UNIVERSIDADE ESTADUAL DE CAMPINAS
INSTITUTO DE ECONOMIA

MURILO ZOCAL DE MACEDO DO AMARAL

VIGILÂNCIA DIGITAL EM MASSA NO SÉCULO XXI:
um dispositivo aplicável a fins diversos e a ascensão da China

Campinas

2021

MURILO ZOCAL DE MACEDO DO AMARAL

VIGILÂNCIA DIGITAL EM MASSA NO SÉCULO XXI:
um dispositivo aplicável a fins diversos e a ascensão da China

Monografia apresentada na disciplina "CE825 – Monografia II" no Instituto de Economia da Universidade Estadual de Campinas.

Orientador: Eduardo Barros Mariutti

Campinas

2021

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Economia
Luana Araujo de Lima - CRB 8/9706

Am13v

Amaral, Murilo Zocal de Macedo do, 1996-
Vigilância digital em massa no século XXI : um dispositivo aplicável a fins diversos e a ascensão da China / Murilo Zocal de Macedo do Amaral. – Campinas, SP : [s.n.], 2021.

Orientador: Eduardo Barros Mariutti.
Trabalho de Conclusão de Curso (graduação) – Universidade Estadual de Campinas, Instituto de Economia.

1. Vigilância eletrônica. 2. Tecnologia - Aspectos sociais. 3. Individualismo. 4. China - Aspectos sociais. I. Mariutti, Eduardo Barros,1974-. II. Universidade Estadual de Campinas. Instituto de Economia. III. Título.

Informações adicionais, complementares

Título em outro idioma: Digital mass surveillance in the 21st century: a dispositive applicable to different purposes and the rise of China
Palavras-chave em inglês:
Electronic surveillance
Technology - Social aspects
Individualism
China - Social aspects
Titulação: Bacharel em Ciências Econômicas
Banca examinadora:
Eduardo Barros Mariutti [Orientador]
Diego Jair Vicentin
Data de entrega do trabalho definitivo: 05-01-2021

AGRADECIMENTOS

A finalização desta monografia simboliza, para mim, o fechamento de um ciclo. Um intenso ciclo pessoal de meia década que coincidiu com um marco da história mundial. Ao longo do ano de 2020, fui percebendo – em ritmo de conta-gotas – diversos planos, atividades, desejos, crenças, pessoas e lugares decantando e ficando cada vez mais distantes enquanto eu esperava um retorno que nunca aconteceria. Conforme me dava conta disto, a sedimentação destas memórias e experiências foi então dando origem a esculturas, transformando a nostalgia em compreensão e gratidão. Fui aprendendo a olhar estas esculturas sem emitir julgamentos sobre sua forma final, abandonando uma suposta necessidade de retomá-las para ajustar aquele último detalhe - ou para adiar eternamente sua finalização. Como uma destas incontáveis esculturas, esta monografia contém fragmentos de pessoas que passaram pela minha vida nestes longos anos. Agradeço imensamente a todas.

Primeiramente, agradeço aos meus avôs e avós, à minha mãe e ao meu pai, por terem me trazido ao mundo, pela paciência, apoio e carinho, e por me incentivarem a manter uma curiosidade infantil de sempre buscar entender como as coisas funcionam - e nesta busca eterna, meu irmão é, sem dúvida, meu maior companheiro. Por trás das palavras complicadas das próximas dezenas de páginas, é esta criança curiosa que escreve.

Agradeço ao meu orientador Eduardo Barros Mariutti, cuja orientação considero ter começado muito antes de eu cogitar qualquer ideia para um trabalho final. Ao longo da minha graduação tive a sorte de participar diversas vezes de suas ótimas aulas, nas quais tive o primeiro contato com ideias que anos depois estariam presentes nesta monografia. Agradeço também ao Diego Jair Vicentin por ter aceitado participar da Banca Examinadora e pelas sugestões que ajudaram a deixar este trabalho mais robusto.

Dedico agradecimentos a todos que compartilharam comigo o espaço do Instituto de Economia: aos alunos, aos professores e especialmente aos funcionários, pelo bom-humor que espalhavam no ambiente e pela prontidão sempre que precisei de qualquer auxílio.

No entanto, seria impossível agradecer apenas a este Instituto no qual estou me formando. Devo agradecimentos a todas as pessoas que dão vida a esta Universidade, incluindo as que não possuem nenhum vínculo institucional e as que estão ali apenas de passagem. Gostaria de registrar também um agradecimento à UNICAMP como um todo, cuja organização do espaço é magistralmente feita para propiciar encontros inesperados e interdisciplinares. Foram incontáveis as vezes nas quais atividades e pessoas apareceram despretensiosamente no meu caminho, algumas das quais teriam grande influência sobre mim e me levariam a outros rumos.

Agradeço em especial dois grupos que foram aos poucos tomando conta das minhas relações pessoais e do meu tempo: o Grupo de Escalada Esportiva e Montanhismo da Unicamp (GEEU) e a UniInter (rede voluntária de alunos voltada para auxiliar e integrar intercambistas durante sua estadia no Brasil). Além das ótimas amizades e experiências, alguns temas essenciais contidos neste trabalho tiveram origem em conversas com pessoas que fizeram parte da minha vida por meio destes grupos, reiterando novamente a importância de se discutir e compartilhar ideias entre pessoas de diferentes formações e experiências de vida.

Por fim, agradeço a você que está lendo, por dar sentido a esta monografia. Afinal, estas palavras são apenas símbolos mortos guardados em alguma estante ou computador sempre à espera de ouvidos que lhes tragam de volta à vida.

RESUMO

A vigilância digital massiva que emerge nas primeiras décadas do século XXI vem se difundindo rapidamente, conforme se consolida como um valioso dispositivo em múltiplas áreas. Esta disseminação, no entanto, desperta tensões que, se por um lado possuem potencial de obstruir esta expansão, por outro provocam uma reorganização de elementos institucionais, legais e discursivos a fim de contornar tais obstáculos. A hipótese desta monografia é que a China hoje possui a forma mais sofisticada de vigilância digital, devido a uma interação mais harmônica entre diversos elementos legais, políticos, sociais, culturais, institucionais, discursivos e técnicos, em contraponto à implementação com mais atrito nas democracias liberais ocidentais, onde valores como privacidade e liberdade individual oferecem uma certa dose de resistência à expansão da vigilância. Para fundamentar tal hipótese, serão analisados três temas: o surgimento de um modelo de vigilância preventiva, ubíqua, instantânea, algorítmica e granularizada nos Estados Unidos no contexto da Guerra ao Terror; outras possibilidades de aplicação da vigilância digital na China, com o Sistema de Crédito Social e o controle da internet sob a doutrina da cibersoberania; e o encontro entre vigilância sanitária e a vigilância digital massiva no combate à pandemia da COVID-19. Por fim, são apresentadas considerações sobre como a vigilância digital em massa que baseia a aceleração tecnocientífica chinesa questiona princípios da ordem liberal, enfatizando que este movimento deve ser analisado em conjunto à projeção internacional da China e das suas propostas que visam ressignificar alguns destes princípios, dando destaque à projeção da soberania nacional no ciberespaço e à relativização, a nível nacional, de direitos humanos universais.

Palavras-chave: Vigilância Eletrônica. Tecnologia – Aspectos Sociais. China. Individualismo.

ABSTRACT

The massive digital surveillance that emerges in the first decades of the 21st century is spreading rapidly, consolidating itself as a valuable dispositive in multiple areas. This spread, however, awakens tensions that, while on the one hand have the potential to obstruct this expansion, on the other they trigger a reorganization of institutional, legal and discursive elements in order to circumvent such obstacles. The hypothesis of this monograph is that China today has the most sophisticated form of digital surveillance, due to a more harmonious interaction between various legal, political, social, cultural, institutional, discursive and technical elements, in counterpoint to the more frictionary implementation in Western liberal democracies, where values such as privacy and individual freedom offer a certain dose of resistance to the expansion of surveillance. To support this hypothesis, three themes will be analyzed: the emergence of a model of preventive, ubiquitous, instantaneous, algorithmic and granularized surveillance in the United States in the context of the War on Terror; other possibilities for applying digital surveillance in China, with the Social Credit System and the control of the Internet under the doctrine of cyber sovereignty; and the meeting between health surveillance and massive digital surveillance in the fight against the COVID-19 pandemic. Finally, considerations are presented on how the mass digital surveillance that underlies the Chinese technoscientific acceleration questions principles of the liberal order, emphasizing that this movement should be analyzed together with the international projection of China and its proposals that aim to re-signify some of these principles, highlighting the projection of national sovereignty in cyberspace and the relativization, at national level, of universal human rights.

Keywords: Electronic Surveillance. Technology – Social Aspects. China. Individualism.

LISTA DE SIGLAS

AIIB – *Asian Infrastructure Investment Bank*

BPC – Banco Popular da China

CAC – *Cyberspace Administration of China*

CIA – *Central Intelligence Agency*

CNDR – Comissão Nacional de Desenvolvimento e Reforma

IA – Inteligência Artificial

IC – *Intelligence Community*

ICANN – *Internet Corporation for Assigned Names and Numbers*

EUA – Estados Unidos da América

FBI – *Federal Bureau of Investigation*

FISA – *Foreign Intelligence Surveillance Act*

FISC – *Foreign Intelligence Surveillance Court*

GCHQ – *Government Communications Headquarters*

NSA – *National Security Agency*

NSCAI – *National Security Comission on Artificial Intelligence*

OMS – Organização Mundial da Saúde

ONU – Organização das Nações Unidas

PCC – Partido Comunista Chinês

PRC – *People's Republic of China*

SCS – Sistema de Crédito Social

SIGINT – *Signals Intelligence*

TSP – *Terrorist Surveillance Program*

VANT – Veículo Aéreo Não Tripulado

SUMÁRIO

INTRODUÇÃO – DISPOSITIVOS, INFORMAÇÃO E CIBERNÉTICA

Numa hipotética reunião global em 2020 entre epidemiologistas do alto escalão da Organização Mundial da Saúde, chefes de Estados, líderes do Vale do Silício, agentes de serviços de inteligência, líderes de forças armadas, estrategistas de guerra e pessoas da área de policiamento e segurança pública, seria bastante provável que – apesar de diferenças quanto a forma e intensidade – todos seriam capazes de identificar utilidades inestimáveis para uma proposta de instaurar um programa de vigilância digital com monitoramento ubíquo[1] das populações em tempo real. O motivo é que, para cada uma destas áreas, um projeto como este atenderia à interesses específicos, como: lucro, manutenção da saúde global, defesa da segurança e interesses nacionais, treinamento de algoritmos de inteligência artificial, uso em estratégias militares, luta contra o crime ou melhorar a estabilidade social. Afinal, a vigilância massiva digitalizada pode ser vista como um dispositivo não vinculado a uma aplicação específica, podendo servir diversos objetivos. Diante desta classificação é relevante explicitar como *dispositivo* será utilizado no contexto deste trabalho.

Agamben (2005) traça a genealogia do termo *dispositivo* utilizado por Foucault no termo *dispositio* presente em escritos de padres latinos, o qual se referia a uma tradução do grego *oikonomia*, que é também a origem etimológica de *economia*, e trata da administração da casa (*oikos*), ou, por extensão, o ato de gerenciar. Por volta dos primeiros séculos da história da Igreja – no intervalo entre os séculos II e VI – houve a introdução do termo *oikonomia* na teologia cristã no contexto do início das discussões sobre uma santíssima Trindade – Pai, Filho e Espírito – que era vista com grande receio por alguns diante de uma possível reintrodução do politeísmo e do paganismo na fé cristã. O argumento utilizado para convencer os céticos era que “Deus, quanto ao seu ser e a sua substância, é, certamente, uno, mas quanto a sua *oikonomia*, isto é, ao modo pelo qual administra a sua casa, a sua vida e o mundo que criou, é, ao invés, tríplice”. Assim Deus confia a Cristo a “economia”, a administração e o governo da história dos homens. E esta é, para Agamben, uma herança deixada à cultura ocidental: a cisão que separa em Deus ser e ação, com a ação não tendo fundamento algum no ser.

[1]A escolha desta palavra ficará mais clara ao longo do texto. Algo ubíquo é algo onipresente, que pode ser encontrado em todo lugar, que está em toda e qualquer parte.

Há, portanto, nos dispositivos de Foucault, por meio da *dispositio* dos teólogos, a referência a uma *oikonomia*, a "um conjunto de práxis, de saberes, de medidas, de instituições cujo objetivo é de administrar, governar, controlar e orientar, em um sentido em que se supõe útil, os comportamentos, os gestos e os pensamentos dos homens". A partir disto, o autor propõe uma "divisão do existente" entre duas classes: de um lado, os seres viventes, a essência, a substância das criaturas e, do outro lado, a *oikonomia* dos dispositivos, que tratam de governar e guiar as criaturas para o bem. Em seguida, apresenta sua definição de dispositivo:

> Generalizando posteriormente a já amplíssima classe dos dispositivos foucaultianos, chamarei literalmente de dispositivo qualquer coisa que tenha de algum modo a capacidade de capturar, orientar, determinar, interceptar, modelar, controlar e assegurar os gestos, as condutas, as opiniões e os discursos dos seres viventes. Não somente, portanto, as prisões, os manicômios, o panóptico, as escolas, as confissões, as fábricas, as disciplinas, as medidas jurídicas, etc, cuja conexão com o poder é em um certo sentido evidente, mas também a caneta, a escritura, a literatura, a filosofia, a agricultura, o cigarro, a navegação, os computadores, os telefones celulares e – porque não – a linguagem mesma, que é talvez o mais antigo dos dispositivos, em que há milhares e milhares de anos um primata – provavelmente sem dar-se conta das consequências que se seguiriam – teve a inconsciência de se deixar capturar. (AGAMBEN, 2005, p. 13)

Da relação entre os seres viventes e os dispositivos resulta uma terceira classe: o sujeito. Dito de outra forma, é na interação entre as duas primeiras classes que acontecem processos de subjetivação, ou seja, a formação de sujeitos. Isto significa que da interação entre um indivíduo humano e um telefone celular, pode surgir o sujeito "usuário de telefone celular", ou "o ser que navega na internet". A distinção entre substância e sujeito acontece pelo fato de um mesmo "ser vivente" poder ser o lugar de diversos processos de subjetivação. Este mesmo "usuário de telefone celular" pode também ser o "apaixonado por tango", o "condutor de um carro" ou o "escritor de contos". Neste raciocínio, os dispositivos têm um papel duplo, sendo o que separa seres viventes de sujeitos e, ao mesmo tempo, o que possibilita a articulação entre eles.

Agamben segue discorrendo sobre a "ilimitada proliferação dos dispositivos, que define a fase presente do capitalismo", na qual pode-se dizer que há uma crescente onipresença de dispositivos na

vida dos indivíduos e, portanto, “uma igualmente ilimitada proliferação de processos de subjetivação” que reforça o “aspecto de mascaramento que sempre acompanhou toda a identidade pessoal”. Contudo, há uma diferença em relação ao passado. Segundo ele, os “dispositivos modernos” presentes na sociedade contemporânea atuam num contexto onde a relação entre ser e dispositivo pode “não dar lugar à recomposição de um novo sujeito”, nem corresponder à “nenhuma subjetivação real”.

A solução de tal problema remontaria à separação teológica cristã já referida e passaria pela profanação dos dispositivos. No direito romano, diz ele, há uma oposição entre a esfera humana e a esfera divina. As coisas de propriedade divina eram definidas como sagradas ou religiosas, e retiradas da esfera de circulação humana. Transgredir estas regras era considerado sacrilégio. No entanto, o ato de consagrar referia-se à retirada de coisas da esfera humana, levando-as para a esfera da propriedade divina, enquanto profanar significava o inverso, ou seja, trazer de volta algo da esfera divina para o uso e propriedade dos homens. Portanto, se a religião carrega este caráter de separação e transferência das coisas para uma esfera à parte, toda separação teria em si “um núcleo genuinamente religioso” e o “dispositivo que realiza e regula a separação” seria o sacrifício. A profanação seria, então, a forma de se unir e restituir o que foi separado.

Diante desta sequência lógica, uma interessante questão pode ser colocada: e se houvesse uma separação não só em relação à esfera humana, mas uma fragmentação do próprio humano? Os dispositivos modernos aos quais Agamben se refere – como leitores biométricos, câmeras de vigilância, telefones celulares e televisões – dizem respeito a aparelhos tecnológicos eletrônico-digitais. Desta forma, se a mudança nos processos de subjetivação tem relação com a disseminação destes novos dispositivos, como apontado, talvez o aspecto novo esteja no próprio impacto destes dispositivos nos seres vivos, incluindo o humano, como destaca Santos (2003a, p. 86):

> Tudo se passa então como se a biotecnologia, a informática e a nanotecnologia estivessem nos levando a passar para um outro plano – o plano da informação –, no qual é esta, e não mais o homem, que se torna a medida de todas as coisas. Antes de mais nada, essa transformação corrói o referencial do humanismo moderno: o homem não é mais a medida de todas as coisas, porque ao privilegiarmos o plano da informação, ao tomá-lo como referência última, passamos a valorizar o molecular, o infra-individual, comprometendo a noção de indivíduo e questionando a de organismo.

Em outras palavras, “o indivíduo dissolve-se em fluxos de dados” (SANTOS, 2003a, p.148) e o humano deixa de ser a unidade de referência. Desta forma, quando a interação de um “dispositivo moderno” acontece não mais com um “ser vivente” em sua unidade, mas apenas com fragmentos deste ser, qual é o processo de subjetivação resultante? Um sujeito fragmentado? Um quase-sujeito? Não há recomposição de um novo sujeito? Talvez a ausência de qualquer subjetivação real se deva a um redirecionamento para o âmbito do virtual?

Independente da resposta, o objetivo é ressaltar que as perguntas surgidas diante da interação entre dispositivos tecnocientíficos avançados e os seres vivos apontam para a fragilização das unidades de análise e provocam uma revisão dos termos utilizados. A existência de dispositivos que possibilitam uma interação com fragmentos dos indivíduos coloca em questão a própria unidade destes indivíduos, e por consequência os valores socioculturais a eles associados.

Finalizando as considerações terminológicas e retomando o tema central a ser tratado nesta monografia, ao definir a vigilância digital massiva que emerge no século XXI como um dispositivo nos termos de Agamben quero dizer que se trata de uma rede, inserida em relações de poder, que se estabelece entre elementos como instituições, discursos, legislações e aparatos tecnocientíficos, e que possui a capacidade de capturar, orientar, determinar, interceptar, modelar, controlar e assegurar os gestos, as condutas, as opiniões e os discursos dos seres viventes, orientando tais capacidades em direção a alguma finalidade – ainda que não exclusivamente a apenas uma.

Destes elementos, destaco a proeminência de um: a avançada estrutura tecnocientífica que opera por fracionamento do indivíduo em fluxos de informação, criando tensões com o ideal liberal de indivíduo construído nas democracias ocidentais e que, por isso, pressiona os discursos, as instituições e as legislações na direção de contornar, suprimir ou reformular esta centralidade do indivíduo.

Neste contexto, a hipótese desta monografia é que atualmente a forma mais sofisticada da vigilância digital massiva é encontrada na China, devido à harmonização entre diversos elementos legais, políticos, sociais, culturais, institucionais, discursivos e técnicos que contrasta com uma implementação mais truncada nas democracias liberais ocidentais, onde valores como privacidade e

liberdade individual oferecem uma certa dose de resistência à expansão da vigilância. Como consequência destas diferenças, a crescente influência global chinesa calcada na vigilância digital massiva contribui para intensificar as fricções supracitadas em relação a conceitos da ordem democrático-liberal centrados no indivíduo.

Para desenvolver esta hipótese é preciso explorar um tema central que perpassa os parágrafos anteriores. A vigilância digital massiva, os "dispositivos modernos" de Agamben, os aparatos tecnocientíficos e o questionamento do indivíduo têm em comum a interação com uma determinada noção de informação, a qual tem suas raízes na cibernética.

O final do século XX assiste uma proliferação de denominações como era "Era da Informação", "Sociedade da Informação" e "Revolução Informacional" num "processo metonímico onde a parte (a informação) passa a representar o todo (a cibernética), invisibilizando a ordem das relações." Cibernética foi o termo cristalizado por Norbert Wiener em seu livro de 1948 "Cibernética: ou controle e comunicação no animal e na máquina", que deriva do grego *Κυβερνήτης* e remete ao timoneiro de um navio. O mesmo termo grego é também a raiz etimológica da palavra "governar", por meio de uma variante latina e ambas as palavras, pela condução de Wiener, são associadas aos mecanismos de *feedback* explorados por James Clerk Maxwell num artigo de 1868. (ISRAEL, 2019, p.34; 57). A segunda parte do título do livro aponta para o objetivo de abstrair a comunicação e o controle de seu substrato, desenvolvendo princípios aplicáveis tanto em animais como em máquinas. A forma encontrada para executar esta comunicação descorporificada foi por meio de um novo conceito de informação.

Também em 1948, uma outra figura central nesta história, Claude Shannon, publica importantes artigos discorrendo sobre uma teoria que separa a informação do significado que ela carrega numa comunicação, inaugurando a ideia de transmitir não o que é dito, mas o que poderia ser dito. Em outras palavras, ao desvincular a informação do campo semântico atribui-se a ela um caráter abstrato e quantificável baseado na quantidade de combinações possíveis de serem transmitidas por meio de determinada sequência de símbolos (*string*). O raciocínio por trás disso é a analogia entre a entropia vinda da segunda lei da termodinâmica e a informação contida numa mensagem, com ambas sendo

uma medida do grau de desordem do sistema[2], medida que será expressa na teoria da informação, pelo *bit*, uma unidade de transmissão (*conveyance*) e não de compreensão (KAISER, 2019).

Embora o conceito de informação de Shannon seja o que ficou eternizado, Wiener tinha uma concepção um pouco diferente. Apesar de ambos concordarem quanto a separação entre informação e meio, há uma diferença fundamental. Enquanto para Shannon a informação era descolada de seu significado, Wiener relutava em aceitar esta separação:

> Quando Wiener caracterizou "informação" durante todo [o livro[3]], por outro lado, ele se inclinou repetidamente para um sentido clássico e humanista do termo. "Um pedaço de informação", ele escreveu – ao invés de um "*bit*" de informação – "a fim de contribuir para a informação geral da comunidade, deve dizer algo substancialmente diferente do estoque de informação comum anterior da comunidade". [...] Para Wiener, esta era a medida adequada de "informação": corpo, espírito, aspiração, expressão (KAISER, 2019).

