https://doi.org/10.23925/2675-8253.2022v3n1A7

SOBERANIA E CIBER-SOBERANIA: A CHINA NA REDEFINIÇÃO DO CIBERESPAÇO

Bernardo João do Rego Monteiro Moreira [74]

RESUMO: O debate contemporâneo da tecnologia tem como um de seus pontos centrais a questão do ciberespaço e da governança da internet, problematizados neste artigo. Para compreender as diversas implicações deste debate, são propostas algumas perguntas que irão orientar as discussões aqui tratadas: qual o papel da China na construção de novas relações com a tecnologia? Como se desenvolve seu processo de governança do ciberespaço? Quais os impactos internacionais da agenda de ciber-soberania chinesa? O que está em jogo na ciber-soberania e qual a centralidade desse conceito para as tendências internacionais de governança da internet?

PALAVRAS-CHAVE: Ciber-soberania. China. Governança da internet. Ciberespaço. Soberania.

SOVEREIGNTY AND CYBER-SOVEREIGNTY: CHINA IN THE REDEFINITION OF CYBERSPACE

ABSTRACT: The key questions of cyberspace and internet governance are central to the contemporary debate on technology, which are discussed in this article. To understand the various implications of this debate and orient the discussion, the further questions are proposed: what is China's role in the development of new relations with technology? How is the process of its cyberspace governance developing? What are the international impacts of the Chinese cyber-sovereign agenda? What is at stake in cyber-sovereignty and what is the centrality of this notion for the international trends of internet governance?

.

KEYWORDS: Cyber-sovereignty. China. Internet Governance. Cyberspace. Sovereignty.

[74] Graduando da Universidade Federal Fluminense, Rio de Janeiro - Brasil

CIBERESPAÇO E CIBER-SOBERANIA

Qual o papel da China na construção de novas relações com a tecnologia? Como se desenvolve seu processo de governança do ciberespaço? Quais os impactos internacionais da agenda de ciber-soberania chinesa? O que está em jogo na ciber-soberania e qual a centralidade desse conceito para as tendências internacionais de governança da internet? A busca por elucidar tais perguntas será iniciada pela discussão do conceito de ciber-soberania, central para a relação da China com o ciberespaço, com a governança da internet, com a tecnologia e com o posicionamento do país no cenário internacional. O presidente Xi Jinping defendeu o conceito de ciber-soberania como o direito de um país de desenvolvimento e regulação de *sua* internet, na *World Internet Conference* em 2015 (QI, SHAO, ZHENG, 2018; GOODNIGHT, HONG, 2019). O conceito é fundamental para a agenda política e legislativa chinesa na promoção de seu *prisma holístico de segurança* cibernética. Considerando a internet como uma das maiores vulnerabilidades do país, esse prisma estratégico constrói a soberania de dados como sua principal defesa, um escudo empunhado pela direção central do Partido (LIU, 2020; IASIELLO, 2017).

Goodnight e Hong (2019) caracterizam a ciber-soberania como uma extensão da soberania nacional no ciberespaço, que garante direitos de jurisdição, autodefesa, independência e igualdade entre os países. Definição que, apesar de estar longe de um consenso internacional nas especificidades de seus termos, é similar à definição proposta pelas Nações Unidas em sua sexta Assembleia Geral de junho de 2013, em um relatório (Documento A/68/98)[75]

[75] Documento completo em: https://digitallibrary.un.org/record/753055

que propõe a extensão da soberania nacional às atividades tecnológicas de informação e comunicação, autorizando sobre estas a elaboração de jurisdições territoriais nacionais (QI, SHAO, ZHENG, 2018; GOODNIGHT, HONG, 2019).

O próprio conceito de ciberespaço se insere em discussões sobre seu estatuto teórico e suas implicações práticas. A ideia de ciberespaço é conceptualizada como um lugar, espaço das comunicações em uma rede digital de computadores. Lugar, portanto, que não se limita a fronteiras geográficas e territoriais e funda um novo limiar entre o espaço virtual e o mundo da materialidade clássica, dominada essencialmente pelo concreto, pela fronteira física (ALLEN, LASTRA, 2020).

Em seu artigo *Reconessaince Wars of the Planetary Frontierland* (2002) Zygmunt Bauman coloca-se na esteira do pensamento sobre o evento, que de certa maneira, inaugura o século XXI. O atentado às torres do World Trade Center em Nova Iorque torna-se considerável como marco no âmbito da análise política e sociológica, quando propõe que o *mainstream* destes campos científicos é abalado pela violência dos novos fenômenos (BAUMAN, 2002).

Bauman compreende o grau de perturbação que as ondas de choque provocam no espaço de validade e aplicabilidade dos conceitos, e para tanto oferece sua análise propondo o fim da *Era do Espaço.* Esta era a sua origem na muralha da China, em pontes e torres medievais e culminou com a linha Maginot e a Linha Siegfried, encerrando-se com o muro de Berlim. Numa época em que o território era a referência para a segurança, a fronteira o limite para a identidade e o reconhecimento do estrangeiro, o espaço territorial significava poder (BAUMAN, 2002: 82).

O evento de 11/09 provou que esta lógica não mais oferecia elementos capazes de garantir a segurança daqueles que se sentiam pertencentes a um lugar. Não existe mais a possibilidade de a delimitação de uma fronteira territorial manter a ameaça distante, posto que não há lugar seguro que não possa ser atingido por um ataque armado. Nestes termos Bauman expõe que *casos extraterritoriais escapam às soluções territoriais* (BAUMAN, 2002).

Embora não-localizável, o ciberespaço é como um sistema implementado *no* espaço[76]. Em paralelo, o paradigma do Estado soberano westfaliano se sustenta em uma reivindicação de uma comunidade com poder independente e exclusivo de legislação sobre um território definido, constituindo assim uma autoridade soberana que se estrutura por instituições políticas estatais que incorporam a soberania. Deste modo, as jurisdições territoriais aparentam assentar-se sobre o mundo real dos átomos. Apesar disso, a jurisdição se constitui como uma delimitação social legalmente constituída do espaço físico como uma fronteira invisível, tendo marcos físicos só como referência. A cartografia foi essencial para a constituição do espaço soberano como um território absoluto e homogêneo de fronteiras contíguas que não se sobrepõem, como ilhas de autoridade (ALLEN, LASTRA, 2020; LAND, 2011).

