REVISTA DE DIREITO DA ADMINISTRAÇÃO PUBLICA

ISSN 2595-5667

REVISTA DE DIREITO DA ADMINISTRAÇÃO PÚBLICA

ANO Nº 08 – VOLUME Nº 01 – EDIÇÃO Nº 02
ISSN 2595-5667

Editor-Chefe:
Prof. Dr. Emerson Affonso da Costa Moura, Universidade Federal do Estado do Rio de Janeiro e Universidade Federal Rural do Rio de Janeiro, Brasil

Rio de Janeiro, 2022.

Revista de Direito da Administração Pública

Law Journal of Public Administration

REGULAÇÃO DO USO DE DADOS E PROTEÇÃO A DIREITOS FUNDAMENTAS: UM ESTUDO COMPARADO A PARTIR DA LEI DE PROTEÇÃO DE DADOS PESSOAIS BRASILEIRA E A LEI DE CIBERSEGURANÇA CHINESA

REGULATION OF THE USE OF DATA AND PROTECTION OF FUNDAMENTAL RIGHTS: A COMPARATIVE STUDY BASED ON THE BRAZILIAN PERSONAL DATA PROTECTION LAW AND THE CHINESE CYBERSECURITY LAW

Arianne Campos Souza[1]
Diva Júlia Sousa Safe Coelho[2]

RESUMO: Este artigo visa analisar a regulação do uso de dados pessoais no contexto do poder público chinês e no contexto do poder público brasileiro. Objetiva, por meio de um estudo comparado da regulação existente nestes dois países, subsidiar analises para possíveis aprimoramentos regulatórios no Brasil, visando a uma mais efetiva proteção dos direitos fundamentais no ambiente cibernético, em que os dados pessoais são a representação da própria pessoa e sua manipulação indiscriminada viola a intimidade, privacidade e autonomia do sujeito. A Lei Geral de Proteção de Dados brasileira e a Lei de Cibersegurança da República Popular da China são analisadas numa perspectiva comparativa integrada, crítica e pautada na alteridade, a partir do referencial teórico de Pierre Legrand. A luz dessas duas legislações, buscou-se entender a relação entre privacidade e proteção de dados, e o que a privacidade significa para cada cultura jurídica analisada. A pesquisa possibilitou discutir os limites para a manipulação dos dados sem que houvesse violação dos direitos da pessoa, utilizando três aspectos principais das leis citadas: consentimento, responsabilidade e segurança. Com isso, procuramos atualizar o estado da arte sobre a regulação do uso de dados pessoais e lançar subsídios para seu aprimoramento incremental.

Palavras-Chave: Lei Geral de Proteção de Dados; Lei de Cibersegurança; Manipulação de Dados; Regulação; Brasil; China.

ABSTRACT: This article aims to analyze the regulation of personal data usage in the context of the Chinese and Brazilian public authorities. It seeks, through a comparative study of the existing regulation in these two countries, to provide insights for potential regulatory improvements in Brazil, aiming for a more effective protection of fundamental rights in the cyberspace environment, where personal data represents the individual themselves and its indiscriminate manipulation violates the subject's privacy, intimacy, and autonomy. The Brazilian General Data Protection Law and the Cybersecurity Law of the People's Republic of China are analyzed from an integrated, critical, and otherness-based comparative perspective, based on Pierre Legrand's theoretical framework. Considering these two legislations, the research sought to understand the relationship between privacy and data protection, and what privacy means in each analyzed legal culture. The study enabled a discussion on the limits for data manipulation without violating individual rights, utilizing three main aspects of the mentioned laws: consent, responsibility, and security. Through this, to update the state of the

[1] Graduanda em Direito da Universidade Federal de Goiás. Servidora Pública junto ao Ministério Público do Estado de Goiás (MPGO).

[2] Professora efetiva da Universidade Federal de Goiás (UFG). Doutora em Cidadania e Direitos Humanos pela Universidade de Barcelona-ES. Professora permanente do PPGDP-UFG, do PPGPJDH-UFT. Pesquisa realizada com apoio institucional do PPGDP-UFG, do PPGPJDH-UFT e entidades profissionais parceiras.

art regarding the regulation of personal data usage and provide insights for its incremental improvement.

Keywords: Brazilian General Data Protection Law; Cybersecurity Law of the People's Republic of China; Data Manipulation; Regulation; Brazil; China.

INTRODUÇÃO

Este artigo pretende procurar resposta para a seguinte pergunta: na realidade cibernética a manipulação de dados se tornou mais um dos perigos aos direitos da personalidade, considerando as previsões da Lei Geral de Proteção de Dados (Lei n 13.709/18) e da Lei de Cibersegurança da República Popular da China? Quais os limites para que a manipulação de dados pessoais não viole direitos fundamentais como a privacidade? Qual o papel do poder público na regulação e controle da atuação de grandes conglomerados empresariais nessa seara? No que se refere a esse questionamento, acreditamos que o mais difícil seja determinar o que é a privacidade, por se tratar de um conceito sem significação fixa. Além disso, considerar o direito à privacidade para duas culturas tão diferentes quanto Brasil e China é realmente desafiador, mas igualmente interessante. Outro aspecto relevante é relacionar o direito à privacidade com a proteção de dados, pois devemos adotar o entendimento de que esses dados são a própria pessoa, e a exposição deles é a exposição dessa pessoa, o que representa um atentado à dignidade humana.

O contexto atual é de inovação e tecnologia, o que permite pensar em uma realidade cibernética, possibilidade dada pela Revolução Industrial 4.0. A necessidade de pensar a manutenção da privacidade na era da exposição, que se dá tão facilmente por conta da existência da Internet das Coisas, da inteligência artificial e outras tecnologias, é urgente. Se pensarmos em uma realidade tangível, pensamos no mundo real onde temos nossos corpos de carne e sangue, mas se nos “vemos” na realidade virtual, somos os dados pessoais que produzimos a todo momento. Assim como é necessário legislações que regulam nossa realidade corpórea, se faz necessário legislações sobre o tratamento de dados que garantam nossos direitos fundamentais também nessa outra realidade (mundo cibernético). Daí a procura por resguardo jurídico na Lei Geral de Proteção de Dados e na Lei de Cibersegurança, primeiro buscando conhecer como é a estrutura dessas leis, e posteriormente buscando através de pontos específicos _consentimento, responsabilidade e segurança_ determinar até que ponto a manipulação dos dados não fere o direito à privacidade.

A metodologia da pesquisa e a análise jurídica comparada nos moldes propostos por Pierre Legrand (2018). Numa compreensão hermenêutica do direito estrangeiro, em que este é encarado como uma oportunidade para a reflexão sobre o direito nacional. Ir ao direito estrangeiro é um exercício de auto-reflexão. As analises aqui apresentadas sobre o direito chinês não possuem o condão de ser explicações certeiras e precisas sobre aquela realidade (a melhor explicação sobre um direito estrangeiro sempre virá dos juristas daquele lugar), mas foram feitas máximo cuidado e profundo exercício de alteridade, com o proposito de auxiliar na reflexão sobre o direito brasileiro na matéria.

Na conclusão, considerando os diversos entendimentos sobre privacidade, a relação entre direito à transparência, à liberdade e ao esquecimento, procuramos analisar a tutela da privacidade na realidade virtual. Também tento estabelecer uma comparação entre a perspectiva de privacidade para Brasil e China, da mesma forma que comparo as previsões legais sobre a tutela dos dados pessoais e sua influência na garantia da privacidade nesses países.

1. QUARTA REVOLUÇÃO INDUSTRIAL

Na Era da 4ª Revolução Industrial, que tem como impulso essencial os dados, é bastante atual e verdadeira a colocação de Rodotà em que afirma que estamos "assediados por computadores, espiados por olhos furtivos, filmados por telecâmeras invisíveis. Os cidadãos da sociedade da informação correm o risco de parecer homens de vidro: uma sociedade que a informática e a telemática estão deixando transparente" (RODOTÀ, 2008, p. 8, *apud* MORAES; QUEIROZ, 2019, p. 115). Estamos em um contexto em que as noções tradicionais de privacidade e divulgação são obsoletas e inadequadas diante das tecnologias.

Precisamos também entender, em breve síntese, que a 4ª Revolução Industrial, também conhecida, segundo Carvalho, como Indústria 4.0, Manufatura Avançada, Indústria Inteligente, Era do *Big Data* ou da Internet das Coisas, entre outras, é resultado de convergência de informações dos mundos físicos, biológicos e digitais (SCHWAB, 2017, p. 23, *apud* CARVALHO, 2019, p. 108). Temos uma nova gestão das organizações, em que "pessoas, dados e tecnologias se complementam em suas ações e finalidades, sendo os dados transformados em inteligência competitiva aplicada em diferentes segmentos." (CARVALHO, 2019, p. 95).

Nessa nova era, estaremos cada vez mais em contato com elementos teóricos e práticos, talvez ainda um pouco desconhecidos, como: Internet das Coisas, o *Big Data*, a Computação

em Nuvem, a Robótica Avançada, a Inteligência Artificial, novos materiais e as novas tecnologias de manufatura aditiva (impressão 3D) e manufatura híbrida (funções aditivas e de usinagem em uma mesma máquina), Mineração de Dados, Ataques Cibernéticos, Proteção de Dados Pessoais, dentre outros. Os sistemas orientados por código estão cada vez mais presentes em nossa realidade, facilitando a vida humana e aumentando nossas capacidades, mas representam ameaças antes inimagináveis, principalmente no que se refere ao mau uso da inteligência artificial para obtenção de lucro por parte das empresas, o que justifica a existência da "ética dos dados". Esse conceito, importante para a realidade atual, considera a moralidade na correta análise e aplicação dos dados. Para a ética digital, Carvalho compreendeu de Schwab (2018) três elementos particularmente relevantes que são: "uso irrestrito de grande volume de dados; crescente dependência de algoritmos para a execução de tarefas, configuração de escolhas e tomada de decisão; e a redução gradual do envolvimento humano – ou mesmo de fiscalização – sobre os processos automatizados". (CARVALHO, 2019, p. 104-105).

No mundo cibernético, a ética na manipulação de dados é essencial, principalmente se considerarmos a economia, que leva muitas multinacionais a desconsiderar valores importantes por conta do dinheiro, e sabe-se que os dados representam econômica e politicamente uma moeda de controle muito valiosa. Daí a ressalva que Carvalho (2019) faz para a utilização consciente dos dados pela *Data Science*, em que se transforma o dado bruto em *insight* e conhecimento para tomada de decisão, da produção ao descarte, indo além do caráter estatístico que é atribuído aos dados, e é composta por uma governança de dados. Pensar em uma utilização consciente e ética dos dados é necessário e atual, visto sua imprescindibilidade na 4ª Revolução Industrial, em que

> [eles] estão permeando o mundo físico e digital, dentro de um verdadeiro ecossistema que abrange desde a sua produção até o seu descarte dos dados, impactando diretamente no desenvolvimento da economia, da promoção e estabilidade social, espalhados em todo mundo, oferecendo oportunidades e ameaças. (CARVALHO, 2019, p. 109).

2. PRIVACIDADE E PROTEÇÃO DE DADOS

O século XXI é marcado pelo desenvolvimento, cada vez maior, do ambiente virtual, principalmente devido à Revolução Industrial 4.0, em que se insere a Internet das Coisas (IoT), inteligência artificial e outras inúmeras inovações. Dado o avançado desenvolvimento da realidade cibernética é preciso que se crie legislações para regulamentá-la e proteger seus usuários, assim como existe legislações que preveem a regulamentação do mundo real, a

exemplo dos Códigos Civil, Penal, Eleitoral, de Trânsito, de Processo Penal, de Processo Civil, de Proteção ao Consumidor, Consolidação das Leis Trabalhistas e outros. Nesse sentido, um dos principais objetos de proteção e regulamentação que se verifica no mundo virtual é a proteção de dados pessoais, o que se relaciona profundamente com a noção de privacidade.

É com o intuito de preservar e regularizar a manipulação de dados, além da procura por reconhecimento internacional como um país que preveja certo nível de proteção a essa manipulação, que muitos Estados estão se preocupando com a criação de legislações específicas para esse fim. Como exemplo dessas regulações pode-se apontar: o Regulamento Geral sobre a Proteção de Dados (RGPD)[3] 2016/679, da União Europeia (UE), aprovada em 2016 e com um prazo de dois anos de transição, entrando em vigor em 2018, para legislar sobre a privacidade e proteção de dados pessoais, sendo aplicável a todos os indivíduos na União Europeia e Espaço Econômico Europeu; a Lei de Cibersegurança da República Popular da China[4], aprovada em 2016 e efetiva em 2017, visando garantir a segurança cibernética e sendo aplicável no território continental da República Popular da China; a Lei Geral de Proteção de Dados Pessoais (LEI DE PROTEÇÃO DE DADOS PESSOAIS)[5] Lei n° 13.709/2018, da República Federativa do Brasil, aprovada em 2018, alterada pela Lei n° 13.853/2019 e Lei n° 14.058/2020, que entrou em vigor em setembro de 2020, essa lei legisla sobre o tratamento de dados pessoais, visando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, sendo aplicável a qualquer operação de tratamento realizada em território nacional.