Como apontado por Israel, o novo conceito de informação era apenas parte de um todo que envolvia outras contribuições. O surgimento da cibernética durante a década de 40 carrega duas pretensões: uma proposta de síntese interdisciplinar do saber científico por meio de princípios similares – informação, comunicação, aprendizado, *feedback* e controle – e uma necessidade decorrente de problemas de coordenação que ficaram claros na II Guerra Mundial, envolvendo “processos que perpassam máquinas, homens e o meio natural em uma velocidade muito mais acelerada do que os sentidos humanos” (MARIUTTI, 2020, p.129).

Contudo, a própria direção da cibernética foi se alterando. Hayles distingue três fases. A primeira, localizada entre 1945 e 1960, inicialmente vinculada às Conferências Macy sobre Cibernética[4]. Além da teoria da informação de Shannon e a extrapolação da cibernética como teoria

[2]Shannon, ao ser questionado sobre a escolha do nome entropia, responde: “Minha maior preocupação era como nomeá-la. Pensei em chamá-la de 'informação', mas a palavra foi usada em demasia, então decidi chamá-la de incerteza. Quando discuti isso com John von Neumann, ele teve uma ideia melhor. Von Neumann me disse: ‘Você deve chamar isso de entropia, por duas razões. Em primeiro lugar, sua função de incerteza foi usada na mecânica estatística sob esse nome, então isso já possui um nome. Em segundo lugar, e mais importante, ninguém sabe o que a entropia realmente é, portanto, em um debate você sempre terá a vantagem’” (TRIBUS; MCIRVINE, 1971).

[3]Referência ao livro de Wiener entitulado “O Uso Humano dos Seres Humanos”, ou *The Human Use of Human Beings.*

[4]Para um estudo mais detalhado sobre as Conferências Macy, ver Massaro (2010)

genérica e não vinculada a uma aplicação específica de Wiener, também são deste período as contribuições de McCulloch, com um modelo que abordava o funcionamento dos neurônios como sistemas de processamento de informação, e trabalho de Von Neumann com computadores que, a partir de códigos binários, podiam rodar seus próprios ciclos de autoreprodução. Enquanto um aproximava os neurônios das máquinas, o outro aproximava as máquinas da biologia. É desta instersecção que vem, o conceito central desta primeira fase. Originalmente, a homeostase é um termo associado a seres vivos, e versa sobre a capacidade de um sistema retornar a sua posição inicial após sofrer perturbações, ou seja, manter-se constante. A extensão desta ideia para as máquinas é relacionada ao servomecanismo e sua correção de comportamentos indesejados por meio de ciclos de *feedback* negativo – outro conceito central na cibernética – que reduz a magnitude de uma perturbação a cada ciclo até retornar ao estado constante (HAYLES, 1999, p.7-8). A interação entre os conceitos de homeostase e *feedback* negativo é bastante fácil de ser verificada empiricamente. Trata-se, por exemplo, da termorregulação nos mamíferos e da regulação automática de temperatura de um ar-condicionado num escritório.

A segunda, entre 1960 e 1980, trata de um ponto crítico ausente nesta primeira fase: o elemento cognitivo, a mente, o pensamento, a inteligência. Mesmo no início das Conferências Macy, alguns dos participantes já tentavam incluir este elemento no processo, como Warren McCulloch, mas o foco acabou ficando restrito sobre os sistemas observados. A questão de como redefinir os sistemas homeostáticos para incluir o observador, a ser visto também como parte do sistema, ficou no ar e foi desenvolvida após o fim das Conferências Macy, por nomes como Margaret Mead, Gregory Bateson, e Heinz von Foerster – tendo este último cunhado o termo “cibernética de segunda ordem”, ao estender os princípios da cibernética aos próprios cibernéticos (BROCKMAN, 2019). O conceito central desta fase é a autopoiese – do grego, autorreprodução ou autocriação – dos biólogos Humberto Maturana e Francisco Varela:

> As máquinas autopoiéticas são máquinas homeostáticas. Sua peculiaridade, porém, não reside nisso, mas na variável fundamental que elas mantêm constante. [...] Segue-se que uma máquina autopoiética gera e especifica continuamente sua própria organização através de sua operação como um sistema de produção de seus próprios componentes, e o faz em uma movimento infinito de componentes sob condições de perturbações contínuas e compensação de perturbações. Portanto, uma máquina autopoiética é um sistema homeostático [...] que tem sua própria organização [...] como a variável fundamental que ela mantém constante (MATURANA; VARELA, 1980).

A figura autopoiética básica é a de uma célula biológica que produz, por meio de suas organelas, compostos bioquímicos que formarão suas próprias organelas, as quais produzirão novos compostos bioquímicos, e assim infinitamente. A sua homeostase tem como finalidade manter constante sua autoorganização. Disto deriva que a interação entre diversas unidades – ou sistemas – autopoiéticos acontece por meio de perturbações mútuas entre eles, e a reação de cada um será determinada pela sua própria organização interna. Assim, o papel dos mecanismos de *feedback* como controle é de certa forma reduzido pois o *feedback* é "encapsulado"[5] e internalizado em cada unidade.

A terceira fase, a da virtualidade, tem início nos anos 1980 e segue até hoje. Ela parte da noção de autopoiese e da interação dinâmica entre sistemas auto-organizados e culmina na geração de evoluções espontâneas em direções imprevisíveis, abraçando o fenômeno da emergência. O *feedback* positivo[6] adquire uma função central, sendo o responsável pela condução destas amplificações de comportamentos em direção uma miríade de futuros, e não mais tendendo apenas à um constante equilíbrio. Esta mudança desloca a atenção para o nível das possibilidades – das virtualidades, segundo Hayles –, sendo que tais possibilidades de futuro englobam cenários de crescimento e evolução, mas também de instabilidade, comportamentos periódicos, caóticos ou complexos.

Durante esta mutação da cibernética, o uso do termo cibernética começa a desaparecer, enquanto os princípios da cibernética, pelo contrário, vão sendo "metabolizados em tudo, de forma que não os enxergamos mais como uma disciplina separada", como aponta Brockman (2019). O autor traça este movimento a partir dos anos 1970 e também aponta dois motivos que ajudam a explicar o desaparecimento do vocabulário:

[5]Termo que emprestei do paradigma de programação computacional orientada a objetos, que guarda muitas semelhanças com os conceitos desta segunda fase da cibernética, além do fato de emergirem no mesmo período, durante a década de 60. Aqui, uma das figuras centrais, Alan Kay, discorre sobre os princípios deste paradigma de programação: http://www.purl.org/stefan_ram/pub/doc_kay_oop_en

[6]Matematicamente, a diferença entre os *feedbacks* negativo e positivo é que num ciclo de feedback negativo a entrada é multiplicada por um número entre 0 e 1, tornando a saída menor que a entrada, enquanto no feedback positivo, a entrada é multiplicada por um número maior que 1, tornando a saída maior que a entrada. No primeiro caso, ciclos sucessivos tendem a reduzir cada vez mais a variação causada por uma perturbação, até que ela desapareça e se estabeleça um equilíbrio. No caso positivo, a tendência é de um aumento a cada ciclo. Entre ambos, há a manutenção de um estado constante, caso no qual o multiplicador é exatamente igual a 1.

> Entre as razões pelas quais não ouvimos muito sobre a cibernética hoje, duas são centrais: Primeiro, embora "O Uso Humano do Seres Humanos" fosse considerado um livro importante em seu tempo, ele foi contrário às aspirações de muitos colegas da Wiener, incluindo John von Neumann e Claude Shannon, que estavam interessados na comercialização das novas tecnologias. Em segundo lugar, o pioneiro da computação John McCarthy não gostava da Wiener e recusou-se a usar o termo "Cibernética", cunhado por Wiener. McCarthy, por sua vez, cunhou o termo "inteligência artificial" e tornou-se um dos fundadores deste campo.

Brockman se refere ao livro "O Uso Humano do Seres Humanos" de Wiener, no qual ele faz críticas ferrenhas a certos uso da cibernética para fins comerciais e militares, e chama a atenção para o potencial distópico que estes usos inescrupulosos poderiam desencadear no futuro. Críticas como estas, não eram do interesse de quem buscava comercializar estas novas tecnologias. Em paralelo, e talvez mais vísivel, seja a transição do uso do termo cibernética de Wiener para o conceito de inteligência artificial de McCarthy[7] que se tornaria bastante difundido no século XXI.

É sobre este mesmo século XXI que escreve Mark Weiser. Em 1991, ele publica um influente artigo chamado *The Computer for the 21st Century*, que começa com as seguintes frases: "As tecnologias mais profundas são aquelas que desaparecem. Aquelas que se mesclam ao tecido da vida cotidiana" (WEISER, 1991). No artigo, ele defende o conceito de computação ubíqua, no qual uma rede distribuída de dispositivos interconectados tornaria a computação onipresente, de forma semelhante à linguagem na vida contemporânea. O contato com a linguagem funciona tão instintivamente quanto funções biológicas autônomas. Principalmente em centros urbanos, onde, por exemplo, pessoas leem palavras em placas e lojas ao andar na rua sem a consciência de estarem praticando o ato da leitura – em outras palavras, torna-se um hábito que passa despercebido por ser tão constante. A proposta é fazer o mesmo com os computadores, ao criar máquinas que se encaixem tão naturalmente na experiência humana a ponto de não haver esforço mental no uso. Mais ainda, criar não máquinas isoladas, mas uma rede de infraestrutura tecnológica que torne algo trivial a obtenção de informações sobre si mesmo, sobre objetos ao seu redor, ou sobre o mundo. É curioso como Weiser,

[7]O termo "inteligência artificial" remonta à Conferência de Dartmouth de 1956, organizada pelo próprio McCarthy. Segundo ele: "Uma das razões para inventar o termo 'inteligência artificial' foi escapar da associação com a cibernética. Sua concentração no *feedback* analógico parecia equivocada, e eu queria evitar ter de aceitar Norbert […] Wiener como guru ou ter de discutir com ele." (MCCARTHY, 1988)

em seu otimismo tecnológico exacerbado característico da ideologia californiana do vale do silício, não destaca possíveis problemas da onipresença computacional. A própria descrição do conceito já revela uma aplicação potencial como ótimo dispositivo de vigilância, ainda que no plano das ideias.

Esta ubiquidade descrita por Weiser é uma das características que destaco ao tratar do modelo de vigilância digital massiva que emerge no século XXI. Além de ubíquo, sugiro que ele também possui caráter preventivo, instantâneo, algorítmico e granularizado. Preventivo pois os indivíduos são observados e constantemente avaliados em relação a possíveis condutas desviantes, ao invés de só monitorados após serem identificados como suspeitos. Instantâneo pela velocidade quase imediata de alimentação, processamento e circulação de informações por grandes redes interligadas. Algorítmico devido à automatização de grandes sequências encadeadas de decisões tomadas por algoritmos. E granularizado em respeito ao nível de detalhe na classificação de informação.

Estas cinco características serão retomadas longo do Capítulo 1, no qual o foco de análise é a construção de uma estrutura de vigilância em massa nos EUA entre o início do século XXI e meados da década de 2010. Serão tratados dois momentos específicos: a aprovação do *Patriot Act* em decorrência da Guerra ao Terror após os atentados de 11 de setembro de 2001 e as revelações de Edward Snowden em 2013 sobre práticas de vigilância global. Por fim, são destacados dois dispositivos discursivos essenciais para que esta estrutura se sustente: a constante ameaça terrorista e o discurso de um inevitável balanço entre liberdade e segurança.

No capítulo seguinte, o objetivo é explorar como certas peculiaridades da China possibilitam o desenvolvimento de uma vigilância que, apesar de tecnologicamente semelhante à estadunidense, acontece de uma forma menos obstruída. A primeira seção trata do Sistema de Crédito Social e de como ele busca construir um sistema de classificação social por meio de experiências locais, enquanto a segunda seção trata do controle da internet na China a partir modelo da cibersoberania que vê a internet como algo que deve ser subordinado aos interesses dos Estados. Segundo esta visão, a soberania nacional deve se projetar sobre o ciberespaço no século XXI da mesma forma como o século XVII assistiu a esta projeção sobre os mares e o século XX sobre o espaço aéreo[8].

[8]Palavras de Lu Wei, figura central na construção deste conceito na China, como reproduzidas por Segal (2020, p. 95-96)

O terceiro capítulo mostra a proximidade entre o monitoramento epidemiológico e a vigilância digital massiva, em três tópicos: a sugestão de Foucault de que os modelos ocidentais de controle dos indivíduos tiveram suas origens em epidemias; a análise sobre a metáfora da pandemia como uma guerra contra um inimigo invisível e o uso da vigilância como estratégia de combate, a partir da tese de Antoine Bousquet que trata de como os paradigmas científicos são projetados sobre as formas de se fazer guerra; e o uso de tecnologias de vigilância em massa por diversos países no combate à pandemia da COVID-19, com a China emergindo como modelo a ser seguido nas recomendações de vigilância sanitária em nome da saúde global.

Por fim, concluo que há uma aproximação das práticas de vigilância digital massiva, ainda que sob diferentes discursos e em diferentes contextos. No entanto, a implementação deste dispositivo desperta fricções em relação às noções de individualidade e privacidade forjadas nas democracias liberais do ocidente. A China, como expoente da aceleração tecnocientífica contemporânea, vem pressionando estas travas de múltiplas formas. Diretamente, por meio da projeção internacional de seus interesses visando ressignificar conceitos como direitos humanos e padrões internacionais de internet, ao mesmo tempo que participa da construção de alternativas institucionais paralelas às instituições centradas no ocidente. E indiretamente, ao influenciar outros Estados a adotarem medidas semelhantes de remoção de obstáculos diante desta aceleração.

CAPÍTULO 1 – A CONSTRUÇÃO DA VIGILÂNCIA ANTITERROR NOS ESTADOS UNIDOS DA AMÉRICA

1.1 – 11 de setembro de 2001

O dia 11 de setembro de 2001 ficou marcado na história após aviões sequestrados atingirem o *World Trade Center*, em Nova Iorque e o Pentágono, em Washington, DC. Nove dias depois, o presidente George W. Bush, num discurso direcionado ao Congresso e à população estadunidense, expõe a estrutura do que viria a caracterizar a Guerra ao Terror (OFFICE, 2001).

Recheada de maniqueísmos, a fala discorre sobre o ressentimento contra os terroristas, contendo explicações sobre quem atacou, e por quê. Sobre como tem sido forte a união nacional e internacional diante desta catástrofe e propõe – a todos os Estados – um alinhamento aos EUA no combate à ameaça terrorista, e colocando um não alinhamento como necessariamente apoiador do terrorismo. Destaca também o caráter diferente desta guerra contra um inimigo que busca destruir um modo de vida, simbolizado pela Liberdade e pela Democracia e associada não só aos EUA, mas à "toda a civilização humana" e que não acabará até que cada grupo terrorista do planeta seja encontrado e derrotado. Para isso, diz que será necessário utilizar todos os meios a disposição – diplomacia, serviços de inteligência, aplicações das leis, influência financeira e armas de guerra – nesta longa batalha sem um final próximo, e é solicitada calma aos cidadãos e confiança no governo, pois a vitória do lado do bem é certa e apoiada por Deus.

Após destacar que os inimigos não eram os muçulmanos, mas a rede de terroristas radicais, e distinguir a população afegã do regime do Talibã, apresenta a este algumas demandas que "não estão abertas a discussão ou negociação", como soltar estrangeiros injustamente presos, entregar cada terrorista para autoridades, fechar todos os centros de treinamento terroristas no Afeganistão e dando acesso aos EUA para conferir se estão realmente fora de operação. Como hoje sabemos, tais demandas não seriam aceitas, e a Guerra no Afeganistão teria início no dia 7 de outubro de 2001

Como o próprio Bush retrata em seu livro de memórias *Decision Point*, o discurso utilizado tem caráter preventivo e ideológico, além de não dissociar Estados de grupos terroristas que estejam abrigados em seus territórios:

> Depois do 11 de setembro, desenvolvi uma estratégia para proteger o país que passou a ser conhecida como a Doutrina Bush: Primeiro, não fazer distinção entre os terroristas e as nações que os abrigam – e responsabilizar a ambos. Segundo, levar a luta até o inimigo no exterior antes que eles possam nos atacar novamente aqui em casa. Terceiro, enfrentar as ameaças antes que elas se materializem completamente. E quarto, avançar a liberdade e a esperança como uma alternativa à ideologia de repressão e medo do inimigo. (BUSH, 2010)

Ainda em outubro, no dia 26, o Congresso aprova o *USA PATRIOT Act*, trazendo esta visão para o campo legislativo e marcando um ponto de clivagem em relação ao exercício da vigilância em massa com o afrouxamento da legislação vigente e concentração de poder nas mãos do executivo e das agências de inteligência para investigar pessoas suspeitas de envolvimento com terrorismo. Além disso, muitos dos debates atuais sobre vigilância digital – como coleta massiva de metadados, vigilância biomédica e coleta por interceptação de redes – tem aqui suas raízes (ÜNVER, 2018).

Mas as raízes de práticas vigilância não estão circunscritas ao século XXI. Mort (2010) recua à segunda metade do século XX para retratar uma sequência de leis que existiram antes do *Patriot Act*. Iniciando em 1968, a *Omnibus Crime Control and Safe Street Act* é aprovada pelo congresso e subordina a prática de espionagem à obtenção de uma ordem judicial (*court order*), e estabelece uma distinção entre a vigilância de casos criminais e a relativa a forças externas, sendo que neste último caso é dispensada a necessidade de uma ordem judicial. Uma decisão judicial em 1972, no entanto, ordena ao governo que torne públicas as informações obtidas num caso específico, com base na IV emenda à constituição estadunidense – que garante aos cidadãos proteção a buscas e apreensões arbitrárias feitas sem ordem judicial.

Este caso, que ficou conhecido como a Decisão de Keith, – nome do juiz – ao se combinar com os abusos do presidente Nixon no escândalo de Watergate, levou a criação do *Church Committee* para avaliar possíveis abusos do FBI e outras agências governamentais em relação a vigilância e obtenção de informações. Um relatório desta comissão revelou que, entre o início de 1960 até 1972, a NSA tinha

incluído certos cidadãos estadunidenses numa lista de observação e interceptava suas comunicações internacionais. Neste momento, o executivo e as agências de inteligência utilizavam como argumento para tais excessos a questão da segurança nacional. Em decorrência das investigações, em 1978 é criado o *Foreign Intelligence Surveillance Act* (FISA), que tinha dois objetivos: criar formas de supervisão onde não houvesse nenhuma, e deixar claro quando a aplicação da lei poderia seguir pelo processo especial relativo a inteligência estrangeira ou agentes relacionados a inteligência estrangeira, e quando deveria seguir um processo criminal comum. (SOMMER, 2014).

Para a primeira questão, foram criadas duas instâncias judiciais supervisoras, a *Foreign Intelligence Surveillance Court (FISC)* e a *Foreign Intelligence Surveillance Court of Review,* além de diferenciar os processos criminais comuns dos processos criminais referentes ao FISA. Estes últimos exigiriam menos requerimentos ao governo. Enquanto a segunda questão foi resolvida com a atribuição da necessidade de se declarar que o "propósito principal" da ação de vigilância fosse para coletar informações sobre inteligência externa. Todavia, FISA não versava sobre atividades conduzidas foras dos EUA, fato que foi resolvido com um decreto (*Executive Order 12.333*) de Reagan em 1981, que excluía do escopo cidadãos estadunidenses residentes em outro país, além de dar a NSA a prerrogativa de coletar e difundir informações para outras agências envolvidas em operações militares. Nos vinte anos seguintes, o FISA e a Ordem Executiva 12.333 permaneceram sendo as principais bases legais para atividades de vigilância (é relevante notar que em 2007 a FISC tinha rejeitado apenas 7 e aceitado 20605 solicitações, sendo que até 2002 o número de rejeições era zero.[9])

1.2 – 2001: O USA Patriot Act

Como resposta aos ataques de 11/9 é aprovado o USA *Patriot Act*, acrônimo bastante longo e auto-explicativo de *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.* Tão amplo quanto o seu título é a quantia de estatutos e leis que ele altera com seu texto de mais de 100 páginas repleto de termos vagos que complicaram a interpretação até mesmo dos juristas. Dentre estes, o FISA é um dos mais impactados (JAEGER; BERTOT; MCCLURE, 2003). Algumas das principais mudanças relativas a coleta e análise de

[9]Ver gráficos de ordens de vigilância tradicionais FISA: https://epic.org/privacy/surveillance/fisa/stats/

informação pessoal são: a substituição do “propósito principal” por um “propósito significativo”, que na prática, afrouxa as restrições aos pedidos de vigilância e espionagem; uma expansão na definição de informações e itens pesquisáveis que inclui virtualmente qualquer coisa relacionada ao sujeito investigado; uma cláusula de sigilo conhecida como “*gag order*” que proíbe a divulgação de informações sobre uma investigação sob o FISA, fazendo com que uma instituição ou indivíduo intimado judicialmente não possa nem dizer que esta ordem judicial exista; a inclusão da permissão de acessar conteúdo e metadados[10] de comunicações eletrônicas, incluindo e-mails e chamadas de voz, assim como registradores (*pen registers*) e rastreadores de chamadas (*trap-and-trace devices*), grampos telefônicos; e a permissão de compartilhamento de informações obtidas por uma investigação sob o FISA entre agências de inteligência do governo, agências judiciais ou mesmo advogados.

A seção 802 amplia o foco do terrorismo internacional para terrorismo doméstico, definido por atividades como: envolver atos perigosos para a vida humana; ocorrer principalmente na jurisdição territoriais dos EUA; e aparentar ter a intenção de intimidar ou coagir uma população civil, influenciar a política do governo ou afetar a conduta do governo por destruição em massa, assassinato ou sequestro. Segundo Burney (2007), o texto traz definições vagas que poderiam ser facilmente aplicadas à ativistas ambientais ou pró-aborto, por exemplo. Além disso, ele também destaca que a seção 805 expande a noção de ofensa criminal para incluir “a provisão de ajuda material a terroristas” podendo tornar crime o oferecimento de conselho ou auxílio profissional a qualquer suspeito de terrorismo.