A soberania parte de uma binaridade: o interno e o externo. Tais categorias relacionais são contingentes e efêmeras: são produzidas a partir de práticas sociopolíticas, onde sua forma é a linha que separa o dentro e o fora do estado e sua função é de segregar a sociedade doméstica do campo internacional; como uma forma simbólica, a soberania produz essa divisão ontológica. As práticas de construção da soberania seriam então padrões de

[76] As referências nesse artigo de *Fanged Noumena: Collected Writings 1987-2007* de Nick Land foram feitas com base na edição original, usando por fins de comparação o trabalho de tradução da obra feito pelo blog Númenos com Presas. Para acessar a tradução de Fanged Noumena feita pelo blog, ver: https://numenoscompresas.wordpress.com/

ação socialmente significativos que encarnam os discursos no mundo material. Ela se torna então um código; deve apresentar signos de seu reconhecimento internacional como Estado soberano e ter a habilidade de simular a fundação de sua autoridade soberana: o povo. Sendo assim, autoriza-se pensar o ciberespaço como um novo tipo de território passível de jurisdição e passível de ser tratado sob o paradigma da soberania westfaliana (autoridade interna, controle de fronteira, autonomia política e direito à não-intervenção de outros Estados), independente de seu status de 'lugar' não-espacial (LOH, HEISKANEN, 2020; ALLEN, LASTRA, 2020).

Ademais, identificam-se questões de extensão e legitimidade da ciber-soberania, pelo seu caráter de transcendência do território físico. A fronteira entre o ciberespaço e o 'mundo real' não é uma clara fronteira entre o físico e o virtual, mas é permeada por uma série de objetos invisíveis, estruturas jurídicas, infraestruturas tecnológicas fisicamente situadas e interações institucionais em espaços abstratos; entre abstrações e abstrações materialmente incorporadas em uma realidade social mediada por tecnologia (LOH, HEISKANEN, 2020; ALLEN, LASTRA, 2020).

Allen e Lastra propõe uma divisão *granular* de quatro camadas do ciberespaço: 1. física (infraestrutura); 2. lógica (legislação); 3. conteúdo (dados); 4. social (determinação entre o real e o fictício – como o que separa criptomoedas de uma moeda de um jogo online). Essa divisão indica outro problema que atravessa as camadas do ciberespaço e problematiza a regulação da tecnologia pelo Estado: com a surpreendente aceleração das atualizações tecnológicas, as regulações precisam acompanhar as inovações; se tudo o que é regulado é permitido, mas sujeito a condições; tudo que não é proibido, é permitido. O exemplo dos autores elucida a questão: não há por que dizer que o espaço aéreo era regulado antes da possibilidade tecnológica do voo no século XX. Tal inovação apresentou a necessidade desse tipo de

regulação. O que deve ser ponderado na governança do ciberespaço encontra-se então um desafio: determinar se uma nova tecnologia permite novas formas de ação (portanto exigindo novas regulações) ou se apenas permite novos jeitos de fazer as mesmas coisas. Resolvendo a problemática da fronteira entre o regulado e o não-regulado, é possível também controlar ações e impossibilitar transgressões no ciberespaço por limites nas próprias estruturas arquitetônicas deste, em adição às normas jurídicas. Diferente do 'mundo real', há como tornar uma ação automaticamente impossível no ciberespaço por meios de tais mecanismos (ALLEN, LASTRA, 2020).

Na ciência política, a soberania é associada ao território, à legitimidade interna e externa e à autoridade; no direito internacional, é associada à competência, imunidade e poder autônomo de decisão. De acordo com a teoria clássica do realismo em relações internacionais (MORGENTHAU, 1978; WALTZ, 1979), a natureza do sistema internacional é anárquica, composta por estruturas internacionais desiguais. Deste modo, em relação à governança da internet, o Estado se encontra em uma arena competitiva internacional no ciberespaço. Para marcar sua posição nessa arena, o Estado deve produzir seus espaços soberanos a partir de diferentes modalidades de práticas de soberania. A orientação geral é da produção contínua e manutenção da divisão ontológica do dentro/fora, do espaço doméstico e do espaço internacional. Para o espaço doméstico, a prática se dirige para construção da unidade da comunidade nacional, sua representação e reprodução; tendo como um de seus aspectos principais as performances sociais cotidianas da linguagem, da arquitetura, da moda, das sinalizações e do uso de objetos oficiais do Estado (moedas, selos postais). Para o espaço internacional, a prática se dirige para o reconhecimento por meio da prática diplomática e pelo âmbito da atuação em organizações internacionais. Uma das problemáticas centrais relacionadas às práticas soberanas de manutenção e reprodução da territorialidade e da soberania são os fluxos de dados

transfronteiriços, que tem resultado em diferentes estratégias de controle, determinadas principalmente pelo desenvolvimento tecnológico, pelo desenvolvimento industrial e pelas demandas de segurança dos países (TIMMERS, 2019; LIU, 2020; LOH, HEISKANEN, 2020).

Por outro lado, o problema de fluxos de comunicação transfronteiriços não é exclusivo ao ciberespaço. Buscando analisar as questões de soberania e territorialidade das comunicações, Taylor (2020) apresenta uma genealogia do processo internacional de regulação sobre comunicações. Historicamente, o princípio basal do poder governamental sobre dados, instituições e tecnologias da informação é a soberania, ou seja, a autoridade suprema do Estado sobre seu território e população. Originária do período da Paz de Westfália[77], a soberania estatal sobre as comunicações assentou-se sobre a determinação do poder soberano de monopólio do Estado sobre todas as modalidades de comunicação, abrangendo novas tecnologias progressivamente à medida que emergiam. Desde o período das comunicações por telégrafo, já havia regulações sobre redes de comunicação transfronteiriças, incluindo interceptações e inspeções das mensagens transmitidas ao passarem pelas fronteiras. As regulações foram padronizadas com a criação da União Internacional dos Telégrafos, posteriormente transformada em União Internacional de Telecomunicações, mantendo, porém, o princípio fundamental de soberania interna dos países sobre suas redes de comunicação. A questão então estende-se a um problema de extraterritorialidade: qual a extensão do espaço soberano de um país sobre os fluxos de comunicação transfronteiriços? (TAYLOR, 2020).

