDADES: PANORAMA DAS LEGISLAÇÕES DE PROTEÇÃO DE DADOS PESSOAIS GDPR, CCPA, LGPD E PIPL

VULNERABILITIES: OVERVIEW OF PERSONAL DATA PROTECTION LEGISLATION GDPR, CCPA, LGPD AND PIPL

Patrícia Guedes Gomide Nascimento Gomes
Hildebrando Herrmann
Vera Botta Silveira Ferrante
Zildo Gallo

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 pela rede mundial de computadores. 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, legislação estadual que não segue exatamente as mesmas bases do GDPR. 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 se as legislações são capazes de garantir proteção aos dados pessoais.

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

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 travels through the world wide web. These data leaks revealed the pressing need to protect and preserve personal data existing in the most diverse databases existing on the world wide web and beyond. The European Union took the lead and enacted the GDPR. Then came the State of California CCPA, state legislation that does not follow exactly the same basis as the GDPR. 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 purpose of this article is to verify if the laws are capable of guaranteeing the protection of personal data.

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

Introdução

O objetivo do presente trabalho é avaliar as legislações de proteção de dados pessoais, sendo o GDPR da União Europeia, o CCPA do Estado da Califórnia-USA, A LGPD do Brasil, e o PIPL da República Popular da China, a fim de entender se efetivamente elas garantem a proteção aos dados pessoais.

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 que contém informações valiosas de cada um dos cidadãos, com indicativos de dados da personalidade e características individuais, que, segundo Rodotá (2008)[1], 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, inclusive, no ambiente virtual (BBC, 2018)[2].

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)[3]. 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).

---

[1] RODOTÁ, Stefano. DE MORAES, Maria Cecília Bodin. A vida na sociedade da vigilância: a privacidade hoje. São Paulo: Renovar, 2008, p.

[2] 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 out. 2019.

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

Esses escândalos demonstraram ao mundo a absoluta vulnerabilidade dos dados pessoais na rede, 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 1º 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, denominada por LGPD – Lei geral de proteção de dados pessoais, nº 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 1º 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 última lei de proteção de dados analisada, a ser promulgada, foi a 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 1º de novembro de 2021, e pode ser considerada como uma legislação mais alinhada ao GDPR e a LGPD, por sua abrangência.

Atentos às legislações acima elucidadas o presente artigo se importou em analisar, em linhas gerais, cada uma das legislações, 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.

1. O GDPR da União Europeia

A União Europeia é composta hoje por 27 países, e foi a responsável por criar o GDPR- General Data Protection Regulation, que em português é denominado por Regulamento Geral de Proteção de Dados, foi promulgado em 24 de maio de 2016, através do Regulamento (EU) 2016/679, e entrou em vigor em 25 de maio de 2018. O GDPR, revoga integralmente a antecessora Diretiva 95/46/CE.

Todos os artigos do GDPR estão vinculados a cento e setenta e três (173) “Considerandos”, adequada e estruturadamente elaborados, sendo que os termos do regulamento são aplicáveis a todos os estados membros da União Europeia, com a finalidade de melhor adequar a proteção de dados pessoais em todo o continente europeu. Isso não quer dizer que os estados membros não possam ter suas próprias legislações de proteção de dados pessoais, de fato podem.

A teor dos “Considerandos” 1 e 2, o Regulamento protege os dados pessoais como direito fundamental do cidadão, tal qual estabelecido no artigo 8º da Carta dos Direitos Fundamentais da União Europeia e artigo 16 do Tratado sobre o funcionamento da União Europeia, dispositivos esses que garantem a proteção e privacidade dos dados pessoais, em conformidade com o estabelecido no Regulamento.

Carvalho Lima (2018), abordando os objetivos e princípios do GDPR, assim estabelece:

> Naturalmente, o foco é a proteção de direitos e garantias fundamentais dos cidadãos, com o objetivo de mitigar os riscos, em relação ao que pode ser levado a efeito, a partir da coleta e do futuro uso, compartilhamento e armazenamento, entre outros, desses dados.
>
> E isso tudo precisa ser pensado de forma a evitar que essa regulamentação não engesse novos modelos de negócios, em especial diante da nova sociedade da informação tecnológica em que vivemos, na qual Internet das Coisas (IoT – Internet of Things), Inteligência Artificial (AI – Artificial Intelligence), Blockchain, Bitcoin, Fintechs, entre outros, passam a ser realidade presente e que cada vez mais se utilizavam de dados pessoais como substrato de geração de valor para praticamente todos os tipos de empresas, desde as pequenas até as grandes corporações (CARVALHO LIMA, 2018, p. 24).

O Regulamento, estabelece as regras para a proteção das pessoas naturais no que diz respeito ao tratamento de dados pessoais e tem por objetivo estabelecer a defesa dos direitos e das liberdades fundamentais dos cidadãos (artigo 1º, 1 a 3 do GDPR), também nesse aspecto.

A aplicação territorial do Regulamento é bastante ampla, a teor do artigo 3º, sendo aplicável às empresas estabelecidas nos territórios da União Europeia, mesmo que os dados estejam armazenados fora de nações membro e se aplica aos dados de todos aqueles titulares que residam nas nações. Logo, mesmo que a empresa, aqui considerado como agente de tratamento de dados, esteja situada em outro continente, se ela tratar dados de titular residente num dos países membros, será aplicado o GDPR.