Na prática, o *Patriot Act* permite a utilização, em casos internos, dos procedimentos menos restritos reservados, até então, para casos de espionagem estrangeira. Nos casos criminais domésticos, a seção 206 do *Patriot Act* dispensa o fornecimento de motivo para a investigação, como pede a IV emenda. No geral, ele propicia a neutralização do poder judiciário em questões de vigilância, centrando o poder nas mãos do executivo. (MORT, 2010)

Transitando para os bastidores da elaboração e tramitação do *Patriot Act,* é notável a velocidade com a qual aconteceu, além da aprovação bastante representativa de 98 a 1 no Senado. Aproximadamente um mês e meio após os atentados de 11 de setembro, ele é assinado por Bush após um breve debate de apenas um dia, e não contou testemunho oficial de oposição à lei. Opositores como

[10]Informações como: os números que se telefonaram, por quanto tempo, em qual data.

Feingold – o único senador a votar contra – questionam a pressa na tramitação diante de algo que desbalanceia o equilíbrio de poderes em direção ao executivo e do caráter secreto das atividades. Também apontam que solicitações várias vezes rejeitadas no passado estavam sendo colocadas no *Patriot Act,* aproveitando-se de um momento de exceção e desespero público para obter aprovação de antigos desejos não-autorizados – como explicitamente retratado na referência de Feingold à uma lista de desejos (*wish list)* do FBI. (SCAHILL, 2006, p. 74).

De fato, a pressão para acelerar o processo com pouco debate fez parte de uma estratégia política na qual dois elementos foram centrais: a comunicação estratégica da administração Bush – aqui analisada a partir de falas de Bush e Ashcroft, o procurador-geral – e o reforço da imprensa convencional (*mainstream*) à agenda colocada pelo governo (DOMKE *et al*., 2006). A construção do discurso em torno da Guerra ao Terror foi pautada por seis principais temas: referências esperançosas em relação a um resultado positivo, como "nós venceremos esta guerra" ou "não seremos derrotados"; questões de segurança nacional e de proteção aos cidadãos; o respeito à constituição e a preservação das liberdades civis; referências à união em diversos níveis – popular, partidária, nacional e internacional – ao mesmo tempo como reconhecimento da união em resposta aos ataques, como uma necessidade presente e um objetivo futuro; urgência e necessidade de rapidez nas respostas aos ataques, incluindo frases como "teremos tempo o bastante para revisões no futuro"; e, inserido neste contexto de urgência, apelo à ação do Congresso. Nos anos seguintes, estes mesmos temas serão recorrentes tanto no discurso público quanto na tramitação e argumentação relativa a novos dispositivos legislativos – além de renovação dos antigos, como é o caso do *Patriot Act*.

Em 2003, é vazado um projeto de lei chamado *Domestic Security Enhancement Act* feito sob supervisão de Ashcroft e que propunha medidas tão fortes quanto o *Patriot Act, o* que lhe rendeu o apelido de *Patriot Act II.* O esboço gerou bastante polêmica e críticas, e o documento nunca foi apresentado ao Congresso. Já em 2005, uma matéria do *New York Times* revela a existência de um programa até então desconhecido iniciado a partir de um decreto sigiloso de Bush em 2002, programa que ficou conhecido como *Terrorist Surveillance Program* (TSP), que dispensava a necessidade de autorizações do FISA para vigiar ligações telefônicas nas quais ao menos uma das pessoas estivesse em solo estrangeiro. O funcionamento do programa contava com colaboração entre a NSA e empresas de telecomunicações, como Verizon, AT&T e South Bell em relação a construção de bases de dados

acessíveis pela agência de inteligência e utilizando de filtragem automática de ligações que continham determinadas palavras sensíveis. Tentando remediar os protestos causados pela revelação, o governo propõe o temporário *Protect America Act* de 2007, logo substituído pelo *FISA Amendments Act* de 2008 que autorizava a vigilância de alvos específicos fora dos EUA, – mesmo sendo cidadãos estadunidenses – desde que aprovado pela FISC (MORT, 2010; SOMMER, 2014)

É neste contexto que a aprovação do *Patriot Act* nos EUA pode ser vista como a institucionalização de um paradigma de vigilância preventiva, ao invés de reativa. Esta última abordagem, que se fundamenta sobre a vigilância de alvos identificados como perigosos, foi sendo substituída pela primeira, a qual trata todos os indivíduos como suspeitos a serem constantemente vigiados, que devem a todo momento provar sua inocência. Tal transição é possibilitada devido à aceleração tecnológica a partir da década de 90 – que criam capacidades de execução de vigilância antes inimagináveis, por exemplo, em termos de armazenamento e processamento de dados – e consolidada tendo como base o discurso do combate ao terrorismo pós-11/9 e o desequilíbrio de poderes, com o executivo recorrentemente contornando as restrições impostas pelo legislativo com programas secretos ou novas legislações, em nome da segurança nacional.

1.3 – 2013: As revelações de Edward Snowden

Em 5 de junho de 2013 acontecem as primeiras revelações – das muitas que viriam nos próximos meses – a partir de documentos roubados por Edward Snowden, um empregado da NSA, que descreviam uma série de diretrizes, procedimentos, capacidades e programas conduzidos pela agência em conjunto com a Comunidade de Inteligência (*Intelligence Community – IC*) dos EUA, além das parcerias com outros países[11]. A IC foi criada em 1981 pela Ordem Executiva 12.333[12] de Reagan e engloba 17 agências[13], dentre as quais a NSA e CIA são as mais famosas. A NSA, por sua vez foi

[11]Bauman *et al* (2014) mostram como esta relação acontece num entrelaçamento entre segurança nacional e vigilância transnacional que tem como objetivo o compartilhamento de informações contornando leis que proíbem ou dificultam a espionagem doméstica de cada Estado sobre seus próprios cidadãos.

[12]Disponível em: https://www.cia.gov/about-cia/eo12333.html

criada em 1952 e se tornou a principal entidade responsável pela inteligência de sinais – ou SIGINT (*signals intelligence*) – dentro da IC.

A centralidade dos EUA na infraestrutura mundial de internet e na transação de informações internacionais (ISRAEL, 2019), aliada ao compartilhamento de inteligência com outros países e programas de obtenção de informação por outros meios – com nomes curiosos como PRISM, TURBINE, FOXACID e TEMPORA – permitia aos EUA espionar o mundo a partir de uma coleta massiva de dados, com classificação automática por categorias e diversas outras etiquetas, que seriam acessíveis pelo superbuscador nomeado XKEYSCORE, que é, nas palavras do próprio Snowden (2019, p. 211-212):

> […] talvez melhor entendido como um mecanismo de busca que permite a um analista fazer uma busca por todos os registros de sua vida. Imagine uma espécie de Google que em vez de mostrar páginas da Internet pública retorna resultados de seus e-mails privados, seus bate-papos privados, seus arquivos privados, tudo. […] A NSA descrevia o XKEYSCORE, nos documentos que mais tarde eu transmitiria aos jornalistas, como sua ferramenta "de maior alcance", usada para pesquisar "praticamente tudo o que um usuário faz na Internet".

O XKEYSCORE, como relatado por Kaufman (2013), tinha acesso a dados armazenados em mais de 700 servidores espalhados por aproximadamente 150 locais ao redor do mundo – a maioria em instalações militares e de inteligência dos EUA e aliados, assim como nas embaixadas e consulados estadunidenses.

A obtenção destas informações – conteúdo e metadados[14] – públicas e privadas acontecia de diferentes formas. Duas das principais eram por meio dos programas UPSTREAM e PRISM, ambos autorizados pela seção 702 do FISA, incluída por meio do *FISA Amendments Act* de 2008. A coleta via UPSTREAM se dava por interceptação na infraestrutura da internet como cabos de fibra ótica

[13]Segundo o site da organização chefe da IC, *Office of the Director of National Intelligence (ODNI):* https://web.archive.org/web/20160302190119/http://www.dni.gov/index.php/intelligence-community/members-of-the-ic

[14]Metadados são dados referentes a outros dados. Por exemplo, num envio de mensagem de um celular para outro, o conteúdo é o que foi escrito, enquanto os metadados são: o número que envia, o número que recebe e o horário da mensagem. A princípio podem parecer pouco importante, mas quando coletados em escala massiva acabam sendo até mais valiosos que o próprio conteúdo.

submarinos que transitam informações entre os EUA e o resto do mundo, diretamente na estrutura das organizações provedoras de internet (*Internet Services Providers*) ou até mesmo em satélites. Já o PRISM permitia que a NSA "coletasse dados diretamente dos servidores de empresas estadunidenses como Google, Facebook, Yahoo, Microsoft e Apple, AOL, Skype, YouTube e PalTalk", como descrito no slide vazado no *Washington Post* (FIDLER; GANGULY, 2015, p. 96-99).

No entanto, esta coleta também incluía informações que não possuíam nenhuma relação com segurança nacional ou ameaças terroristas, mostrando o uso indevido dos poderes cedidos à inteligência estadunidense. Pétiniaud (2014) destaca algumas como: espionagem industrial da Petrobrás, conversas telefônicas de Angela Merkel, a ONG de origem francesa *Médecins du monde*, assim como instituições internacionais e ministros de outros países – especialmente ministros de relações exteriores. Os vazamentos causaram diversas reações mundo afora, impulsionando debates sobre privacidade, liberdade e legislação em respeito à descoberta de uma vigilância global com extensão e capacidades. Neste contexto, as revelações de Snowden jogaram luz sobre uma estrutura global de vigilância digital digna de ficções científicas distópicas, a qual foi construída sob um véu de sigilo com seus acordos e práticas confidenciais a partir da aplicação de um paradigma preventivo de vigilância apoiado no discurso da Guerra ao Terror.

Tal estrutura, obviamente, não seria possível sem o imenso avanço técnico que acompanhou o período. Este mesmo avanço técnico é o que possibilitou o surgimento de outras três características – além do caráter preventivo – da vigilância massiva que se forma no século XXI, que talvez não fossem tão perceptíveis em 2001 na época do *Patriot Act*, mas já eram parte integrante dos programas revelados em 2013: granularidade, instantaneidade e algoritmicidade.

A granularidade diz respeito ao nível de especificidade e detalhe na classificação de um dado. Por exemplo, o endereço de uma casa sendo descrito como "Rua dos jequitibás, 290, ap 193 – Campinas, SP" é menos granular que a mesma informação descrita na forma "Rua = jequitibás; Número = 290; Apartamento = 193; Cidade = Campinas; Estado = SP", ou seja, quanto mais granular é uma informação, mais organizada e fácil é de ser tratada com máquinas. Tal característica é facilmente verificada no XKEYSCORE. Seu sistema de filtragem em tempo real e de classificação para busca de informações, que, como descrito nos seus slides e na matéria do *The Guardian* do dia 31 de julho de

2013, permite cruzar as informações entre e-mails e determinados assuntos em seu conteúdo, ou mesmo selecionar e copiar automaticamente todas as pesquisas feitas no Google que buscam por determinada frase (THE GUARDIAN, 2013a, 2013b).

A instantaneidade trata da velocidade destes processos que acontecem praticamente em tempo real – para noções humanas – enquanto a algoritmicidade se refere a julgamentos e decisões sendo tomadas por algoritmos (ou, em outros termos, linhas de instruções escritas por humanos e executadas pelos computadores). Uma combinação das duas fica evidente num outro conjunto de programas da NSA de interceptação de tráfego, que será explicado com um exemplo, na tentativa de evitar o uso de uma linguagem técnica demais. Suponhamos que João more no Brasil e pesquise pelo termo "Osama Bin Laden" no Google. A pesquisa de João atravessa o oceano via cabos de fibra ótica submarinos e chega num servidor do Google localizado na Califórnia. Ao entrar nos EUA, as informações vindas pelos cabos submarinos são coletadas via UPSTREAM – como explicado anteriormente – e passam por uma ferramenta chamada TURMOIL que, caso detecte qualquer informação contendo determinadas palavras chave, a desvia para um outro programa chamado TURBINE, que por sua vez redireciona a informação para servidores da NSA. Aqui, algoritmos decidem qual dos diversos tipos de código malicioso (*malware, exploit*) será utilizado e o enviam de volta ao TURBINE, que injeta o código malicioso no fluxo de dados junto com a resposta à solicitação (*request*) inicial. E o que isso significa para o João é que se o termo "Osama Bin Laden" for uma das palavras-chave, agora João tem em seu computador não apenas uma tela de pesquisa do Google com resultados para o termo "Osama Bin Laden", mas também algum código malicioso que pode desde ter acesso remoto ao seu computador até fazê-lo parar de funcionar, a depender de qual for a escolha dos algoritmos nos servidores da NSA. Tudo isso acontece em fração de segundos com um encadeamento de decisões tomadas por algoritmos, exemplificando o caráter instantâneo e algorítmico do modelo de vigilância utilizado. Este processo está detalhado em documentos vazados da NSA presentes em Fidler e Ganguly (2015, p. 175-180), além de uma explicação menos técnica poder ser encontrada em Snowden (2019, p. 174).

Além da preventividade e destas três características possibilitadas pela aceleração tecnológica – granularidade, instantaneidade e algoritmicidade – há uma quinta que em 2013 ainda estava em plena ascensão: a ubiquidade. Embora Weiser (1991) tenha tratado dela há décadas, houve uma expansão substancial nos anos mais recentes com a disseminação dos *smartphones* e das câmeras de vigilância,

que, como mostram Bankston e Soltani (2014), contribuem para baratear a vigilância e torná-la cada vez mais onipresente, ou ubíqua.

1.4 – Os pilares da vigilância nos Estados Unidos

Contudo, apesar das mudanças técnicas, certas coisas não mudaram, como a necessidade da constante ameaça ao terrorismo como aparato discursivo para sustentar toda esta estrutura de vigilância e a consequente argumentação relativa à necessidade de se abrir mão de liberdades em prol da segurança. É relevante elucidar estes dois pontos que estão presentes em qualquer debate sobre os temas da vigilância dos EUA após os ataques de 11 de setembro, começando pelo último.

Cullather (2015) argumenta que a noção do balanço entre segurança e liberdade nos EUA é uma invenção recente, destacando que o país passou por três grandes crises sem nem citar esta ideia de *trade-off* – A 1ª Guerra Mundial, a Grande Depressão e a 2ª Guerra Mundial – mas utilizando outros caminhos discursivos. Em 1917, o governo Woodrow Wilson aprovou leis de espionagem sob o pretexto de exceção em tempos de guerra, quando seria legítimo abrir exceções que em circunstâncias comuns seriam perigosas. Já Franklin Roosevelt ao pedir ampliação do poder executivo para lidar com a Crise de 1929 e com a 2ª Guerra Mundial, argumentou que a constituição era ampla o bastante para acomodar liberdade e defesa nacional, e que era possível fazer arranjos excepcionais sem perder a forma essencial. Ambos os presidentes violaram as liberdades civis, mas reconhecendo este excesso, se referindo às suas obrigações constitucionais, e dizendo que os direitos seriam restaurados ao normal após o período de exceção.

A palavra segurança (*security*) – e com ela a metáfora do balanço – só apareceria nos anos 40, significando “proteção dos segredos de estado”, ou “o termo das forças armadas para o que a população chama de sigilo (*secrecy*)”, no contexto da Guerra Fria, da ameaça comunista, da era nuclear e de grampeamentos telefônicos feitos pela FBI. E o primeiro uso desta metáfora foi pelo governo Truman, em 1951, ao nomear Chester Nimitz para uma comissão presidencial sobre sigilo e designar a ele a função de “buscar o melhor balanço possível entre segurança e liberdade.”

Este processo acontece como uma substituição para programas de lealdade que estavam em crise com o excesso de acusações maccartistas. Tais programas, iniciados em 1941 por Roosevelt com a autorização do FBI para investigar todos os empregados federais, tinham se tornado alvo de críticas sob alegações de investigações descuidadas e de acusações infundadas. A solução foi então um novo sistema de autorizações de segurança (*security clearance*) em diferentes níveis, com os documentos sendo classificados de acordo com o nível de sigilo, e as pessoas da equipe possuindo diferentes credenciais para acessar tais documentos, conforme posição hierárquica e adequação, que incluía caracterização (*profiling*) psicológica e pesquisas sobre o histórico do indivíduo.

Desta forma, a metáfora do balanço entre liberdade e segurança, foi introduzida para descrever a relação entre o pequeno grupo de pessoas que possuía algum nível de autorização a informações restritas, e o resto da sociedade estadunidense, que foi cada vez mais ficando a parte das práticas do governo esfumaçadas sob um véu de sigilo. Neste sentido, o binômio segurança-liberdade carrega em si um outro: sigilo-transparência.

Transitando para o segundo ponto, Welch (2006) mostra que a exploração de grandes catástrofes para ganhos políticos não é uma prática rara. A administração e manipulação do medo público permitem movimentos impossíveis de serem realizados em circunstâncias comuns. A construção de um discurso em torno do terrorismo após 11/9 segue esta lógica que, por exemplo, foi utilizada pelo governo Bush ao sustentar a invasão do Iraque em 2003 mesmo após não haver evidências do motivo inicial utilizado para a invasão: que o governo de Saddam Hussein teria desenvolvido armas de destruição em massa.

Estratégias discursivas como uma linguagem associada a emoções negativas, falas que alimentam o medo público, o uso de termos vagos e amplos, e sinalizações que lembrem a população que estão vivendo um longo estado de exceção possuem grande eficácia para mantê-la população se sentindo vulnerável, e portanto, mais disposta a aceitar violações de privacidade e liberdade individual (WELCH, 2006, p. 12).

O problema é quando estas mudanças se tornam perenes. Diferentemente dos exemplos citados acima referentes a Franklin Roosevelt e Woodrow Wilson, a guerra ao terror não dá qualquer sinalização sobre estar próxima do fim. (SCAHILL, 2006). Afinal, o próprio discurso de Bush sobre não parar enquanto não "varrer os terroristas" do globo, e suas declarações de uma extensão longa e incerta da guerra, sinalizam um estado de exceção sempre possível de ser alongado, desde que o trabalho de legitimação desta extensibilidade seja feito.

Conjuntamente, também existem questões relativas à perenidade de legislações e práticas adotadas em períodos de exceção. Afinal, quando práticas intensas de vigilância mantidas por longos períodos sofrem tentativas de interrupção, elas tendem a se perpetuar, ainda que com outro formato. Como um evento da história recente nos mostra, após a revelação, em 2005, do programa secreto de espionagem telefônica de Bush (o *Terrorist Surveillance Program*) iniciado em 2002, a pressão pública por seu desligamento ocasionou na verdade a aprovação do *Protect America Act* em 2007, uma medida temporária que seria substituída pelo *FISA Amendments Act* de 2008 (SOMMER, 2014). Mas, em 2013, os documentos vazados da NSA mostraram que apesar das mudanças legislativas, não necessariamente as práticas do TSP foram abandonadas.

Tal aprisionamento em determinadas práticas reforça – e é igualmente reforçado por – uma interdependência entre agentes e instituições difícil de ser modificada. O complexo industrial de vigilância nos EUA, como chama Ünver (2018) em alusão ao complexo industrial-militar, está todo estruturado sobre uma legislação que depende da manutenção da constante ameaça do terrorismo para justificar a violação dos direitos e liberdade civis em prol da segurança, a suposta outra ponta da balança, que tende a ser acompanhada pelo sigilo.

Embora este conflito de valores e discursos sustentem a estrutura de vigilância nos EUA, outros Estados construíram aparatos de vigilância e executam práticas semelhantes utilizando-se de diferentes discursos, apoiados sobre diferentes valores. Veremos como é a aplicação desta estrutura na China, onde encontramos outras características políticas, culturais e sociais.

CAPÍTULO 2 – AS EXPERIMENTAÇÕES CHINESAS DE VIGILÂNCIA E CONTROLE SOCIAL

2.1 – O Sistema de Crédito Social

Antes de entrar na descrição do Sistema de Crédito Social (SCS), é interessante retomar algumas práticas da China sobre o tema de classificação, registro e controle social. Liu (p. 28-29, 2019) aponta três: o sistema de arquivos pessoais (*renshi dang'an*), o status de classe de origem (*jieji chengfen*) e o registro domiciliar (*hukou*).

O Dang'an é um tradicional sistema de registros contendo informações dos cidadãos consideradas relevantes. Dados como histórico de educação e trabalho, prêmios, antecedentes criminais e de más condutas são agregados numa ficha individual, que fica guardada num arquivo do governo. Neste sentido, o SCS pode ser interpretado como uma digitalização e intensificação deste processo de coleta de dados e vigilância.

Porém, as próximas duas tratam de outra camada mais coletiva, à nível populacional: a de classificação de pessoas em diferentes categorias e a utilização desta organização para direcionar oportunidades ou restrições a segmentos da população.

Entre 1950 e 2004, na recente criada República Popular da China sob o comando de Mao Tsé-Tung, tem origem o sistema de "status de classe originária", que contava com 45 rótulos a serem atribuídos aos cidadãos com base nas atividades e no histórico econômico-político do chefe de família no período pré-Mao. Ser rotulado como "trabalhador" ou "camponês", por exemplo, daria mais acesso a recursos sociais e educacionais – sendo Xi Jinping um exemplo destes beneficiados –, enquanto "contrarrevolucionários" seriam estigmatizados e não teriam direito de frequentar educação de nível superior na época da Revolução Cultural (1966-1976).

Já o sistema de registro domiciliar (*hukou*) foi introduzido um pouco mais tarde, em 1958 e funciona até hoje. Cada *hukou* possui duas informações: local de residência registrada e a classificação de habitante rural ou não-rural. Contudo, na prática um *hukou* trazia consigo rotulações morais e socioeconômicas, como um *hukou* "não-rural" ser visto como retrógrado, pobre e pouco instruído. Esta distinção foi abolida em 2016 e o sistema de registro domiciliar chinês vem se tornando menos importante, mas seu impacto ainda persiste, como mostra Siqueira Cassiano (2019) ao trazer o sistema como uma peça de convergência entre três pontos essenciais de cada indivíduo: o nascimento (que exige um pedido de permissão), o documento de identidade e o número de celular. Ao vincular estes marcos da vida de uma pessoa ao *hukou*, cria-se uma rede interligada de informações que inclui as relações familiares, tornando fácil uma política de vigilância e controle que vincula o comportamento individual a impactos não só individuais, mas também a benefícios ou punições a nível familiar. Além disso, o reforço da instituição familiar como um valor essencial do "Sonho Chinês" por parte do Partido Comunista Chinês, na direção de Xi Jinping, termina de completar este panorama. (BAIJIE, 2018).