[77] Ao nos referirmos a Paz de Westfália, queremos indicar especificamente os Tratados de Münster e Osnabruque de 1648, os quais puseram fim a Guerra dos Trinta anos, e criaram as condições para o reconhecimento da autoridade dos príncipes e reis sobre determinados territórios e populações permitindo o reconhecimento da Soberania secular.

O ciberespaço apresenta um desafio à soberania, por pôr em questão a capacidade do Estado de regular a movimentação dos fluxos de dados por suas fronteiras, se pensado à luz do conceito clássico da teoria das relações internacionais: o dilema de segurança. A própria concepção de um espaço transfronteiriço ou que desconhece as fronteiras físicas clássicas, desloca o conceito para um lugar no qual a ideia de segurança *de quem* e *do que* se torna cada vez mais complexa. Devido à incerteza legal frente a um espaço cibernético sem fronteiras e com dados armazenados nas *nuvens* de terceiros, se evidencia uma tendência de países e blocos regionais à localização de dados a partir da legislação e institucionalização do controle sobre o ciberespaço, principalmente em relação à cibersegurança, ao armazenamento de dados e às normas de privacidade e proteção de dados. O ciberespaço não está desconectado da soberania estatal; ele exige uma estrutura física para funcionar e uma entidade para monitorar seu desenvolvimento. A partir disso, se inicia a *corrida armamentista* no ciberespaço entre a desregulamentação e o Estado. Khanna argumenta que apesar de uma entidade abstrata, o ciberespaço tem manifestações físicas que se tornam sujeitas à legislação estatal, tanto sua infraestrutura como seus atores. Para proteger suas ciber-fronteiras, é necessária a regulação da infraestrutura de tecnologia da informação situada no interior de seu território (TAYLOR, 2020; LAND, 2011; KHANNA, 2018).

Todavia, o problema do fluxo de dados se intensifica na contradição entre a localização física da infraestrutura das redes (inserida em uma territorialidade nacional soberana) e o fluxo de dados que atravessa múltiplas jurisdições em um milissegundo. Schulze expõe o exemplo de um ciberataque no fim da década de 90 que gerou tensões geopolíticas e

especulações de uma ciberguerra entre os Estados Unidos e o país de possível origem do ataque (Irã, China ou Rússia), sendo descoberto posteriormente que o autor se tratava de um adolescente da Califórnia. Isso demonstra a insegurança e a incerteza gerada pela ausência de controle de dados e de ciber-soberania (SCHULZE, 2017).

Situada no eixo do comércio internacional e da proteção de direitos humanos, as políticas de dados encontram-se então neste duplo impasse: o livre fluxo de informação que garante a liberdade e o estimula o comércio, mas ameaça a soberania dos países e torna vulneráveis a privacidade e a segurança da população; ou o caminho do protecionismo digital, que garante a ciber-soberania e a segurança nacional pela localização dos dados e regulação dos fluxos de informação, porém dificulta e cria barreiras para a livre competição no âmbito do *e-commerce* (consequentemente beneficiando grandes empresas capazes de seguir as normas e lidar com os custos das regulações), além de abrir espaço para práticas de censura e controle estatal de informações. Tal impasse atravessa o debate sobre a capacidade do direito internacional de regular a conduta do Estado no ciberespaço. A ausência de consenso internacional sobre os valores normativos referentes aos fluxos de dados entre nações agrava o problema; resultando em casos de "isolacionismo digital" por uma afirmação simbólica do poder nacional contra o "colonialismo de dados" do ocidente, como é o caso da China (TAYLOR, 2020).

Esse impasse instaura então um debate que demarca um confronto entre a posição ciber-libertária em relação ao ciberespaço – que prega o livre fluxo de informação e a ausência de fronteiras – contra a posição ciber-soberana – que prega a regulamentação nacional e soberana do ciberespaço. Enquanto a arquitetura do ciberespaço tende a um ciber-libertarianismo pela sua formação e funcionamento análogo a uma *terra nullius* supra-territorial (um

espaço livre de regulações governamentais), a questão técnica se encontra atravessada por questões geopolíticas complexas. Mesmo com tal arquitetura de alta distribuição dinâmica e descentralizada, o sonho ciber-libertário de uma internet como bem global declinou progressivamente. Timmers (2019) atribui tal problema a um defeito essencial: o design determinante para o funcionamento da internet é deficitário de segurança e privacidade. Além disso, houve um impacto inesperado da internet sobre a economia e sociedade, resultando em uma capitulação da rede por empresas oligopolistas, cibercriminosos e governos. Com a soberania estatal se assentando sobre o ciberespaço, a internet se desmembra em uma *splinternet*. Testemunha-se progressivamente então um processo de territorialização parcial do ciberespaço por meio de mecanismos de segurança e vigilância, já que a independência soberana deste não é expressivamente reconhecida por nenhum país. A tendência de fronteiras defensivas no ciberespaço para a demarcação de um ciberespaço nacional ciber-soberano se concretiza em um novo ciber-mundo westfaliano com fronteiras virtuais. Independente dos elementos físicos do ciberespaço que exigem uma sede localizada geograficamente, a arquitetura técnica torna-se cada vez mais governada por estruturas soberanas apesar de sua estrutura originalmente livre e descentralizada. Considerada uma ameaça à liberdade da internet enquanto espaço global sem fronteiras pelos ciber-libertários, a ciber-soberania é defendida pela China como uma proteção contra a ameaça ao império da lei por uma internet desregulada e sem fronteiras, enfatizando a natureza geopolítica do ciberespaço (GOODNIGHT, HONG, 2019; TIMMERS, 2019; KHANNA, 2018; BARAM, MENASHRI, 2019).

O dilema não apresenta solução simples: o ciberespaço é como um continente recém-descoberto pronto para ser dividido entre os atores geopolíticos ou é como os oceanos, além da possibilidade de um controle soberano? Allen e Lastra (2020) expõe tendência da emergência de múltiplas

internets: uma internet aberta da ideologia californiana do Vale do Silício, baseada numa síntese de neoliberalismo, contracultura radical e determinismo tecnológico; uma internet burguesa de Bruxelas, protetora da privacidade; uma internet chinesa, focada na vigilância e controle para manter a coesão social e a segurança; e uma internet comercial de Washington, que busca a monetização e privatização dos recursos digitais. Os diversos gradientes de possíveis futuros da internet situam-se então entre a balcanização por firewalls nacionais e um 'Velho Oeste' digital (ALLEN, LASTRA, 2020).