Carvalho Lima (2018), na sua obra, colaciona seis casos práticos de situações de aplicação extraterritorial ou não do GDPR, bastando para esse

trabalho colacionar apenas dois deles, de modo a demonstrar de forma exemplificada a aplicação territorial do Regulamento, vejamos:

> a) Considere a situação em que determinado provedor de conexão oferece plano de internet móvel a seus consumidores que estão fisicamente no Brasil – os usuários assinam contrato em português, havendo disposição sobre a aplicabilidade das leis brasileiras. Imagine que em determinado momento algum dos usuários desse provedor viaja para país no território da União e passa a utilizar os serviços de internet providos por essa operadora. Nessa situação, é possível a interpretação de que o GDPR não será aplicável extraterritorialmente, tendo em vista não restar configurada a oferta dos serviços a quem se encontrava no território da União, mas tão somente o seu gozo, decorrente de contratação levada a efeito em país não pertencente ao território da União. Pensamento em sentido diferente seria extrapolar a intenção trazida no GDPR, subvertendo a sua lógica de proteção.
> b) Considere a situação em que ao chegar ao Aeroporto de Lisboa o usuário se depara com o anúncio de provedor de conexão oferecendo desconto para usuários brasileiros que ativarem plano de roaming internacional. Nessa situação, ainda que o provedor em referência seja brasileiro, tendo em vista que há a oferta de serviços a usuário que se encontra no território da União – independentemente da sua nacionalidade – é possível o entendimento de que haverá a incidência do GDPR nessa relação (CARVALHO LIMA, 2018, p. 32).

Pois bem, traçados e delineados alguns passos acerca da aplicação territorial e extraterritorial do Regulamento, necessário avaliar que dados do titular são protegidos e o que o Regulamento entende por dado pessoal. Nesse ponto, importante verificar que o artigo 4º do Regulamento, contempla as definições legais dos termos e expressões versadas no GDPR, assim estabelecendo:

> Para efeitos do presente regulamento, entende-se por:
> 1) Dados pessoais, informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;
>
> 2) Tratamento, uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

> (...)
>
> 11) Consentimento do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;
>
> 12) Violação de dados pessoais, uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento (GDPR, 2016, p. 33 – tradução livre).

Com efeito, tudo o que pode identificar a pessoa, seja em que sentido for: pessoal, social, político, genético, fisiológico, étnico e outros, direta ou indiretamente, é considerado dado pessoal, passível, pois, de proteção pelo GDPR, cujo uso depende de consentimento específico, livre, informado e explícito, ressalvadas, claro, as exceções estabelecidas no Regulamento. Nesse sentido, o "considerando" nº 26 do Regulamento estabelece que tudo o que puder de qualquer forma identificar o indivíduo é considerado dado pessoal, passível, pois, de proteção.

Por sua vez, o artigo 9º, do Regulamento, impõe regras mais restritivas para o processamento de dados pessoais, no qual estão incluídos dados como: raça, religião, vida sexual, dados relativos à saúde, genética e biometria, bem como os dados pessoais concernentes a condenações criminais, que vem estabelecido no artigo 10º do GDPR.

O referido "considerando" nº 26, faz menção aos princípios que devem permear o tratamento de dados, os quais vem estabelecidos no artigo 5º do GDPR, são eles: a) princípio da licitude, segundo o qual o tratamento do dado pessoal deve ser norteado pela possibilidade e licitude, b) princípio da lealdade, segundo o qual o tratamento deve se dar de forma justa e amparada por lei, c) princípio da transparência, segundo o qual o titular deve ter o total e completo conhecimento acerca da finalidade do tratamento, d) princípio da limitação da finalidade, segundo o qual o dado deve ser tratado para uma finalidade específica e delimitada, não sendo possível a realização de outros tratamentos através do mesmo consentimento, e) princípio da limitação e da conservação, segundo o qual serão solicitados apenas os dados necessários e indispensáveis ao respectivo tratamento, f) princípio da exatidão, segundo o qual os dados a serem tratados representam os dados exatos e específicos do respectivo titular, e g) princípio da integridade e confidencialidade, segundo o qual o dado deve ser mantido íntegro e confidencial, pois não pode ser tratado em situações distintas da qual solicitado (VAINZOF, 2018).

Importante asseverar que a absoluta e ampla preocupação com o processamento dos dados pessoais é evidente nos dispositivos inseridos no Regulamento, sendo certo que o artigo 6º estabelece em quais situações o tratamento de dados é considerado lícito, ou seja, em que circunstâncias o responsável pelo tratamento poderá tratar os dados do titular, são elas: a) quando houver expresso e livre consentimento do titular do dado; b) quando o

tratamento se fizer necessário para a execução de contrato no qual o titular é parte ou em caso de diligências preliminares ao contrato; c) quando o tratamento for necessário para o cumprimento de uma obrigação jurídica; d) quando o tratamento for necessário para a defesa de interesses vitais do titular; e) quando o tratamento for necessário para o exercício de funções de interesse público ou a que a autoridade esteja investida; f) quando o tratamento for necessário para atender a legítimos interesses do responsável pelo tratamento ou por terceiros, exceto se prevalecerem os direitos ou liberdades do titular.

Esses dispositivos são os mais importantes do GDPR, pois estabelecem em que situações os dados dos titulares podem ser objeto de tratamento, demonstrando que há preocupação com o processamento dos dados pessoais e com as circunstâncias através das quais os dados são processados e tratados.

A união europeia já tratava dados pessoais como um direito fundamental do cidadão, por conta da Convenção Europeia dos Direitos Humanos de 1950, firmada com base na Declaração Universal dos Direitos Humanos de 1948, logo, não poderia ser diferente o tratamento adotado pela Carta dos Direitos Fundamentais da União Europeia de 2000 (MALDONADO, 2018).

Acerca do entendimento de que o dado pessoal é um direito personalíssimo, que é capaz de identificar uma pessoa, de forma direta ou indireta, interessante pontuar a necessidade de se proteger esses dados, pois estão interligados à pessoa, “adquirindo a característica de serem pessoais, significa resguardar a própria personalidade do ser humano, pois ela constitui “as características ou o conjunto de características que distinguem uma pessoa”, e o Direito visa proteger violações de todos os atributos, corpóreos e incorpóreos, que forma a projeção da pessoa humana” (VAINZOF, 2018, p. 40).