Adentrando, enfim, a temática principal deste capítulo, é necessário esclarecer possíveis más interpretações do termo 社会信用 (shèhuì xìnyòng). Apesar da tradução ocidental para "crédito social" ser rapidamente associada a uma forma de *credit scoring* expandida para questões extraeconômicas, o termo pode ser interpretado no sentido de uma "confiabilidade social" ou mesmo "confiabilidade pública", ou seja, "crédito" aqui não adquire exclusivamente o caráter econômico-financeiro, mas sua forma mais geral relativa a confiança e credibilidade. Outra palavra muito utilizada é 诚信 (chéngxìn), que pode ser traduzida como honestidade, sinceridade ou integridade. A importância que justifica sua repetição exaustiva no texto vem do fato de ser um dos doze "valores socialistas fundamentais".

Engelmann *et al* (2019) apontam três fatores que influenciam a criação do Social de Crédito Social chinês: o primeiro diz respeito à falta de honestidade e de confiança, evidenciada em envenenamentos por comida, vazamentos de produtos químicos, fraudes financeiras e em telecomunicações e desonestidade acadêmica nos últimos 20 anos, com respaldo em pesquisas de opinião da população, nas quais quase metade aponta o "declínio moral" como maior problema do país.

O segundo trata de crescimento econômico via expansão do mercado doméstico. De pouco mais de 1.4 bilhões de habitantes, apenas 320 milhões possuem histórico de crédito, e 225 milhões nem possuem contas bancárias. Diante de uma economia que na década passada tinha suas transações feitas majoritariamente em dinheiro vivo, o SCS ofereceria uma solução para ceder crédito com base em indicadores não-financeiros para pessoas que não possuem histórico de crédito, possibilitando, assim, uma constância na expansão de seu mercado interno e, consequentemente, contribuindo para o crescimento econômico nacional.

Por fim, as noções chinesas de identidade pessoal e privacidade diferem bastante das ideias ocidentais sobre estes conceitos. Os princípios confucianos sob os quais se assentam parte da moralidade chinesa contribuem para que não haja linhas tão segregantes entre os âmbitos público e privado dos indivíduos, além, é claro da pressão do Partido Comunista Chinês para institucionalizar esta visão, que está inclusive inserida na legislação civil chinesa, segundo a qual informações pessoais só são consideradas privadas – nos termos ocidentais – caso não sejam de interesse público. Logo, esta abordagem abre espaço para intrusão de autoridades públicas e deixa a privacidade na prática desprotegida (CHEN; CHEUNG, 2019, p. 372), ou em outras palavras, evita que o governo tenha que se justificar ou legitimar tais intrusões, pois elas estão em conformidade com a lei.

O "Esboço de Planejamento para a Construção de um Sistema de Crédito Social" (STATE COUNCIL, 2014) é publicado em 2014, pelo Conselho de Estado da República Popular da China e chama a atenção de estrangeiros ocidentais pela curiosa mistura de uma certa espécie de confucionismo com psicologia comportamental. O discurso moral tradicional chinês vem sendo reforçado pela nova esquerda desde a virada do século, sob a proposta da integração das "três tradições" – confucionista, maoista e dengista (ANSHU *et al*, 2018, p. 151). É esta formulação que sustenta a ideia da integridade como uma virtude que justifica um tratamento dos agentes de uma forma behaviorista, condicionados via reforço positivo ou negativo de comportamentos que na prática representam alinhamento com as diretrizes governamentais.

Segundo a própria redação, o sistema tem sua base num requerimento do 18º Congresso Nacional do Partido Comunista para "fortalecer a integridade governamental, comercial, social e

judicial"; além de estabelecer e completar a execução de um sistema de crédito social, que incentive a integridade e puna comportamentos desviantes.

Após estas curtas palavras introdutórias, o documento inicia traçando o panorama para a construção do projeto. Fala sobre a proposta e o estado inicial de desenvolvimento, mas foca principalmente nas deficiências a serem superadas, que envolvem: ineficiência do sistema, falta de interconectividade dos sistemas locais numa plataforma unificada que já foi criada, inconsistência na qualidade da alimentação de informações ao sistema e a não-convergência entre a credibilidade esperada do governo e do sistema jurídico e a visão das massas. Ao que parece, a ideia é buscar uma convergência de crenças e expectativas da população em relação ao governo, por dois caminhos paralelos: aumento da eficiência na organização da sociedade buscando uma estabilidade que almeja à perfeição, e intensificação do abismo entre punição e recompensa como forma de disciplinar a população.

Para justificar o direcionamento das políticas o texto passa por uma contextualização da situação chinesa atualmente, argumentando que um sistema de crédito social é importante para prevenir os riscos de uma economia baseada na credibilidade, como é caracterizada uma a economia de mercado moderna a ser mesclada com o modelo socialista chinês. Outra justificativa apontada é que, devido ao "momento crucial de transformação econômico-social", vem surgindo uma pluralidade de ideias e contradições sociais, que por serem prejudiciais a uma organização social harmônica, podem ser reduzidas por meio de incrementos na confiança mútua entre os membros da sociedade. O trecho seguinte esclarece um pouco melhor a possível raiz desta preocupação:

> Nosso país está em um período de expansão no qual os níveis de abertura da economia estão aumentando numa escala ainda maior, em áreas ainda mais amplos, e em níveis ainda mais profundos. A globalização econômica permitiu um aumento incessante da abertura de nosso país ao mundo, e a interação econômica e social com outros países e regiões está se tornando cada vez mais estreita. O aperfeiçoamento do sistema de crédito social é uma condição necessária para aprofundar a cooperação e o intercâmbio internacional, estabelecendo marcas e reputações internacionais, reduzindo os custos de transação relacionados ao exterior e melhorando o poder brando (*soft power*) e a influência internacional do país, além de ser um requisito urgente para promover o estabelecimento de um sistema de classificação de crédito (*credit rating system*) internacional objetivo, justo, razoável e equilibrado, para se adaptar às

> novas circunstâncias da globalização e (*master*) as novas estruturas globalizadas. (STATE COUNCIL, 2014, Item I.2)

A compreensão deste trecho é indissociável do chamado “Pensamento de Xi Jinping”, referente ao líder chinês, um conjunto de valores e ideais situados à “nova esquerda” e incorporados oficialmente em 2017 que dizem respeito ao projeto de país – e de mundo – que visa orientar e coordenar as decisões chinesas. Um de seus principais expoentes teóricos atualmente é Jiang Shigong (2019), que, ao defender a inevitabilidade de um “império global”, propõe que a China se prepare para tomar a frente, absorvendo num modelo híbrido os erros e acertos do falho modelo soviético e do decadente modelo das democracias liberais, que tem o Reino Unido como propulsor e os Estados Unidos como principal representante atualmente. É neste contexto que o sistema de crédito social aparece como necessário a fim de blindar um núcleo de ideias político-culturais de influências e críticas estrangeiras, as quais certamente virão diante do dito aumento da abertura da economia, que implicitamente é parte do projeto imperialista chinês.

A partir do exposto, ao se considerar a crítica ferrenha feita pela nova esquerda chinesa às democracias liberais, fica evidente que uma das principais preocupações é criar um certo protecionismo de ideias. Ideias estas que podem vir a minar todo o esforço de construção de uma sociedade mais harmônica, nos termos do documento. Afinal, seria bem mais complexo sustentar estes argumentos diante de uma população que, por exemplo, venha a defender como valor inegociável o ideal de liberdade individual.

Seguindo o documento, são apresentados os objetivos centrais do projeto: até 2020, ter estabelecido as leis, regulações e padronizações fundamentais; ter completado um sistema de credibilidade que inclua toda sociedade, com o compartilhamento de recursos como base; ter uma eficaz supervisão de credibilidade e sistemas de gerenciamento; ter um bem desenvolvido sistema de mercado de serviços de crédito; e estabelecer, em nível de plena aplicação, mecanismos de incentivo à confiabilidade e punição da deslealdade. Bem como fazer progressos claros relativos à construção de integridade e confiabilidade em assuntos governamentais, comerciais, sociais e jurídicos, com um aumento substancial nos níveis de satisfação da sociedade e do mercado, a fim de fortalecer um ambiente de credibilidade para o desenvolvimento econômico e social, e obter uma melhoria significativa na ordem econômica e social.

Os fundamentos para atingir tais objetivos são apresentados em quatro blocos, referentes ao papel de coordenação do Estado no processo, numa construção conjunta com a sociedade e dando um certo espaço para os mecanismos de mercado; à estruturação de um sistema legal e à padronização do desenvolvimento dos diferentes sistemas regionais em termos regulatórios, garantindo a segurança das informações, os direitos e interesses dos sujeitos aos quais as informações se referem; ao papel central do planejamento, aliado a uma implementação gradual e constantemente avaliada; e por fim, à priorização de modelos regionais como forma de demonstração e experimentação, e o compartilhamento e interação entre as diversas experiências quanto ao andamento do projeto que busca construir um ambiente de honestidade, autodisciplina e confiabilidade mútua.

O documento apresenta uma linguagem vaga e repetitiva, que parece ter sua função de dar as diretrizes gerais para que projetos-piloto localmente coordenados sejam implementados. De fato, ao não dar definições claras sobre o que é considerado confiabilidade, integridade e outras palavras com conotação moral e maleável, fica a critério dos implementadores atribuir o significado específico ao seu contexto. Por exemplo, é possível supor que a atribuição de sentido a estes conceitos tenderá a ser diferente na capital Pequim, ou mesmo em Hong Kong quando comparadas à região de Xinjiang[15].

É exatamente no caráter não centralizado de implementação que se encontra uma das principais más interpretações sobre o projeto chinês, referente ao fato de existirem múltiplos sistemas de crédito social, ao invés de um único centralizado. O documento do Partido Comunista Chinês realmente aponta para uma progressiva centralização e integração de diversos sistemas locais, mas a realidade parece estar um pouco mais distante disto. Portanto, Liu (2019) propõe alterar a pergunta central que costuma ser feita por quem adentra esta análise, visando transferir o ponto de partida de “O que é o sistema de crédito social chinês?” para “O que são os sistemas de crédito social chineses e como eles funcionam?”

O próprio autor traz uma segmentação entre quatro tipos baseados em duas abordagens. A primeira, liderada pelo Banco Popular da China (BPC), vê o sistema de crédito social (SCS) como uma infraestrutura para atividades econômico-financeiras – nada muito diferente de como fazem os

[15]A província de Xinjiang é casa de uma minoria étnica muçulmana de origem túrquica chamada Uigur. A região é palco de tensões constantes, com o governo central chinês utilizando de discursos antiterrorismo para adotar práticas extremas na província, que constantemente são apontadas como violações dos direitos humanos.

ocidentais nos sistemas de *credit scoring* para indivíduos e corporações. As manifestações desta visão são um sistema nacional de análise de risco de crédito e sistemas de classificação comerciais de crédito, feito por organizações privadas sob supervisão do BPC. Já a segunda abordagem é apoiada na Comissão Nacional de Desenvolvimento e Reforma (CNDR), a agência de gerenciamento macroeconômico sob o Governo Central, e vê o SCS como uma ferramenta de potencial uso para a governança social. Sua implementação se dá em dois níveis: nacional, com listas elaboradas por diversos entes do governo central contendo nomes de pessoas e instituições em *blacklists/redlists*, conforme comportamento descreditado ou admirável; e municipal, com os governos locais sendo supervisionados pelo CNDR.

Em relação a abordagem comercial, supervisionada pelo BPC, é relevante destacar que desde 1990 existem empresas de avaliação de risco de crédito, com foco no comportamento de mercado de empresas e capacidade de honrar suas dívidas. Tais práticas despertaram críticas do BPC, como supervisor. Além disso, em 2017 a licença destas oito empresas vence, e, em vez de renová-las, o governo decide suspender as atividades destas na área de *credit scoring* e criar uma única empresa estatal – Baihang Credit – a ser também a única licenciada para a prática, a fim de evitar problemas de ausência de coordenação e compartilhamento de informações entre as oito empresas, além de aplicações indesejáveis como as já citadas da Ant Financial.

Por outro lado, a evolução da abordagem interessada em governança social acontece em paralelo, tendo em 2015 o lançamento da plataforma nacional – *Credit China* – onde seriam publicados os nomes de indivíduos e instituições nas listas negras e vermelhas (*blacklist/redlist*), sendo a primeira relacionada a comportamentos indesejáveis e a segunda a práticas elogiadas. Logo após seguem as versões municipais, como *Credit Beijing* e *Credit Shangai*. Apesar da sinalização de centralizar as informações num sistema nacional unificado, a questão é que antes disto, há uma dificuldade na integração dos sistemas municipais entre si. Fato este que leva o anúncio conjunto do BPC e da CNDR em 2017 da designação de doze cidades modelo (CREEMERS, 2018, p. 18), a serem utilizadas como referência pelas restantes, buscando uma convergência de práticas e consequente padronização para unificação, como versa um dos objetivos do projeto nacional. Duas destas são Weihai e Rongcheng, cidades portuárias da península de Shandong, no leste da China. A primeira é elogiada pela forma eficiente de acesso ao sistema de informação de crédito, com listas claras sobre recompensas e

punições, além do sistema de ranking para empresas, conforme conformidade com as regulamentações de mercado. Já Rongcheng foi a primeira cidade a iniciar um modelo quantitativo após a publicação do Esboço de Planejamento de 2014 pelo governo central e traz uma classificação dos indivíduos por bandas, conforme sua nota.

Sistemas quantitativos como o de Rongcheng estão concentrados na região da costa leste chinesa em cidades com grande importância econômico-política, que na maioria possuem populações superiores a 1 milhão de habitantes, como Shanghai, Suzhou, Xiamen, Hangzhou, Fuzhou e Shenyang. Os dados costumam vir de agências governamentais e instituições públicas, como órgãos jurídicos, policiais, tributários e geralmente são publicizados Informações de saúde e educação são ausentes em muitos destes, assim como características biológicas, religiosas e socioeconômicas. No entanto, Rongcheng é novamente pioneira em incluir dados de comportamento moral, político, social e até mesmo relações familiares (LIU, 2019, p. 26). Contudo, estas controversas práticas não são novas e tem um correlato num passado recente na província de Jiangsu, vizinha de Shandong ao sul. Ali, em 2010, o distrito de Suining na cidade de Xuzhou, iniciou um projeto que atraiu bastante atenção, incluindo críticas da mídia chinesa, devido ao nível de controle e classificação social almejada. Os cidadãos teriam 1000 pontos de início, e seriam classificados de A a D – além de constantemente reavaliados e suas ações registradas – com base em cumprimento de leis, comportamentos considerados bons ou ruins, exposição pública de pessoas indignas de confiança, e diversas outras práticas que visavam incentivos desproporcionais entre cumprir a ordem e descumpri-la. Uma pessoa “A” teria benefícios que pessoas “D” não teria, como melhores oportunidades de emprego, direito a subsídios e menores taxas em empréstimos.

Então, a partir de uma perspectiva mais detalhada, é possível abordar o projeto de um SCS unificado e interligado como uma iniciativa do Partido Comunista Chinês que, dadas as condições atuais dos múltiplos e diferentes SCSs, dificilmente atingirá seu objetivo no prazo previsto de 2020 – se é que algum dia o atinja. Afinal, o país não é um monólito ideológico livre de tensões, mas contempla uma fragmentação de correntes teóricas divergentes e concordantes em diversos graus do atual Pensamento do Xi Jinping, além de tensões mais práticas a nível institucional, como entre o BPC e a CNDR em relação às diferentes abordagens de SCSs já descritas.

Talvez, inclusive, estas tensões sejam parte da motivação de um projeto tão abrangente de vigilância, como parte da crise de confiabilidade presente no país, uma das principais justificativas. O discurso oficial chinês se apoia sobre valores que são apelativos à sua população, utilizando de tradicionalismos e noções nas quais a unidade é o coletivo, não o indivíduo. Valores reforçados e construídos por meio de uma das mídias mais fechadas do mundo[16] e diversas práticas contínuas de classificação, registro e controle social há, pelo menos, algumas décadas. Parte do esforço do Governo Central parece ser exatamente evitar que estes valores estejam em risco já que, sem eles, a estratégia discursiva utilizada para justificar e legitimar manifestações de controle social – como o SCS – desmoronaria.

De qualquer forma, também é possível enxergar o ambicioso projeto chinês como uma plataforma para experimentações, como uma base de dados histórica sobre diferentes práticas de vigilância. A implementação com coordenação central a partir de práticas locais é bastante poderosa como forma de testar diversos modelos de controle social em pequena escala, para depois se efetuar progressivos ajustes, mescla de práticas bem avaliadas e, por fim, ampliação da escala de aplicação. É importante lembrar que este laboratório chinês conta com um número de potenciais cobaias de quase um bilhão e meio, – representando algo entre um sexto e um quinto da população mundial – o que torna suas experiências e resultados regionais e gerais algo sedutor de ser estudado e aplicado por diversos outros Estados ao redor do planeta, ainda mais com a China tendo interesse nesta internacionalização, como já vem sendo feito em relação ao modelo chinês de internet.

2.2 – A internet na China e o modelo da cibersoberania

Em 1982, o professor alemão Werner Zorn da Universidade de Karlsruhe, por meio de um projeto do Banco Mundial[17], foi o responsável pela chegada de 19 computadores *mainframe* Siemens BS2000 na China, onde o intermédio foi feito pelo professor Wang Yuen Fung, do Institute for Computer Applications (ICA) em Pequim. Pelos próximos cinco anos, os dois encabeçariam uma

[16]Entre 2018 e 2020, China tem estado entre os 5 países com piores indíces de liberdade de imprensa, segundo a ONG Repórteres sem Fronteiras. (Link para o ranking de 2020: https://rsf.org/en/ranking/2020)

[17]*World Bank China University Development Project*. Documento disponível no site do Banco Mundial

cooperação entre seus países que almejava incluir China na CSNET, uma rede internacional de e-mails. Em setembro de 1987, é enviado o primeiro e-mail de China para outros países, por meio da CSNET. A conexão permanente à internet via Estados Unidos só viria em 1994 (ZORN; HAUBEN; PLUBELL, 2014).

Naquele tempo, a internet na china era composta basicamente de serviços de e-mails utilizados por acadêmicos, mas viria a crescer rapidamente nos próximos anos, com a chegada da primeira internet comercial. O aumento de usuários e do fluxo de informações pareceu preocupar o governo, afinal, os protestos – e o massacre – de 1989 na praça Tiananmen ainda eram muito recentes, e esta era uma das lembranças que o Partido Comunista Chinês (PCC) queria apagar da história. Assim, o primeiro-ministro Li Peng assina em Fevereiro de 1996 a *State Council Order 195,* a primeira de uma série de regulações sobre as redes digitais que permitiria ao Estado controlá-las. Neste sentido, desde o princípio da internet na China a vigilância e a censura do Estado estiveram presentes (GRIFFITHS, 2019)[18].

No final de 1997, o Ministro de Segurança Pública aprova a *Computer Information Network and Internet Security, Protection and Management Regulations* (STATE COUNCIL, 1997) que se aplica a toda e qualquer rede e apresenta o ciberespaço como um lugar não desvinculado do território sob o qual o Estado atua, mas como um espaço a ser vigiado. No qual cada indivíduo é responsabilizável pelos seus atos, estabelecendo multas com as devidas quantias monetárias em caso de uso da internet para uma ampla gama de atividades como: causar danos à segurança nacional; atentar contra a constituição; incitar a derrubada do governo e a divisão do país; espalhar rumores ou distorcer a verdade; destruir a ordem da sociedade; promover superstições feudais, materiais sexualmente sugestivos, jogos de azar, assassinatos ou violência; terrorismo ou incitação a atividades criminais; ferir a reputação dos órgãos do Estado; e outras atividades que confrontem a Constituição, as leis e regulações administrativas.

Assim, foi sendo construída a infraestrutura para executar este monitoramento e filtragem. No início, a base tecnológica foi fornecida pela Cisco, empresa do Vale do Silício, e a estrutura não era nada complexa, já que se tratava de um produto existente utilizado por empresas para bloquear o acesso

[18]Capítulo 2

de seus funcionários a determinados sites durante o expediente, de acordo com uma lista de endereços proibidos previamente definida. O que a China fez foi aplicar isto em escala nacional para filtrar o acesso a sites internacionais, resultando numa censura sutil, que retornava ao usuário uma mensagem de “site não encontrado”, a mesma que se obtém com conexões ruins ou quando sites estão fora do ar. Para complementar a filtragem externa, foi também instituído o controle interno das redes via provedores de internet e empresas de tecnologia, cujo nome “Golden Shield” foi dado pelo Ministro da Segurança Pública ao projeto iniciado no ano 2000 (GOLDSMITH; WU, 2006, p.93). Hoje, cada vez mais ambos os projetos vem sendo referidos como *Great Firewall of China*, – que inicialmente se referia apenas a filtragem internacional – termo que remete à censura do ciberespaço feito pela china, a qual tem ficado mais sofisticada. Além dos métodos clássicos de filtragem de endereços IP e URLs, também é efetuada uma inspeção dos pacotes de informação *(packet inspection*) em busca de palavras-chave e marcadores suspeitos. (GRIFFITHS, 2019)

Além de impedir a aparição de determinados conteúdos, o objetivo era também rastrear e punir potenciais ameaças, como mostra o caso de Shi Tao e a Yahoo. Goldsmith e Wu (2006) relatam que em 1999 a empresa estadunidense busca entrar no mercado Chinês. A condição inegociável do Partido Comunista Chinês (PCC) era que a Yahoo filtrasse materiais que pudessem ser ameaçadores ao governo, tornando-a, na prática uma censuradora da internet. Em 2002, a empresa assina o documento *Public Pledge on Self-Discipline for the Chinese Internet Industry* concordando em monitorar a internet doméstica e externa e compartilhar informações com autoridades chinesas. Dois anos depois, Shi Tao, um jornalista chinês envia um e-mail a um fórum baseado nos EUA com um anexo contendo trechos de um documento do PCC que discutia como lidar com possíveis ameaças vindas do aniversário do massacre de Tiananmen, referido no documento como o “evento de 4 de junho” (COMMITTEE TO PROTECT JOURNALISTS, 2005). Apesar de não ser a primeira vez que ele fazia publicações com pseudônimos contendo críticas ao governo, desta vez ele usou seu e-mail do Yahoo, possibilitando as autoridades Chinesas solicitarem legalmente ao Yahoo mais informações sobre o responsável. Desta forma, Shi Tao foi preso por 10 anos.