A problemática da conectividade explorada por Culp (2020) permite relacionar as diferentes concepções de tecnologia com as tendências ciber-utopianistas e ciber-realistas, assim como a passagem da hegemonia de uma para a outra. Segundo Culp, a concepção cosmopolita e universalista vê como objetivo da conectividade o fazer com que tudo e todos sejam parte de um único mundo; para Land (2011), o ciberespaço aparece inicialmente como um valor de uso humano; relacionada assim à tendência ciber-utopianista. Por outro lado, há outra concepção explicitada pelo autor a partir de uma citação de Gilles Deleuze: "a tecnologia... é social antes de ser técnica" (Deleuze, 2005 apud Culp, 2020, p. 31); indicando a indissociabilidade da tecnologia de sua produção *cosmotécnica*, ou seja, como permeada por uma cosmologia tecnológica inserida em processos históricos, políticos, sociais e culturais. Esta segunda concepção é compatível à tendência atualmente hegemônica do ciber-realismo, que ascende devido a inserção de um discurso geopolítico na governança do ciberespaço (CULP, 2020; LAND, 2011; HUI, 2016).

De forma semelhante, Timmers analisa o processo de soberania digital sob o prisma da relação entre tecnologia, direito e governança. A partir da frase de Lawrence Lessig em 1999, "*code is law*", ou seja, a arquitetura da tecnologia digital condiciona as leis aplicadas à economia e à sociedade, atesta-se uma

inversão: 20 anos depois, com o crescente controle dos governos sobre a internet, as leis da sociedade passam a condicionar as arquiteturas tecnológicas, ou seja, *"law is code"*. O impasse em relação à falta de segurança de tecnologias como o AI, 5G e a IoT reflete-se em um intenso processo de legislação e institucionalização de medidas de cibersegurança que moldam a arquitetura dessas tecnologias. A partir de Baudrillard, Timmers afirma: a tecnologia media nossa relação com a realidade, a arquitetura tecnológica influencia fortemente nossa construção social do real e a tecnologia não é neutra, portanto as leis e arquiteturas tecnológicas devem ser moldadas para garantir os valores sociais desejados (TIMMERS, 2019).

Essa inversão na hegemonia das concepções sobre o ciberespaço se atesta na observação de alguns episódios ocorridos na virada do século. Tal transição teria tido como um de seus marcos os governos de Clinton e Bush nos EUA, onde aumentou a tendência a um discurso de uma estratégia nacional para proteger o ciberespaço. Nesse contexto de militarização e controle da internet, há cisão interessante: enquanto países como China e Rússia não passaram por nenhuma grande mudança normativa (a China começou sua vigilância e controle da internet em 1996, com sua *intranet* tornada funcional no início do século XXI), as democracias liberais do ocidente fizeram uma transição de um ciber-utopianismo baseado no livre fluxo de dados para um ciber-realismo baseado na soberania e no controle de dados, resultando numa arquitetura de rede propensa à censura (apesar da existência de atividades clandestinas de vigilância da internet realizadas pelos Estados Unidos iniciadas por volta de 1998) (SCHULZE, 2017).

O ciber-realismo então se concretiza internacionalmente como a agenda de governança de internet, baseada no princípio da ciber-soberania e da segurança nacional e articulada na disputa pela nova ordem global

cibernética, apresentando tendências a um ciberespaço westfaliano e balcanizado ou uma *splinternet*. Isso resulta numa condição global de pressão sobre a soberania devido às tensões internacionais e à transformação digital disruptiva para a economia e para a sociedade, caracterizada por uma condição de ausência de paz. A brecha da soberania amplia-se com a persistência dos ciberataques e da ascensão de empresas de tecnologia como atores não-estatais cada vez mais influentes no sistema global. Tais tensões internacionais orbitam em torno do medo de uma ciberguerra e do impacto das ciberarmas. Há entretanto disputas conceituais sobre a questão da ciber-soberania em relação às ciberarmas: a discordância de o que constitui uma ciberarma e se informação pode ser considerada uma; bem como se o direito internacional se aplica à incidentes que não cabem no padrão tradicional de uso de força. Partindo desse problema, questiona-se ainda se as ciberarmas seriam uma nova forma de fazer guerra ou apenas mais uma ferramenta para ser usada nos moldes já existentes de conflito. Além do problema das fronteiras, a questão da extensão da ameaça a segurança nacional é cada vez mais ampla: com possibilidades de afetar infraestruturas críticas, como a governança de internet pode manter sua ciber-soberania territorial quando há discordância internacional sobre o que qualifica uma ciber ameaça, uma medida defensiva e uma medida ofensiva no ciberespaço? Em meio a este cenário inconclusivo, velhos inimigos como China/Rússia e Estados Unidos se percebem como atores potenciais de onde podem se originar operações de inteligência, espionagem e ciberataques (SCHULZE, 2017; TIMMERS, 2019; BARAM, MENASHRI, 2019).

Uma das principais tecnologias de controle e cibersegurança da China chama-se *Golden Shield*, também conhecido como *Great Firewall*, implementado em 2003 para maior regulação dos conteúdos online. Além da regulação, o armazenamento local e o controle dos fluxos de dados transfronteiriços são essenciais para a estratégia de ciber-soberania da China. As primeiras medidas regulatórias para armazenamento local de dados na China ocorreram em 2011, após o Banco Popular da China exigir que informações financeiras pessoais fossem armazenadas na China e as condições de saída fossem estritamente reguladas. A competição internacional e as revelações de Edward Snowden sobre os esquemas de espionagem internacional do governo dos Estados Unidos aceleraram a institucionalização da estratégia de *re-centralização do governo*, levando ao protagonismo da *Central Cyberspace Affairs Commission* na governança de internet, tendo como foco principal a cibersegurança como estritamente ligada à segurança nacional, política, econômica, cultural e social (MUELLER, YANG, 2014; LIU, 2020).