Antes de qualquer aprofundamento sobre a garantia da privacidade na manipulação de dados pessoais, baseado nas previsões da Lei de Proteção de Dados Pessoais brasileira e na Lei de Segurança Cibernética chinesa, é preciso estabelecer a relação entre privacidade e proteção de dados no ambiente virtual, e ainda, antes mesmo de estabelecer essa relação, é necessário determinar o que é privacidade, o que representa uma procura bastante profunda. Ademais, também é importante pensar o que representa a privacidade para o Brasil e a República Popular da China.

[3] UNIÃO EUROPEIA. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO. Bruxelas: 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 11 abr. 2022.

[4] Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ . Acesso em: 11 abr. 2022.

[5] BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 abr. 2022.

2.1 DIREITO À PRIVACIDADE E SUA RELAÇÃO COM A PROTEÇÃO DE DADOS PESSOAIS

No mundo virtual, o direito à privacidade deve ser pensado com ainda mais atenção, visto que diante da flexibilização de relações, manipulação dos dados pessoais, novos serviços oferecidos pelas tecnologias e intensificação da vigilância, facilitada pelo escrutínio automatizado, há a possibilidade de interferência na autoidentificação do indivíduo, sua subjetivação. Law aponta que essa realidade virtual facilita a reprimenda de "emoções, preferências, comportamentos, pensamentos e escolhas" (LAW, 2020, p. 43), daí a importância de garantir a proteção de dados pessoais e o direito à privacidade, evitando a manipulação desses dados de forma incorreta, que pode levar a uma manipulação de escolhas e pensamentos. Garcia, ressalta que:

> A questão da proteção à privacidade na rede mundial de computadores é muito delicada e envolve o surgimento de diversos recursos, como *spams*, *cookies*, códigos maliciosos, banco de dados e guarda de registro. A garantia à privacidade somente se tornou de fato uma necessidade presente na era da informação, porque somente nela foram criados instrumentos de violação intensa e constante. (GARCIA, 2013, p.112).

A garantia da privacidade passa ser extremamente necessária, a partir do advento da internet que funciona como uma intensificadora e facilitadora da vigilância constante e geral dos sujeitos, chegando a um atentado à livre tomada de decisões e a formação da personalidade, como destaca Garcia (2013, p. 112-113). No contexto da realidade virtual, a violação da privacidade passa a estar relacionado a possibilidade de utilização indevida de informações pessoais, como aponta Podestá, "a violação da privacidade no âmbito da *Internet* geralmente ocorre quando informações pessoais do usuário ou a publicidade de sua vida íntima passa a ser do conhecimento de pessoas não autorizadas."(PODESTÀ, 2000, p. 160, *apud* GARCIA, 2013, p. 113).

Atualmente, a possibilidade de violação da privacidade é muito mais fácil por conta da enorme quantidade de dados que estão em diversos bancos de dados, os quais podem ser usados de forma indevida, visto a ausência de leis regulamentadoras sobre a proteção de dados ou com intenção criminosa por parte dos processadores e controladores de dados, bem como a autorização descuidada e impensada de usuários da rede para determinados aplicativos e sites, a exemplo da prática comum e reiterada da não ler os termos de uso e políticas de privacidade[6]

[6] Disponível em: https://originalmy.readthedocs.io/pt_BR/latest/91-termos_de_uso.html. Acesso em: 11 abr. 2022.

Garcia, cita que entre os "casos específicos de violação do direito à privacidade, sem entrar na esfera em que este se liga aos direitos da personalidade, destacam-se o envio de *spams*, a venda de bancos de dados, o armazenamento de *cookies*, a remessa de códigos maliciosos e a guarda de registros." (GARCIA, 2013, p. 114).

Esmiuçando esses casos específicos de violação, Garcia (2013, p. 114-116) apresenta que há dois sistemas de envio de *spam*, o *opt-in*, para o qual é necessário que o usuário concorde previamente com o envio do spam, e o *opt-out*, no qual o usuário deve requisitar que o *spam* não seja mais enviado. O principal problema relacionado ao *spam* é que os dados adquiridos para os bancos de dados podem ser vendidos pelos proprietários desses bancos de dados. Ao apontar sobre a venda de banco de dados, a autora problematiza a questão da autorização, da propriedade e da proteção, o que envolve uma discussão complexa, mas em resumo e focando na violação da privacidade, cabe destacar que os dados que compõem certos bancos de dados pertencem à muitas pessoas, e a venda sem autorização destas representa possível ingerência do direito à privacidade. Os *cookies* representam possibilidade de atentado à privacidade do usuário quando não se expõe a possibilidade de configurar a máquina de acesso à internet para que não faça o registro dos *cookies* e as informações dos *cookies* podem ser aproveitada por mal intencionados que visam as vulnerabilidades da máquina. Há também os vírus, *worms*, *Trojans*, *backdoors* e os *rootkits* que são códigos maliciosos (*malwers*), ou seja, "programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador."[7] Por fim, o armazenamento de registro, além de estar relacionado ao direito à privacidade, é também essencial a tutela do direito à segurança, visto que prevê a importância de armazenar os registros para que possibilite a punição de atos ilícitos.

> Em suma, são atos de indevida ingerência nos limites éticos do exercício do direito à privacidade na *Internet*: a) envio de *spam* sem prévia autorização do usuário; b) vendas de bancos de dados sem a permissão dos que possuem informações nele registradas; c) armazenamento de *cookies* quando da expressa recusa do usuário por configuração do sistema; d) envio de vírus e códigos maliciosos em geral, notadamente quando obtido o acesso indevido aos dados informáticos. (GARCIA, 2013, p. 116).

É óbvio que no mundo cibernético os dados podem ser considerado moeda muito valiosa, mas sua importância há muito transcende o mundo virtual, chegando a representar alta relevância para o mundo real, por isso sua manipulação muitas vezes leva a alterações sociais, econômicas e políticas muito relevantes para a realidade tangível. É importante frisar que o direito a transparência, altamente procurado no contexto atual, que está relacionado a

[7] Disponível em: https://cartilha.cert.br/malware/. Acesso em: 11 abr. 2022.

publicização de determinadas informações, não é um facilitador da manipulação de dados, pois não há previsão que todas as ações e pensamentos dos proprietários de dados sejam publicizados, por isso não há conflito entre esse direito e o direito à privacidade. A relação entre a garantia de transparência e de privacidade abrange muitos entendimentos, mas esse trabalho não busca aprofundá-lo, e sim ressaltar a relevância da legislação para determinar e garantir o equilíbrio entre esses dois direitos.

O direito à privacidade, que garante, de certa forma, a autonomia de pensamento e ação do sujeito, está diretamente relacionado à proteção de dados pessoais. Por isso, é importante a criação de leis que legislam sobre a proteção de dados pessoais, garantindo o equilíbrio entre as partes (proprietário dos dados e controladores e processadores dos dados), protegendo as escolhas e preferências individuais da tirania da maioria, isso tudo para que mesmo a realidade virtual seja compatível com o caráter de sociedade democrática e valores fundamentais.

Para o contexto atual, a internet é dinâmica e liberalista, mas é justamente quando se pensa a manipulação de dados pessoais de forma descuidada e baseada em uma liberdade sem limites, que se tem a violação do direito à privacidade e à intimidade, influenciando na garantia de dignidade humana e autonomia. Essa situação de desrespeito, se dá baseado na sensação de que quando o ciberespaço surgiu tratava-se de um território sem lei e sem dono, onde os usuários e processadores utilizavam de um direito à liberdade sem fronteiras, para a manipulação dos dados pessoais, monetização de dados[8] e marketing direcionado, além de utilizar de um direito ao anonimato, sobre o qual recai muitas controvérsias, a exemplo do contexto brasileiro que não o prevê constitucionalmente, e como afirma Garcia, não é admitido moralmente, já que seu uso, quase sempre, está relacionado a intenções maliciosas e prejudiciais a outrem, bem como se trata de uma falsa impressão, pois existem técnicas de redirecionamento de IP que facilmente identifica o autor e quem acessou determinado conteúdo.

Ao pensar a relação entre a proteção de dados e a tutela da privacidade, Magrani (2019, p. 57-58.) aponta que existe uma relação de derivação entre a proteção de dados, como uma garantia instrumental, e a defesa da privacidade, mas não é uma relação limitadora, pois a proteção aos dados visa à proteção da pessoa, e para isso é importante que se referencie no

[8] Essa monetização se dá no âmbito do chamado "Big data" 11 — conceito que envolve a captação, armazenamento, processamento e capitalização de dados e informações com o intuito de auferir toda sorte de vantagens. Através do tratamento de dados, é possível aprimorar, por exemplo, a publicidade dirigida, baseada em padrões de acesso e consumo, e até mesmo influir no hábito do usuário da internet, escolhendo o que mostrar e o que não mostrar, capitalizando também em cima disto (e até mesmo influenciando o resultado de processos políticos, como sugerem certos estudiosos). (CARVALHO; GUIMARÃES; OLIVEIRA, 2018, p. 382-383)

leque de garantias fundamentais que os ordenamentos jurídicos oferecem. Nesse sentido, ele aproxima o conceito de proteção de dados ao direito da personalidade, por conta de seu caráter personalíssimo, pois esses dados pessoais são a pessoa, já que apontam números, características e qualificações pessoais, dados genéticos e outros de determinado sujeito. Portanto, para proteger essas pessoas, "bem como proteger a dignidade humana, é necessário assegurar a tutela dos dados pessoais." (MAGRANI, 2019, p. 58). Sobre essa relação Magrani afirma que:

> O direito à privacidade, esfera do direito à vida privada, está intimamente conectado à proteção da dignidade e personalidade humana, e pode ser extraído do reconhecimento constitucional dado à intimidade, à vida privada e à inviolabilidade de dados. Dentre as previsões constitucionais sobre o tema, destaca-se que a Constituição Federal de 1988 apontou o habeas data como instrumento apto a assegurar a proteção de informações e dados pessoais. (MAGRANI, 2019, p. 86)

Na nova sociedade da informação, a tecnologia contribui para que a esfera privada esteja mais exposta e frágil, mas também traz inúmeras facilidades para seus usuários. Então, para que haja uma efetiva tutela da privacidade é importante que o sujeito possa "conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas." (RODOTÀ, 2008, p. 92, *apud* MAGRANI, 2019, p. 87). Daí a importância do controle de coleta, armazenamento e utilização dos dados pessoais.

Outro aspecto bastante relevante quanto a manipulação dos dados é sobre a eliminação desses dados. Não se deve esperar que os dados sejam armazenados perpetuamente, até porque sua coleta, geralmente está ligada a algum objetivo, e se este for cumprido, passa a ser desnecessário que se mantenha armazenado determinado dado. Há, ainda, outras possibilidades que se cumpridas, devem ser consideradas para a eliminação dos dados e garantia do direito ao esquecimento. No entanto, a eliminação dos dados não deve ser considerada um caminho fácil, como aponta Fernanda Zuffa, pois para a devida eliminação os agentes de tratamento devem realizar análise sobre o adequado alcance da finalidade, criar mecanismos fáceis e acessíveis para que o titular dos dados revogue o consentimento, além de assegurar tecnologia que garanta que apagamentos de determinados dados não corrompa ou prejudique o banco de dados do qual ele fazia parte. A eliminação de dados e o direito ao esquecimento é assunto complexo, posto que apenas a eliminação desses dados não garante efetivamente o direito ao esquecimento, a exemplo de casos em que a publicização já tenha ocorrido, bem como haverá tentativas por parte dos operadores e controladores de evitar a eliminação dos dados, por conta de seu alto valor econômico.

É preciso destacar, que, pelo menos, no que se refere a eliminação de dados segundo a Lei de Proteção de Dados Pessoais, a previsão legal não garante efetividade total ao direito do

esquecimento, já que se os dados do sujeito tiverem sido repassados adiante, a legislação não obriga que esse terceiro apague os dados, estabelecendo uma relação apenas entre o titular dos dados e o responsável primeiro por seu tratamento. Como destaca Zuffa:

> Isto é, mesmo que o responsável pelo tratamento dos dados os tenha tornado públicos, e que, em razão de sua conduta, muitos outros agentes tenham acesso aos mesmos, não é compelido pela legislação a informá-los sobre a requisição de eliminação. Principalmente no meio digital, uma vez tornadas públicas, as informações se espalham e se multiplicam de maneira ágil e descontrolada, de modo que tão somente a comunicação aos agentes com quem fora compartilhado os dados é medida frágil e ineficaz no que concerne à proteção dos princípios norteadores da Lei de Proteção de Dados Pessoais, principalmente, no respeito à privacidade, previsto no artigo 2ª, I, da referida Lei. (ZUFFA, 2021, p. 98-99).