Esta tentativa de estender os tentáculos de controle de informação à internet era bastante desacreditada na época. A internet, para muitos, carregava uma promessa de um mundo paralelo aos territórios dos Estados nacionais, inacessível ao Estado e suas regulações. John Perry Barlow, deixa

clara este tecno-libertarianismo na sua "Declaração de Independência do Ciberespaço" de 1996, dizendo que os governos não teria "direito nem métodos para controlar" um mundo que "está em todo lugar e em lugar nenhum". Assim, tentar "impedir o vírus da liberdade", de se espalhar – como vinham tentando alguns países como China, EUA, Rússia, Alemanha, França, Itália e Singapura – poderia apenas adiar o contágio, mas não funcionaria num mundo que "em breve será coberto por meios de comunicação que suportam bits". Barlow finaliza com a seguinte frase: "Nós nos espalharemos pelo planeta para que ninguém possa aprisionar nossos pensamentos" (BARLOW, 1996).

É irônico notar que apenas quatro anos depois, o presidente dos EUA, Bill Clinton estaria se apropriando deste discurso para duvidar da empreitada chinesa:

> No século XXI, a liberdade se espalhará por telefone celular e modem a cabo. No ano passado, o número de endereços de Internet na China quadruplicou de 2 milhões para 9 milhões. Este ano, espera-se que o número cresça para mais de 20 milhões. Quando a China aderir à OMC, até 2005, eliminará as tarifas sobre produtos de tecnologia da informação, tornando as ferramentas de comunicação ainda mais baratas, melhores e mais amplamente disponíveis. Sabemos o quanto a Internet mudou os Estados Unidos, e nós já somos uma sociedade aberta. Imagine o quanto ela poderia mudar a China. Agora, não há dúvida de que a China tem tentado controlar a Internet – boa sorte. Isso é como tentar "grudar gelatina na parede" (*nailing jello to the wall*[19]). (CLINTON, 2000)

Ao que parece, tanto Barlow como Clinton estavam errados. O século XXI assistiu a uma crescente projeção dos Estados no ciberespaço, e a China viria a se tornar um modelo de controle das redes a ser exportado e copiado. Lespinois (2017) contribue para a discussão com a classificação de três visões que atualmente co-existem: a libertariana, explicitada na declaração de Barlow sobre um espaço segregado da autoridade do Estado e governado por órgãos comunitários; a liberal, – que pode ser vista no discurso de Clinton – que compreende o ciberespaço como uma "rede de redes sem fronteiras com livre-circulação de dados regida por organismos como ICANN e ISOC[20], baseados nos EUA e subsidiados pelo governo estadunidense" e estando, assim, sob sua influência; e um modelo westfaliano[21] que considera o ciberespaço como um prolongamento do mundo real, sujeito à soberania dos estados nacionais, assim como às competições, cooperações e regulações envolvidas. O modelo

[19]Expressão que se refere a algo muito difícil ou impossível de ser feito.

[20] *Internet Corporation for Assigned Names and Numbers* e *Internet Society*, respectivamente

libertário, diz Lespinois, está hoje em declínio, enquanto o liberal é o principal e o westfaliano vem ganhando espaço.

A China é, sem dúvida, o maior expoente deste último modelo. Em 2010 é publicado um documento intitulado *The Internet in China* (STATE COUNCIL, 2010) dizendo que "dentro do território chinês a internet está sob jurisdicão da soberania chinesa. A soberania da internet – ou cibersoberania – deve ser respeitada e protegida", assim como as diferentes precupações específicas dos diferentes países devem ser respeitadas pelos outros Estados. O documento diz ainda que a administração internacional da Internet deveria ficar sob comando da ONU e que a China apoia o estabelecimento de uma administração justa por meio de procedimentos democráticos em escala global. Uma das preocupações centrais por trás destas linhas era a fraca posição da China na distribuição geográfica de controle da internet, em grande parte centralizada nos EUA por meio de organizações mantenedoras e decisoras sobre protocolos e padrões mundiais, além dos grandes conglomerados privados de tecnologia e da pesquisa e desenvolvimento de tecnologias chave no cenário mundial. No entanto, a explicação oficial desta doutrina seria melhor desenvolvida alguns anos depois no *International Strategy of Cooperation on Cyberspace* de 2017:

> Como norma básica nas relações internacionais contemporâneas, o princípio da soberania consagrado na Carta das Nações Unidas cobre todos os aspectos das relações entre os Estados, o que também inclui o ciberespaço. Os países devem respeitar o direito uns dos outros de escolher seu próprio caminho de ciber-desenvolvimento, modelo de ciber-regulamentação e políticas públicas da Internet, e participar da governança do ciberespaço internacional em pé de igualdade. Nenhum país deve buscar a ciber-hegemonia cibernética, interferir nos assuntos internos de outros países ou se envolver, tolerar ou apoiar ciber-atividades que minem a segurança nacional de outros países (PRC'S MINISTRY OF FOREIGN AFFAIRS, 2017).

Este movimento toma velocidade com a subida de Xi Jinping ao poder. Até então a autoridade sobre estes assuntos era fragmentada entre diversos ministérios, se estendendo até as forças armadas. Em fevereiro de 2014, o novo líder diz que "não há segurança nacional sem cibersegurança" e anuncia

[21]Termo que remete ao Tratado de Westfália, de 1648, que "é unanimemente reconhecido como o marco histórico que estabeleceu e reconheceu o princípio de soberania dos Estados nações sobre seus respectivos territórios e, consequentemente, o preceito de não ingerência extraterritorial, limitando o poder do soberano aos limites internos de suas fronteiras." (ISRAEL, 2019)

que assumirá a presidência do órgão hoje conhecido como *Central Commission for Cybersecurity and Informatization* e criar uma agência subordinada a ele, a *Cyberspace Administration of China* (CAC) com a função de controlar conteúdo online, reforçar a cibersegurança e desenvolver a economia digital. A agência viria a aumentar as restrições e monitoramento no fluxo de informações intervindo em plataformas como WeChat, Tencent e Weibo, Twitter e Bing e em 2018, emitiu novas diretrizes englobando uma ampla gama de serviços online requerendo que mantivessem os registros de informações do usuário, incluindo nomes reais, horários de *login* e *logout*, fonte de rede endereços e tipos de hardware usados. Além disso, a CAC também é responsável por organizar a Conferência Mundial da Internet[22] que acontece, desde 2014, anualmente na cidade de Wuzhen e vem servindo como uma plataforma para dar visibilidade às pretensões chinesas quanto ao ciberespaço (SEGAL, 2020, p.91-93).

Como complemento, afirma Segal (2020, p.93-95), a China tem desenvolvido um sistema sofisticado de legislações e práticas voltadas para o controle da infraestrutura e para a definição de regulações para diversos setores e padrões de proteção da informação, como apontam a *Cyber Security Law*, de 2017 e a *Personal Information Security Specification* de 2018, ao tratar de temas como a redução da dependência externa por meio de uma autosuficiência de infraestrutura, a obrigação do processamento de dados acontecer dentro de território chinês, a imposição de regras e restrições quanto à coleta, processamento e compartilhamento de informações. Tais movimentos podem ser vistos em ação ao Ministério da Indústria e de Tecnologia da Informação multar centenas de empresas por coleta excessiva de dados privados. Em 2014, uma medida emitida pela Comissão Regulatória Bancária da China pedia para que todos os códigos-fonte e protocolos de encriptação utilizados pelos bancos fossem submetidos a reguladores governamentais para testagem e certificação, assim como os obrigava a implementar *backdoors*[23] nos hardwares e softwares utilizados. Já em 2019, PCC deu um prazo de 3 anos para que todos os escritórios governamentais e instituições públicas removessem softwares e hardwares estrangeiros.

[22] *World Internet Conference*

[23] *Backdoors* são métodos de contornar processos de autenticação ou encriptação de um sistema, seja físico ou digital. Uma empresa, ao implementar um *backdoor* para o Estado no seu sistema, na prática permite que este Estado monitore seu sistema, ou que ele acesse o sistema para obter alguma informação desejada.

Durante os anos em que foram lapidados estes conceitos e práticas, os objetivos se mantiveram firmes: promover a independência tecnológica e se contrapor a influência dos EUA e prevenir o fluxo de informações que ameace a estabilidade nacional. No entanto, em relação a este último, cabe o questionamento sobre o que realmente é classificado dentro do vago conceito de "ameaça à estabilidade nacional", afinal, diz Griffiths (2019):

> Uma das coisas mais surpreendentes para estrangeiros sobre a internet chinesa é como ela pode parecer gratuita sob a luz certa. Problemas políticos são discutidos, a corrupção é exposta e criticada, os líderes nacionais são satirizados e a poluição do ar é discutida interminavelmente e longamente. […] Isso pode levar alguns observadores a duvidar da severidade da censura chinesa. […] [No entanto], nada atrairá a atenção da censura e dos serviços de segurança como apelos à solidariedade ou à ação coletiva, e é aqui que residem as verdadeiras fronteiras da Internet chinesa.[24]

Assim, o controle da internet na china visa evitar a união de grupos em torno de um propósito que tenha potencial de se contrapor ao governo. Entende-se então, o temor do governo em relação ao massacre de Tiananmen e a consequente tentativa constante de apagar este evento da história, por ser um evento que tem grande potencial de gerar uma união da população num nível emocional – ou solidário – que culmine em agitações sociais. Aqui se entende, com outros olhos, a prisão de Shi Tao, e o monitoramento constante efetuado pela CAC com suas restrições à internet. O objetivo não é bloquear conteúdos gerais, mas suprimir o quanto antes conteúdos e movimentos estratégicos que carreguem qualquer semente de solidariedade e ação coletiva com um esforço de identificação dos responsáveis e consequente punição.

Desta forma, pode-se concluir que o modelo chinês da cibersoberania, apesar de ainda em construção, já demonstra uma certa maturidade para dar frutos à China e despontar globalmente como uma alternativa aos modelos de internet estadunidense e europeia. A crescente independência tecnológica chinesa permite uma maior proteção de interferências externas e maior possibilidades de agir e se projetar em assuntos internacionais de acordo com seus próprios interesses, com reduzidos temores, por exemplo, em relação a sanções dos Estados Unidos, sejam elas comerciais ou tecnológicas. Além disso o modelo chinês vem sendo impulsionado na última década após a Primavera Árabe e as revelações de Snowden sobre a espionagem global. Em decorrência destes acontecimentos,

[24]O autor desenvolve e retoma esta ideia diversas vezes ao longo do livro, mas este trecho se encontra no Capítulo 6.

vários Estados passaram a olhar o ciberespaço com outros olhos, e a China, principalmente após a subida de Xi Jinping, esteve disposta a oferecer seu conhecimento e exportar suas tecnologias para quem se interessasse. Como vem fazendo ao promover treinamentos sobre gerenciamento de internet e cibersegurança e mostrar ao governo etíope como a China monitora, guia e administra a opinião pública, incluindo as legislações e tecnologias utilizadas; ou simplesmente servindo de exemplo, já que países como Egito, Laos, Paquistão, Uganda, Vietnã e Zimbábue "propuseram ou aprovaram legislação que imita o bloqueio de sites, registro de nome real, compartilhamento de dados e remoção de conteúdo que caracterizam as regulamentações chinesas" com a Tanzânia aprovando uma legislação semelhante à chinesa. Em paralelo, a China vem tendo crescente influência na definição de padrões e protocolos de internet dentro de organismos internacionais, e uma maior adoção de seu modelo por outros países é essencial para pressionar a forma como a internet mundial é definida e organizada. É neste contexto que "a reorganização do ciberespaço em torno da cibersoberania pode não apenas reduzir as vantagens dos EUA, mas também redirecionar para a China os benefícios econômicos, de inteligência e políticos que atualmente fluem em direção aos Estados Unidos" (SEGAL, 2020, p.87; 94-95).

Esta disputa no entanto vem se misturando a uma outra, relacionada a vigilância digital massiva em nome da segurança e da saúde pública global: o combate à COVID-19 durante a pandemia de 2020.

CAPÍTULO 3 – A PANDEMIA E A VIGILÂNCIA SANITÁRIA DIGITALIZADA

Conforme a epidemia do coronavírus foi se alastrando pelo mundo nos primeiros meses de 2020, com ela proliferaram as comparações bélicas. Xi Jinping declarou estar numa "guerra do povo contra um inimigo invisível"[25]. Emmanuel Macron, em 16 de março disse: "Estamos em guerra. Em uma guerra de saúde, é claro. Não estamos lutando contra um exército ou outra nação, mas o inimigo está lá, invisível e insaciável ele avança, e isso requer nossa mobilização geral.[26]". No dia seguinte, Boris Johnson do Reino Unido também seguiu a mesma analogia: "Nós devemos agir como qualquer governo em tempos de guerra" adicionando que "este inimigo pode ser fatal, mas ele também é combatível"[27]. Com Donald Trump, não foi diferente: "Estamos em guerra, enfrentando um inimigo invisível"[28]. Assim como António Guterres, secretário-geral da ONU: "Estamos em guerra com um vírus. E não estamos vencendo"[29]. Já Benjamin Netanyahu, Primeiro-Ministro de Israel, disse que seria necessário utilizar contra a população tecnologias que tem sido usadas no combate ao terrorismo, já que "não havia escolha" diante da necessidade de localizar um inimigo invisível[30].

Tais declarações trazem importantes pontos a serem explorados. O primeiro deles é encarar a pandemia como um estado de exceção, que permite movimentos extremos relativos à vigilância e supressão de direitos e liberdades. O segundo é figura da pandemia como uma guerra contra um inimigo invisível e consequente busca por estratégias para combatê-lo. O terceiro é o uso de ferramentas de inteligência e vigilância contra o vírus, ou em outras palavras, a utilização de tecnologias de guerra contra os próprios cidadãos. Estas três linhas orientam a discussão deste capítulo.

[25](XINHUA, 2020b)

[26]Ver minuto 9:40 do vídeo do anúncio oficial de 16 de março.

[27]Ver minutos 1:56 e 3:47 do vídeo do anúncio oficial de 17 de março.

[28]Trecho do vídeo no *The Guardian*

[29]Transcrição disponível no site da ONU sobre sua fala na Cúpula Virtual do G20 sobre a pandemia, em 26 de março.

[30]Matéria na Reuters, por Lubell (2020)

3.1 – A expansão do poder de policiamento na pandemia

Os discursos acima citados apresentam uma estrutura argumentativa similar àquela utilizada para legitimar vigilância antiterror nos EUA[31], possuindo os mesmos elementos já expostos relativos à necessidade de um motivo grandioso que desperte o medo coletivo e justifique a instauração, a continuidade ou a intensificação de um estado de exceção, e à ideia do balanço entre segurança e liberdade. Apesar das similaridades entre a vigilância justificada pelo terrorismo e a justificada pela pandemia, esta última nos remete às origens dos próprios modelos ocidentais de vigilância, como aponta Foucault:

> Parece-me que, no fundo, no que diz respeito ao controle dos indivíduos, o Ocidente só teve dois grandes modelos: um é o da exclusão do leproso; o outro é o modelo da inclusão do pestífero. E creio que a substituição, como modelo de controle, da exclusão do leproso pela inclusão do pestifero é um dos grandes fenômenos ocorridos no século XVIII (FOUCAULT, 2001, p.55)

Ambos compartilham a prática de se delimitar um território a ser fechado. A partir disto, a exclusão do leproso ocorre por meio da eliminação dos indivíduos infectados para fora deste ambiente fechado, rejeitando-se o leproso com a finalidade de purificar a comunidade. Neste modelo, o poder é exercido por meio de práticas de marginalização, caracterizando a via negativa. No entanto, sua variante é muito mais sofisticada, e o grande fenômeno nesta transição para o modelo da inclusão do pestífero é a "invenção das tecnologias positivas de poder". Aqui, trata-se de observar, de adquirir conhecimento, de trazer para perto os infectados por meio de um policiamento constante que penetra na individualidade em nome da verificação de seu estado de saúde em comparação com a norma estabelecida. Uma análise minuciosa feita por vigias, inspetores, sentinelas, governadores distribuídos nas cidades e suas subdivisões em distritos, quarteirões e ruas, nas quais inspetores passavam diariamente nas casas, janela a janela, conferindo – e registrando – a presença dos cidadãos por meio de uma chamada. Aos nomes que não aparecessem na janela para a chamada seguia-se a suposição de que estavam de cama, logo, doentes, sendo isto alarmante e necessitando uma intervenção. O modelo da inclusão do pestífero, portanto, não diz respeito a uma inclusão inerte, mas a uma que acompanha recorrentemente a adequação à norma, e intervém em casos que fogem à regra. Assim, conclui

[31]Ver Capítulo 1.

Foucault, o momento da peste traz consigo o sonho político de um poder exaustivo, sem obstáculos, que se exerce plenamente e "cujas ramificações capilares atingem sem cessar o próprio grão dos indivíduos, seu tempo, seu habitat, sua localização, seu corpo" (FOUCAULT, 2001, p. 54-65).

As tecnologias positivas de poder se espalham cada vez mais pelo cotidiano contemporâneo, e são certamente as bases da vigilância sanitária na pandemia da COVID-19 embora existam diferenças substanciais. Por um lado, a pandemia de 2020 é a primeira a acontecer em escala global com uma infraestrutura técnica instalada que permite a alimentação, processamento e consumo de informações em tempo real, e por outro, esta mesma infraestrutura possibilita a manutenção de atividades rotineiras como "uma simulação de normalidade por meio de contatos-distantes", como dito por Evangelista (2020).

Lukas Engelmann (2020) destaca que em praticamente toda epidemia da história houve um intervalo temporal considerável entre sua emergência e a consolidação de parâmetros como sua escala, distribuição e dinâmica geral – ofício dos historiadores de pandemia. Na COVID-19 vemos esse intervalo ser reduzido, com a epidemiologia digital oferecendo uma vigilância quase em tempo real, que traz consigo uma ilusão de controle e redução das incertezas por meio do acompanhamento instantâneo do "teatro do contágio global". Isto, no entanto, traz consigo questões políticas e éticas, predições descuidadas e espalhamento acelerado de desinformação, fazendo deste acúmulo de informação uma verdadeira Biblioteca de Babel[32]. Ou seja, o encurtamento do intervalo temporal entre a emergência e a análise crítica acaba por deslocar a vigilância em tempo real e seus resultados para o ambiente das simulações de possibilidades, da dimensão virtual da realidade.

Além disso, a transição das relações sociais para o mundo digital – os "contatos-distantes" – por meio da intermediação técnica talvez seja o sonho político da COVID-19, que de forma alguma contradiz o sonho político da peste, mas o intensifica por meio das novas capacidades tecnocientíficas de se exercer o poder[33]. A digitalização do mundo, que já vinha em crescente aceleração, agora sofre

[32]Alusão à analogia presente no conto do argentino Jorge Luis Borges na qual a infinitude da disponibilidade de todas as possibilidades de combinações de livros acaba por dificultar, diante das limitações humanas, o acesso a informações compreensíveis e significativas.

[33]Não será abordado nesta monografia se estas diferenças apontam para um terceiro modelo ou se são apenas uma intensificação do modelo de inclusão do pestífero. Fernanda Bruno (2020), por exemplo, esboça uma terceira vertente para

uma inflexão diante da oportunidade de acessar a intimidade dos indivíduos com mais granularidade, instantaneidade e ubiquidade[34], permitindo uma caricatura muito mais fiel, e, consequentemente, mais lucrativa – sob o conceito de capitalismo de vigilância como descrito por Zuboff (2019).

Tendo elaborado um panorama sobre pandemia e estado de exceção, nos centraremos agora sobre a metáfora da guerra contra um inimigo invisível, analisando este inimigo e suas estratégias, para depois avaliar a melhor forma de combate.

3.2 – A guerra contra um inimigo invisível e a vigilância como estratégia de combate

Antoine Bousquet, em sua tese de doutorado *The scientific way of warfare: Order and chaos on the battlefields of modernity*, aborda a questão das diferentes formas de se fazer guerra a partir de um "conjunto de ideias e práticas que refletem grandes mudanças ocorridas nos paradigmas científicos e no desenvolvimento tecnológico". Cada uma possui uma abordagem sobre como lidar com ordem e caos na guerra, assim como questões relacionadas como previsibilidade, controle, e o binômio centralização-descentralização. Ele delimita quatro.

A primeira é a mecânica, dominante entre os séculos XVII e XVIII[35], metaforizada na figura do relógio e baseada na ciência linear e num mundo newtoniano-euclidiano. Em seguida, situada entre o fim do século XVIII e a 2ª Guerra Mundial, a termodinâmica, com a metáfora do motor, simbolizando também a industrialização da guerra e o direcionamento cada vez maior da energia como arma – sendo a bomba atômica, por exemplo. Aqui a noção de entropia vinda da segunda lei da termodinâmica representa a inevitável incerteza do mundo que começa a quebrar com as previsibilidades imaginadas e prometidas pelo modelo, dando lugar a uma abordagem probabilística – como na mecânica estatística de Ludwig Boltzmann. A terceira forma, a cibernética, com a figura do computador como unidade

o infectado hiperconectado.

[34]Ver Capítulo 1, Seção 1.3

[35]As escalas temporais por Bousquet são aproximadas e tem função didática, visto que diferentes abordagens se misturam e a vigência de uma nova forma não exclui totalmente as anteriores, podendo uma se apropriar de características das antigas.

central de processamento de informação tem suas origens no período da 2 Guerra Mundial, e as palavras de ordem passam a ser controle, comunicação e comando. A quarta, a caopléxica (*chaoplex*)[36] é metaforizada nas redes distribuídas, englobando conceitos como não-linearidade e auto-organização e tem suas raízes no questionamento de certas características da forma cibernética de guerra já nos anos 60, com grande avanço teórico a partir dos anos 80 (BOUSQUET, 2007, p. 10; 19-21; 44-48; 225-228). Nos centraremos nestas últimas duas.

No paradigma cibernético, a informação tem papel de destaque, devido à crença de que mais informação levaria a mais previsibilidade e controle, contribuindo para o sucesso na batalha. Contudo, o fracasso dos EUA na Guerra do Vietnã utilizando esta estratégia mostrou que tal crença não era necessariamente verdadeira. Na mesma época, a própria cibernética estava passando por mudanças, transitando o foco da estabilidade e da autorregulação para processos de interações dinâmicas entre unidades autopoiéticas[37]. Em paralelo, estavam em ascensão as ciências da complexidade[38] e a teoria do caos[39], que viriam a fundamentar o paradigma caopléxico. (Retomando a discussão sobre cibernética feita na introdução, a primeira fase de Hayles equivale ao paradigma cibernético de Bousquet, enquanto as fases dois e três equivalem ao paradigma caopléxico).