O *Central Cyberspace Affairs Commission* surgiu em fevereiro de 2014 sob o nome de *Central Internet Security and Informatization Leading Group*, com Xi Jinping no cargo de diretor. O órgão foi criado para cumprir a função de coordenação do desenvolvimento de políticas de cibersegurança. Subordinado ao Comitê Central, acelera-se o processo legislativo e possibilita a concretização do plano de ampliar a cibersegurança para todo o ciberespaço nacional da China. A criação do CCAC representou uma centralização sobre a governança do ciberespaço, até então feita de maneira descentralizada por diferentes ministérios e agências; com isso, as principais regulações e políticas em nível nacional passaram a ser emitidas pelo CCAC e seus órgãos subordinados (MUELLER, YANG, 2014; IASIELLO, 2017).

No contexto de tais mudanças institucionais, políticas e legislativas, foi aprovada a Lei de Cibersegurança[78] em novembro de 2016, introduzida pela *Cyberspace Administration of China* (CAC), uma secretaria da CCAC. Cumprindo as metas de elevação da cibersegurança em nível nacional, a Lei significou um passo importante em direção à ciber-soberania do país, com a construção de uma jurisdição de cibersegurança que permite uma capacidade maior de monitoramento registro e controle de dados na internet, além de exigir o cumprimento de tais diretrizes por empresas estrangeiras (IASIELLO, 2017; QI, SHAO, ZHENG, 2018; GOODNIGHT, HONG, 2019; KOKAS, 2018).

A Lei é a protagonista de um processo legislativo amplo que busca o desenvolvimento de uma governança cibernética centralizada, um protecionismo que favorece a atuação de empresas chinesas no mercado doméstico, um alto controle sobre o fluxo e o armazenamento de dados e informações na internet do país e um corpo legal para garantir o cumprimento de regulações e normas padronizadas de cibersegurança sobre uma série de produtos e infraestruturas cibernéticas. O controle de informação é um dos pontos críticos de manutenção da estabilidade do regime, indicando o aspecto político subjacente às normas técnicas que reposicionam relações sociais e políticas na sua mediação pela internet, visando também um maior poder de resposta às insurreições e o terrorismo em Xinjiang e Hong Kong. Além da Lei, a promulgação da Estratégia de Segurança do Ciberespaço da China (2016) e a Estratégia Internacional de Cooperação no Ciberespaço em (2017), são também marcos importantes para a consolidação do princípio da ciber-soberania como central para a agenda de cibersegurança da China. O livre fluxo de dados fronteiriços dá lugar então ao controle ciber-soberano, dando espaço apenas a iniciativas de

[78] Abreviada aqui como “a Lei”.

acordos bilaterais ou multilaterais, especialmente no âmbito de blocos regionais e da iniciativa da Nova Rota da Seda (LIU, 2020; IASIELLO, 2017, QI, SHAO, ZHENG, 2018; GOODNIGHT, HONG, 2019; KOKAS, 2018).

Com grandes esforços direcionados para a localização dos dados, a China desenvolveu uma estratégia pragmática de institucionalização, armazenamento local e avaliação de saída. Com a Lei, a China passou a ter um design institucional que protege os fluxos de dados transfronteiriços, construindo uma infraestrutura de proteção de informação crítica (dados ligados à segurança nacional, desenvolvimento econômico e interesses sociais e públicos) e implementando uma regulação robusta sobre os operadores de rede e provedores de serviços cibernéticos na China. A legislação de proteção de dados tem como um dos principais objetivos o desenvolvimento do setor doméstico de tecnologia, sendo a independência e autossuficiência frequentemente enfatizadas no discurso oficial dos planos quinquenais e estratégias nacionais. Tal nacionalismo tecnológico, visto pelo governo da China como uma estratégia de administração do ciber-poder, têm resultado em uma quantidade massiva de dados armazenados no país, levando a um desenvolvimento acelerado da indústria tecnológica, especialmente os setores de big data, chegando a crescimentos de 30% ao ano e consagrando a economia digital chinesa com a fatia de 34.8% do PIB em 2018, o equivalente à 31.3 trilhões de yuan (RMB) (LIU, 2020).

A agenda estratégica tecno-nacionalista e ciber-soberana chinesa têm como ferramentas de regulação da internet uma série de medidas de controle como a exigência de registros com nomes reais, uma polícia especializada para a internet que lida com a vigilância e os ciber-crimes e uma série de regulações de conteúdo para plataformas online (PLANTIN, DE SETA, 2019; QI, SHAO, ZHENG, 2018; MUELLER, YANG, 2014).

A repercussão internacional desse processo é multiforme: a Lei e a estratégia geraram acusações de protecionismo, censura e obstrução da competitividade econômica; por outro lado, é considerada também como uma garantia de segurança e privacidade da população, comparada inclusive com o corpo normativo de privacidade cibernética da União Europeia[79]. Mas apesar da extrema localização e regulação sobre seu ciberespaço, a China mantém-se inserida nas transmissões e redes de comércio cibernéticas internacionais, inclusive pela dependência do mercado chinês das tecnologias estadunidenses. Para se livrar de tal dependência, a China busca substituir importações a partir da estratégia *Made In China 2025*, que tem como objetivo o impulsionamento de inovações tecnológicas domésticas nos setores informacionais e de tecnologia de ponta, estimulando então competidores locais e os beneficiando frente aos competidores estrangeiros. Tal protecionismo chinês tem resultado em *protecionismos* recíprocos por parte dos países ocidentais, especialmente os Estados Unidos, chegando a alegar que a China violaria os acordos da OMC e tomando uma série de medidas retaliatórias. Por meio de sua *legal warfare*, a China se arma na guerra comercial com ferramentas jurídicas e legais para a justificativa e resolução de conflitos decorrentes das sanções ao governo dos Estados Unidos. Além disso, as atividades de *hacking* alegadamente usada pelas agências militares e de inteligência dos governos dos Estados Unidos e da China aprofundam a insegurança e a crise no ciberespaço (IASIELLO, 2017; GOODNIGHT, HONG, 2019; LIU, 2020; QI, SHAO, ZHENG, 2018; KOKAS, 2018).