Acerca da relação entre o direito à transparência e o direito à privacidade, é preciso considerar que para os dias atuais, segundo Paesani (2006, p. 24, *apud* GARCIA, 2013, p. 108) "toda liberdade, por mais ampla que seja, encontra limites, que servem para garantir o desenvolvimento ordenado da sociedade e dos direitos fundamentais de qualquer sujeito, e este princípio se aplica também ao direito à liberdade de informação". Isso aponta a necessidade de um equilíbrio entre o direito à transparência, que está relacionado à liberdade de informações, e o direito à privacidade, de forma que a garantia de um e outro não gere danos na garantia recíproca desses direitos.

Relacionado a liberdade de informação e manipulação de dados, um outro tema importante é a censura, sobre a qual Garcia faz a seguinte consideração

> A respeito da censura prévia, tem-se [que] não cabe impedir a divulgação e o acesso a informações como modo de controle do poder. A censura somente é cabível quando necessária ao interesse público numa ordem democrática, por exemplo, censurar a publicação de um conteúdo de exploração sexual infanto-juvenil é adequado sob o aspecto ético. Contudo, não se pode ser aceita a censura política, que seleciona as informações que chegarão aos internautas. (GARCIA, 2013, p. 109).

Sobre isso, mesmo que não seja objeto desse estudo, é importante destacar a rigorosidade com que o governo chinês controla determinadas informações e expressões no território da República Popular da China. A censura chinesa é globalmente reconhecida e sujeita meios de comunicações com ampla audiência como televisão, cinema, teatro, literatura, internet e outros, seu objeto costuma ser assuntos relacionados a LGBTQIA+, democracia, violência policial, anarquismo e outros.

2.2 TUTELA DA PRIVACIDADE E PROTEÇÃO DE DADOS NA CHINA

Law (2020, p. 94-103) aponta que o conceito de privacidade é difícil de se estabelecer, visto que pode estar relacionado a muitas noções como a de a pessoa ser deixada em paz, de autonomia, de controle sobre assuntos pessoais significativos, de intimidade e de acesso restrito. Essa ampla relação caracteriza o conceito de privacidade como expansivo, o que não é recomendado na cultura chinesa. O autor destaca a necessidade de se estabelecer pelo menos uma noção base, e não tão expansiva, para que o ordenamento chinês garanta o direito à privacidade, isto é, quanto mais claro o conceito de privacidade, mais precisos serão os julgamentos para decidir quando ela pode ser devidamente tutelada. Nesse sentido, ele destaca que com o estabelecimento de diferentes interesses de privacidade na China, é impossível que eles não colidam, compitam e coexistam com outros valores da cultura chinesa, como a liberdade de imprensa, liberdade de expressão, proteção da receita e operação efetiva do governo. Para um conceito funcional de privacidade na China é preciso se satisfaça dois critérios, segundo Law, são eles:

> Primeiro, os indivíduos devem entender todos os (ou pelo menos a maioria dos) aspectos de suas informações pessoais que estão sendo abordadas. Em outras palavras, os indivíduos devem saber quando a privacidade é, ou não, conquistada ou perdida. Caso contrário, a definição de privacidade será imprecisa. Segundo a definição de privacidade deve ser aplicável às práticas sociais e legais chinesas. As práticas sociais e legais incluem o uso e teste da definição por tribunais, advogados e outras agências governamentais chinesas. (LAW, 2020, p. 101-102)

Atualmente, se encara uma necessidade crescente de que a tutela a privacidade seja respeitada na China, tanto por pessoas e grupos, quanto pelo governo chinês, visto que muitos interesses de privacidade no país estão ameaçados, por conta de determinadas características da sociedade chinesa contemporânea como o rápido desenvolvimento da economia chinesa, que levou os comerciantes a encontrar e procurar clientes ativamente em seu local ou espaço pessoal; e com o rápido desenvolvimento de tecnologias da informação e dispositivos de processamento de dados, a exemplo da IoT[9], se tornou muito fácil para que a população manipule, acesse e salve informações pessoais.

A China passou muito tempo sem legislação específica para a privacidade, contando principalmente com a tutela da privacidade e proteção de dados a partir de outras legislações

[9] Internet das Coisas: descreve a rede de objetos físicos—"coisas"—que são incorporados a sensores, software e outras tecnologias com o objetivo de conectar e trocar dados com outros dispositivos e sistemas pela internet. Esses dispositivos variam de objetos domésticos comuns a ferramentas industriais sofisticadas. Disponível em: https://www.oracle.com/br/internet-of-things/what-is-iot/. Acesso em: 12 abr. 2022.

esparsas que surgiram, principalmente, após a Revolução Cultural chinesa, com a liderança de Deng Xiaoping. Esse líder, apresentava uma visão bastante interessante que impulsionou o desenvolvimento legislativo, de que era melhor ter algumas leis do que não ter nenhuma, sendo melhor fazê-las mais cedo, do que mais tarde, e com o passar do tempo a legislação poderia ser aprimorada. Sobre esse período, Law destaca:

> Como consequência, sob a liderança de Deng Xiaoping, nos trinta anos de reforma e abertura de mercado, a China testemunhou a promulgação maciça e rápida de leis e regulamentos. Com relação a esse fenômeno social, o professor Chen Jianfu salienta que essa fragmentação e o desenvolvimento não sistemático do sistema jurídico da China produziram várias leis, que incluem muitos estatutos, decisões, ordens, regulamentos administrativos e regras individuais feitas sob diferentes orientações políticas. Algumas delas autorizam poderes intrusivos a agências governamentais. Com base nessas leis, hoje, as autoridades chinesas têm inúmeros poderes de intrusão. (LAW, 2020, p. 107).

Pode-se notar o poder de intrusão com a existência dos fiscais chineses, admitidos pela lei de administração tributária, em que muitos casos não preveem limitações ao exercício dos poderes, inclusive com acesso total e gratuito às informações pessoais. Ademais, há também o Regulamento de Despacho Aduaneiro, que concede amplos poderes de intrusão aos funcionários aduaneiros da China, ou seja, a alfândega chinesa tem poderes quase que ilimitados, em alguns sentidos. Tais previsões legais mostram uma certa fragilidade na tutela e previsão da privacidade na China, já que baseado em sua natureza nacionalista e no "desenvolvimento jurídico sistemático, os poderes intrusivos são numerosos e amplamente aplicados. Isso pode incluir o poder de entrar em qualquer lugar pessoal ou de inspecionar e obter informações pessoais." (LAW, 2020, p. 113).

De fato, são inúmeros os exemplos de poderes intrusivos a privacidade, liberdade e aos direitos individuais na China, até porque "não existem princípios legais abrangentes que protejam os interesses de privacidade [no país]"(LAW, 2020, p. 122)" e a legislação só consegue dar uma resposta parcial às invasões de privacidade. A privacidade na China se encontra em uma situação tão conturbada que nem mesmo a Constituição chinesa[10] expressa claramente sobre sua tutela em seus artigos. Além disso, Carvalho traz em sua pesquisa uma importante consideração retirada dos estudos de Yu e Zhao (2019), que mostra a situação complicada da privacidade chinesa, de que "na China, os usuários da Internet encontram-se em uma prisão transparente, na qual todos os seus comportamentos e dados pessoais estão sob a

[10] Disponível em: http://www.dhnet.org.br/direitos/anthist/marcos/hdh_constituicao_chinesa_1982.pdf. Acesso em: 12 abr. 2022.

estrita supervisão de um terceiro olhar, sendo a essência do Big Data seguir os dados que o público cria." (CARVALHO, 2019, p. 106).

Para entender melhor em qual contexto se encontra a tutela da privacidade e dos dados pessoais, precisamos entender que a princípio o conceito de privacidade ou informações pessoais nem mesmo existia para a cultura chinesa. Na legislação chinesa se adotou a noção de *Yin Si* _ "caso particular" _, termo difundido nas tradições históricas e folclóricas chinesas. Foi somente a partir da abertura econômica e política da China, com as reformas legislativas entre os anos de 1980 e 1990, que o conceito de privacidade substituiu o de *Yin Si*, passando a ser usado pelas autoridades judiciárias, legislativas e executivas. Mas mesmo assim, sobre o conceito de privacidade, no que concerne ao direito substantivo, as leis e regulamentos ainda "não fornecem definição e descrição claras do escopo desse direito, com a consequência de que os limites do direito substantivo à privacidade permanecem obscuros tanto na teoria legislativa quanto na prática judicial."(LAW, 2020, p. 126).

Não se restringindo a apenas a proteção de dados do consumidor, as leis apresentadas por Law, são leis que atualmente versam sobre a segurança da privacidade e proteção de dados pessoais no território chinês. Sobre isso ele apresenta:

> Os principais regulamentos relativos à proteção de dados do consumidor podem ser encontrados nos seguintes instrumentos legais: a Constituição, a Lei de Segurança Cibernética, a Lei dos Direitos do Consumidor, a Decisão do Comitê Permanente do Congresso Nacional do Povo sobre Fortalecimento da Proteção de Informação da Rede, a Decisão do Estatuto Permanente Comitê do Congresso Popular Nacional sobre a Revisão da Lei de Proteção de Direitos do Consumidor da República Popular da China (Lei de Direitos do Consumidor), o Regulamento de Proteção de Informações Pessoais de Usuários de Telecomunicações e Internet, as Medidas Administrativas para Transação On-line, Medidas de Segurança de Informações Pessoais para Serviços de Correio, Medidas de Administração de Registros Médicos de Instituições Médicas e Medidas de Administração de Informação de Saúde da População. (LAW, 2020, p. 124)

O que se verifica é um país grandioso, com acelerado crescimento econômico, mas que o legislativo não está conseguindo acompanhar ou não deseja acompanhar as mudanças e necessidades reais. A garantia da privacidade, junto com o direito a dignidade e a liberdade se configuram como direitos fundamentais que quando violados podem configurar possíveis atentados ao regime democrático e autonomia dos cidadãos. Por isso, se observa uma necessidade urgente de se estabelecer na China um conceito de privacidade, que se adequando a sua cultura, permita uma melhor utilização por parte do legislativo, para criar as leis específicas, e do judiciário, para aplicá-las.

No que concerne a proteção de dados, é preciso destacar o esforço da China de melhorar seu sistema de proteção de dados, principalmente a partir da orientação do presidente Xi Jinping, que objetiva converter o país em uma potência cibernética, o que faz surgir a necessidade de leis que regulam sobre a realidade virtual e os dados pessoais, os quais circulam na rede. Entre as principais normativas, se tem a Lei de Cibersegurança Chinesa, a Especificação sobre Segurança das Informações Pessoais[11] (comumente denominada "Especificação"), a Diretriz para a Proteção e Segurança de Informações Pessoais na Internet[12] (doravante denominada "Diretriz") _essas duas citadas anteriormente não tem caráter vinculativo) _ e os Projetos de Medidas sobre Administração de Segurança de Dados[13] (denominada "Medidas") _que possui caráter vinculativo.

Zhou, acadêmica em Direito pela Universidade de Tsinghua, afirma que:

> […] a China se dedicou a criar e melhorar seu próprio sistema de proteção de dados. Com a Lei de Cibersegurança como base geral, os três documentos normativos oferecem parâmetros de referência mais detalhados sob a perspectiva de diferentes reguladores. Como a Especificação e a Diretriz carecem de força legal, elas formulam principalmente uma estrutura voluntária como referência para empresas, já as Medidas podem servir como uma diretriz mais importante para complementar a aplicação da Lei de Cibersegurança.
> […]
> Como a Lei de Cibersegurança visa proteger a soberania geral da rede, não é uma regulamentação conclusiva e completa dos direitos dos indivíduos, como a proteção de dados e privacidade. O sistema suplementar definitivamente beneficiará a implementação da Lei de Cibersegurança e, inevitavelmente, tratará uma certa inconstância e confusão quanto ao que seguir.[14]

A respeito dessa "certa inconstância e confusão" que a autora cita é fácil de identificar quando se analisa comparativamente o corpo desses documentos normativos. Como documentos diferentes, há diferentes categorizações e definição de informações pessoais, de níveis de proteção, de exceções quanto ao consentimento para coleta de dados e outros. No entanto, esse sistema multidimensional singular de proteção de dados, como é chamado por Zhou, que se deu pela emissão desses documentos normativos complementares à Lei de

11 Entrou em vigor em 2018 e foi emitida pela Administração de Normalização da China. Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/. Acesso em: 12 abr. 2022.