O paradigma caopléxico traz algumas inovações em relação aos anteriores. Em primeiro lugar, a não-linearidade e a sensitividade das condições iniciais, fazem com que pequenas variações iniciais possam gerar imprevisibilidades tremendas. Isto faz com que os conceitos de controle e previsibilidade sejam reformulados – mas não abandonados – para um entendimento mais qualitativo das tendências, principalmente a curto prazo. Além disto, as redes descentralizadas e o *feedback* positivo possibilitam a evolução de sistemas complexos na direção de emergências[40]. Estas mudanças, trazem consigo uma

[36]Junção das palavras *chaos* e *complexity*, se referindo a teoria do caos e às ciências da complexidade. Usarei o termo caopléxico na falta de uma tradução melhor.

[37]Conceitos discutidos na Introdução desta monografia

[38]O termo é utilizado no plural por se tratar mais de um "amplo campo de pesquisa sobre sistemas dinâmicos não-lineares" do que uma teoria científica específica precisamente definida, como destaca Bousquet (2007, p.170).

[39]A diferenciação entre ciências da complexidade e teoria do caos foge ao escopo deste trabalho. Para o uso que será feito aqui, a aglutinação de ambas como "caoplexidade" é suficiente. Em caso de interesse sobre as diferenças, ver o Capítulo 7 de Bousquet (2007).

[40]Emergência é um fenômeno no qual o comportamento de um sistema surge a partir das interações de partes autônomas, de forma que as propriedades do todo não podem ser deduzidas a partir das propriedades das partes.

capacidade de adaptação rápida, característica que torna o paradigma caopléxico flexível para responder a ambientes incertos ou à constantes mudanças (BOUSQUET, 2007, p.177-178).

Um exemplo de organização caopléxica, segundo o próprio Bousquet (2007, p. 197-204), são as redes jihadistas. A estrutura organizacional da Al-Qaeda revela características de descentralização intencional com recursos financeiros e operacionais distribuídos geograficamente em organizações associadas que se auto-organizam. A busca pela estratégia e pelos líderes por trás do 11 de setembro descobriu que a operação tinha sido ainda mais descentralizada do que se supunha inicialmente. O depoimento de Sheik Mohammed[41] – uma das pessoas centrais por trás dos ataques – revela que muitas das pessoas próximas a Bin Laden nunca souberam do plano, e os próprios líderes não possuem todas as informações. Isto aponta para uma rede distribuída de dependência mútua na qual cada jihadista possui informações e recursos relevantes para os outros, enquanto nenhum tem o suficiente para agir isoladamente. Neste sentido, o conjunto pode reagir rapidamente a perturbações sem sobrecarregar um ponto central. A resiliência desta forma de organização parece ter sido posta à prova também, afinal, mesmo após um direcionamento de imensas forças militares e coalizões entre Estados para aniquilar diversos líderes, não se pode dizer que o movimento radical islâmico foi destruído.

Um outro caso que apresenta princípios semelhantes é o “inimigo invisível” da guerra pandêmica. Seu comportamento completamente descentralizado, formado por redes de unidades autônomas resulta em grande adaptabilidade e resiliência. Disto deriva uma capacidade de ataque ininterrupto que é desafiadora. Além disto, não é possível criar uma estratégia de combate direta para que “cada coronavírus do planeta seja encontrado e derrotado” – parafraseando o discurso de Bush contra o terrorismo[42] – devido ao fato de eles serem encontrados exatamente nos corpos das pessoas. Sendo assim, a única estratégia possível é a de um combate indireto ao vírus, direcionado necessariamente aos infectados e seus corpos.

[41]O depoimento (que pode ser encontrado aqui) entitulado *Substitution for the Testimony of Khalid Sheikh Mohammed* é bastante interessante. Principalmente as duas páginas finais, que reproduzem depoimentos escritos por Mohammed com frases como: “Sei que a mente materialista do Ocidente não consegue entender a ideia, que é difícil para eles acreditar que o alto escalão da Al-Qaeda não conheçam as operações realizadas por seus inferiores, mas é assim que funciona. Não enviamos relatórios escritos para nossos superiores” e “Vocês precisam estudar estes assuntos para entender a enorme diferença entre a mentalidade de gestão ocidental e a mentalidade oriental, especificamente na Al-Qaeda”.

[42]Ver Capítulo 1, Seção 1.1.

Esta estratégia pode ser vista como uma espécie de modelo da inclusão do pestífero incrementado pelo modelo caopléxico de Bousquet, pois é exercida vigiando o alvo (não só na materialidade do seu corpo, mas também no nível imaterial por meio dos seus fluxos de informação), olhando-o de perto, comparando-o à norma, enquanto se adquire conhecimento sobre como obter sucesso contra o inimigo sem matar o hospedeiro. O contexto de constante incerteza e sensibilidade quanto às condições iniciais pede por ações rápidas, sendo que a adaptabilidade destas ações também é importante devido à velocidade com que surgem novas informações.

Obviamente, nesta estratégia a hierarquia não desaparece, afinal, no topo está o Estado, ramificando seu poder de policiamento ao nível da intimidade privada do indivíduo – sua casa, sua localização, seu corpo, sua mente, suas relações sociais – por meio das tecnologias de informação e comunicação. Contudo, a mescla de uma estratégia de redes descentralizadas sob uma hierarquia não é necessariamente um problema, e pode, inclusive, ser uma das melhores opções, desde que se resista à tentação de intensificar a centralização e o microgerenciamento[43]. Nas palavras de pesquisadores da RAND Corporation:

> Como observado, a literatura sobre a revolução da informação exige inovações organizacionais para que diferentes partes de uma instituição funcionem como redes interconectadas em vez de hierarquias separadas. [...] A mudança para estruturas em rede pode exigir alguma descentralização de comando e controle, o que pode muito bem ser resistido à luz de visões anteriores de que a nova tecnologia proporcionaria maior controle central das operações militares. Mas a descentralização é apenas parte do quadro; a nova tecnologia também pode proporcionar maior "supervisão" (*topsight*) – uma compreensão central do quadro geral que melhora a gestão da complexidade. [...] A descentralização por si só não é a questão-chave. O emparelhamento da descentralização com a topsight traz os ganhos reais. (ARQUILLA; RONFELDT, 1997, p.30-31)

Centralização e descentralização são extremos de um contínuo e nenhuma prática de guerra se posiciona totalmente em um dos extremos (BOUSQUET, 2007, p.234). Sendo assim, o desafio para qualquer estratégia que transite do comando e controle cibernético para a adaptabilidade e

[43]Tentação que Bousquet diz ser um erro histórico recorrente da hierarquia militar estadunidense (BOUSQUET, 2007, p.218)

distributividade caopléxica se dá no delicado ajuste de onde se posicionar nesta régua, e em como esta mudança será aplicada. No caso do trecho acima a aposta é no gerenciamento da complexidade por meio de uma espécie de supervisão *(topsight).*

Partindo desta opção destacada por Arquilla e Ronfeldt, – caracterizada por *topsight* e descentralização – com alguns incrementos pode-se projetar um modelo realmente potente. Nele, o grande fluxo de informações continua disponível para o alto escalão responsável pelo "gerenciamento da complexidade", enquanto a diferença está na distribuição do controle e na forma de execução. A primeira necessidade é abrir mão de um controle que busca a previsibilidade de um objetivo único e rígido, permitindo-se trabalhar com atualização e análise de cenários de curto ou curtíssimo prazo, com periódica reorganização de parâmetros. Tendo definida esta estrutura, o controle é diluído em dois pontos do sistema: nas unidades semi-autônomas e nas redes que as conectam. No primeiro caso, trata-se de estabelecer um controle indireto sobre as unidades – idealmente sobre cada uma separadamente – por meio da manipulação dos parâmetros que ditam seus ciclos de *feedback*, podendo alterá-los entre positivo e negativo, com variados multiplicadores[44]. No segundo caso, trata-se de uma interferência direta nas redes que interligam as unidades. Um sistema de identificação e filtragem automática da rede pode alterar o fluxo nela por meio de adição, modificação ou remoção de informações. Na escala macro deste sistema, é de grande valia que haja o seu próprio ciclo de *feedback* contendo registros detalhando o histórico de evolução e a situação atual das unidades, da rede e do sistema como um todo. A atualização destes registros torna possível acompanhar as emergências no sistema e tomar decisões sobre quais – e como – interferências serão orquestradas.

Apesar de haver uma certa dose de administração da complexidade neste modelo que mescla entre os paradigmas cibernéticos e caopléxico, ele está longe de ser imune a falhas. Primeiro porque ele estaria sempre sujeito a perturbações inesperadas com efeitos igualmente incertos. Segundo pois, se o objetivo do sistema é fazer ajustes finos nos parâmetros de controle e criar regras automáticas para que a emergência aconteça pela autorreprodução das unidades, a interferência é a exceção, não a regra. E

[44]Matematicamente, a diferença é que num ciclo de *feedback* negativo a entrada é multiplicada por um número menor que um, tornando a saída menor que a entrada, enquanto no *feedback* positivo, a entrada é multiplicada por um número maior que um, tornando a saída maior que a entrada. No primeiro caso, ciclos sucessivos tendem a reduzir cada vez mais a variação causada por uma perturbação, até que ela desapareça e se estabeleça um equilíbrio. No caso positivo, a tendência é de um aumento a cada ciclo.

no caso do *topsight* ser exercido por humanos, é importante lembrar do recorrente erro já citado presente na tentação de microgerenciar e centralizar informação. Por fim, a terceira falha é também a sua própria virtude, uma concepção diferente de controle mais aberta à incerteza, como diz Bousquet (2007, p.176) sobre a abordagem de interação com sistemas complexos, onde a abordagem tradicional de controle preciso e quantitativo deve dar espaço a uma versão mais limitada e com entendimento qualitativo que se baseia numa certa forma de "intuição".

Pesquisadores do Programa de Pesquisa sobre Comando e Controle vinculado ao Departamento de Defesa dos EUA chegam a uma conclusão semelhante:

> Como podemos melhor atingir nosso(s) objetivo(s) de controle? [...] Na Era da Informação, o controle precisa ser pensado e abordado de maneira diferente. O controle, ou seja, assegurar que o comportamento permaneça dentro ou se mova para dentro de limites aceitáveis, só pode ser alcançado indiretamente. A abordagem mais promissora envolve estabelecer, na medida do possível, um conjunto de condições iniciais que resultarão[45] no comportamento desejado. Em outras palavras, o controle não é alcançado pela imposição de um processo paralelo, mas emerge da influência sobre os comportamentos dos agentes independentes (ALBERTS; HAYES, 2003, p.208)

O curioso é que estas estratégias de guerra podem facilmente se assemelhar a outras aplicações. Afinal, esta citação de Alberts e Hayes não ficaria nem um pouco deslocada se inserida no contexto do Sistema de Crédito Social chinês, ou se aplicada à contenção da pandemia onde o controle é igualmente atingido ao influenciar o comportamento de agentes independentes, sem muitas certezas sobre o resultado final, e com imensa dependência de ação rápida frente a grandes sensibilidades iniciais. Foucault (2001, p.59) já dizia que "Entre o sonho de uma sociedade militar e o sonho de uma sociedade empesteada, entre esses dois sonhos que vemos nascer nos séculos XVI-XVII, se estabelece, como vocês veem, uma pertinência".

Observamos então, uma conexão entre a estratégia de guerra caopléxica de Bousquet, a vigilância digital massiva e o sonho político da peste de Foucault. Esta conexão, como veremos a seguir, tem sido apontada como arma essencial no combate à pandemia causada pela COVID-19.

[45]Nota dos autores: Ou tem uma probabilidade arbitrariamente alta de resultar. *(It has an arbitrarily high probability of doing so)*

3.3 – O combate à pandemia

A vigilância sanitária, ao se mesclar com o mundo digital, adentra um território antes restrito às agências de inteligência e, mais recentemente, às empresas de tecnologia. É neste contexto que o "uso de tecnologias antiterrorismo" numa "guerra contra um inimigo invisível" se encaixa, afinal, serviços de inteligência, estado e as forças armadas sempre andaram juntos. Desta forma, agora a vigilância digital massiva ganha, como estratégia central no combate à pandemia, um novo pilar discursivo além do antiterrorismo. A diferença reside na facilidade com que se pode empurrar o balanço entre segurança e liberdade na direção da supressão destas últimas, possibilitando uma ampliação da aplicação de tecnologias de guerra e de inteligência à nível populacional, já que todo e qualquer corpo é passível de infecção.[46]

Segundo Bernard, Bowsher e Sullivan (2020), a inteligência de sinais (SIGINT), tradicionalmente restrita aos estados-nação devido aos altos custos de operação e de análises associadas, é a área que trata da coleta de dados e metadados obtidos a partir de comunicações e dispositivos eletrônicos, como ligações telefônicas, mensagens, e-mails, localização, compras feitas online, informações de saúde geradas por aplicativos de celulares. Contudo, algumas técnicas de SIGINT vêm sendo utilizada no enfrentamento da COVID-19, descritas a seguir.

Primeiramente, a coleta de dados em massa anonimizados[47] e o compartilhamento de dados de localização de usuários entre empresas de telecomunicações e Estados. Os EUA, a União Europeia, o Canadá e a Coreia do Sul têm utilizado este meio para rastrear o cumprimento geral das medidas de

[46]Sobre o discurso antiterrorismo e o balanço liberdade-segurança, ver Capítulo 1.4

[47]A questão da anonimização dos dados é bastante delicada pois, como mostram De Montjoye *et al*. (2013) para dados de mobilidade, com quatro pontos espaçotemporais escolhidos aleatoriamente – e pouco uso de informações adicionais – é possível identificar 95% dos indivíduos por meio de trajetos únicos. Com apenas dois pontos ainda é possível identificar mais de 50% dos usuários. Outra pesquisa mais atual, feita por Rocher, Hendrickx e De Montjoye (2019) demonstram um modelo com o qual "99.98% dos estadunidenses seriam corretamente re-identificados a partir de qualquer conjunto de dados utilizando 15 atributos demográficos".

distanciamento social ou para identificar grandes grupos de indivíduos. Em segundo lugar, o *Geofencing* que, numa definição simples, significa a instituição de perímetro virtual que diz respeito a uma área real. Taiwan e Coreia do Sul utilizaram dados de redes de celulares para alertar autoridades se indivíduos quarentenados saíssem do perímetro permitido, estando sujeito a punições como multas. Por fim, o monitoramento e rastreio por meio de aplicativos de celulares. Grande parte dos países desenvolveram aplicativos que, apesar de variarem em critérios como eficiência, invasividade e obrigatoriedade, têm em comum a execução da antiga prática epidemiológica de rastreamento de contatos (*contact tracing)* numa versão digital que grava – via bluetooth ou geolocalização – os contatos físicos entre pessoas durante sua movimentação para avisá-las caso algum destes contatos venha a testar positivo nos próximos dias. São exemplos: Coreia do Sul, Singapura, Índia, Hong Kong, Romênia, Eslováquia, Polônia e China, o caso mais polêmico devido à centralização e ao cruzamento de informações nas bases de dados do governo.

Tratando especificamente de alguns destes aplicativos, Cascón-Katchadourian (2020, p. 10-12) destaca como o uso do não-obrigatório aplicativo sul-coreano *Self-quarantine safety protection* é complementado com outros métodos de rastreio como dados de geolocalização, rastreio de transações feitas com cartões de crédito e débito e uso de reconhecimento facial em camêras para associar as localizações com o movimento das pessoas, além da capacidade de realizar testes massivos em indivíduos sintomáticos ou que apenas tenham tido contato com pessoas infectadas. Já o aplicativo de Singapura *TraceTogether* se tornou o exemplo de rastreamento via bluetooth – em oposição ao uso da geolocalização – com armazenamento descentralizado nos próprios dispositivos, evitando uma centralização excessiva de dados e servindo de inspiração para o projeto europeu nomeado *Pan-European Privacy-Preserving Proximity Tracing* que traz a proposta de um aplicativo interestatal de acordo com o Regulamento Geral sobre a Proteção de Dados[48] europeu. Em contraposição temos o agressivo modelo israelense mesclando o aplicativo *Hamaguen* – que conta com rastreamento via geolocalização – às tecnologias de espionagem e vigilância em massa da agência de inteligência *Shin Bet*[49] utilizadas primariamente com finalidade antiterrorismo, como intrusão em celulares e outros dispositivos para captar informações, o rastreamento de cartões de crédito, e cruzamento de informações nas suas bases de dados (GROSS, 2020).

[48]Mais conhecido pela sigla GDPR (*General Data Protection Regulation)*

[49]Em Israel, houveram disputas legais vindas do judiciário, de grupos de direitos civis e de grupos palestinos para tentar barrar esta expansão da atuação da *Shin Bet* (KAMPMARK, 2020, p.66; GROSS, 2020)

Ainda assim, nem a Coreia do Sul nem Israel superam a China, onde as plataformas Alipay e WeChat – que intermediam grande parte da vida social, profissional e econômica dos chineses – lançaram o *Health Code,* aplicativo de rastreamento que busca identificar e conter pessoas potencialmente expostas à COVID-19 por meio da agregação de três tipos de dados: informações pessoais como nome, número de identificação nacional e condições físicas (cansaço, febre, tosse seca) que devem ser atualizadas diariamente, com o registro sendo feito por reconhecimento facial, que é exigido para se cadastrar; também são usados dados espaçotemporais obtidos via geolocalização e redes de telefonia por aplicativos de uso rotineiro como os próprios Alipay e WeChat, a fim examinar onde, quando e por quanto tempo as pessoas estiveram, e se passaram por áreas com alto risco de contágio; além disso, transações econômicas online e dados de redes sociais colaboram com mais formas de inserção de dados de movimentação e contato. A partir destas informações, cada usuário recebe um *QR Code* verde, amarelo ou vermelho, atualizado diariamente, que serve como uma espécie de passaporte obrigatório para visitar espaços públicos, usar transportes públicos, viajar e entrar em restaurantes, hóteis e lojas ou mesmo locais de trabalho. Apenas as pessoas com sinal verde são permitidas, pois nos casos de maior risco de contágio – vermelho e amarelo – a pessoa deve ficar de quarentena de 7 a 14 dias, a depender da cor e da cidade (LIANG, 2020).

É importante lembrar que são raros os casos de tecnologias utilizadas no combate à pandemia em que tenham sido criadas para isso. Geralmente são técnicas e infraestruturas já existentes para outros fins que encontram novas possibilidades de aplicação diante do estado de exceção pandêmico. Assim, além do surgimento deste "grande número de aplicativos e sites que fazem uso de dados massivos (*big data*), inteligência artificial, geolocalização de dados e posicionamento de celulares via satélite ou bluetooth" (CASCÓN-KATCHADOURIAN, 2020), também observa-se a expansão do uso de drones com câmeras – sejam elas de vigilância padrão (CCTV, ou *closed-circuit television*), abarcando sistemas de reconhecimento facial ou mesmo câmeras térmicas – apesar de questionamentos e embates relativos à eficácia, adequação e legalidade destas medidas[50].

Drones vêm sendo usados durante a pandemia para diversas atividades como entrega de suprimentos alimentares e médicos em Ruanda, Chile, Gana e China; higienização de grandes espaços

[50]Para uma boa coletânea de artigos introdutórios envolvendo discussões sobre a aplicabilidade destas e de outras medidas, ver a página *COVID-19 and Digital Rights*, da *Electronic Frontier Foundation.*

públicos na Índia, na China e na Coréia do Sul, e, principalmente, vigilância. Utilizados para monitorar o cumprimento de quarentenas ou *lockdowns* e o uso de máscaras por meio de câmeras vinculadas à polícia na França e na Índia, ou ainda com alto-falantes acoplados – chamados de *shout drones* – que reproduziam mensagens gravadas ou falas em tempo real em países como Itália, China, Grécia e Reino Unido[51]. Também houveram usos experimentais na China, Índia, Itália, Omã e Colômbia em relação a drones equipados com câmeras térmicas visando identificar cidadãos potencialmente infectados, apesar de críticas quanto a esta aplicação[52] (INTERNATIONAL TRANSPORT FORUM, 2020; SCHIPPERS, 2020). É curioso notar que a China aparece como exemplo em todas as diferentes aplicações de drones citadas acima. Tal fato não é coincidência, já que ela foi o país pioneiro no emprego de drones no combate à pandemia, servindo de exemplo para outros países, e tem a indústria de veículos aéreos não tripulados (VANTs) indicada como área de desenvolvimento prioritário nacional desde 2013 – indústria que em 2020 está em plena expansão. As mais de 300 empresas fabricantes de VANTs baseadas em Shenzhen, um grande pólo tecnológico chinês, respondem por 70% de mercado global de drones para uso civil. Duas destas empresas, a *MicroMultiCopter Aero Technology* e a *Smart Drone UAV*[53] relatam que seus clientes mais importantes são governamentais (LIU, 2020).

Por outro lado, os próprios agentes governamentais têm sido centrais no estabelecimento destas ferramentas. A empresa Megvii contou com assistência do Ministro da Indústria e Tecnologia da Informação e do governo do distrito de Haidian para desenvolver um sistema de inteligência artificial para medição de temperatura utilizando câmeras termais vinculadas a reconhecimento facial para identificação dos indivíduos. A aplicação, segundo a própria empresa, seria para identificação de altas temperaturas corporais em locais com alta concentração de pessoas, como aeroportos, rodoviárias e estações de metrô. Enquanto no desenvolvimento do *Health Code* houve participação da *China Electronics Technology Group Corporation* – empresa estatal produtora de diversos produtos de uso civil e militar – e de vários departamentos do Estado, além da utilização de dados vindos das áreas de

[51]Os seguintes links levam para vídeos ou matérias sobre os *shout drones* no respectivo país: Itália (*Euronews*), China (*Xinhua*), Grécia (*The Guardian*) e Reino Unido (*The Guardian*)

[52]As câmeras térmicas captam a radiação infravermelha que emana dos corpos, possibilitando – supostamente – a identificação de pequenas variações na temperatura dos corpos humanos, acusando assim, indivíduos em estado febril – um dos sintomas da COVID-19. No entanto, críticos apontam que as câmeras termais podem não ser precisas o bastante para esta finalidade, principalmente se acopladas a drones, como exposto pela *Electronic Frontier Foundation* e por Greenwood (2020)

[53]*Unmanned Aerial Vehicle*, tradução de VANT.

transporte e saúde do governo. (KAMPMARK, 2020, p. 62). De fato, sugere Liu (2020), o *Health Code* mostra que plataformas como o Alipay e o WeChat mediam as relações entre Estado e cidadãos capturando dados pessoais para a vigilância sanitária coordenada pelo setor público.