Sendo um contra-protecionismo frente a ciberpolítica chinesa ou uma consequência da exposição das atividades cibernéticas das agências de inteligência (principalmente a NSA dos EUA, responsável por casos de espionagem e ataques às infraestruturas de rede – como a operação

[79] Ver normas da UE em: https://bityli.com/Djy41

direcionada a Huawei em 2010 e outros casos expostos por Snowden), há uma iniciativa global de vigilância e controle na internet, como a busca da União Europeia e Estados Unidos para acessos excepcionais à criptografia de aplicativos de mensagens e a aprovação de legislações que multiplicam as abordagens de governança do ciberespaço. Enquanto a Rússia parece seguir o caminho da China com a tentativa de construir a RuNet, os Estados Unidos parecem então deixar sua retórica liberal e transitar para um realismo protecionista, baseado principalmente em seu antagonismo contra a China. A União Europeia também segue o caminho da ciber-soberania, afirmando os "valores europeus" da democracia e dos direitos fundamentais (SCHULZE, 2017; TAYLOR, 2020).

Há recentemente uma popularização do termo *autonomia estratégica*, utilizado anteriormente apenas pela França e pela Índia para expressar sua independência de Washington, Pequim e Moscou, devido às crescentes tensões no campo da soberania. Entretanto, tal estratégia não é alcançável para a maioria dos países. Segundo Timmers, a tendência é que apenas os Estados Unidos e a China, capazes de resistir à dissociação de cadeias produtivas, às restrições de comércio e investimento e à transição para a dependência do mercado nacional poderão alcançar tal autonomia estratégica, tendo como um dos pilares a ciber-soberania. No Ocidente, porém, a inversão estratégica protecionista ainda encontra resistências e impasses ideológicos e legislativos, o que acarreta uma vantagem para a China em seu processo ciber-soberano, tendo avançado para a criação de redes quânticas de internet e a iniciativa de uma plataforma nacional de blockchain, podendo assim aumentar a eficiência dos fluxos internos de dados. O problema da dependência das tecnologias da *info-esfera integrada* (Big Data, Internet of Things e Artificial Intelligence) sobre os servidores globais das *nuvens* é também mais facilmente superado no cenário chinês, devido a imensa quantidade de dados armazenados localmente pela sua

massiva população e tráfego cibernético, além da sua capacidade econômica de arcar com os altos custos do processo de localização de dados (TIMMERS, 2019; TAYLOR 2020).

Mesmo com tal inversão na tendência hegemônica de governança da internet, mantém-se as acusações à estratégia chinesa. Mas apesar dos protestos internacionais de governos e entidades comerciais, além de episódios de consulta e intercâmbio entre a CAC e acionistas internacionais, a China não recuou em seu processo legal e institucional (o projeto da Lei foi pouco alterado até sua versão final, por exemplo). Liu (2020) apresenta uma reflexão sobre tais protestos contra um suposto aprofundamento da vigilância governamental com uma análise do texto da Lei, afirmando que é improvável que a localização de dados seja uma iniciativa de tal natureza, tendo em vista que as especificações para o armazenamento local de dados foram mantidas fora das provisões gerais e situada apenas para setores de informação crítica. Além disso, o autor defende que a supervisão, vigilância e controle bem-sucedidos do governo chinês sobre a internet nos últimos 25 anos foi independente do armazenamento local de dados (LIU, 2020).

O caso do WeChat e do governo da China é importante para entender como a China molda sua arquitetura tecnológica e promove sua agenda de governança da internet. Plantin e De Seta (2019) ressaltam o fenômeno da plataformização e da infra-estruturalização do modelo de plataforma, onde grandes empresas donas de plataformas digitais reestruturam atividades econômicas e sociais para obter vantagens e maiores lucros e moldam o ambiente virtual a partir de sua plataforma. O projeto tecno-nacionalista da China, que tem como origem as iniciativas do Golden Firewall e dos Golden Projetcs, construiu uma estrutura informacional cibernética que é atualmente caracterizada por tal infraestrutura baseada em plataformas, fruto da ação conjunta do governo chinês e de grandes empresas nacionais

(PLANTIN, DE SETA, 2019). Segundo Srnicek, devido à impossibilidade de acesso ao mercado chinês por grandes companhias donas de plataformas no Ocidente, abriu-se espaço para o crescimento e desenvolvimento de um mercado nacional, atualmente dominado pelas gigantes chinesas Baidu, Alibaba e Tencent, que possuem relações próximas com as autoridades reguladoras e políticas chinesas (há inclusive casos de diretores de tais empresas que são deputados da Assembleia Nacional) (SRNICEK apud PLANTIN, DE SETA, 2019).

O WeChat é o principal expoente do processo de plataformização, sendo o aplicativo de redes sociais mais popular da China, desenvolvido pela Tencent. Com uma lógica de plataforma extremamente variada e constantemente proliferante, seus serviços vão de mensagens instantâneas a mecanismos de busca, de uma carteira virtual a um sistema de reservas de serviços urbanos; seu ecossistema permite aplicativos de terceiros interiores a sua plataforma, em uma arquitetura de software descentralizada combinada com uma re-centralização dos fluxos de dados e códigos de programação. Sua ascensão é intimamente ligada a sua relação com a governança de internet da China de agenda tecno-nacionalista e ciber-soberana, onde sua plataforma foi infra-estrutralizada principalmente em função de seu sistema de pagamentos por carteira virtual, o WeChat Pay. O WeChat Pay surge em 2013 com o objetivo de superar as limitações da infraestrutura bancária chinesa e torna-se a forma de pagamento padrão na China por uma iniciativa conjunta com o governo, que promoveu o serviço em rede nacional em um dos maiores eventos do país, o Festival de Primavera da CCTV, maior rede de televisão chinesa (PLANTIN, DE SETA, 2019).