12 Com sua versão final divulgada em 2019, foi feita pelo Ministério da Segurança Pública da China, como uma reafirmação e validação da Especificação. Disponível em: https://mlaw.wkinfo.com.cn/legislation/detail/MTAxMDAxMzEzODVfRW4%3D. Acesso em: 12 abr. 2022.

13 Promulgada pela Administração do Ciberespaço da China, com o auxílio de consulta pública, em 2019. Disponível em: https://www.insideprivacy.com/wp-content/uploads/sites/6/2019/05/Measures-for-Data-Security-Management_Bilingual-1.pdf. Acesso em: 12 abr. 2022.

14 ZHOU, 2020, p. 304.

Cibersegurança, é bastante interessante, visto a ausência de precedentes e experiência da jurisprudência chinesa com casos sobre o espaço cibernético, proteção de dados e proteção da privacidade, bem como a rapidez com que a inovação do ciberespaço se dá na China, possibilitando os surgimentos de casos que a Lei de Cibersegurança ainda não previa, mas que pode vir a ser orientado nos outros documentos normativos que a seguiu. Nesse sentido, a implementação desses documentos complementares pode ajudar os tribunais chineses a ganharem experiência e preencher a lacuna entre política e realidade, e testarem determinadas previsões, mas por conta da ausência de caráter vinculativo[15], de parte desses documentos, pode haver empresas que se recusam a seguir as previsões, o que não geraria nenhuma experiência e proveito para a jurisprudência chinesa. Por isso, Zhou (2020, p. 306) destaca a importância de que o sistema multidimensional seja superado e seja criado para a regulamentação do espaço cibernético com uma legislação única e integrada.

Analisando o texto da Lei de Cibersegurança, nos chama a atenção a ausência da expressão "dados pessoais", o que ocorre, talvez, por um distanciamento do conceito da cultura chinesa, assim como aconteceu com o conceito de "privacidade", julgamos assim pois a lei, a todo momento, reforça e cita em seu corpo o conceito de informações pessoais[16], o que em seu art. 76, é elucidado como sendo informações de todos os tipos, registradas eletronicamente ou não, que podem ser tomadas isoladamente ou em conjunto com outras informações, as quais são suficientes para identificar uma pessoa física. O conceito de informações pessoais sobre o qual se desdobra a legislação chinesa é muito similar ao conceito de dados pessoais[17] adotado pela legislação brasileira de proteção de dados _ Lei de Proteção de Dados Pessoais. Além disso, na legislação chinesa também consta o conceito de dados de rede[18], que segundo seu art. 76, são "todos os tipos de dados eletrônicos coletados, armazenados, transmitidos, processados e produzidos por meio das redes"[19].

Considerando esses dois conceitos comparativamente com os conceitos brasileiros da Lei de Proteção de Dados Pessoais, percebe-se que mesmo sem citar ou usar o conceito de dados pessoais, a Lei de Cibersegurança regula sobre sua manipulação e protege esses dados

15 A Especificação e Diretriz serve apenas como *compliance* para as empresas que coletam dados pessoais, mas não pode ser exigida em juízo.

16 个人 信息

17 Art. 5°, I -dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

18 网络 数据

19 Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Acesso em: 11 maio 2022.

ao proteger as informações pessoais. Outro detalhe é a proteção dos dados pessoais sensíveis[20], que extrapolam a identificação do sujeito, possibilitando a identificação de sua personalidade. Esse conceito está presente na Lei de Proteção de Dados Pessoais brasileira, mas não é citado em nenhum momento na legislação chinesa, no entanto ao definir "informações pessoais" a Lei de Cibersegurança se preocupa em apresentar um rol exemplificativo de informações que são protegidas pela lei, e é justamente nesse momento que se tem um encontro com a legislação brasileira, ao definir que as informações biométricas pessoais são informações pessoais reguladas pela Lei de Cibersegurança, bem como, no conceito brasileiro de dado pessoal sensível também se vincula ao dado biométrico. Portanto, podemos entender que a legislação chinesa, mesmo não citando o conceito ocidental com o qual estamos acostumados, protege e regula sobre os dados pessoais e dados pessoais sensíveis. Da mesma forma, mesmo que haja apenas uma vez a citação da palavra "privacidade", podemos identificar a defesa do direito à privacidade ao garantir sigilo e confidencialidade às informações pessoais que são manipuladas pelos operadores de rede.

2.3 TUTELA DA PRIVACIDADE E PROTEÇÃO DE DADOS NO BRASIL

A cultura brasileira possui muitas influências, mas sem dúvidas uma das maiores é a europeia, já que fomos "colonizados" pelos portugueses. Devido a isso, muito da cultura europeia foi absorvida e se tornou, também, cultura brasileira, entre os numerosos exemplos está o *civil law*, que adveio da ideia de direito da família romano-germânica, e se refere a imprescindibilidade da legislação escrita. Não é estranho que o ordenamento jurídico brasileiro esteja repleto de códigos e doutrinas. Talvez seja em decorrência da cultura jurídica do *civil law*, adotado no Brasil, que há uma preocupação e a existência da previsão do direito à privacidade, intimidade e proteção de dados, estando estabelecidos pela Constituição Federal de 1988 (CF/1988), pelo Código Civil (CC), pela Lei de Acesso à Informação (Lei n 12.527/11), pelo Código de Defesa do Consumidor (CDC), pela Lei Geral de Proteção de Dados (LGPD) e em outras legislações. Atualmente, o Brasil possui uma maior gama de proteção no âmbito da privacidade e da transparência, tendo conseguido sua primeira lei específica de proteção de dados com a aprovação da Lei de Proteção de Dados Pessoais.

[20] Art. 5, II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

A priori, é dever destacar que na Constituição Federal de 1988, em seu artigo 5°, certos incisos preveem garantia ao direito à privacidade[21], inviolabilidade de dados[22] e o *habeas data*[23]. Por ser a carta magna de nosso país é bastante simbólica a previsão de tais garantias, mesmo que em relação à inviolabilidade dos dados não seja nada específico. É importante destacar que o *habeas datas*, regulamentado na Lei Federal n° 9.507/97, é um importante remédio constitucional que será concedido para garantir o direito de conhecimento de dados sobre a pessoa que o impetrou constantes em bancos de dados governamentais ou de caráter público; a retificação de dados; e a anotação nos assentamentos do interessado de contestação ou explicação sobre dado verdadeiro, justificável e que está sob pendência judicial ou amigável.[24] O *habeas data* se mostra relacionado ao direito de transparência, liberdade de informação e proteção aos dados pessoais, portanto também se apresenta parcialmente regulado pela Lei de Acesso à Informação, segundo Lima e Monteiro (LIMA; MONTEIRO, 2013, p. 62).

A respeito da privacidade, há também previsão legal no Código Civil em seu artigo 21, em que prevê que "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma."[25]. Ademais, outro assunto relacionado e que consta na legislação é o anonimato, o qual é vedado, segundo o artigo 5°, inciso IV, sendo garantido a livre manifestação do pensamento, no entanto há a proteção ao pseudônimo, como se protege o nome da pessoa natural, para fins lícitos, está assegurada no artigo 19 do Código Civil.

Em síntese, também há proteção de dados se analisados a Lei Geral de Telecomunicação[26] (Lei n° 9.472/97), bem como o Código de Defesa do Consumidor[27], ambos com uma proteção em sentido específico dos dados tutelados, mas que serviam como base de

21 Constituição Federal de 1988, art. 5º: "[...] X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

22 Constituição Federal de 1988, art. 5º: "XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

23 Constituição Federal de 1988, art. 5º: "LXXII – conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo".

24 Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9507.htm. Acesso em: 13 abr. 2022.

25 Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 13 abr 2022.

26 Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 13 de abr 2022.

27 Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 13 abr. 2022.

previsão legal para a época, já que não havia legislação de aplicação ampla sobre proteção de dados, e cujo objeto fosse especificamente este. Outro importante texto jurídico que traz sobre o direito à privacidade e a proteção de dados é o Marco Civil da Internet, o qual situou sua previsão dentro da rede. Seu texto legal explicita:

> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
> Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:
> I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
> II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

Lima e Monteiro apontam também que a Lei Federal n° 7.232/84 [28], que dispõe sobre a Política Nacional de Informática, contribui com o alargamento do conceito de privacidade e para a proteção de dados em seu art. 2°. O Estatuto da Criança e do Adolescente também traz, focado na criança e no adolescente, em seu art. 100 o direito à privacidade como um princípio que deve ser seguido para a aplicação de medidas socioeducativas. Além disso, a Agência Nacional de Telecomunicação (ANATEL) e o Comitê Gestor da Internet Brasileira (CGI.br) quanto a privacidade na internet, estabelece um princípio de neutralidade, segundo o qual o provedor de internet deve manter sigilo sobre os dados de seus usuários perante outrem, só podendo revelá-los em caso de ordem judicial, e não podendo ser responsabilizado pelo acesso do usuário que cometer ato ilícito (LIMA; MONTEIRO, 2013, p. 64).

Existem ainda outras legislações que contribuem para a tutela do direito à privacidade, proteção de dados e transparência, mas ao apontar essas, já se faz um breve resumo do cenário brasileiro sobre a privacidade e proteção de dados.

Outro ponto importante é sobre a classificação dos dados na cultura brasileira, que ocorreu na Lei de Proteção de Dados Pessoais. Além dos dados pessoais[29], a legislação brasileira também apresenta os dados pessoais sensíveis[30], uma categoria especial dos dados pessoais que também se encontra presente no Regulamento Geral sobre a Proteção de Dados

[28] Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L7232.htm. Acesso em: 13 abr. 2022.

[29] Disponível em: https://www.serpro.gov.br/Lei de Proteção de Dados Pessoais /menu/protecao-de-dados/dados-pessoais-Lei de Proteção de Dados Pessoais . Acesso em: 11 maio 2022.

[30] Disponível em: https://www.serpro.gov.br/Lei de Proteção de Dados Pessoais /menu/protecao-de-dados/dados-sensiveis-Lei de Proteção de Dados Pessoais . Acesso em: 11 maio 2022.

europeu, e os dados anonimizados[31] e dados públicos[32]. Esses três conceitos[33] estão presentes na Lei de Proteção de Dados Pessoais, logo em seu art. 5, e identificam tipos de dados diferentes para o ordenamento jurídico brasileiro. Se considera dados pessoais aqueles através dos quais pode se identificar uma pessoa, a exemplo do nome, endereço de residência, endereço eletrônico, endereço IP e outros. Os dados pessoais sensíveis são aqueles que descrevem características íntimas da pessoa e sua personalidade, a exemplo dos dados que revelem origem racial ou étnica, opiniões políticas, religiosidade, convicção filosófica, dados genéticos ou biométricos, dados relacionados a vida sexual ou orientação sexual, dados relacionados a saúde, a filiação sindical e outros. Já os dados anonimizados são aqueles que não permitem identificar seu titular, sua anonimização pode ter ocorrido por utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, a exemplo dos dados estatísticos. E os dados públicos são aqueles que a lei prevê como dados pessoais cujo acesso é público, isso porque se foram tornados anterior e manifestamente públicos por seu titular, a organização não precisa pedir novamente o consentimento para utilizá-los, a não ser que se pretenda compartilhar esses dados, o que necessita de novo consentimento.

A respeito dos dados pessoais sensíveis, há uma discussão sobre a necessidade e importância de regulá-los com mais de rigor do que os demais, isso porque os dados pessoais sensíveis podem possibilitar a discriminação de seu titular caso sejam publicizados. Esses dados se referem à intimidade do sujeito, portanto devemos chamar a atenção para sua manipulação que está bastante relacionada ao direito à privacidade, que é, essencialmente, o poder de controlar a publicização de suas informações pessoais.

31 Disponível em: https://www.serpro.gov.br/Lei de Proteção de Dados Pessoais /menu/protecao-de-dados/dados-anonimizados-Lei de Proteção de Dados Pessoais . Acesso em: 11 maio 2022.

32 Disponível em: https://www.serpro.gov.br/Lei de Proteção de Dados Pessoais /menu/protecao-de-dados/dados-publicos-Lei de Proteção de Dados Pessoais . Acesso em: 11 maio 2022.

33 Art. 5º Para os fins desta Lei, considera-se:
I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; [...] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 maio 2022.