Pois bem, atentos à definição de dado pessoal e a forma como pode ser tratado, observadas as disposições do Regulamento, fica evidente que ele é rígido na sua aplicação e quanto a forma como pode ou não ser tratado um dado pessoal.

Com efeito, as possibilidades de tratamento dos dados pessoais são claras e estão delimitadas no Regulamento, sendo que o primeiro uso considerado lícito, é aquele que decorre do consentimento do titular. Mas, para que o titular possa adequadamente dar o seu consentimento é preciso que conheça com detalhes qual a finalidade do tratamento, como será tratado, em que circunstâncias, se haverá necessidade de ser compartilhado, com quem será compartilhado, para que a empresa necessita de seus dados, por quanto tempo os dados ficarão na base de dados da empresa, como os dados são armazenados, dentre tantas outras informações indispensáveis e pertinentes, a fim de que o titular possa dar seu consentimento informado, de forma que esse consentimento possa ser considerado livre. Ora, para que o consentimento seja informado e livre, é necessário que o titular tenha pleno conhecimento da forma como os dados serão tratados, a exemplo do quanto aqui descrito, caso contrário, não haverá consentimento livre.

Outra possibilidade de tratamento dos dados pessoais ocorre em casos de celebração de contrato ou pré-contrato entre o titular e determinada empresa, o que motiva o tratamento de alguns dados que sejam necessários à consecução desse contrato, e torna o tratamento lícito. É o que estabelece o “Considerando” 44 do GDPR: “(44) O tratamento deverá ser considerado lícito caso seja necessário no contexto de um contrato ou da intenção de celebrar um contrato” (GDPR, 2016).

Quando o tratamento for necessário para o cumprimento de uma obrigação jurídica, ou quando o tratamento for necessário para o exercício de funções de interesse público ou a que a autoridade esteja investida, deve ser observado o quanto estabelecido nos “Considerandos” 10 e 45, do GDPR, a fim de assegurar proteção coerente ao dado pessoal e descartar obstáculos, sempre preservando as liberdades individuais e o interesse do titular.

O tratamento destinado a defesa de interesses vitais do titular, ocorre quando indispensável ao titular, especialmente em casos de saúde, como por exemplo em casos de epidemias, é o que consta no “Considerando” 46 do Regulamento.

O mais polêmico dos tratamentos considerados lícitos é aquele que visa atender a legítimo interesse do responsável pelo tratamento ou por terceiros. Essa possibilidade de tratamento é bastante subjetiva e precisa ser mais bem avaliada e definido o que é considerado legítimo interesse. O GDPR buscou melhor esclarecer quanto a essa possibilidade de tratamento lícito, no “Considerando” 47, abaixo transcrito, vejamos:

> (47) Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas

> atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controle da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta (GDPR, 2016, p. 9 - tradução livre).

Embora sobredito “Considerando” não solucione efetivamente a questão, o dispositivo contempla importantes interpretações sobre o legítimo interesse, e reforça que é necessário que fique evidente ao titular que o dado será tratado com fundamento nesta base legal. Reafirma ainda que os interesses e direitos fundamentais do titular do dado são sempre superiores aos da empresa responsável pelo tratamento.

Portanto, a base legal do legítimo interesse, a teor do Regulamento, ainda vai depender de legislações esparsas a serem criadas para justificar e especificar em que circunstâncias e situações pode ser considerado e aplicado o legítimo interesse da empresa para realizar o tratamento do dado através dessa base legal.

No entanto, observado todo o acima narrado, vemos que o GDPR é um regulamento bem estruturado, adequadamente fundamentado em todos os seus explicativos e elucidativos “Considerandos”, que tornam a sua aplicação mais inteligível. Importante, no entanto, deixar claro que o regulamento não deduz como as empresas devem atuar para garantir a segurança de dados dos titulares.

As multas por violação ao Regulamento são pesadíssimas, justamente com a intenção de criar uma conformidade, responsabilidade, respeito aos dados, e governança por parte das empresas no tratamento de dados, para evitar vazamento.

O GDPR criou o CEPD – Comitê Europeu de Proteção de Dados, que nada mais é do que um organismo independente que tem por objetivo assegurar a aplicação do regulamento em toda a União Europeia, e é composto por representantes das autoridades das nações membro e também da AEPD que é a Autoridade Europeia para a Proteção de Dados, criada através do Regulamento 2018/1725, que é autoridade independente da União Europeia, a qual foi atribuída a responsabilidade por acompanhar a aplicação do regulamento atinente a proteção de dados.

Não é demais esclarecer que o GDPR é de aplicação irrestrita a todos os países membros da União Europeia. No entanto, a sua existência não impede que cada qual das nações membro promulgue suas próprias e específicas legislações de proteção de dados pessoais. A interpretação de aplicação das legislações, em casos como tais, será feita de forma conjunta, mas prevalecerá o GDPR se a lei de um determinado país contiver proteção inferior ou distinta daquela atribuída pelo Regulamento.

O Regulamento da comunidade europeia, robusto e sério, levou-a a vanguarda da proteção de dados pessoais. Forte, específico, dotado de órgãos

de proteção atuantes, garantem e impõem o estrito cumprimento do Regulamento.

2 O CCPA da Califórnia

Nos Estados Unidos da América não existe uma lei federal abrangente que trate especificamente da proteção de dados pessoais e não há no texto constitucional americano específica proteção à privacidade dos dados pessoais. Há um emaranhado de distintas leis, e leis em cada qual dos seus estados, que tratam da privacidade e segurança de dados.

As legislações sobre privacidade de dados existentes na América do Norte são aquelas que se aplicam a instituições financeiras, empresas de telecomunicações, agências de relatórios de crédito e prestadores de serviços de saúde, bem como registros de condução, privacidade infantil, telemarketing, marketing de e-mail e leis de privacidade de comunicações (TROJAN, 2019).