Após o enorme crescimento do serviço, o Banco Popular da China definiu em 2018 a obrigatoriedade de transferência de todos os dados das transações online de serviços como o WeChat Pay para um banco de dados estatal

nacional. Desta forma, o governo da China conseguiu resolver sua incapacidade estrutural de controle de dados bancários, por meio da infra-estruturalização da plataforma WeChat e sua subsequente supervisão re-centralizadora. Baseada em sua tecnologia de pagamentos por *QR codes*, essa forma de pagamento, protagonizada pelo WeChat Pay, corresponde atualmente a 60% de todos os pagamentos online na China. Além do WeChat Pay, a plataforma WeChat atualmente é usada por quase todas as organizações da China, havendo inclusive casos de governos locais usando a plataforma para distribuição de auxílios de assistência social. Por isso, tal relacionamento próximo com o governo beneficia essas empresas pelo ambiente protecionista que é constituído pela alta regulação e pela proibição de várias empresas estrangeiras, diminuindo a competição e favorecendo as gigantes chinesas. Por meio de tal infra-estruturalização de plataformas seguindo o modelo chinês, constrói-se uma governança protecionista, regulada e nacionalizada do ciberespaço (PLANTIN, DE SETA, 2019).

Os âmbitos comercial e financeiro são centrais para o debate sobre o ciberespaço chinês. O processo do WeChat Pay está inserido numa questão mais abrangente, explorada por Allen e Lastra em sua análise sobre a *Fintech* (tecnologia financeira) e os *problemas de fronteira* causados pela expansão desta. Entre atividades e entidades reguladas e não-reguladas e entre jurisdições nacionais diferentes, emerge uma nova fronteira: entre o 'mundo real' e o ciberespaço. Essa terceira fronteira explicita a essência do problema: as tecnologias financeiras operam em um espaço não-territorial e difícil de ser definido em termos de jurisdição territorial. Portanto, aprofundam-se problemas de não-regulação de atividades e entidades além de sobreposições jurídicas entre diferentes territórios nacionais. As moedas virtuais e cripto moedas, por exemplo, são um grande desafio para os governos, por sua frequente operação paralela aos serviços financeiros regulados. Há na China um crescimento de arranjos financeiros informais,

como a plataforma Ren-ren Dai, de empréstimos entre pares (*peer-to-peer*). Com o processo de construção de ciber-soberania, busca-se trazer o ciberespaço para o quadro normativo da jurisdição territorial para solucionar os 'problemas de fronteira' - regulado e não-regulado, nacional e internacional, real e digital - e regular novas tecnologias de informação e comunicação (ALLEN, LASTRA, 2020).

Outro exemplo, este, porém articulando a China com empresas estrangeiras, permite o aprofundamento da análise sobre a ciberpolítica chinesa. Explorando as tensões da divisão ontológica dentro/fora, Loh e Heiskanen fazem uma análise pós-estruturalista do conceito de soberania buscando construir a noção de liminaridade, tensionar abordagens essencialistas e demonstrar a produção social da soberania em sua instabilidade. O espaço nacional (dentro) e o espaço internacional (fora) fundam um terceiro espaço dependente, o espaço liminar, que tensiona e/ou reforça a divisão ontológica. No espaço liminar, a disputa pela ciber-soberania encontra um de seus campos de batalha. O caso do Google na China ilustra tal problemática: a empresa multinacional que executa o papel de um poderoso ator não-estatal, negociava com a China em 2018 para o desenvolvimento de um mecanismo de busca que comportasse as regulações e censuras de conteúdo exigidas no ciberespaço chinês, para poder assim ter a licença para operar no país. Desta forma, os ímpetos capitalistas das práticas corporativas do Google dão apoio às práticas soberanas da China ao facilitar a execução de sua soberania doméstica por meio de sua ciber-soberania. Portanto, há uma expansão da fronteira entre o dentro e o fora do Estado, por meio do que os autores chamam de práticas de soberania intersticial, ou seja, a interação do Estado com atores não-estatais que atuam em um espaço paralelo como atores liminares intersticiais, podendo tanto tensionar quanto reforçar a divisão ontológica; territorializando assim suas ciber-fronteiras, ainda porosas (LOH, HEISKANEN, 2020; GOODNIGHT, HONG, 2018).

Além do Google, outras empresas estadunidenses como a Netflix e a Amazon buscaram se enquadrar nas novas normas chinesas. Em 2017, a Apple fez um acordo com o governo chinês para operar no país sob condição de estabelecer um banco de dados na China[80]. Apesar das iniciativas protecionistas do governo de Donald Trump de construir um corpo legal ciber-soberano e sancionar as empresas chinesas, o mercado estadunidense ainda é um ambiente *laissez-faire* com ausência de uma legislação substantiva para a regulação do ciberespaço e a proteção da privacidade dos usuários. Por outro lado, na China o ambiente de *segurança dos interesses nacionais* exige armazenamento de dados em servidores locais chineses, uma série de padrões de segurança e medidas retaliatórias caso haja não-cumprimento das diretrizes. Com a falta de uma governança centralizada de cibersegurança nos Estados Unidos, a estratégia chinesa se sobressai na guerra comercial entre os dois países e a China expande assim seu ciberespaço, seu poderio de informação e sua economia (IASIELLO, 2017; KOKAS, 2018).

CONCLUSÃO

O ciberespaço em disputa está em processo de formação. Como tornar o ciberespaço seguro, ou seja, como neutralizar os perigos cibernéticos? (GIDDENS, 1991) Com a decadência do sonho libertário do ciberespaço, o Estado contra-ataca. Protagonista nesse processo, a China orienta suas políticas ciber-soberanas para construir um ciberespaço *com características chinesas*. Diante disso, tensões geopolíticas decorrentes dessa partilha do novo continente cibernético se aprofundam: os Estados Unidos se voltam

[80] Sobre o acordo, ver: https://news.cgtn.com/news/3d4d444d7a63444e/share_p.html

para garantir a competitividade extrema com a China[81], especialmente no âmbito econômico; a União Europeia defende a primazia da privacidade dos cidadãos europeus; a China e a Rússia partem para a abordagem ciber-soberana crescentemente insular. Apesar das disparidades, há um denominador comum: a defesa da regulamentação do ciberespaço. O impasse se torna então uma questão de *quem* e *como*: haveria possibilidade de uma legislação abrangente internacional? Em que medida a norma internacional infringe o direito à ciber-soberania?

Ainda longe de um consenso internacional, as políticas de ciber-soberania passam a priorizar a segurança dos interesses nacionais. A China articula então suas ferramentas para garantir sua cibersegurança: mecanismos institucionais para acelerar o processo legislativo, centralização dos agentes decisórios para o tema da cibersegurança, mobilização de empresas nacionais (estatais, privadas e mistas) para o desenvolvimento de infraestruturas necessárias e investimento na iniciativa tecno-nacionalista para garantir a independência soberana da indústria chinesa de tecnologia da informação e comunicação. Deste modo, o mercado chinês passa a condicionar não só as diretrizes necessárias para que empresas estrangeiras operem na China, mas a moldar o processo ciberpolítico internacional que se depara com uma nova forma de garantir a ciber-soberania.