2.4 AS GRANDES EMPRESAS E A GARANTIA DA PRIVACIDADE DOS DADOS PESSOAIS MANIPULADOS

Nosso cotidiano está cada vez mais ligado e dependente de tecnologias, em que o consentimento de uso, ao aderir aos contratos de adesão _ firmados entre as partes, em que uma delas aceita as cláusulas e condições de portabilidade previamente estabelecidas pela outra _ por anuir com termos e condições de uso, é necessário para que tenhamos acessos a essas tecnologias, sendo que o não consentimento, muitas vezes nos veda do acesso de determinados bens e serviços. Assim como Moraes e Queiroz apontam, o consentimento do titular de dados, bem como sua autodeterminação informativa, não devem ficar a mercê do "tudo ou nada" que a anuência com os termos e uso de condições dos aplicativos e plataformas representa. Tal situação é absurda se pensarmos que o acesso a determinados serviços depende de uma total concordância com cláusulas e condições previamente estabelecidas pelo provedor do serviço, sem possibilidade de discussão sobre os termos ou concordância parcial com os mesmos, e que tradicionalmente representa autorização irrestrita para o uso dos dados pessoais. Portanto, o usuário "torna-se refém do "consentimento" para a aquisição de produtos e serviços cada vez mais essenciais à vida em sociedade."(MORAES; QUEIROZ, 2019, p.122-123).

É inegável, que nesse contexto, que um dos principais interessados nos dados pessoais que oferecemos são as empresas multinacionais e quanto mais dados fornecemos, melhor é a eficiência no consumo, economia, mobilidade e outros aspectos da vida quotidiana, isso porque os perfis traçados são mais precisos, possibilitando a individualização de demandas e a otimização dos resultados que cada indivíduo deseja (CAMARA; RODRIGUES, 2019, p. 73). Nesse contexto, em que os dados são fornecidos a todo momento, a garantia de privacidade desses dados passou a ser um ponto nevrálgico do universo jurídico.

O que é ainda mais preocupante, é que se sabe, baseado em casos recentes como os escândalos de privacidade do Facebook e ainda sua responsabilidade nos dados pessoais usados pela empresa de consultoria política Cambridge Analytica _ possibilitando campanhas direcionadas de marketing que influenciaram as eleições em alguns países_, todos casos de usos de dados sem consentimento de acesso por parte de seus titulares, que as empresas multinacionais não respeitam, em muitos casos, a privacidade dos dados de seus usuários. Essa manipulação sem compromisso se torna ainda mais preocupante se considerarmos, diante dos casos já vistos na sociedade, que se trata um atentado à democracia representativa, visto que essas grandes empresas estão tendo atuação relevante no cenário político internacional. Camara

e Rodrigues também apontam que em uma perspectiva geopolítica o tratamento de dados pode influenciar no comportamento humano, além de quem os atentados à privacidade também prejudicam à autonomia, dignidade, empoderamento e autodeterminação das pessoas (CAMARA; RODRIGUES, 2019, p. 73-74).

Essa insegurança justifica o surgimento de legislações de proteção de dados, como a Lei de Proteção de Dados Pessoais brasileira, a RGPD europeia e a Lei de Cibersegurança chinesa, traçando um limite jurisdicional que garanta a proteção dos dados pessoais, o que poderia colocar essas empresas à mercê dos interesses estatais, se pensamos de forma mais superficial. Além disso, podemos pensar que economicamente as transnacionais estariam vinculadas às regulamentações de proteção de dados nacionais, representando uma barreira de acesso ao mercado interno.

No entanto, não se pode imaginar que Estado e multinacionais estão em "desacordo" com suas legislações de proteção aos dados pessoais, até porque, como afirma Camara e Rodrigues:

> [As] grandes empresas de tecnologia parecem apresentar um papel duplo, tanto econômico quanto estratégico-político, podendo fornecer o aparato tecnológico necessário para realizar operações ilícitas em território estrangeiro, mas em compliance com as normas de uma nação rival. (CAMARA; RODRIGUES, 2019, p. 79).

O que mostra a necessidade de as multinacionais serem estratégicas e saberem lidar com os interesses dos estados, lhes dando um certo poder perante os governos desses, se firmadas parcerias ou acordos de interesse mútuo. Não é difícil que esses acordos sejam firmados, visto que se sabe que em busca da maximização do lucro muitas empresas desconsideram as questões éticas e legais, as sujeitando aos interesses econômicos. Também devemos considerar que em países menos democráticos, o poder político e o poder econômico não estão totalmente desvinculados, e as liberdade individuais e transparência do processo de regulamentação também não estão totalmente garantidas, o que facilita o estabelecimento de acordos para a coleta e uso indevido de dados (CAMARA; RODRIGUES, 2019, p. 79-81). A exemplo da relação entre a Google e a China, que a empresa vem trabalhando em parceria com pesquisa em inteligência artificial no país com os responsáveis pelo desenvolvimento do sistema de segurança da província de Xinjiang, local em que há mais de 1 milhão de cidadãos de minorias étnicas detidos em campos de concentração, o que se tornou possível pela coleta de dados sensíveis e os padrões de comportamento, levando a identificação, categorização e cerceamento de liberdade (CAMARA; RODRIGUES, 2019, p. 80).

Sobre o poder das multinacionais, citado anteriormente, Camara e Rodrigues fazem a seguinte contribuição:

> Este **poder** dá contorno a um **cenário internacional em que estas companhias passam de coadjuvantes a protagonistas, não só sendo operacionalizadas para fins de garantir interesses Estatais, mas prevalecendo-se de uma liberdade em adequar-se a situações econômica e politicamente mais interessantes possíveis**. Leis de proteção de dados e demais normas tornam-se então ferramentas de política internacional, não prezando pelos princípios da cooperação internacional e dos agentes interessados, tornando a efetiva garantia dos direitos dos titulares uma questão secundária. Dito isto, não significa que não houve ganhos a garantias individuais. Aqui, discute-se, fundamentalmente, as motivações de tais normativas. (CAMARA; RODRIGUES, 2019, p. 86) (grifo nosso)

Interessante destacar que Camara e Rodrigues (2019. P. 76-82) apontam que para algumas legislações nacionais o estado pode exercer a quebra da privacidade de dados pessoais, como no caso da legislação chinesa de cibersegurança por requisição do governo, e também nos Estados Unidos em seu "Ato de Inteligência e Vigilância Estrangeira", de 1978, que permite por autorização judicial, desde que seja uma operação sigilosa sob pretexto de segurança nacional, para o combate da espionagem e terrorismo.

2.6 SOLUÇÕES PARA A PROTEÇÃO DA PRIVACIDADE DE DADOS PESSOAIS

Tendo considerado as dificuldades da efetiva garantia de privacidade dos dados pessoais, é preciso pensar também em soluções. Nesse sentido, um dos melhores modelos para o tratamento de dados pessoais é o uso "privacidade desde a concepção (*privacy by design*), apresentado por Ronald Hes, que visa diminuir a possibilidade de uma plataforma ser um local de comprometimento de dados pessoais, já que se utiliza alguma tecnologia que impossibilita, de alguma forma, a lidar diretamente com os dados dos usuários, o que pode evitar, por exemplo, que a empresa precise escolher compliance entre diferentes legislações. Entre as ferramentas úteis para esse fim, pode-se destacar, segundo Camara e Rodrigues: i) uso de assinaturas digitais (criptografa os dados do titular para que só possam ser operados na plataforma em que se deu o consentimento); ii) assinatura digital cega (a identidade do titular nunca é compartilhada, mas se têm necessário a assinatura para que se possa acessar determinado serviço que tenha dados pessoais como imprescindíveis); iii) pseudônimo digital (teoricamente similar a ocultação da identidade do usuário, isto é, se coleta estrategicamente uma mínima quantidade de dados que impossibilita a identificação do indivíduo). (CAMARA; RODRIGUES, 2019, p. 83).

Outras soluções são: a utilização de VPNs (*Virtual Private Networks*)[34], que utiliza a rede pública de provedores de "internet para estabelecer serviços seguros e confiáveis de acordo com os Contratos de Níveis de Serviço assinados"(CAMARA; RODRIGUES, 2019, p. 84)"; a tecnologia *blockchain* (código aberto, governança de maneira distribuída e transparência e supervisão independente) "utilizando um *smart contract* para gerenciamento automatizado da plataforma, com três tipos de *tokens"*(CAMARA; RODRIGUES, 2019, p. 84)", cada qual com algumas especificidades; "predileção a ferramentas que não as do controlador, mas sim de terceiros autorizados cujo escrutínio público lhes garantisse permissão de tratamento dos dados" (CAMARA; RODRIGUES, 2019, p. 85) (o terceiro estaria limitado a armazenar e tratar os dados, serviços estes que só seriam realizados quando a empresa interessada ou o usuário final solicitassem).

3. LEI DE CIBERSEGURANÇA DA REPÚBLICA POPULAR DA CHINA

A priori, precisamos entender como se dá a formação da cultura jurídica chinesa, já que em muitos aspectos essa civilização se diferencia dos modos ocidentais. Nesse quesito, nos baseando em pesquisa feita pela professora Diva Julia Sousa da Cunha Safe Coelho, que aponta certos aspectos culturais chineses como sua noção particular de superioridade diante de outras culturas, que é um dos fatores fundamentais de seu isolacionismo, bem como seu desapego aos modos da cultura ocidental de codificar deveres, isto é, aquilo que deve ser já é, e não precisa ser postulado em legislação para ser exigido ou verificado, entre outros aspectos culturais. Em sua pesquisa, a referida professora analisa o desenvolvimento da normatividade chinesa em três etapas que são: etapa do devenir da normatividade tradicional chinesa durante as dinastias (771 a. C - 1911 d. C); etapa da peculiar modernização da matriz essencialmente socialista (1911-1978); e etapa do Direito chinês atual (1978-atual) (SAFE COELHO, 2017, p. 327). Também se destaca a influência, no desenvolvimento normativo chinês, da base Confucionista (*li*) e a Legalista (*fa*).

É importante nos atentar em alguns aspectos sobre as características dessas duas bases, sendo que a base Confuncionista está ligada a noção de relações naturalmente hierárquicas entre indivíduos e um apego à moral e a conciliação, além de que se pregava a constituição e resolução dos conflitos por meio de uma perspectiva parental, já a base Legalista é o início de

[34] Redes Privadas Virtuais são redes de comunicação privadas construídas sobre uma rede de comunicação pública. Assim, o tráfego de dados é feito através da rede de comunicação pública, seguindo seus protocolos padrões. Funciona como se fosse um túnel construído sobre uma infraestrutura pública, como a internet

uma normatividade, que como a aponta a professora Diva Júlia, se analisada pelos nossos referentes ocidentais, marcada pelo lema "uma má lei é melhor do que nenhuma lei", com ênfase na utilidade e na técnica. A base confucionista se opunha à aplicação de normas gerais e abstratas pois elas desconsideram as particularidades de cada caso concreto e atender aos interessados, fazendo jus ao status social deste. Enquanto que na base legalista se coloca contra ao privilégio nobiliárquico, pregando uma igualdade perante as leis, em que a forma de manutenção da ordem social está diretamente relacionada a submissão da população e do imperador ao *Fa*, sob a possibilidade de punição para aqueles que não cumprissem as determinações (SAFE COELHO, 2017, p. 330-336).

Sabendo disso, podemos considerar a modernização socialista da China, em um primeiro momento, essencialmente nacionalista, como a tentativa, inspirada no êxito das codificações japonesas baseadas nas alemãs, de processo de codificação, que optou pela tradição jurídica continental europeia (Civil Law). Essa foi a contribuição e início de um processo de modernização e organização jurídica chinesa se aproximando da prática de criação de leis e códigos, típicas dos ocidentais (SAFE COELHO, 2017, p. 339-342).

A Lei de Cibersegurança[35] é fruto desse processo de construção normativo e uma evolução de normas e regulamentos pré-existentes e trata-se de um marco legal em relação a segurança no ambiente virtual. Ela estabelece regras de proteção da privacidade de dados e de segurança cibernética.

A lei é rígida com as empresas, no sentido de determinar que todas as corporações e empresas multinacionais fiquem atentas às questões operacionais de cibersegurança e proteção de dados do próprio negócio. O Estado determina o desenvolvimento da informatização e a segurança cibernética, apontando em seu artigo 3° que segue os princípios de uso ativo, administração de acordo com a lei, desenvolvimento científico e garantia de segurança, além de promover a construção de infraestrutura de rede e interconectividade. Há também a indicação para que os "proprietários de redes de computadores, gerentes e provedores de serviços ("operadores de rede") adotem medidas de segurança de dados, como prevenção de vírus de computador e registro de incidentes de segurança." (LAW, 2020, p. 157).