De uma forma geral, as leis de cada estado se aplicam a informações pessoais sobre residentes desse estado ou atividades que ocorrem dentro desse estado, de modo que as diversas empresas que atuam nos Estados Unidos da América devem cumprir não apenas a lei federal aplicável, mas as leis e regulamentos estaduais de privacidade e segurança.

O CCPA do estado da Califórnia, nos Estados Unidos da América, tem aplicação territorial local, pois se aplica a todas as empresas estabelecidas ou que fazem negócios na Califórnia, ou que tratam dados de titulares lá residentes, desde que ela tenha uma receita anual de 25 milhões de dólares ou mais, ou que a metade de sua receita anual seja obtida através da venda de informações pessoais de titulares de dados, ou, realize o tratamento de dados pessoais de mais de 50.000 titulares. Para a aplicação da lei, basta a incidência de apenas um dos indicativos acima, que vêm descritos no item (1) do 1798.140, do CCPA.

Para a legislação da California, dados pessoais ou informações pessoais ou de consumidores, incluem as informações capazes de identificar, descrever, e relacionar a uma pessoa o respectivo dado, tais como nome, informações de contato, dentre outros, vejamos 1798.140:

> (u) "Pessoa" significa um indivíduo, propriedade, empresa, parceria, joint venture, sindicato, business trust, empresa, corporação, sociedade limitada, associação, comitê e qualquer outra organização ou grupo de pessoas que atuem em conjunto.
> v (1) "Informações pessoais" significa que as informações que identificam, relacionam-se, descrevem, são razoavelmente capazes de estar associadas, ou poderiam estar razoavelmente ligadas, direta ou indiretamente, a um determinado consumidor ou família. As informações pessoais incluem, mas não se limitam a, se identificar, se relacionar, descrever, é razoavelmente capaz de ser associada, ou pode ser razoavelmente ligada, direta ou indiretamente, a um determinado consumidor ou familiar:
> (A) Identificadores como nome real, pseudônimo, endereço postal, identificador pessoal exclusivo, identificador on-line,

> endereço do Protocolo da Internet, endereço de e-mail, nome da conta, número de segurança social, número da carteira de motorista, número do passaporte ou outros identificadores semelhantes (CCPA, 2018 – tradução livre).

A principal base legal para o tratamento do dado do consumidor é o consentimento, que pode ser prévio ou posterior. A legislação utiliza expressamente o uso do consentimento através do sistema opt-in ou opt-out. O consentimento opt-in é necessário para coletar, usar e divulgar determinados dados sensíveis, como informações de saúde, relatórios de crédito, informações financeiras, informações pessoais de crianças, dados biométricos, escolhas de visualização de vídeo, dados de geolocalização e informações de uso de telecomunicações. Especificamente no caso de crianças, há uma legislação federal de proteção à privacidade online infantil – COPPA, que exige o consentimento verificável dos pais antes da coleta de qualquer dado ou informação pessoal de criança menor de 13 anos.

Boa parte dos autores consultados, dos quais citamos Marcheti (2021) e Trojan (2019) manifestam que apesar de um pouco diferente do GDPR, o CCPA é considerado nela embasado. O conceito de compartilhamento de dados é mais amplo na legislação da Califórnia e abrange a opção de vender/comercializar dados, e inclusive aceita o registro de empresas específicas para coletar e vender dados, o que não ocorre no Brasil.

A lei da Califórnia também obriga o consentimento opt-in quando a empresa pretender tratar o dado de forma diversa para a qual consentida, obrigando a empresa a solicitar consentimento para outro tratamento que não o inicialmente consentido (artigos 1798. 120 e 1798.121).

Pois bem, as empresas devem obter o consentimento de opt-in antes de usar, divulgar ou tratar de forma distinta para o qual inicialmente coletados os dados. Desta forma, é possível concluir que não há obrigatoriedade de consentimento prévio para o tratamento dos dados, pois o consentimento pode ser obtido depois. A legislação não prevê outras formas de consentimento como o fazem o GDPR e a LGPD. A obrigatoriedade de consentimento prévio se dá a teor do CCPA, quando se trata de dados de menores de idade.

O CCPA confere aos consumidores a possibilidade de promover ações contra as empresas que tratam dados, a teor da legislação, quando houver violação e o fazem pelo fato de a lei não impor e estabelecer requisitos específicos de segurança de dados, como ocorre, por exemplo, no GDPR, que obriga que os controladores implementem medidas de segurança adequadas aos riscos envolvidos.

O não cumprimento do quanto estabelecido na legislação enseja o pagamento de multa de até US$7.500,00 (sete mil e quinhentos dólares americanos) por violação individual intencional, conforme 1798.155.

Nos Estados Unidos da América, a FTC – Comissão Federal do Comércio, que funciona como a autoridade que trata das questões atinentes à privacidade dos americanos, é um órgão federal, logo, trata de todas as questões atinentes

à privacidade de dados pessoais. No estado da Califórnia, o responsável é o Procurador Geral do Estado da Califórnia. Não há, portanto, uma única autoridade nacional.

A FTC tem jurisdição sobre a maioria das empresas e tem autoridade para criar e aplicar regulamentos federais de privacidade, exceto para instituições financeiras, cooperativas de crédito, e companhias de seguro, de forma que pode adotar medidas para proteger consumidores contra práticas comerciais injustas ou enganosas, incluindo violações de privacidade e segurança de dados.

A toda evidência, após a leitura de todo o acima relatado, que não representa um estudo exaustivo da legislação da Califórnia, vemos que os Estados Unidos da América, apenas com legislações estaduais está na retaguarda da proteção de dados.

3. A LGPD do Brasil

O Brasil, assim como os demais países, se viu compelido a promulgar a sua específica legislação de proteção de dados pessoais, o que, inclusive, já se fazia premente, face a todos os problemas havidos em nosso país, no que diz respeito aos constantes vazamentos de dados, e aos inúmeros prejuízos e violações vivenciados pela sociedade brasileira com o uso indevido e exacerbado de dados pessoais.