[81] Em um pronunciamento no início de fevereiro de 2021, o presidente Joe Biden, eleito após o mandato de Donald Trump, defendeu que o conflito com a China será sustentado em outros termos que os de Trump, favorecendo porém a "competitividade extrema" entre os países. Ver: https://www.cnbc.com/2021/02/07/biden-will-compete-with-china-but-wont-take-trump-approach.html

REFERÊNCIAS

ALLEN, Jason Grant; LASTRA, Rosa María. Border Problems: Mapping the Third Border. The Modern Law Review, vol. 83, nº 3, p. 505–538, 30 jan. 2020. DOI 10.1111/1468-2230.12506. Disponível em: http://dx.doi.org/10.1111/1468-2230.12506

BARAM, Gil; MENASHRI, Harel. Why can't we be friends? Challenges to international cyberwarfare cooperation efforts and the way ahead. Comparative Strategy, vol. 38, nº 2, p. 89–97, 4 mar. 2019. DOI 10.1080/01495933.2019.1573069. Disponível em: http://dx.doi.org/10.1080/01495933.2019.1573069.

BAUMAN, Zygmunt. Reconnaissance Wars of the Planetary Frontierland. Theory, Culture & Society, vol. 19, nº 4, p. 81–90, ago. 2002. DOI 10.1177/0263276402019004006. Disponível em: http://dx.doi.org/10.1177/0263276402019004006.

CULP, Andrew. Dark Deleuze. São Paulo: GLAC edições, abril de 2020.

GIDDENS, Anthony. As consequências da modernidade. São Paulo: Editora Unesp, 1991.

HONG, Yu; GOODNIGHT, G. Thomas. How to think about cyber sovereignty: the case of China. Chinese Journal of Communication, vol. 13, nº 1, p. 8–26, 12

nov. 2019. DOI 10.1080/17544750.2019.1687536. Disponível em: http://dx.doi.org/10.1080/17544750.2019.1687536.

HUI, Yuk. The Question Concerning Technology In China: An Essay in Cosmotechnics. Falmouth: Urbanomic, 2016.

IASIELLO, Emilio. China's Cyber Initiatives Counter International Pressure. Journal of Strategic Security, vol. 10, nº 1, p. 1–16, mar. 2017. DOI 10.5038/1944-0472.10.1.1548. Disponível em: http://dx.doi.org/10.5038/1944-0472.10.1.1548.

KHANNA, Pallavi. STATE SOVEREIGNTY AND SELF-DEFENCE IN CYBERSPACE. BRICS Law Journal, vol. 5, nº 4, p. 139–154, 15 dez. 2018. DOI 10.21684/2412-2343-2018-5-4-139-154. Disponível em: http://dx.doi.org/10.21684/2412-2343-2018-5-4-139-154.

KOKAS, Aynne. Platform Patrol: China, the United States, and the Global Battle for Data Security. The Journal of Asian Studies, vol. 77, nº 4, p. 923–933, nov. 2018. DOI 10.1017/s0021911818002541. Disponível em: http://dx.doi.org/10.1017/s0021911818002541.

LAND, Nick. Fanged Noumena: Collected Writings 1987-2007. Falmouth/New York: Urbanomic/Sequence Press, 2011.

LOH, Dylan MH; HEISKANEN, Jaakko. Liminal sovereignty practices: Rethinking the inside/outside dichotomy. Cooperation and Conflict, vol. 55, nº 3, p. 284–304, 9 mar. 2020. DOI 10.1177/0010836720911391. Disponível em: http://dx.doi.org/10.1177/0010836720911391.

LIU, Jinhe. China's data localization. Chinese Journal of Communication, vol. 13, nº 1, p. 84–103, 20 ago. 2019. DOI 10.1080/17544750.2019.1649289. Disponível em: http://dx.doi.org/10.1080/17544750.2019.1649289.

MORGENTHAU, Hans Joachim. Politics among nations: the struggle for power and peace. New York: Knopf, 1976.

PLANTIN, Jean-Christophe; DE SETA, Gabriele. WeChat as infrastructure: the techno-nationalist shaping of Chinese digital platforms. Chinese Journal of Communication, vol. 12, nº 3, p. 257–273, 21 fev. 2019. DOI 10.1080/17544750.2019.1572633. Disponível em: http://dx.doi.org/10.1080/17544750.2019.1572633.

QI, Aimin; SHAO, Guosong; ZHENG, Wentong. Assessing China's Cybersecurity Law. Computer Law & Security Review, vol. 34, nº 6, p. 1342–1354, dez. 2018. DOI 10.1016/j.clsr.2018.08.007. Disponível em: http://dx.doi.org/10.1016/j.clsr.2018.08.007.

SCHULZE, Matthias. From cyber-utopia to cyber-war: normative change in cyberspace. 2018. Friedrich-Schiller-Universität Jena, 2018. DOI 10.22032/DBT.35107. Disponível em: https://www.db-thueringen.de/receive/dbt_mods_00035107.

TAYLOR, Richard D. "Data localization": The internet in the balance. Telecommunications Policy, vol. 44, nº 8, p. 102003, set. 2020. DOI 10.1016/j.telpol.2020.102003. Disponível em: http://dx.doi.org/10.1016/j.telpol.2020.102003.

TIMMERS, Paul. CHALLENGED BY "DIGITAL SOVEREIGNTY". Journal of Internet Law, vol 23, (6), pp. 1-20, 2019.

WALTZ, K. N. Theory of international politics. Long Grove, IL: Waveland Press, 2010.

YANG, Feng; MUELLER, Milton L. Internet governance in China: a content analysis. Chinese Journal of Communication, vol. 7, nº 4, p. 446–465, 16 jul. 2014. DOI 10.1080/17544750.2014.936954. Disponível em: http://dx.doi.org/10.1080/17544750.2014.936954.

Recebido em 23/02/2021
Aprovado em 23/09/2022