[35] Dividida em sete capítulos: 1- Provisões Gerais; 2 – Promoção e Apoio da Segurança Cibernética; 3 – Segurança da Operação de Rede; Seção 1- provisões ordinárias, Seção 2- segurança da operação de infraestrutura de informação crucial; 4- Segurança das Informações de Rede; 5 – Monitoramento, Aviso Prévio e Resposta Emergencial; 6 – Responsabilidade Legal; e 7- Provisões Suplementares. Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Acesso em: 11 abr 2022.

O Estado se indica como responsável por muitos pontos como tomar medidas para monitorar, prevenir e lidar com riscos extraterritoriais ou intraterritoriais, além de se colocar como protetor contra-ataques, interferências, invasões da infraestrutura chave. Prevê que desenvolvimento de trocas e cooperação internacional, principalmente por conta do fluxo internacional de dados.

A Lei de Segurança Cibernética sujeita todos que operam com a rede, independente de qual atividade, portanto, esses sujeitos devem respeitar a moralidade pública, ética comercial e proteger a segurança cibernética, respeitando as leis e regulamentos administrativos. Ademais, também coloca que a Internet deve ser usada de acordo com a Constituição e outras leis, obedecendo a ordem pública e moralidade pública, não devendo ser usada para incitar a subversão da soberania, a derrubada do sistema socialista, o separatismo, a quebra de união nacional, nem perturbar a ordem econômica ou social, nem criar propagandas falsas que violem a reputação, privacidade, propriedade intelectual ou outros interesses legítimos de terceiros (LAW, 2020, p. 159).

No que se refere às penalidades, Law cita que:

> […] as empresas podem estar sujeitas a aviso, multas, confisco de renda ilegal, cancelamento de licenças ou cancelamento de arquivamento da empresa, fechamento de sites, proibição da pessoa responsável pela empresa ou sócio em contratações em serviço público e outras punições. Além disso, tais atos são inseridos em arquivos de crédito social e publicados; quando os atos constituem violações da gestão da ordem pública são impostas de acordo com a lei. Quando constituem um crime, a responsabilidade penal é processada de acordo com a lei. Quando os direitos civis de outras pessoas são violados, a responsabilidade civil é suportada de acordo com a lei. (LAW, 2020, p. 159).

Essas e outras previsões mostram o forte caráter coercitivo da Lei de Cibersegurança. Um aspecto interessante, é que as disposições sobre a Proteção Cibernética de Informações Pessoais de Criança, tem um padrão de consentimento mais alto que a Lei de Cibersegurança, e o foco dessa legislação está na proteção de privacidade online de menores de 14 anos, inclusive os operadores de rede só podem acessar determinada informação da criança com o consentimento de um tutor. Em síntese, praticamente todos os atos relacionados à criança devem ser autorizados pelos responsáveis dela, ou um administrador autorizado, o que se mostra bastante interessante se o intuito é proteger a criança da exposição, que é tão comum atualmente.

Com relação às violações que podem ser cometidas sobre os dados pessoais, Law afirma:

> Com efeito, com base na Lei de Segurança Cibernética chinesa, as possíveis violações que empresas e corporações do mundo digital podem configurar são: uso errado ou sem consentimento prévio e adequado, venda, divulgação ou compartilhamento; informações básicas pessoais, informações de identificação pessoal, informações pessoais de fisiologia da saúde e educação pessoal ou informações de trabalho. A materialização da violação pode se dar da seguinte forma: (1) os controladores violam as disposições das leis e regulamentos na coleta ou utilização de ações pessoais; (2) controladores violam acordos com sujeitos dos dados na coleta ou utilização de informações pessoais; (3) sem o consentimento explícito necessário para coleta, processamento, uso ou transferência; (4) quando há exposição forçada de anúncios comerciais, compartilhamento e divulgação ou fornecimento de informações pessoais sem se retirar o consentimento. (LAW, 2019, p. 163).

São muitas as previsões na Lei de Cibersegurança, mas certamente é preciso entender as violações pois elas estão ligadas diretamente à violação da privacidade. Outra ressalva interessante é que a lei aponta em seu art. 52 que os departamentos responsáveis pela proteção de segurança da infraestrutura da informação devem sempre se atentar a melhorar o sistema de informação, monitoramento e aviso-prévio, tudo para que se evite qualquer corrupção aos direitos que essa lei visa garantir.

3.1 LEI DE CIBERSEGURANÇA DA REPÚBLICA POPULAR DA CHINA: SÍNTESE

A Lei de Cibersegurança da República Popular da China foi aprovada em 6 de novembro de 2016 e entrou em vigor em 1° de junho de 2017. Essa lei tem 79 artigos, organizados em sete capítulos, sendo: Capítulo I: Disposições Gerais; Capítulo II: Suporte e promoção da segurança cibernética; Capítulo III: Segurança de Operações de Rede (Seção 1: Disposições Gerais; Seção 2: Segurança de operações para infraestrutura crítica de informações); Capítulo IV: Segurança da Informação da Rede; Capítulo V: Monitoramento, Alerta Precoce e Resposta a Emergências; Capítulo VI: Responsabilidade Legal; e Capítulo VII: Disposições Suplementares.

No primeiro artigo, do primeiro capítulo, se tem os objetivos da Lei de Cibersegurança[36], e no art. 2, a aplicabilidade da lei para construção, operação, manutenção e uso de redes, e também para a supervisão da segurança cibernética no território continental da República Popular da China. No terceiro artigo, há garantias que o Estado se compromete a promover e enfatizar, bem como os princípios para segurança cibernética e o desenvolvimento

[36] garantir a segurança cibernética; salvaguardar a soberania do ciberespaço e a segurança nacional, e os interesses sociais e públicos; proteger os direitos e interesses legítimos dos cidadãos, pessoas jurídicas e outras organizações; e promover o desenvolvimento saudável da informatização da economia e da sociedade. Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Acesso em: 11 maio 2022.

da informação. Os próximos artigos das disposições gerais também seguem a tendência do artigo terceiro em declarar as obrigações, garantias, incentivos, proteção e estruturas que o Estado da República Popular da China se compromete a cumprir. É interessante destacar, que no art. 5 se apresenta a competência territorial da lei, ao declarar que o Estado toma medidas de monitoramento, prevenção e para lidar com os riscos e ameaças cibernéticas que surgirem dentro e fora do território continental. No art. 7 está estabelecida a regulamentação do intercâmbio e cooperação internacional do ciberespaço.

A respeito do comprometimento dos operadores da rede com a moralidade social, ética comercial, honestidade e confiabilidade, respeito às obrigações para proteger a segurança cibernética, aceitar a supervisão do governo e do público e assumir a responsabilidade social, em suas atividades comerciais e de serviços estão previstas no art. 9.Sendo que no art. 10, se ressalta o dever de preservar a integridade, sigilo e usabilidade dos dados online, e no art. 14 está estabelecido o direito de denúncia por qualquer organização ou indivíduo de condutas que gerem insegurança no ciberespaço, bem como o dever de os departamentos que receberem a denúncia (relatório) preservarem a confidencialidade das informações dos informantes e proteger os direitos e interesses legítimos dos informantes. Outro ponto de destaque está no art. 13 em que se define, brevemente, a obrigação do Estado de garantir um ciberespaço seguro e saudável para os menores de idade.

O segundo capítulo é composto por cinco artigos que definem o suporte e promoção da cibersegurança. Ainda centrado no Estado, são definidos os apoios e comprometimentos que se comprometem a assumir principalmente para promover e garantir a segurança cibernética, inclusive incentivando empresas e instituições de educação ou treinamento, como escolas de ensino superior e escolas profissionais, para realizarem pesquisas, testes, certificações e treinamentos, e também para garantir o fim anteriormente citado. No art. 19, se tem o estabelecimento do princípio de publicidade e educação sobre a segurança cibernética que deve ser seguido pelo governo popular e seus departamentos relevantes.

O terceiro capítulo sobre a segurança de operações de rede, está subdivido em duas seções, e comporta 18 artigos. Mesmo em outras partes da lei a questão da segurança é fortemente declarada e reforçada em muitos artigos, mas nesse capítulo se terá a forma e os métodos que deverão garantir essa segurança. Sobre isso está previsto em seu art. 21, na primeira seção:

> Article 21: The State implements a cybersecurity multi-level protection system [MLPS]. Network operators shall perform the following security protection duties according to the requirements of the cybersecurity multi-level protection system to

> ensure the network is free from interference, damage, or unauthorized access, and to prevent network data leaks, theft, or falsification:
> (1) Formulate internal security management systems and operating rules, determine persons who are responsible for cybersecurity, and implement cybersecurity protection responsibility;
> (2) Adopt technical measures to prevent computer viruses, cyber attacks, network intrusions, and other actions endangering cybersecurity;
> (3) Adopt technical measures for monitoring and recording network operational statuses and cybersecurity incidents, and follow provisions to store network logs for at least six months;
> (4) Adopt measures such as data classification, backup of important data, and encryption;
> (5) Other obligations provided by law or administrative regulations..[37]

Nos demais artigos tem-se a preocupação de estabelecer a obrigatoriedade de que os fornecedores de produtos e serviços de rede, os equipamentos de rede críticos e produtos especializados em segurança sigam os padrões nacionais e quesitos obrigatórios. Ainda nessa seção, outro artigo relevante é o art. 24, em que se apresenta:

> Article 24: Network operators handling network access and domain name registration services for users, handling stationary or mobile phone network access, or providing users with information publication or instant messaging services, shall require users to provide real identity information when signing agreements with users or confirming the provision of services. **Where users do not provide real identity information, network operators must not provide them with relevant services.**
> The State implements a network identity credibility strategy and supports research and development of secure and convenient electronic identity authentication technologies, promoting reciprocal acceptance among different electronic identity authentication methods.[38] (grifo nosso)

Fica claro que nesse artigo, se visa coibir a anonimização e possíveis infrações que seriam cometidas com o auxílio desse método, já que com a exigência da identidade real se tem a possibilidade de responsabilização civil e penalmente.

Na seção I se tem também artigos que visam definir as obrigações de ações que devem ser tomadas em casos de intrusão ilegal, invasões de rede, respostas de emergência para incidentes de segurança cibernética e outros riscos de segurança cibernética. No art. 28, também ressalta o dever dos operadores de rede fornecer apoio técnico e assistência aos órgãos de segurança pública e órgãos de segurança nacional, esses que garantem a segurança nacional e investigam atividades criminosas de acordo com a lei. Há também o estabelecimento da utilização das informações obtidas pelos departamentos de segurança cibernética e informatização apenas conforme o necessário para a proteção da segurança cibernética.

[37] Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Acesso em: 11 maio 2022.
[38] Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Acesso em: 11 maio 2022.

A seção II, do terceiro capítulo, diz respeito a segurança de operações para infraestrutura crítica de informações, sendo no art. 31, assegurado que o Estado implementa proteção chave com base no sistema de proteção multinível de segurança cibernética [MLPS], referido no art. 21, para serviços de comunicação e informação, energia, tráfego, recursos hídricos, finanças serviço público, governo eletrônico e outras infraestruturas de informações críticas. Também relacionado ao que se prevê no art. 21, o art. 34 traz as seguintes previsões:

> Article 34: In addition to the provisions of Article 21 of this Law, critical information infrastructure operators shall also perform the following security protection duties:
> (1) Set up specialized security management bodies and persons responsible for security management, and conduct security background checks on those responsible persons and personnel in critical positions;
> (2) Periodically conduct cybersecurity education, technical training, and skills evaluations for employees;
> (3) Conduct disaster recovery backups of important systems and databases;
> (4) Formulate emergency response plans for cybersecurity incidents, and periodically organize drills;
> (5) Other duties provided by law or administrative regulations.[39]

Isto é, para além do que se prevê no art. 21, os operadores de infra-estrutura de informação crítica também devem observar as disposições do art. 34. Os demais artigos também trazem outras disposições sobre os operadores de infraestrutura de informação crítica. É importante destacar que a lei, em seu art. 31, conceitua como infraestruturas de informação críticas aquelas que se destruída, sofrendo uma perda de função ou experimentando vazamento de dados, pode colocar seriamente em risco a segurança nacional, o bem-estar nacional, a subsistência do povo ou o interesse público.

O capítulo IV legisla sobre a segurança da informação da rede e contém dez artigos. Logo no art. 40, estabelece a obrigação dos operadores de rede de manter a confidencialidade das informações dos usuários que tiverem coletado e estabelecer e completar sistemas de proteção das informações dos usuários, além disso, no art. 41 há os princípios que os operadores de rede devem observar ao coletar e usar as informações pessoais, os quais são: legalidade, propriedade e necessidade. Também se estabelece o dever de publicizar as regras de coleta e uso, bem como obter o consentimento das pessoas que tiverem seus dados coletados. Os outros artigos contêm outras previsões sobre: o que os operadores de rede não devem fazer; caso haja descoberta por parte dos indivíduos de que os operadores violaram as disposições das leis; a proibição de roubar ou usar os dados de forma ilegal; dever de confidencialidade por parte dos

[39] Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Acesso em: 11 maio 2022.

departamentos com função de supervisão e gerenciamento de segurança cibernética; e outras disposições.