Embora houvesse no país diversos projetos de lei discutindo a questão da privacidade de dados pessoais, o tema já estivesse em discussão desde 2010, e o Projeto de Lei nº 5276/2016, de autoria do Poder Executivo, tivesse sido aprovado pela Câmara dos Deputados, após os referidos escândalos internacionais, todas as propostas legislativas que debatiam o tema foram reunidas gerando o Projeto de lei da Câmara - PLC nº 53/2018, que foi apresentado ao Senado como projeto central para a proteção de dados pessoais (CÂMARA, 2020).

O PLC nº 53/2018 foi elaborado com a participação de diversos segmentos empresariais nacionais e internacionais e votado em regime de urgência, e sancionado pelo então Presidente Michel Temer como Lei nº 13.709, de 14 de agosto de 2018, com vetos, em especial o veto à criação da Autoridade Nacional de Proteção de Dados (ANPD). A justificativa presidencial para o veto a criação da ANPD foi a de que apenas o executivo federal poderia legislar sobre a criação de cargos e gastos públicos e não o legislativo (SENADO, 2020).

A legislação ficou parcialmente sem sentido sem a criação da ANPD, então disposta como modelo autárquico, de maior autonomia, por funcionar como órgão consultor da aplicação da legislação, o que levou a Presidência da República a editar a Medida Provisória nº 869/2018, com a finalidade de alterar a LGPD e criar a ANPD como órgão da administração pública federal, integrante da Presidência da República, composta por conselhos, corregedoria, ouvidoria, órgão jurídico próprio, unidades administrativas e especializadas para a efetivação da lei. Estabeleceu também que após dois anos de vigência da lei a ANPD deveria ser transformada em autarquia (SENADO, 2022).

A Medida Provisória nº 869/2018, sofreu diversas emendas parlamentares, de forma que ao final foi apresentado um Projeto de Lei de Conversão, o PLV nº 7/2019, que foi aprovado pelo Congresso e encaminhado para sanção presidencial, originando a Lei nº 13.853/2019. O então Presidente Jair Bolsonaro vetou nove dispositivos do projeto, de forma que o PLV retornou à Câmara, que derrubou seis vetos presidenciais.

A Lei geral de proteção de dados pessoais brasileira foi sancionada em 14 de agosto de 2018, publicada em 15 de agosto de 2018, e entrou em vigor em 18 de setembro de 2020, o que ainda está levando empresas públicas e privadas que tratam, armazenam e coletam dados pessoais à corrida para a adequação às disposições legais, traçando planos de conformidade, 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, uma vez que a parte sancionadora da lei, que estabelece elevadas multas pelo seu descumprimento, entrou em vigor em 1º de agosto de 2021.

Através da Medida Provisória nº 1.124/2022, publicada aos 14 de junho de 2022, a ANPD foi transformada em autarquia de natureza especial, com a criação de um cargo comissionado de diretor-presidente. A ANPD adquiriu, pois, personalidade jurídica e tem funções semelhantes, por exemplo, às da Anatel, embora não possa ser considerada como uma agência reguladora, já que não tem por finalidade regular uma atividade específica.

Em 19 de agosto de 2022, a sobredita Medida Provisória teve sua vigência prorrogada por mais sessenta dias, a fim de ser providenciada e votada a lei que transforma a ANPD em autarquia.

Pois bem, a base para a criação da legislação de proteção de dados brasileira, foi, sem dúvida alguma, o GDPR, que é o regulamento de proteção de dados da comunidade europeia, e foi o primeiro regulamento atualizado e específico sobre proteção de dados pessoais (MALDONADO, 2018). Referido regulamento é dos mais completos de que se tem notícia no âmbito da proteção à privacidade dos dados pessoais.

No entanto, cumpre esclarecer que para o desenvolvimento de uma legislação específica de proteção de dados, há necessidade de observar e cumprir certos princípios, sob os quais se fundam a própria proteção a ser criada, que são os denominados “fair information principles” (DONEDA, 2011, p. 100).

O GDPR, se funda nesses princípios, em especial no que trata a proteção de dados pessoais como um direito fundamental, pois havia referência a esse direito na Convenção Europeia para os Direitos do Homem (artigo 8º) e na revogada Diretiva 95/46/CE, da comunidade europeia. A LGPD também se funda nos *fair information principles* e relaciona outros princípios sob os quais a lei se estabelece, no artigo 6º.

O primeiro princípio, o da publicidade, vem estabelecido nos dispositivos da lei como um todo, quando a legislação impõe que aquele que detém um banco de dados, seja pessoa física ou jurídica, o denominado pela lei por agente de

dados, deve informar as bases legais que utiliza para manter dados de titulares em seu banco. Não há necessidade de pedir autorização específica para funcionar, pois hoje em dia, todas as empresas mantêm bancos de dados.

O princípio da exatidão dos dados vem estabelecido nos artigos 9º e 18 da LGPD, segundo os quais os bancos de dados têm de manter dados exatos do titular, e o titular pode solicitar a correção do dado que estiver incorreto.

O princípio da finalidade vem insculpido no inciso XII, do artigo 5º, incisos I, II, III, V, do artigo 6º, parágrafo 4º, do artigo 8º e artigo 10, que obrigam a que o agente de dados informe de forma clara qual a finalidade para a coleta e tratamento de dados, ou seja, para que finalidade o agente necessita do dado e a finalidade específica para o tratamento pretendido, a fim de possibilitar que o titular dê, ou não, seu consentimento de maneira inconteste para o tratamento.

O princípio do livre acesso vem disposto na previsão estabelecida nos artigos 6º, 9º e 18, nos quais o legislador estabeleceu que o titular tem o direito de livre acesso a seus dados pessoais, podendo revogar consentimento antes outorgado e também pedir que o dado seja anonimizado ou apagado.