Este imenso cruzamento de tecnologias e bases de dados levanta questões de privacidade e segurança, assim como questões relativas à eficácia e real necessidade de tanta informação para se combater o vírus. No entanto, há pouca transparência sobre como o *Health Code* é regulado e sobre quem tem acesso a estes dados. Apesar disto, no final de 2020 já se observam movimento de órgãos governamentais chineses da área da saúde pedindo por uma maior padronização nacional do *Health Code* (XINHUA, 2020a) e mesmo sua internacionalização, como propôs Xi Jinping em seu discurso na décima quinta reunião do G20 *Leaders' Summit*, ao dizer que a China propunha "um mecanismo global de reconhecimento mútuo de certificados de saúde baseados em resultados de testes de ácidos nucleicos na forma de *QR Codes* internacionalmente aceitos" e "convidava outros países a participar"[54] (XINHUA, 2020c).

Propostas que, como esta, visam internacionalizar protocolos de vigilância sanitária não são novas, muito menos exclusivas à pandemia da COVID-19. Kampmark (2020) recua à epidemias e pandemias passadas para mostrar como a vigilância e a detecção rápida de infectados se consolidam como essencial para conter surtos, ajudando no planejamento, intervenção e prevenção de doenças. Assim, a história da vigilância é construída associada a "uma promessa de controle de doenças e um espectro de intrusão". Tal intrusão sempre carrega em si um potencial de supressão de declarações e acordos relacionados à individualidade, tanto na legislação internacional como nacional. Afinal, para epidemiologistas e autoridades na área da saúde, salvar vidas e preservar o bom funcionamento do sistema de saúde subordinava outros objetivos e liberdades. A coleta e disseminação de informações sobre infecções são prioridades acima daquelas que tratam de privacidade do indivíduo. Eles enfatizavam, em sua maioria, mais a nobreza da cura do que a transgressão da privacidade. Nas últimas décadas, tal visão foi institucionalizada sob a alcunha da defesa da saúde global:

[54]Tradução livre do trecho original: *China has proposed a global mechanism on the mutual recognition of health certificates based on nucleic acid test results in the form of internationally accepted QR codes. We hope more countries will join this mechanism.*

> [...] o século XXI deu início a outro desenvolvimento, um que enfatiza a biopolítica da saúde global. Tal saúde podia ser observada, medida, calibrada, agregada. Como afirma Katherine E. Kenny, “Os anos iniciais do século XXI testemunharam o surgimento da 'saúde global' como o rótulo preferido para governar a saúde da população global”. [...] A natureza institucional da vigilância global da saúde pode ser localizada nas deliberações da Organização Mundial da Saúde, e particularmente através de seu órgão decisório, a Assembleia Mundial da Saúde. (Kampmark, 2020, p.60)

Desta forma, há uma institucionalização da biopolítica em nome da saúde global e, em sequência, da saúde econômica. Esta é exatamente a visão que Organização Mundial da Saúde (OMS) reproduziu em fevereiro de 2020, ao relatar que “a China efetuou talvez a mais ambiciosa, ágil e agressiva contenção de doenças na história”, um feito “extraordinário para um país com 1.4 bilhões de pessoas”. Destaca também o papel central de tecnologias de ponta neste processo, como *big data*, inteligência artificial e 5G que, por um lado, aumentaram a acessibilidade a serviços de saúde, reduziram a desinformação e minimizaram o impacto de notícias falsas (*fake news*) e, por outro, possibilitaram uma “vigilância extremamente proativa” que foi fundamental para a rápida detecção de casos e diagnóstico, o rastreamento rigoroso e a instituição de quarentena para contatos próximos de infectados, além do alto grau de compreensão e aceitação da população e em relação a estas medidas. Desta forma, outros países precisam “urgentemente ter acesso à experiência chinesa e aos bens materiais que ela fornece para a resposta mundial”. Todavia, diz o relatório, “grande parte da comunidade global ainda não está pronta, tanto em mentalidade quanto materialmente, para implementar as medidas que foram empregadas para conter a COVID-19 na China.” (WORLD HEALTH ORGANIZATION, 2020, p.16-19; 31)

CONSIDERAÇÕES FINAIS

Se os modelos de vigilância de populações tiveram origem em epidemias e foram transplantados para usos políticos e militares, como aponta Foucault[55], pode-se dizer que a pandemia global de 2020 demonstra uma completa harmonia e complementariedade entre a vigilância digital massiva chinesa e a vigilância sanitária em nome da saúde pública global:

> Na vanguarda das sugestões da OMS sobre vigilância em saúde pública, está uma fraternidade competente e agressiva especializada em epidemiologia. Nos últimos anos, aqueles que estudam, identificam e rastreiam surtos virais têm incitado a criação de regimes vigorosos de detecção e vigilância como parte da biopolítica da saúde global. Em 2018, Edward C. Holmes, Andrew Rambaut e Kristian G. Anderson disseram para que "aqueles que trabalham com doenças infecciosas concentrassem fundos e esforços em uma forma muito mais simples e mais econômica de mitigar surtos: uma proativa vigilância em tempo real das populações humanas" (KAMPMARK, 2020, p. 61).

A aproximação entre o Estado vigilante chinês e a epidemiologia global mostra o interesse em comum na execução de um monitoramento preventivo, ubíquo, instantâneo, algorítmico e granularizado, que compartilha das mesmas características que estruturam o modelo estadunidense de vigilância antiterrorista[56]. Esta similaridade aponta para uma confirmação da hipótese inicial desta monografia, de que um menor nível de fricções entre elementos diversos posiciona a vigilância massiva digital chinesa na vanguarda. Além da capacidade técnica, a implementação de dispositivos de vigilância passa também por questões legais, sociais, culturais, econômicas e políticas. Podemos citar, como exemplo a discrepância de desempenho na contenção da pandemia entre China e EUA, apesar de ambos possuírem enormes capacidades técnicas para implementar um ambicioso sistema de vigilância sanitária. A China parece possuir peculiaridades que lhe deram vantagem nesta corrida biopolítica que, junto ao fato de ter sido o epicentro da pandemia, tem a colocado – em conjunto com outros países do sudeste asiático – em posição de destaque no cenário internacional como modelo de práticas eficazes

[55]Ver Capítulo 3.1

[56]Estudado ao longo do Capítulo 1

solucionadoras, principalmente quando o passar do tempo revela uma piora cada vez maior no cenário global de contágio.

Neste contexto, surgem afirmações como “a resposta da China demonstrou ser eficaz, [enquanto] a Europa continua a ficar para trás” (GRIFFITHS, 2020), e comparações feitas entre, por exemplo, as medidas tomadas por Itália e Espanha e as executadas na China e Coreia do Sul, que revelam uma curiosa “dicotomia entre o direito de sair de casa e levar uma vida relativamente normal e o direito à privacidade” (CASCÓN-KATCHADOURIAN, 2020, p.13). São comentários que tocam em pontos tão diversos quanto coordenação de resposta, capacidade de realizar grandes quantidades de testes em curto prazo, e, principalmente, a relação entre a intrusão na vida individual em nome da segurança, evocando a discussão de qual deve ser o balanço entre os direitos individuais e os direitos pelo bem-estar da população (KAMPMARK, 2020, p.63).

Não é exagero afirmar que alguns direitos civis centrados na figura do indivíduo liberal e forjados nas democracias ocidentais constituem travas para a expansão da vigilância digital massiva, independente de qual seja sua finalidade. Observa-se esta tensão desde o sonho político da peste de Foucault, mas também na renovação e expansão da legislação antiterrorismo que permite a vigilância nos EUA, no discurso de balanço entre liberdade e segurança e nas propostas epidemiológicas de intrusão em nome da saúde global. Mas é na China que é possível observar as possibilidades de aplicação da vigilância em seu estado menos obstruído, e a legitimação destes movimentos diante da população – de forma voluntária ou coerciva – é fundamental para isso. Do contrário, não seria possível propor e executar um projeto como o Sistema de Crédito Social, nem construir uma internet sob a doutrina da cibersoberania, ou mesmo executar o combate a pandemia da forma como foi feita pela China.

Fricções entre os ideais de individualidade, liberdade e privacidade e a expansão tecnológica não são novas e pertencem a um movimento mais amplo. Santos (2003b, p.10-11; 17) denomina “virada cibernética” o movimento enraizado na cibernética da década de 1940 e impulsionado a partir dos anos 70 que “sela a aliança entre o capital e as tecnociências”, conferindo a estas últimas a função de “motor de uma acumulação” que “transforma o mundo num inesgotável banco de dados”. Este movimento torna possível – e mais interessante – ao capitalismo disputar mais as “potências,

virtualidades e performances do que as coisas mesmas" como espaços de apropriação e valorização. É este movimento de aceleração tecnocientífica que pressiona quaisquer obstáculos que se coloquem a sua frente, como observa Heiner Müller quanto ao genocídio feito pela Alemanha sob comando nazista:

> [...] a doutrina militar dos nazistas repousava sobre o conceito estratégico de aceleração total. O problema não era a Wehrmacht derrotar o Exército Vermelho ou Rommel derrotar Montgomery. Isso era apenas o aspecto superficial, o teatro da guerra. Ao contrário, sua realidade era totalmente econômica e tecnológica. Tratava-se de experimentar a tecnologia, de introduzir a tecnologia no cotidiano, de tecnicizar a vida. Toda tentativa de aceleração total encontra nas minorias seu principal adversário. Pois as minorias sempre representam algo autônomo; elas são um obstáculo à aceleração. As minorias são freios. Daí nasce a necessidade de aniquilá-las, pois elas persistem em sua velocidade própria (MÜLLER, 1991, p.189 *apud* SANTOS, 2003b, p.22-23).

A aceleração chinesa – ainda que vista como draconiana, autoritária e supressora de direitos civis e humanos – não tem pretensão de eliminar estes freios diretamente, mas por meio um movimento duplo de ressignificar conceitos e instituições vigentes, enquanto, em paralelo, constrói alternativas. Críticas que caracterizem o movimento chinês como destrutor, perdem de vista a estratégia central que é remodelar o significado de autoritarismo, democracia, direitos humanos e civis, subordinando-os a critérios de interesse e segurança nacional. Como vem fazendo ao projetar seu modelo de internet em órgãos e padrões internacionais, exportar sua versão de urbanismo e segurança pública baseada em monitoramento constante e servir de exemplo para moldar as práticas de vigilância sanitária e saúde pública global via OMS. A aceleração chinesa foi edificada sobre os pilares da vigilância digital massiva e da cibersoberania, fazendo com que toda e qualquer segmentação do seu modelo a ser exportado para outros Estados, carrega consigo estes princípios.

Cabe, portanto, explorar como chegamos até aqui. Shigong (2020, p.26-33), em setembro de 2020[57], ao escrever sobre as relações entre Estados Unidos e China[58] coloca o ano de 2008 como um marco que viria a mudar a direção da estratégia chinesa, e dando início à "década crítica" que abriu

[57]A referência às páginas é feita em relação à versão em pdf, disponível no site.

[58]Nota do tradutor: "Outras visões chinesas concorrentes sobre as relações sino-americanas, que considero geralmente mais claras e convincentes, estão disponíveis aqui e aqui. Mas Jiang sempre vale a pena de ser lido tanto em seus próprios termos, quanto por causa de sua proximidade com a liderança central da China."

uma janela de oportunidade estratégica para o desenvolvimento econômico chinês e que teria seu fim em 2018 com a guerra comercial instaurada pelo governo Trump. A crise de 2008 demonstrou à China a fragilidade de se posicionar como "quintal produtivo do mundo", e depender de liquidez e demanda externa, afinal, mesmo mantendo boas taxas de crescimento, o recuo da atividade internacional funcionava como rédeas à expansão chinesa. Foi então que outras estratégias começaram a se formar, as quais, diz Shigong, seriam inevitavelmente encaradas como desafiantes à hegemonia estadunidense. A mudança nas políticas industriais foi marcada pelo plano *Made in China 2025* que tem como objetivo posicionar a China como liderança na produção de tecnologias de ponta. A iniciativa *One Belt, One Road*, que tem raízes numa proposta de Xu Shanda em 2009, mas só foi oficializada em 2015, visa escoar a produção chinesa para não estagnar a economia doméstica e auxiliar o desenvolvimento econômico internacional que, apesar da associação com uma "nova Rota da Seda", se estende também à América Latina e à África, onde a China mantém importantes relações diplomáticas e econômicas. O autor não explicita que, na prática, isto significa projetar poder geopolítico e econômico levando o modelo chinês para outras regiões. Para suprir a necessidade de financiamento desta expansão, é criado o *Asian Infrastructure Investment Bank* (AIIB), que contribue para a internacionalização do renmibi, o terceiro ponto destacado. O renmibi foi incluído pelo Fundo Monetário Internacional a partir de 2016 na cesta de moedas que compõem o Direito Especial de Saque[59], além disso o Centro Financeiro Internacional de Shanghai busca ser a plataforma para projetar o renmibi no mercado financeiro internacional.

Trata-se, portanto, de um movimento conjunto de reestruturação interna da China e da sua posição no cenário global, por meio do estabelecimento de instituições alternativas às instituições centradas no ocidente, aumentando a importância da Ásia. Stuenkel (2016), faz uma boa compilação destas ações[60] e seus contrapontos tradicionais em diversas áreas como finanças, comércio, investimento, segurança, diplomacia e infraestrutura. Vemos, além dos pontos já destacados por Jiang Shigong, alguns exemplos sendo o China Union Pay como alternativa à dupla VISA e MasterCard; a Parceria Regional Econômica Abrangente[61] assinada em novembro de 2020, que coloca a China num

[59]Anunciado em novembro de 2015 no *Press Release* No. 15/540

[60]O autor trabalha estes assuntos nos Capítulos 4 e 5, mas uma boa organização e resumo da discussão pode ser encontrada na página 122.

[61]*Regional Comprehensive Economic Partnership (RCEP)*

acordo de livre-comércio com os 10 países da Associação de Nações do Sudeste Asiático[62], além de Austrália, Japão, Nova Zelândia e Coreia do Sul; o Fórum de Boao para a Ásia complementando o Fórum Econômico Mundial; a Organização para Cooperação de Xangai, com finalidades principalmente securitárias e militares e hoje composta por China, Cazaquistão, Quirguistão, Rússia, Tadjiquistão, Uzbequistão, Índia e Paquistão. Um outro ponto central para a independência tecnológica da China é o sistema de navegação por satélite BeiDou, concluído em 2020, que se coloca como alternativa ao GPS estadunidense, ao Galileo europeu e ao GLONASS russo.

Na Europa, a "Cooperação entre a China e os países da Europa Central e Oriental", também chamada de 17+1 ou China-CEE, foi estabelecida em abril de 2012 como um fórum para tratar de temas econômicos e políticos entre a China e outros dezesseis países[63], que passaram a ser dezessete com a entrada da Grécia em 2019. A iniciativa parece ser uma forma da China gerenciar suas relações exteriores numa escala regional e criar um círculo de influência, que vem dando para Pequim mais benefícios políticos do que econômicos. A projeção dos interesses chineses na Europa, e reproduzidos por países locais, como Sérvia, Grécia e Hungria, é importante para legitimar práticas chinesas e, no caso destes dois últimos países, representá-las na União Européia. Outro fator importante é que a presença da China oferece alternativas aos países, e pode ajudar a segmentar a União Européia, como é notável na fala de Viktor Órban, primeiro ministro húngaro, em 2018: "A Europa Central tem sérias desvantagens a superar em termos de infraestrutura, ainda há muito a ser feito nesta área. Se a União Européia não puder fornecer apoio financeiro, recorreremos à China." (SZCZUDLIK, 2020)

A China também tem se esforçado para ressignificar o conceito de direitos humanos. O entendimento do PCC sobre este tema pode ser encontrado num documento oficial de 1991, entitulado Direitos Humanos na China:

> Sob longos anos de opressão pelas "três grandes montanhas" – imperialismo, feudalismo e burocracia-capitalismo – as pessoas na velha China não tinham direitos humanos dignos de nota. Sofrendo amargamente com isso, o povo chinês lutou por mais de um século, desafiando a morte e os sacrifícios pessoais e avançando onda após onda, em uma árdua luta para derrubar as "três grandes montanhas" e conquistar seus direitos humanos. […] O governo chinês também

[62]Brunei, Camboja, Indonésia, Laos, Malásia, Mianmar, Filipinas, Singapura, Tailândia e Vietnã.

[63]Albânia, Bósnia e Herzegovina, Bulgária, Croácia, República Tcheca, Estônia, Hungria, Macedônia, Montenegro, Letônia, Lituânia, Polônia, Romênia, Sérvia, Eslováquia e Eslovênia.

> apreciou muito a Declaração Universal dos Direitos Humanos. […] Entretanto, a evolução da situação em relação aos direitos humanos é circunscrita pelas condições históricas, sociais, econômicas e culturais de várias nações, e envolve um processo de desenvolvimento histórico. Devido às tremendas diferenças no contexto histórico, sistema social, tradição cultural e desenvolvimento econômico, os países diferem em sua compreensão e prática dos direitos humanos. Portanto, a situação dos direitos humanos de um país não deve ser julgada em total desconsideração de sua história e condições nacionais, nem pode ser avaliada de acordo com um modelo preconcebido ou as condições de outro país ou região. (STATE COUNCIL, 1991)

Nesta visão os direitos humanos não deveriam ser universais, mas definidos internamente e subordinados às peculiaridades de cada país e à sua soberania. Este documento cria as bases do discurso chinês sobre direitos humanos utilizado até hoje, o qual destaca o direito à subsistência – "o mais importante direito humano pelo qual o povo chinês há muito tempo luta" – e o direito ao desenvolvimento, conceitos que contrastam com os estabelecidos na legislação liberal ocidental construída sob os princípios de império da lei (*rule of law*), indivisibilidade e universalidade (OUD, 2020, p.70-73).

A partir de 2012, já é visível a defesa chinesa desta sua visão no Conselho de Direitos Humanos da ONU, em 2017 ela se intensifica, e em 2018 a saída dos EUA abre um vácuo, com a China estando bem posicionada para preenchê-lo. A estratégia chinesa pode ser separada em três itens: intensificar esforços para bloquear as críticas e evitar a responsabilização por seus abusos dos direitos humanos; amplificar os discursos e ideias por meio de aliados e figuras importantes, incluindo o secretário-geral António Guterres, fazendo com que seja cada vez mais difundido o uso da terminologia e dos conceitos chineses – termos como *mutual benefit, win-win cooperation,* e *a community of a shared future for humankind*; e consolidar sua visão em práticas e documentos que institucionalizem uma nova versão dos direitos humanos. Sabendo da resistência oferecida por alguns países, a China vem se posicionando como líder e oradora do Sul global, com o objetivo de trazer para seu lado estes países – ou seus grupos, como o G77 – e obter força númerica nas votações da ONU. Até o momento estas estratégias vêm se mostrando bem-sucedidas. (WORDEN, 2020, p.35-37; 48)

Ainda em relação a órgãos multilaterais, Segal (2020, p. 95-98) aponta como a China tem se mantido constante na proposta de colocar a governança da internet e a regulação do ciberespaço nas

mãos da ONU, a fim de retirar poder de organizações que simbolizam o modelo liberal[64] de internet como o ICANN e a I*nternet Engineering Task Force.* Além disso, Pequim tem se concentrado em definir padrões de novas tecnologias, como o 5G, a internet das coisas e a inteligência artificial, incluindo neste último caso, padrões éticos e de segurança. Também tem suas empresas bastante ativas em fóruns internacionais de estabelecimento de padrões, como no caso do *3rd Generation Partnership Program*, uma coalizão internacional de sete organizações de padrões trabalhando em 5G, havia presença da China em 10 dos 57 cargos de presidência e vice-presidência. Além disso, empresas chinesas como "ZTE, Huawei, Hikvision e Dahua foram as responsáveis por submeter todas as vinte normas relativas à vigilância desde 2016 à União Internacional de Telecomunicações (ITU)."[65]

Portanto, a aceleração chinesa é indissociável da projeção internacional da China e sua crescente influência em outros Estados, em organismos multilaterais e na definição de padrões globais técnicos e legais que versam sobre temas como: o que é e como funciona a internet; como deve ser feita a proteção de dados pessoais; qual é a definição de direitos humanos; ou qual é a melhor maneira de efetuar a contenção de surtos epidêmicos. Junto com isso, vemos as bases da tecnocracia chinesa ganharem espaço. A cibersoberania e vigilância digital massiva à moda chinesa vem pressionando os obstáculos à sua aceleração, inclusive nos EUA. Afinal, se a Grande Muralha do ciberespaço chinês foi feita com "tijolos americanos"[66], assim como as tecnologias que hoje baseiam o aparato de vigilância preventiva, ubíqua, instantânea, algorítmica e granularizada, a China vem demonstrando aos EUA como a aplicação de tecnologias semelhantes num substrato político-cultural diferente pode resultar em poderosas remoções de determinadas rédeas.

Os EUA, então, enfrentam a questão de como se posicionar diante disto. Segal (2020, p.100) trata do tema nas linhas finais de seu artigo ao apontar opções de políticas a serem seguidas:

> A crescente aceitação da cibersoberania representa um verdadeiro dilema político para os formuladores de políticas dos EUA. [...] É difícil proteger a ideia de uma internet aberta, livre e

[64]Conceito apresentado no Capítulo 2.2, referente a classificação de Lespinois (2017) sobre as três visões de ciberespaço.

[65]O autor não explicita, mas é relevante lembrar que a ITU é uma agência da ONU que no passado já teve sérias desavenças com a ICANN, com a ITU sendo apoiada por países alinhados com o doutrina da cibersoberania chinesa, visando reduzir a força dos EUA sobre a internet global, como descrito nos Capítulos 19 e 20 de Griffiths (2019). Para uma visão mais aprofundada sobre normas internacionais e órgãos reguladores, ver Israel (2019), especialmente o capítulo 4.

[66]Termo utilizado por Goldsmith e Wu (2006, p. 93), fazendo referência ao *Great Firewall of China.*

> global quando os próprios Estados Unidos estão considerando a localização de dados, a moderação de conteúdo online e a regulamentação de empresas de tecnologia. Embora Washington possa salientar que estes processos ocorrem de forma transparente e através do império da lei (*rule of law*), para países que enfrentam pressões semelhantes, tais medidas não parecem muito diferentes dos apelos chineses à cibersoberania. Qualquer esforço dos EUA para reduzir a disseminação da cibersoberania requer primeiro um consenso interno sobre como a Internet deve ser regulada, o que não parece provável no atual ambiente de polarização política.