O quinto capítulo trata sobre monitoramento, alerta precoce e resposta a emergências, sendo dever do Estado estabelecer um sistema para esse fim, além de contar com o auxílio dos departamentos estaduais de cibersegurança e informatização para fortalecer os esforços de coleta, análise e relatórios para informação de cibersegurança. O art. 53 estabelece a coordenação dos departamentos estaduais e departamentos relevantes para estabelecer e implementar mecanismos de avaliação e risco e esforços para respostas de emergências. Nesse capítulo se estabelece que o plano de resposta a emergências incidentes deve classificar os incidentes com base em fatores como grau de dano após a ocorrência do incidente e o escopo do impacto. Também se prevê que quando ocorre um incidente de cibersegurança, o plano de resposta à emergência do incidente deve ser iniciado imediatamente, segundo o art. 55. Caso o risco incidente de cibersegurança aumente, as medidas que devem ser implementadas são descritas no art. 54. Ademais, há no art 57 a previsão de que se uma emergência repentina ou acidentes de segurança de produção ocorrem como resultado de incidentes de segurança cibernética, eles devem ser tratados conforme o disposto nas "Lei de Resposta de Emergência da República Popular da China", a "Lei de Segurança de Produção da República Popular da China China" e outras leis e regulamentos administrativos relevantes. Por fim, para a garantia da segurança nacional e da ordem pública social, a legislação também prevê a tomada de medidas provisórias pelo Estado em relação à rede de comunicação em uma região especialmente designada, a exemplo da limitação dessas comunicações.

O capítulo seguinte, sobre a responsabilidade legal, legisla sobre a responsabilidade e sanção que decorre da inobservância do que foi previsto em artigos anteriores da lei. As sanções vão desde multas, até proibição vitalícia em se envolverem com gerenciamento de segurança cibernética dos sujeitos que receberam punição criminal. Cada um dos artigos desse capítulo, com poucas exceções, dita a sanção que advém da violação do disposto em outro determinado artigo, o que em síntese pode ser descrito: art. 59 (caput) prevê a sanção para inobservância das previsões nos artigos 21 e 25 e em seu parágrafo único, as sanções relacionadas à violação do disposto dos artigos 33, 34, 36 e 38; art. 60, violação dos art. 22, parágrafo primeiro e segundo, e art. 48, parágrafo primeiro; art. 61, violação do art. 24, parágrafo único; art. 62, violação ao art.c26; art. 63, violação do art. 27; art. 64, violação do art. 22, parágrafo 3, ou art. 41-43 ou art. 44; art. 65, violação do art. 35; art. 66, violação do art. 37; art. 67, violação do art. 46; art. 68, violação do art. 47 ou 48 (segundo parágrafo); e outras disposições. É importante destacar

que a responsabilidade legal decorrente da inobservância do previsto na Lei de Cibersegurança podem levar a sanções dispostas em outras leis e regulamentos administrativos pertinentes, outro ponto relevante é que se legisla também sobre os danos a terceiros por violação aos dispostos na lei, o que será arcado de acordo com a lei. No último artigo do capítulo, se determina a responsabilidade legal de instituições, organizações ou indivíduos estrangeiros que se envolverem com invasões, ataques, interferências, danos ou outras atividades de risco para a infraestrutura da informação da República Popular Chinesa.

Enfim, no último capítulo (Capítulo VII), das disposições suplementares, se tem no art. 76[40] os conceitos mais relevantes para a Lei de Cibersegurança, os quais são: rede; cibersegurança; operadores de rede; dados de rede; e informações pessoais. Interessante destacar que a proteção da segurança operacional das redes que armazenam ou processam informações sobre segredos nacionais obedece a Lei de Cibersegurança e outras disposições legais e regulamentares relativos à proteção do sigilo, mas as regras de proteção da segurança para redes militares são formuladas pela Comissão Militar Central, segundo os artigos 77 e 78, respectivamente. O último artigo dessa lei, art. 79, versa sobre a data de entrada em vigor da lei.

3.2 LEI DE CIBERSEGURANÇA DA REPÚBLICA POPULAR DA CHINA: ANALISANDO O CONSENTIMENTO, RESPONSABILIDADE E SEGURANÇA DA INFORMAÇÃO

Pensar sobre a até que ponto a manipulação de dados fere ou não a privacidade é bastante complexa, visto a complexidade de definir o que é privacidade, mas se pensado baseado na

[40] "(1) "Network" [网络, also "cyber"] refers to a system comprised of computers or other information terminals and related equipment that follows certain rules and procedures for information gathering, storage, transmission, exchange, and processing.

(2) "Cybersecurity" [网络安全, also "network security"] refers to taking the necessary measures to prevent cyber attacks, intrusions, interference, destruction, and unlawful use, as well as unexpected accidents, to place networks in a state of stable and reliable operation, as well as ensuring the capacity for network data to be complete, confidential, and usable.

(3) "Network operators" [网络运营者] refers to network owners, managers, and network service providers.

(4) "Network data" [网络数据] refers to all kinds of electronic data collected, stored, transmitted, processed, and produced through networks.

(5) "Personal information" [个人信息] refers to all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including but not limited to natural persons' full names, birth dates, national identification numbers, personal biometric information, addresses, telephone numbers, and so forth." Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Acesso em: 11 maio 2022.

legislação específica de proteção de dados, no caso a Lei de Cibersegurança, certamente é preciso analisar o consentimento, a responsabilidade e a segurança da informação.

A respeito do consentimento, a lei chinesa não expõe claramente como ele deve se dar, o que abre muitas brechas, mas deixa claro no artigo 22 e artigo 41, que é necessário **obter** o consentimento para poder coletar, usar e repassar os dados pessoais. Quanto a responsabilidade há um capítulo específico na legislação[41], que vai do artigo 59 ao artigo 75. Entre esses, gostaria de destacar o artigo 64, que prevê responsabilidade e sanção para os operadores de rede que violarem o artigo 41-43 e artigo 44, do capítulo de segurança da informação, bem como o artigo 22.

> **Article 64:** Network operators, and network product or service providers violating Article 22 Paragraph 3 or Articles 41-43 of this Law by infringing on personal information that is protected in accordance with law, shall be ordered to make corrections by the relevant competent department and may, either independently or concurrently, be given warnings, be subject to confiscation of unlawful gains, and/or be fined between 1 to 10 times the amount of unlawful gains; where there are no unlawful gains, the fine shall be up to RMB 1,000,000, and a fine of between RMB 10,000 and 100,000 shall be given to persons who are directly in charge and other directly responsible personnel; where the circumstances are serious, the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses.
> Where Article 44 of this Law is violated in stealing or using other illegal means to obtain, illegally sell, or illegally provide others with personal information, and this does not constitute a crime, public security organizations shall confiscate unlawful gains and levy a fine of between 1 and 10 times the amount of unlawful gains, and where there are no unlawful gains, levy a fine of up to RMB 1,000,000.[42]

No que se refere aos artigos que se descumpridos levam a referida responsabilização e punição, em resumo, dos artigos 41-43, trata-se do dever do operador da rede que coleta e usa os dados pessoais obedecerem aos princípios da legalidade, propriedade e necessidade, expondo para os usuários as regras de coleta e uso, e os objetivos, não podendo divulgar adulterar ou destruir as informações pessoais que coletarem, sempre observando a obtenção de consentimento, o qual caso não sendo concedido impede que os dados sejam repassados a terceiros, além disso, os usuários podem requerer que os operadores de dados excluam seus dados em caso de violação ou até, que eles os corrijam, em caso de erro; sobre o artigo 44 prevê que organizações e indivíduos não devem roubar ou usar métodos ilegais para obter determinadas informações pessoais, nem mesmo devem vendê-las ou fornecê-las ilegalmente a outros; quanto ao artigo 22, parágrafo 3º, se refere ao dever do provedor indicar claramente

41 Capítulo VI: Responsabilidade Legal

42 Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Acesso em: 11 abr. 2022.

quando um produto ou serviço de rede coleta de informações dos usuários, além de obter o consentimento do usuário para esse fim, e cumprir as leis e regulamentos sobre a proteção de informações pessoais.

Nessa referida lei, são numerosos os artigos sobre a responsabilidade legal, sendo que a maioria deles, indica determinado artigo ao qual a ofensa ou descumprimento se realizou e determina um intervalo de valores em que a multa pode se dar. Pode-se notar uma diferença nessa estrutura a partir do artigo 70, a começar pelo próprio artigo 70 que determina que caso seja publicada ou transmitida alguma das opções apresentadas no rol do artigo 12, parágrafo 2°, a punição se dará segundo as leis e regulamentos administrativos pertinentes. Acerca desses artigos que se diferenciam estruturalmente dos demais, ressalto, também, o artigo 71, que aponta que a conduta que infrinja a Lei de Cibersegurança será averbada em cadastro de crédito e divulgada de acordo com leis e regulamentos pertinentes; e o artigo 74, que aponta a responsabilidade civil para aqueles que cometerem violação a alguma das disposições da lei e cause danos a terceiros.

Outro ponto relevante para a privacidade é o que foi disposto no capítulo IV da Lei de Cibersegurança, onde se aponta a segurança da informação da rede, envolvendo 10 (dez) artigos, do artigo 40 ao artigo 50. Se analisarmos o artigo 40, o primeiro do capítulo, ele prevê que os operadores da rede devem manter a confidencialidade das informações dos usuários que foram coletadas e completar sistemas de proteção das informações dos usuários.[43] Esses artigos focam, principalmente, no dever do operador da rede: de manter a confidencialidade das informações pessoais e segredos comerciais que terão acesso através dos dados pessoais, não os vendendo ou fornecendo ilegalmente para outro, não deixando, por descuido ou intencionalmente, que eles vazem; de descobrir as informações que as leis ou regulamentos proíbem a publicação ou transmissão, e interromper imediatamente a transmissão, inclusive procedendo a eliminação dessas informações para evitar que elas se espalhem _ essa previsão contida no artigo 48, assim como em outros artigos, a exemplo do artigo 50, que determina a cooperação entre os departamentos de cibersegurança e informação do Estado e departamento relevantes, para controle de publicação ou transmissão de assuntos proibidos por lei, apontam o firme controle de censura que o governo chinês mantém sobre determinados assuntos.

Em análise a esses três pontos _ consentimento, responsabilidade de segurança_ considerando como a lei entende a invasão à privacidade, se percebe que a luz da Lei de

[43] Article 40: Network operators shall strictly maintain the confidentiality of user information they collect, and establish and complete user information protection systems.

Cibersegurança, há uma preocupação menos rigorosa com o consentimento, pois não se aponta como essa lei exige ou espera que seja obtido esse consentimento, e essa noção está intrinsecamente relacionada à privacidade. No que se refere a responsabilidade, entendo que a lei tenta garantir o máximo de previsões e possibilidades, sempre as relacionando a algum desrespeito, intencional ou não, de outros artigos do texto, acompanhado de sanções, o que garante um forte caráter coercitivo, caso chegue a ser exposto o erro de responsabilidade. Por fim, quanto à segurança, é notória a preocupação em estabelecer princípios que estão relacionados à privacidade, como é o caso da confidencialidade, legalidade e necessidade.

Considerando a cultura chinesa e sua dificuldade de determinar e garantir a privacidade, entendo que a Lei de Cibersegurança é uma avanço significativo no rumo de uma grande potência cibernética, como o presidente Xi Jinping deseja, mas também mostra as disposições ditatoriais chinesas ao colocar em seu artigo 1° que a lei objetiva garantir a segurança cibernética, salvaguardar a soberania do ciberespaço e a segurança nacional, e os interesse sociais e públicos; proteger os direitos e interesses legítimos dos cidadãos e pessoas jurídicas e outras organizações; e promover o desenvolvimento saudável da informatização da economia e da sociedade[44], sem nada ressaltar, explicitamente, em seu primeiro artigo sobre a proteção da privacidade e a proteção de dados pessoais. Também é necessário repensar o excessivo controle (censura) que se mantém sobre o fluxo de determinados tipos de informação.