O princípio da segurança lógica vem nos artigos 11, 12, 13, 34, 40, 44, 46 e seguintes e através dele a legislação determina que o agente de tratamento de dados deve manter uma base segura e protegida de dados pessoais, a fim de evitar vazamentos e o conhecimento dos dados por terceiros, preservando a privacidade do titular.

Os princípios insculpidos no artigo 6º, devem ser lidos em conjunto com os estabelecidos no *Fair Information Principles*, justamente porque estão interligados, e são todos decorrentes do princípio maior que é o da tutela da personalidade, de modo que todos os demais princípios foram criados à partir desse movimento e os consideramos, tal qual descritos na lei, autoexplicativos, não demandando grandes digressões, pois a interpretação de seu contexto é bastante clara.

Importante asseverar que o legislador inseriu no artigo 5º, da LGPD, dispositivo que aborda as definições legais, a palavra tratamento, com o objetivo de definir que tipo de operação realizada pelo agente de tratamento será considerada como tratamento de dados pessoais, nele insculpindo: “coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (artigo 5º, inciso X, da LGPD). Sendo assim no presente trabalho será utilizada a palavra tratamento para se referir a quaisquer das formas previstas na lei.

Pois bem, no que diz respeito à aplicação territorial, é importante esclarecer que a lei incide independentemente de endereço residencial ou de nacionalidade. A lei se aplica aos dados pessoais cujo tratamento ocorra em território nacional, a dados coletados no Brasil e tratados em outros países, e

aos dados que tenham por objetivo a oferta de serviço ou fornecimento de bens a indivíduos que estejam no território nacional por ocasião da coleta.

A legislação traz, contudo, exceções específicas no que diz respeito a sua aplicação, estabelecendo que em determinados casos ela não é aplicável, o que ocorre nos casos prescritos no artigo 4º.

A LGPD se aplica a todo e qualquer dado pessoal, seja na internet ou fora dela (artigo 1º), e a base legal primordial de tratamento é o consentimento prévio e informado. A lei considera como dado pessoal qualquer dado relativo à pessoa natural identificada ou identificável (art. 5º, inciso I). O dado anonimizado só é considerado dado pessoal se puder identificar o titular, caso contrário, não é considerado dado pessoal. Dado sensível é o dado pessoal sobre raça, credo, opinião política, filiação a sindicatos ou organizações, de saúde, sexual, genético, biométrico, quando vinculados a uma pessoa física (art. 5º, inciso II).

As bases legais aptas a realização do tratamento de dados pessoais estão descritas nos incisos do artigo 7º da Lei, e são: a) consentimento prévio e informado, b) cumprimento de obrigação legal ou regulatória pela administração pública, c) quando necessário a execução de políticas públicas previstas em leis ou regulamentos, ou respaldadas em contratos, convênios ou instrumentos semelhantes, d) para a realização de estudos por órgãos de pesquisa, e) para a execução de contratos ou procedimentos preliminares a contratos do qual o titular seja parte, f) para o exercício regular de direitos em processos judicial, administrativo ou arbitral, g) para a proteção da vida ou incolumidade física do titular, h) para a tutela da saúde, i) para atender a legítimo interesse do controlador ou de terceiros, j) para a proteção do crédito.

A LGPD estabelece mais bases legais que possibilitam o tratamento de dados pessoais do que o GDPR, mas é importante estabelecer que, sempre deve ser considerado que aquele que estiver tratando dados pessoais de outrem deverá agir com boa-fé. O princípio da boa-fé é pautado em todas as áreas e atos da vida civil, a teor de disposição de ordem pública, inserida nos artigos 113 e 422 do Código Civil.

Além disso, a boa-fé objetiva exige que as partes contratantes cumpram determinadas atribuições específicas de conduta, também denominadas por deveres auxiliares de conduta que estão relacionadas à formação e desempenho de obrigações contratuais. É, pois, o que se espera das partes durante a realização do tratamento de dados pessoais.

A LGPD estabelece que os agentes de tratamentos de dados devem garantir segurança aos dados tratados, adotando medidas de segurança aptas e compatíveis com a adequada técnica para a proteção dos dados inseridos em suas respectivas bases. Essas medidas de segurança devem proteger os dados de acessos desautorizados e de acidentes, lícitos ou não, inclusive da perda, comunicação ou qualquer forma de tratamento inadequado ou ilícito (artigo 46). A teor da lei essas medidas de segurança e conformidade poderão ser estabelecidas pela própria ANPD, que poderá dispor quanto aos padrões técnicos mínimos que devem ser observados pelos agentes de tratamento para

o adequado tratamento dos dados, visando a sua preservação e de modo a prevenir acidentes (parágrafo 1º do artigo 46), havendo expressa obrigação de garantir a segurança da informação (artigo 47).

O controlador de dados, deverá comunicar a ANPD a ocorrência de alguma desconformidade ou incidente de segurança que gere risco aos titulares. A lei dispõe que o prazo para tal comunicação deve ser razoável, sem estabelecer um prazo concreto considerado razoável (artigo 48). Para resolver essa questão, face a questionamento das empresas, a ANPD estabeleceu que o prazo considerado razoável para a comunicação de eventual incidente de segurança é de 2 dias úteis, e assim definiu levando em consideração o estabelecido no §1º, do artigo 18, do Decreto nº 9.936, de 24 de julho de 2019.

A legislação obriga ainda que os sistemas automatizados de tratamento de dados pessoais devem deter estrutura adequada ao tratamento, garantindo segurança, é o que estabelece o artigo 49: “Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares”. As regras de boas práticas e governança a serem adotadas pelos agentes de tratamento estão dispostas nos artigos 50 e 51 da legislação. As sanções, de natureza civil e administrativa, previstas na legislação pela sua violação são um pouco mais brandas do que as dispostas no GDPR, e estão previstas no artigo 52 da lei.