CONCLUSÃO

O contexto atual apresenta uma dupla realidade _ física e virtual_ entre as quais há uma enorme diferença de “idades”, o que pode ser entendido como a realidade tangível, já estando em desenvolvimento, e a realidade cibernética, que teve sua gênese mais recente, e por isso muitos conceitos e previsões devem ser repensados e adaptados ao novo formato (digital). Nesse sentido, considerando a Revolução Industrial 4.0, que trouxe consigo ainda mais avanços tecnológicos, como a IoT e a inteligência artificial, aumentando exponencialmente o fluxo de dados pessoais na esfera digital, se tornou urgente repensar a concepção de privacidade diante da manipulação dos dados, em especial, por um estudo comparado entre Brasil e China, com

[44] Article 1: This Law is formulated in order to: ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons, and other organizations; and promote the healthy development of the informatization of the economy and society.

suas respectivas legislações, Lei Geral de Proteção de Dados e Lei de Cibersegurança da República Popular da China.

Para o contexto cibernético, o direito à privacidade está relacionado ao titular dos dados conhecer, controlar, endereçar, interromper o fluxo das informações que estiverem relacionadas a si. É preciso entender que a tutela à privacidade na manipulação de dados deve ser garantida principalmente porque os dados pessoais são a representação da própria pessoa na realidade virtual, e por isso, a manipulação de dados consciente e sigilosa se configura como um direito à personalidade, estando relacionado à garantia da dignidade humana. Além de que a manipulação incorreta e descuidada de dados pode expor seu titular e ferir sua autonomia, lhe tornando vulnerável para a tirania da maioria. Outro aspecto relevante é a importância da legislação sobre proteção de dados, em estabelecer um equilíbrio e intermediar o direito à privacidade, à transparência e à liberdade, para que a efetiva garantia desses direitos não se viole. Há também a importância de que o texto legal aponte expressamente sobre o consentimento, responsabilidade e segurança do sistema de informações, tudo para que se evite ambiguidades que sejam prejudiciais à proteção dos dados dos usuários e ao direito à privacidade, dando abertura para que os controladores e operadores da rede utilizem de forma maliciosa os dados aos quais tenham acesso. Ademais, é importante garantir o efetivo direito ao esquecimento, referindo a legislação (Lei de Proteção de Dados Pessoais e Lei de Cibersegurança) principalmente no que se refere a eliminação de dados, pois estão diretamente relacionados à noção de controle e interrupção do fluxo de dados que também se inclui no que optamos por entender como privacidade neste trabalho.

Uma análise comparativa entre as realidades brasileira e chinesa é uma tentativa de identificar pontos semelhantes em culturas e situações sociais e econômicas muito diversas, mas há um ponto em comum entre esses dois países o qual é: o aumento da difusão da internet e outras tecnologias, bem como o crescimento do fluxo de dados pessoais de todos os tipos e seu armazenamento. Sobre a noção de privacidade, vemos que a China partiu de um conceito unitário histórico de assuntos privados, o Yin Si, que evoluiu para privacidade, estando prevista e garantida na Lei de Cibersegurança e outras leis esparsas, além disso, também se verifica um apego mais recente à codificação de leis, diferente do costume de *civil law* brasileiro. Em relação à privacidade para o Brasil, percebe-se o cuidado de prevê-la em muitos textos normativos do ordenamento jurídico brasileiro, entre eles a Lei Geral de Proteção de Dados, ainda em *vacatio legis*. Esse costume brasileiro não significa que a privacidade é efetivamente

garantida no território brasileiro, mas significa um certo avanço se comparado ao ordenamento chinês, que tem o conceito de privacidade ainda muito confuso em seus textos.

Comparando as previsões da Lei de Proteção de Dados Pessoais e da Lei de Cibersegurança, encontramos a semelhança sobre a questão do consentimento do usuário para que seus dados sejam coletados, usados e manipulados. Em relação às diferenças, percebemos que a Lei de Cibersegurança tem um caráter coercitivo forte, com regras e punições severas, além de envolver o Estado, empresários e cidadãos em sua proteção. Quanto à Lei de Proteção de Dados Pessoais, possui um caráter mais orientador e conceituador (conceitos fixos logo no início do texto normativo), o que acontece em pequena quantidade apenas no fim da lei chinesa, e sobre as punições prevê: advertência, aplicação de multas, suspensão e até a proibição de atividades relacionadas ao tratamento de dados. Essas punições variam a cada caso, sendo que as multas diárias ou simples estão baseadas no valor relativo a 2% do faturamento da organização privada, com um teto estabelecido de R$ 50 milhões por infração, o que se comparado ao Regulamento Geral de Proteção de Dados (GRPD) em que a lei brasileira se baseou, é um valor menor. Sobre esse teto, estabelecido pela Lei de Proteção de Dados Pessoais, não nos parece muito indicado, visto que a realidade sempre pode ultrapassar o que foi previsto na legislação, e com sua previsão se estabeleceu um limite legal para o valor da multa, independente do fato ocorrido na situação real.

Ainda se comparando os textos normativos da Lei de Proteção de Dados Pessoais e da Lei de Cibersegurança Chinesa percebe-se que a legislação chinesa não traz o conceito de dados pessoais, mas se refere, protege e regula as "informações pessoais", conceito o qual se comparado ao conceito de "dados pessoais" previsto na legislação brasileira mostram o mesmo sentido. É interessante também, que o conceito de dados sensíveis também não aparece na lei chinesa, mas se inclui no conceito de "informações pessoais". Essas diferenças conceituais mostram expressamente as diferenças culturais entre Brasil e China, mas nem por isso afastam da tutela jurídica a manipulação de dados pessoais, já que mesmo que os termos sejam diferentes, os conceitos em sua essência são similares. Outra forte diferença está na expressão do direito à privacidade nessas leis, já que a lei brasileira opta por expressar em mais de um artigo sua proteção ao direito à privacidade, enquanto que a lei brasileira cita o termo apenas uma vez, mas nem por isso deixa de garantir esse direito, ao prever o dever de sigilo e confidencialidade dos operadores de rede em suas atividades.

As leis, chinesa e brasileira, têm assuntos similares, mas o foco é diferente, e podemos perceber isso pelo "tom" que essas leis apresentam, bem como pela cultura de ambos os países.

A lei chinesa foca mais na ordem, na determinação, estabelecendo o Estado como figura central na garantia da segurança do espaço cibernético, principalmente para manutenção da ordem pública social e segurança nacional. Já a lei brasileira tem seu cerne na manipulação e tratamento dos dados pessoais, visando garantir o direito à privacidade e outros princípios, como a não discriminação, segurança, finalidade, transparência e outros, isso porque o Brasil vem se desenvolvendo como país emergente e com o advento da internet e valorização, econômica e social, dos dados, tornou-se uma necessidade social e jurídica, além de um requisito internacional para manutenção das relações globalizadas.

Por fim, a privacidade no contexto cibernético precisa estar relacionada ao consentimento e confidencialidade, portanto os controladores e operadores da rede devem se ater a esses conceitos no que tange a manipulação de dados consciente e respeitosa com a garantia de privacidade. Conforme afirma Moraes e Queiroz, os dados pessoais podem até ser entendidos como bens jurídicos apropriáveis e circuláveis, mas isso não pode ser aplicado a privacidade, que é direito, portanto, a coleta e tratamento de dados pessoais, principalmente em relação aos dados sensíveis, identificado como núcleo duro da dignidade humana, deve ser precedida de medidas rigorosas e eficazes de proteção (MORAES; QUEIROZ, 2019, p.123). Tal proteção pode ser alcançada se implementar a privacidade desde a concepção, que possui muitas ferramentas que podem alcançar a devida proteção à privacidade que se requer aos dados pessoais, no entanto, para que essa solução se dê é necessário o desenvolvimento de tecnologias e métodos de gestão integrados. Outrossim, espera-se que os Estados objeto desse estudo se atentem a aplicação dos dispostos em suas leis específicas (Lei Geral de Proteção de Dados e Lei de Cibersegurança da República Popular da China) e vigilância quanto ao devido cumprimento da legislação, se atentando às constantes mudanças que acontecem na realidade, para que a legislação não fique obsoleta e inutilizável.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 abr. 2022.

_____. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr 2022.

CAMARA, Maria Amália Oliveira de Arruda; RODRIGUES, Walter de Macedo. A gestão de dados pessoais por grandes empresas: considerações geopolíticas e jurídicas. *In*: **Proteção de dados pessoais**: privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, 2019. (Cadernos Adenauer xx (2019), nº3). p. 71-92.

CARVALHO, Antonio Ramalho de Souza. Os dados no contexto da quarta revolução industrial. *In*: **Proteção de dados pessoais**: privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, 2019. (Cadernos Adenauer xx (2019), nº3). p. 93-111.

CARVALHO, Victor Miguel Barros de; GUIMARÃES, Patrícia Borba Vilar; OLIVEIRA, Adriana Carla Silva de. Monetização de Dados Pessoais na Internet: Competência Regulatória a partir do Decreto Nº 8.771/2016. **Revista de Estudos Institucionais**, v. 4, n. 1, 2018, p. 376-416. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/215. Acesso em: 10 abr. 2022.

SAFE COELHO, Diva Júlia Sousa da Cunha. A FORMAÇÃO DA CULTURA CONSTITUCIONAL CHINESA. *In*: COELHO, Diva Júlia Sousa da Cunha Safe. **A IDEIA DE DIGNIDADE ENTRE O OCIDENTE E AS CULTURAS DE MODERNIDADE RECENTE:** Uma Macro-comparação da Compreensão do Direito à Dignidade nos Países do BRICS. 2017. Tese (Doutorado em Cidadania e Direitos Humanos) – Universitat de Barcelona Barcelona, UB, 2017. p. 325-363. Disponível em: http://diposit.ub.edu/dspace/bitstream/2445/111152/1/DJSdCSC_TESE.pdf. Acesso em: 04 jun. 2022.

COELHO, Diva Júlia Sousa da Cunha Safe. DIREITOS FUNDAMENTAIS E DIGNIDADE HUMANA NO CONSTITUCIONALISMO CHINÊS. *In*: COELHO, Diva Júlia Sousa da Cunha Safe; COELHO, Saulo de Oliveira Pinto; DINIZ, Ricardo Martins Spindola (Colaboradores). **Direitos fundamentais e dignidade humana nos países BRICs**: comparação reflexiva dos constitucionalismos russo, indiano, chinês e brasileiro. Uberlândia: LAECC, 2020. p. 147-188.

CHINA. **Constituição de 4 de dezembro de 1982 da República Popular da China**. Disponível em: http://www.dhnet.org.br/direitos/anthist/marcos/hdh_constituicao_chinesa_1982.pdf. Acesso em: 10 abr. 2022.

GARCIA, Bruna Pinotti. Colisões de princípios na Internet e a Ética como base de solução. *In*: GARCIA, Bruna Pinotti. **Ética na *Internet***: um estudo da autodisciplina moral no ciberespaço e de seus reflexos jurídicos. 2013. Dissertação (Mestrado em Direito) – Fundação de Ensino "Eurípedes Soares da Rocha", Centro Universitário Eurípides de Marília, Marília, 2013. p. 98-121.

LAW, Thomas. **A Lei Geral de Proteção de Dados**: uma análise comparada ao novo modelo chinês. 2020. Tese (Doutorado em Direito Comercial) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2020.

LEGRAND, Pierre. **Como Ler o Direito Estrangeiro**. Editora Contracorrente; 1ª edição, 2018

LIMA, Caio César Carvalho; MONTEIRO, Renato Leite. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. **AtoZ: novas práticas em informação e conhecimento**, v. 2, n. 1, 2013, p. 60-76. Disponível em: https://revistas.ufpr.br/atoz/article/view/41320 . Acesso em: 11 abr. 2022.

MAGRANI, Eduardo. **Entre dados e robôs:** ética e privacidade na era da hiperconectividade. Arquipélago editorial, 2019.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LEI DE PROTEÇÃO DE DADOS PESSOAIS . *In*: **Proteção de dados pessoais**: privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, 2019. (Cadernos Adenauer xx (2019), nº3). p. 113-135.

ZHOU, Yuexin. Proteção cibernética de informações pessoais em um sistema multidimensional. Tradução da equipe da revista. **Revista Internet & Sociedade**, v. 1, n. 2, 2020, p. 297-309. Disponível em: https://revista.internetlab.org.br/protecao-cibernetica-de-informacoes-pessoais-em-um-sistema-multidimensional/. Acesso em: 12 abr. 2022.

ZUFFA, Fernanda Shimomura. A Obrigatoriedade de Eliminação de Dados Pessoais Após o Término de seu Tratamento e Aplicação do Direito ao Esquecimento. In: TEIXEIRA, Tarcísio e MAGRO, Américo Ribeiro (Coords.). **Proteção de dados. Fundamentos jurídicos.** São Paulo: Editora Podivm, 2020, p. 87- 113.