As sanções administrativas devem ser aplicadas pela ANPD, que, quando comunicada do vazamento de dados ou de alguma violação à legislação, deve instaurar o procedimento administrativo competente e ao final decidir pela aplicação ou não de sanção. Dentre as sanções impostas, são consideradas extremamente graves as dispostas nos incisos VI a XII do artigo 52, porquanto, a depender da atividade realizada pelo agente de tratamento, a sanção pode inviabilizar e até extinguir o negócio da empresa, pois implica na eliminação dos dados pessoais vazados, suspensão do funcionamento do banco de dados, suspensão da atividade de tratamento e proibição total ou parcial do exercício da atividade.

Com efeito, deve ser esclarecido que outros órgãos da administração não podem aplicar aos agentes de tratamento as sanções estabelecidas na LGPD, no entanto, a teor de suas legislações específicas, quando a violação à lei ensejar a violação de outra legislação, outros órgãos são considerados aptos a instaurar procedimentos e aplicar as penalidades que lhes compete, não com base na LGPD, mas com base em suas próprias legislações, é o caso, por exemplo, de violações que também se verifiquem no âmbito do Código de Defesa do Consumidor, quando os Procons são os responsáveis por realizar a autuação.

Importante asseverar, atento ao princípio da boa-fé objetiva, que o legislador estabeleceu a impossibilidade de cumprir o quanto prescrito na legislação *a posteriori*, ou seja, não é possível pedir o consentimento do usuário depois de realizado o tratamento, ou solicitar o tratamento de dados sem especificar os motivos, a finalidade do tratamento, ou seja, sem dar

transparência e legalidade ao que se pretende. É preciso agir com boa-fé, caso contrário, o agente poderá ser autuado pelo descumprimento da legislação e o tratamento será considerado irregular, conforme artigo 44 da LGPD.

O dispositivo supra tem relação com os pressupostos da responsabilidade civil e já ocorre um grande debate na doutrina acerca do tema, pois parte entende que a lei adotou a teoria subjetiva da responsabilidade civil dos agentes de tratamento de dados, e outra parte a teoria objetiva da responsabilidade civil.

A teoria subjetiva, grosso modo, é a que se baseia na conduta adotada pelo agente e a teoria objetiva decorre do próprio risco do negócio. Entendemos da mesma forma que Doneda (2021), que a lei adotou a teoria objetiva, considerando que a atividade desenvolvida pelos agentes de tratamento, ou seja, o tratamento de dados em si, contempla um risco intrínseco, pelo fato de que o dado tratado tem natureza de direito personalíssimo, sendo, pois, um direito fundamental.

No artigo 58-A, a legislação cria o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, a ser composto por 23 representantes, titulares e suplentes da iniciativa pública e privada, dentre esses, cinco são do governo federal, dois dos parlamentos, um do CNJ, um do CNMP, um do CGI, e o restante pertencente à sociedade civil, sindicatos, confederações sindicais, instituições científicas e outros. As atribuições do Conselho estão descritas no artigo 58-B.

É de ser constatado que a legislação é boa, poderia ser melhor, mas avaliando como legislação posta, em vigor, temos que ela restabelece o direito à privacidade, e confere a garantia ao direito à privacidade dos dados pessoais. Tudo o que se seguiu após a promulgação da lei também demonstra a seriedade com que o país vem tratando da matéria.

4 O PIPL da China

Recentemente, a China aprovou 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 1º de novembro de 2021, e pode ser considerada como uma legislação mais 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 1º de junho de 2017, e de uma lei de segurança de dados (DSL), que entrou em vigor em 1º de setembro de 2021, o Código Civil Chines, e outras (PEÇANHA DE SOUZA, 2021).

Pois bem, um detalhe bastante importante da legislação chinesa é a de que ela protege o titular do dado contra empresas privadas, logo, o governo e empresas públicas estão de fora da vedação, sendo certo que 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, o que também ocorre no Brasil.

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 na China.

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 3º). O tratamento transfronteiriço de dados deve obedecer ao estabelecido no respectivo tópico da legislação, do qual destacamos os artigos 38 e 39.

Os princípios aplicáveis na legislação no que concerne ao tratamento de dados são os da transparência, legalidade, decoro, necessidade e sinceridade, 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 proibida a coleta excessiva de dados, ou seja, viola a lei, é o que dispõem os artigos 5º, 6º e 7º do PIPL. 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, indicando ainda a necessidade para o dado ser tratado.

A legislação define dados pessoais como qualquer tipo de informação relativa a uma pessoa natural identificada ou identificável, seja por que forma for, excluindo informações que foram anonimizadas, e define dados sensíveis como os dados confidenciais, aqueles que garantem a proteção da dignidade humana, ou que, se divulgados, podem levar a dano a segurança do titular, seja segurança pessoal ou patrimonial, dentre os quais: dados biométricos, credo, social específico, informações de saúde, dados financeiros, geolocalização e dados de menores.

O titular do dado tem o direito de solicitar a adequação do dado, a exclusão, a anonimização e pode também cancelar o consentimento antes concedido.

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 13º, 14º e 15º).

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 16º e 17º do PIPL, 2021).

O artigo 26 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.

O tratamento de informações sensíveis deve ocorrer de forma distinta e ser obtido um consentimento específico para o tratamento. São dados considerados sensíveis pelo PIPL, a teor do artigo 28, a biometria, credo, saúde, informações financeiras, geolocalização, dentre outras não especificadas na lei, e as informações pessoais de menores de 14 anos.

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).

A 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 53 do PIPL).

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, quando a empresa tiver mais de 200 colaboradores em sua linha de negócios que envolva o tratamento de dados pessoais, quando a empresa tratar dados de mais de um milhão de pessoas, ou tratar dados pessoais confidenciais de mais de cem mil pessoas.

A autoridade pode aplicar sanções às empresas em caso de violação da legislação, a teor dos artigos 66 a 71 da lei, que estabelece multas de mais de

um milhão de Yuan. 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).

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.

5. Conclusão

As legislações de proteção de dados pessoais analisadas possuem certa semelhança, sendo certo que boa parte delas está realmente embasada no Regulamento da União Europeia.

É o caso da legislação brasileira e da chinesa. A legislação do estado da Califórnia, é a menos restritiva, pois, dentre outras coisas, autoriza que se obtenha o consentimento após coletado e tratado o dado.

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.

Outros países também possuem legislação de proteção de dados pessoais, mas não foi possível no presente trabalho, analisar todas as legislações promulgadas.

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 out. 2019.

BIONI, Bruno Ricardo. De 2010 a 2018: A discussão brasileira sobre uma lei geral de proteção de dados. Jota, 2018. Disponível em:

https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade. Acesso em: 10 out. 2019.

BRASIL. Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988.

_____. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências.

_____. Lei nº 10.406 de 10 de janeiro de 2002. Institui o Código Civil.

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei geral de proteção de dados pessoais.

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

_____. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 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.

BULOS, Uadi Lammêgo**. Curso de Direito Constitucional**. 9ª edição. São Paulo: Saraiva, 2015.

BURGESS, Matt. Ignore China's New Data Privacy Law at Your Peril. 2021. Disponível em: https://www.wired.com/story/china-personal-data-law-pipl/. Acesso em 20 nov. 2021.

BYGRAVE, Lee A. **Data protection law: approaching its rationale, logic and limits**. New York: Kluwer law international, 2002.

CÂMARA Federal. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 21 ago. 2020.

CARVALHO LIMA, Caio César. Objeto, aplicação material e aplicação territorial. In: MALDONADO, Viviane Nóbrega. OPICE BLUM, Renato. Coordenadores. **Comentários ao GDPR – Regulamento geral de proteção de dados da união europeia.** São Paulo: Thomson Reuters Revista dos Tribunais, p. 23-36. 2018.

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 out. 2020.

DECLARAÇÃO Universal dos Direitos Humanos – DUDH, de 10 de dezembro de 1948. Disponível em: https://nacoesunidas.org/artigo-12-direito-a-privacidade/. Acesso em: 18 set. 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Joaçaba: **Espaço Jurídico**, v. 12, n. 2, p. 91-108, jul/dez. 2011.

_____. **Da privacidade à proteção de dados pessoais**. Fundamentos da lei geral de proteção de dados. Thomson Reuters Revista dos Tribunais. 3ª edição. São Paulo: 2021.

_____. A proteção dos dados pessoais como um direito fundamental. Joaçaba: **Espaço Jurídico**, v. 12, n. 2, p. 91-108, jul/dez. 2011.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: O direito à privacidade e os limites à função fiscalizadora do estado. **Revista da Faculdade de Direito**, Universidade de São Paulo, São Paulo, vol. 88, p. 439-459, 1993. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 13 out. 2020.

GDPR. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 10 mai 2019.

GOGONI, Ronaldo. 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 nov. 2021.

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

KUCEK, Gisele Bolonhez. 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, Alexa; SHI, Mingli; CHEN, Qiheng; HORSLEY, Jamie P.; SCHAEFER, Kendra; CREEMERS, Rogier; WEBSTER, Graham. 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. 2022

LENZA, Pedro. **Direito constitucional esquematizado**. 23ª ed. São Paulo: Saraiva Educação, 2019.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

MALDONADO, Viviane Nóbrega, ÓPICE BLUM, Renato. **Comentários ao GDPR – Regulamento geral de proteção de dados da união europeia**. São Paulo: Thomson Reuters Revista dos Tribunais, 2018.

MARCHETI, Renata. Uma brevíssima comparação entre GDPR, CCPA, POPIA e LGPD - Parte III. 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/350014/uma-brevissima-comparacao-entre-gdpr-ccpa-popia-e-lgpd--parte-iii. Acesso em 15 set. 2021.

MONTEIRO, Renato Leite. 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 out. 2019.

ONU – Organização das Nações Unidas. A declaração universal dos direitos humanos. Brasil. Disponível em: https://nacoesunidas.org/direitoshumanos/declaracao/. Acesso em: 18 set. 2020.

PEÇANHA DE SOUZA, Carolina. 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, Patrícia Peck. **Proteção de dados pessoais** – Comentários à Lei nº 13.709/2018 (LGPD). São Paulo: Saraiva jur, 2018.

_____. Palestra proferida no ScaleUp, Rio de Janeiro, nov. 2019. Disponível em: https://www.youtube.com/watch?v=_H7iz9powFc. Acesso em: 10 jul. 2020.

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.2022

PRESSE, France. 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. 2019.

RODOTÁ, Stefano. DE MORAES, Maria Cecília Bodin. **A vida na sociedade da vigilância: a privacidade hoje**. São Paulo: Renovar, 2008.

SENADO Federal. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acesso em: 21 ago. 2020.

TROJAN, Viviane. 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: 11 jul. 2022.

UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to

the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Official Journal, Luxemburgo, L. 119/1, 4. Mai. 2016, p. 1–88. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 11 jul. 2020.

VAINZOF, Rony. Dados pessoais, tratamento e princípios. In: MALDONADO, Viviane Nóbrega. OPICE BLUM, Renato. Coordenadores. **Comentários ao GDPR – Regulamento geral de proteção de dados da união europeia.** São Paulo: Thomson Reuters Revista dos Tribunais, p. 37-85. 2018.

_____. LGPD "finalizada". Isso é bom para a indústria e para o Brasil? 2019. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/lei-geral-de-protecao-de-dados-finalizada-isso-e-bom-para-a-industria-e-para-o-brasil/. Acesso em: 25 set. 2019.