Além disto, os EUA desempenham um papel central na geografia da internet e no modelo liberal de ciberespaço. Desta forma, seu posicionamento – ou sua omissão – é algo bastante relevante no cenário internacional. Porém, estas questões relativas à aceleração chinesa não aparecem apenas no campo de formuladores de políticas, são também utilizadas como argumento no Vale do Silício.

Em abril de 2018, Mark Zuckerberg, do Facebook, disse numa audiência do Senado estadunidense que a legislação em áreas sensíveis como reconhecimento facial deveriam levar em conta a ameaça competitiva representada pelas empresas de tecnologias chinesas para que a regulação não prejudicasse a inovação, "senão nós vamos ficar para trás dos competidores chinesas e outros ao redor do mundo que possuem diferentes regimes para novas funcionalidades como esta"[67].

No entanto, este argumento de "estar ficando pra trás da China" toma outras proporções com Eric Schmidt, antigo CEO do Google e da Alphabet Inc – onde agora atua como conselheiro técnico – e atual presidente do *Defense Innovation Board* e da *National Security Comission on Artificial Intelligence* (NSCAI). Como mostra Naomi Klein (2020), numa apresentação[68] interna da NSCAI de Maio de 2019 – que veio a público por meio da Lei de Liberdade da Informação dos EUA – Schmidt discorre sobre o panorama da tecnologia chinesa num tom alarmista sobre como a China estava ultrapassando os EUA em diversas áreas.

[67]A transcrição completa da audiência pode ser encontrada no Washington Post (2018), assim como o trecho original: o*r else we're going to fall behind Chinese competitors and others around the world who have different regimes for — for different new features like that.*

[68]Disponível diretamente aqui, ou no site do *Electronic Privacy Information Center*, sob o título: *Third AI Commission Production (Mar. 31, 2020), Records Part 9.* Muitos outros documentos interessantíssimos também estão disponíveis no site.

A parte 8 da apresentação[69], entitulada “Inteligência Artificial (IA) / Vigilância / Governo como um consumidor âncora” é iniciada com a seguinte sentença:

> Na imprensa e na política da América e da Europa, a inteligência artificial é colocada como algo a ser temido por estar corroendo a privacidade e roubando empregos. Por outro lado, a China a vê tanto como uma ferramenta para resolver os principais desafios macroeconômicos a fim de sustentar seu milagre econômico e como uma oportunidade para assumir a liderança tecnológica no cenário mundial.

Em seguida, para ilustrar este movimento chinês são citadas duas empresas chinesas (Yitu e SenseTime), destacando como o caminho de ambas até se tornarem “unicórnios”[70] contou com participação essencial de contratos vinculados à área de segurança do governo e departamentos policiais. O envolvimento do Estado seria então essencial no início dos projetos de IA para compensar os custos iniciais até que se adquira escala, a qual, uma vez estabelecida, permite à empresa ampliar seu escopo. Afinal, segundo a apresentação, a vigilância é um dos “primeiros e melhores consumidores” da IA.

Segue-se então uma análise da tecnologia de reconhecimento facial. Apesar do uso inicial de aprendizado de máquina para reconhecimento de imagens ter sido nos EUA, a adoção na China favoreceu um avanço em relação aos EUA por três fatores: ausência de barreiras regulatórias, permitindo mais casos de uso de vigilância; uma imensa base populacional, que neste contexto é sinônimo de mercado consumidor; e enormes bancos de dados governamentais, demonstrando o apoio explícito do governo no setor de tecnologia.

Um próximo slide cita este último fator como central, e se refere à duas supostas bases de dados nacionais: uma contendo 1 bilhão de imagens de rostos de todos os maiores de 18 anos com registro de identificação oficial[71] e outra da polícia chinesa contendo 40 milhões de amostras de DNA – coletadas coercivamente e em grande parte referentes aos Uigures de Xinjiang, onde são gestadas diversas tecnologias de vigilância que serão posteriormente difundidas[72]. A conclusão é que para uma empresa privada seria praticamente impossível se obter bases deste tamanho e fidelidade, assim, a cooperação

[69]Slides 87-99, intervalo no qual se pode encontrar todos os slides citados a seguir.

[70]Termo que se refere a empresas avaliadas em mais de 1 bilhão de dólares.

[71]Matéria de Chen (2017) no South China Morning Post.

público-privada vai além do incentivo financeiro, já que os dados governamentais, coletados sob justificativa de vigilância e segurança pública por exemplo, poderiam ser utilizados para outras finalidades, como construir aplicações em cima desta base, ou treinar algoritmos. Neste sentido, bases de dados estatais são absolutamente poderosas e fornecem uma vantagem competitiva inestimável às empresas de tecnologia. Assim, a vigilância digital massiva é muito valiosa como forma de aquisição de dados.

Para lidar esta competição estratégica contra a China na qual a "IA está no centro" e que o "futuro da segurança nacional e da economia estão em risco", nas palavras de um outro relatório da NSCAI, seriam então necessários "gastos públicos maciços em pesquisa e infraestrutura de alta tecnologia, uma série de 'parcerias público-privadas' em IA e o afrouxamento de uma miríade de proteções de privacidade e segurança". Apesar deste receituário acontecer antes da pandemia de 2020, após o surgimento da COVID-19 estas seriam as mesmas medidas ditas necessárias para combatê-la (KLEIN, 2020). Schmidt acabou estabelecendo uma parceria com o governador de Nova Iorque Andrew Cuomo, na qual sua "iniciativa filantrópica" *Schmidt Futures* vai liderar "uma comissão *Blue Ribbon* do estado, com 16 membros, que utilizará as lições aprendidas com a pandemia COVID-19 para melhorar e modernizar os sistemas estaduais para o futuro", como descrito no próprio site da organização[73].

Atualmente, seja nos EUA ou nos países asiáticos, em regimes mais ou menos democráticos, no Norte ou no Sul global, é possível observar a aceleração técnica aliada ao capital atuando na remoção de seus obstáculos durante o "teatro da pandemia" – para retomar a citação de Heiner Müller sobre o "teatro da guerra". E numa sucessão de teatros que carrega a aceleração nos bastidores, a vigilância digital massiva, preventiva, ubíqua, instantânea, algorítmica e granularizada, vem recebendo cada vez mais atenção conforme múltiplos interesses econômicos, políticos, sanitários e tecnológicos convergem a ela. Exatamente por isso, sua implementação, manutenção ou intensificação parece encontrar intermináveis justificativas em outras peças, outros enredos e outras personagens. Talvez, após o

[72]Base de dados construída com amostra de DNAs provenientes de habitantes de Xinjiang, dissidentes políticos e migrantes (HUMAN RIGHTS WATCH, 2017) feitas com auxílio de conhecimento e tecnologia estadunidense (WEE, 2019). Xinjiang vêm sendo usada como um laboratório de tecnologias e práticas que são posteriormente disseminadas ao restante da China. Sobre isso, ver o Capítulo 17 de Griffiths (2019) e o Capítulo *The Eye* em Strittmatter (2020), por exemplo.

[73]Disponível em: https://schmidtfutures.com/our-method/our-people/

fechamento das cortinas da vigilância pandêmica, vejamos em cartaz títulos como: “Ameaça Terrorista: o retorno”, “O Tabuleiro Geopolítico: EUA x China”, “O Laboratório do Dr. Xi: de Xinjiang para o Mundo”, “O Pacote Anticrime: A Batalha da Segurança Pública”, “A Próxima Peste: Saúde Global em Cheque” e “Direitos Humanos: A Última Fronteira”. A vigilância digital massiva seria, sem dúvida, uma versátil protagonista que se encaixaria a uma miríade de temas por não ser necessariamente vinculada a nenhum.

REFERÊNCIAS BIBLIOGRÁFICAS

AGAMBEN, G. O que é um dispositivo? **Outra Travessia**, n. 5, p. 9–16, 2005. Tradução de Nilcéia Valdati. Disponível em: <https://periodicos.ufsc.br/index.php/Outra/article/view/12576>. Acesso em: 7 jan. 2021.

ALBERTS, D. S.; HAYES, R. E. **Power to the Edge: Command ... Control ... in the Information Age**. Washington, DC: Department of Defense CCRP, 2003.

ANSHU, S.; LACHAPELLE, F.; GALWAY, M. The recasting of Chinese socialism: The Chinese New Left since 2000. **China Information**, v. 32, n. 1, p. 139-159, mar. 2018.

ARQUILLA, J.; RONFELDT, D. F. (EDS.). **In Athena's Camp: Preparing for Conflict in the Information Age**. California: RAND, 1997.

BAIJIE, A. **Family binds nation, its people, Xi says.** 2018. Disponível em: http://www.chinadaily.com.cn/a/201802/22/WS5a8dfb08a3106e7dcc13d42a.html. Acesso em: 2 ago. 2020.

BANKSTON, K. S.; SOLTANI, A. Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones. **The Yale Law Journal Online**, 2014.

BARLOW, J. P. **A Declaration of the Independence of Cyberspace**, 1996 Disponível em: <https://www.eff.org/cyberspace-independence>. Acesso em: 13 dez. 2020.

BAUMAN, Z. et al. After Snowden: Rethinking the Impact of Surveillance. **INTERNATIONAL POLITICAL SOCIOLOGY**, n. 2, p. 121, 2014.

BERNARD, R.; BOWSHER, G.; SULLIVAN, R. COVID-19 and the Rise of Participatory SIGINT: An Examination of the Rise in Government Surveillance Through Mobile Applications. **American Journal of Public Health**, v. 110, n. 12, p. 1780–1785, dez. 2020.

BOUSQUET, A. J. A. **The scientific way of warfare: Order and chaos on the battlefields of modernity.** phd—London School of Economics and Political Science (United Kingdom), 2007.

BROCKMAN, J. (ED.). **Possible minds: twenty-five ways of looking at AI**. New York: Penguin Press, 2019.

BRUNO, F. **Vigilância Digital, Hiperconexão e Pandemia**, 2020. Disponível em: <https://lavits.org/lavits_covid19_14-vigilancia-digital-hiperconexao-e-pandemia/?lang=pt>. Acesso em: 21 nov. 2020

BURNEY, B. The Patriot Act. **GPSolo**, v. 24, n. 5, p. 26-30, 2007.

BUSH, G. W. **Decision points**. New York: Crown Publishers, 2010.

CASCÓN-KATCHADOURIAN, J.-D. Tecnologías para luchar contra la pandemia Covid-19: geolocalización, rastreo, big data, SIG, inteligencia artificial y privacidad. **Profesional de la información**, v. 29, n. 4, p. 1–20, 7 jul. 2020.

CHEN, S. **China plans giant facial recognition database to ID its 1.3bn people**, 2017. Disponível em: <https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any>. Acesso em: 15 dez. 2020.

CHEN, Y.; CHEUNG, A. S. Y. The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System. Vol. 12, No. 2, **The Journal of Comparative Law (2017)** 356-378, University of Hong Kong Faculty of Law Research Paper No. 2017/011. 2017. Disponível em: https://ssrn.com/abstract=2992537 ou http://dx.doi.org/10.2139/ssrn.2992537

CLINTON, B. **Address by Bill Clinton at John Hopkins University on Permanent Normal Trade Relations Status for China**, 2000. Disponível em: <http://www.techlawjournal.com/cong106/pntr/20000308sp.htm>. Acesso em: 13 dez. 2020.

COMMITTEE TO PROTECT JOURNALISTS. **International Press Freedom Awards 2005 - Shi TaoCommittee to Protect Journalists**, 2005. Disponível em: <https://cpj.org/awards/shi-tao/>. Acesso em: 13 dez. 2020

CREEMERS, R. **China's Social Credit System: An Evolving Practice of Control**, 2018. Disponível em: https://ssrn.com/abstract=3175792 ou http://dx.doi.org/10.2139/ssrn.3175792.

CULLATHER, N. Security and Liberty: The Imaginary Balance. In: FIDLER, D. P.; GANGULY, S. (EDS.). **The Snowden reader.** Bloomington, Indiana: Indiana University Press, 2015. p. 19-25.

DE MONTJOYE, Y.-A. et al. Unique in the Crowd: The privacy bounds of human mobility. **Scientific Reports**, v. 3, n. 1, p. 1376, dez. 2013.

DOMKE, D. et al. Going public as political strategy: The Bush administration, an echoing press, and passage of the Patriot Act. **Political Communication**, v. 23, n. 3, p. 291-312, 2006.

ENGELMANN, L. **#COVID19: The Spectacle of Real-Time SurveillanceSomatosphere**, 6 mar. 2020. Disponível em: <http://somatosphere.net/forumpost/covid19-spectacle-surveillance/>. Acesso em: 17 nov. 2020

ENGELMANN, S. et al. **Clear Sanctions, Vague Rewards: How China's Social Credit System Currently Defines "Good" and "Bad" Behavior**. Proceedings of the Conference on Fairness, Accountability, and Transparency – FAT 19. **Anais**. In: THE CONFERENCE. Atlanta, GA, USA: ACM Press, 2019. Disponível em: <http://dl.acm.org/citation.cfm?doid=3287560.3287585>. Acesso em: 28 out. 2020

EVANGELISTA, R. **Aceleração, exceção e ruptura: disputas tecnopolíticas num mundo pandêmico – _comciência**, 2020. Disponível em: <https://www.comciencia.br/aceleracao-excecao-e-ruptura-disputas-tecnopoliticas-num-mundo-pandemico/>. Acesso em: 22 nov. 2020

FIDLER, D. P.; GANGULY, S. (EDS.). **The Snowden reader**. Bloomington, Indiana: Indiana University Press, 2015.

FOUCAULT, M. **Os Anormais: curso no Collège de France, 1974-1975**. São Paulo: Martins Fontes, 2001.

GOLDSMITH, J. L.; WU, T. **Who controls the Internet? illusions of a borderless world**. New York: Oxford University Press, 2006.

GREENWOOD, F. **Fever-Detecting Drones Don't Work**. Disponível em: <https://slate.com/technology/2020/05/fever-detecting-drones-coronavirus-draganfly-research.html>. Acesso em: 10 dez. 2020.

GRIFFITHS, J. **China's Covid success compared to Europe shows lockdowns are the first step, not a solution**. Disponível em: <https://www.cnn.com/2020/10/20/asia/china-europe-coronavirus-intl-hnk/index.html>. Acesso em: 11 dez. 2020.

GRIFFITHS, J. **The great firewall of China: how to build and control an alternative version of the internet**. Ebook ed. London: Zed Books, 2019.

GROSS, J. A. **Shin Bet says it found 500 coronavirus carriers with its mass surveillance**. Disponível em: <https://www.timesofisrael.com/shin-bet-says-it-found-500-coronavirus-carriers-with-its-mass-surveillance/>. Acesso em: 10 dez. 2020.

HAYLES, N. K. **How we became posthuman: virtual bodies in cybernetics, literature, and informatics**. Chicago, Ill: University of Chicago Press, 1999.

HUMAN RIGHTS WATCH. **China: Police DNA Database Threatens Privacy**, 2017. Disponível em: <https://www.hrw.org/news/2017/05/15/china-police-dna-database-threatens-privacy>. Acesso em: 15 dez. 2020.

ISRAEL, C. B. **Redes digitais, espaços de poder: sobre conflitos na reconfiguração da internet e as estratégias de apropriação civil**. Tese (Doutorado em Geografia Humana)—São Paulo: Universidade de São Paulo, 11 fev. 2019.

JAEGER, P. T.; BERTOT, J. C.; MCCLURE, C. R. The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. **Government Information Quarterly**, v. 20, n. 3, p. 295-314, 2003.

KAISER, D. "Information" For Wiener, For Shannon, And For Us. In: BROCKMAN, J. (ED.). **Possible minds: twenty-five ways of looking at AI**. New York: Penguin Press, 2019.

KAMPMARK, B. The pandemic surveillance state: an enduring legacy of COVID-19. **Journal of Global Faultlines**, v. 7, n. 1, p. 59–70, 2020.

KAUFMAN, B. M. **A Guide to What We Now Know About the NSA's Dragnet Searches of Your Communications**, 2013. Disponível em: <https://www.aclu.org/blog/national-security/secrecy/guide-what-we-now-know-about-nsas-dragnet-searches-your>. Acesso em: 8 nov. 2020.

KLEIN, N. **Under Cover of Mass Death, Andrew Cuomo Calls in the Billionaires to Build a High-Tech Dystopia**, 2020. Disponível em: <https://theintercept.com/2020/05/08/andrew-cuomo-eric-schmidt-coronavirus-tech-shock-doctrine/>. Acesso em: 10 dez. 2020.

LESPINOIS, J. DE. La territorialisation du cyberespace : la fin de la mondialisation ? **Prospective et strategie**, v. Numéro 8, n. 1, p. 47–56, 2017.

LIANG, F. COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China. **Social Media and Society**, v. 6, n. 3, 01 2020.

LIU, C. Multiple Social Credit Systems in China. **Economic Sociology: The European Electronic Newsletter** 21 (1): 22-32. 2019. Disponível em: https://ssrn.com/abstract=3423057 ou http://dx.doi.org/10.2139/ssrn.3423057

LIU, Y. **China adapts survey drones to enforce world's largest quarantine**. Disponível em: <https://www.scmp.com/business/china-business/article/3064986/china-adapts-surveying-mapping-delivery-drones-task>. Acesso em: 10 dez. 2020.

LUBELL, M. **Israel to use anti-terror tech to counter coronavirus "invisible enemy"**, 2020. Disponível em: <https://www.reuters.com/article/us-health-coronavirus-israel-idUSKBN21113V>. Acesso em: 21 nov. 2020.

MARIUTTI, E. B. Guerra, Complexidade E Informação: Automação Da Percepção E Os Sistemas Preditivos De Vigilância. **Revista da Escola Superior de Guerra,** v. 35, n. 74, p. 117–137, maio/set. 2020.

MASSARO, L. **Cibernética: ciência e técnica.** Dissertação de Mestrado em Sociologia. Campinas: Unicamp, 2010.

MATURANA, H. R.; VARELA, F. J. **Autopoiesis and cognition: the realization of the living**. Dordrecht, Holland ; Boston: D. Reidel Pub. Co, 1980.

MCCARTHY, J. Review of The Question of Artificial Intelligence. In: ASPRAY, W. Reviews. **Annals of the History of Computing**, v. 10, n. 3, p. 224–229, set. 1988. Disponível em: <https://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=4640964&punumber=5488650>. Acesso em: 7 jan. 2021.

MORT, S. Surveillance des correspondances privées dans le cyberespace aux États-Unis: un contrôle marqué au sceau du secret. **Revue française d'études américaines**, n. 123, p. 33-53, 2010.

MÜLLER , Heiner. "Penser est fondamentalement coupable – Entretien avec Frank M. Raddatz". In: MÜLLER , H. Fautes d'impression – Textes et entretiens. L'Arche, Paris, 1991, Tradução de J. Jourdheuil e J.-F. Peyret. *apud* SANTOS, L. G. (ED.). **Revolução tecnológica, internet e socialismo**. São Paulo, SP, Brasil: Editora Fundação Perseu Abramo, 2003b.

OFFICE, of the Press Secretary. **Adress to a joint Session of congress and the American People**, 2001. Disponível em:

<https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html>. Acesso em: 7 nov. 2020.

OUD, M. **Harmonic Convergence: China and the Right to Development**, 2020. In: An emerging china-centric order China's Vision for a New World Order in Practice. Seattle, Washington: The National Bureau of Asian Research, 25 ago. 2020. Disponível em: <https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/>. Acesso em: 8 dez. 2020.

PERON, A. E. R. Predictive Surveillance Systems and the Dispositif of Precautionary Risk: An Approach on Big Data Technologies in United States' Armed Drones and Policing Activity. **Strife Journal, Issue 10 (Spring 2019)**, p. 66–83, 2019.

PÉTINIAUD, L. Cartographie de l'affaire Snowden. **Herodote**, v. n° 152-153, n. 1, p. 35-42, 20 jun. 2014.

PRC'S MINISTRY OF FOREIGN AFFAIRS. **International Strategy of Cooperation on Cyberspace**, mar. 2017. Disponível em: <https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzfjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml>. Acesso em: 13 dez. 2020

ROCHER, L.; HENDRICKX, J. M.; DE MONTJOYE, Y.-A. Estimating the success of re-identifications in incomplete datasets using generative models. **Nature Communications**, v. 10, n. 1, p. 3069, 23 jul. 2019.

SANTOS, L. G. **Politizar as novas tecnologias: O Impacto sociotécnico da informação digital e genética.** São Paulo: Editora 34, 2003a.

SANTOS, L. G. (ED.). **Revolução tecnológica, internet e socialismo**. São Paulo, SP, Brasil: Editora Fundação Perseu Abramo, 2003b.

SCAHILL, T. The Domestic Security Enhancement Act of 2003: A Glimpse into a Post-PATRIOT Act Approach to Combating Domestic Terrorism. **CR: The New Centennial Review**, v. 6, n. 1, p. 69-94, 2006.

SCHIPPERS, B. **Coronavirus: drones used to enforce lockdown pose a real threat to our civil liberties**, 2020. Disponível em: <http://theconversation.com/coronavirus-drones-used-to-enforce-lockdown-pose-a-real-threat-to-our-civil-liberties-138058>. Acesso em: 8 dez. 2020.

SEGAL, A. **China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace**: an emerging china-centric order China's Vision for a New World Order in Practice. Seattle, Washington: The National Bureau of Asian Research, 25 ago. 2020. Disponível em: <https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/>. Acesso em: 8 dez. 2020.

SHIGONG, J. **The "Critical Decade" in the Sino-American Relationship: the "New Roman Empire" and the "New Great Struggle"**, 2020. Disponível em:

<https://www.readingthechinadream.com/jiang-shigong-ten-crucial-years.html>. Acesso em: 2 dez. 2020.

SHIGONG, Jiang. **The Internal Logic of Super-Sized Political Entities: 'Empire' and World Order.** Tradução de David Ownby. Reading the China Dream, 2019. Disponível em: https://www.readingthechinadream.com/jiang-shigong-empire-and-world-order.html. Acesso em: 11 jun. 2020.

SIQUEIRA CASSIANO, M. China's Hukou Platform: Windows into the Family. **Surveillance & Society**, v. 17, n. 1/2, p. 232-239, 2019.

SNOWDEN, E. J. **Permanent record**. New York: Metropolitan Books/Henry Holt and Company, 2019.

SOMMER, J. FISA Authority and Blanket Surveillance: A Gatekeeper Without Opposition. **Litigation**, v. 40, n. 3, p. 40-46, 2014.

STATE COUNCIL. **Computer Information Network and Internet Security, Protection and Management Regulations**, 1997. Disponível em: <http://lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/computer-information-network-and-internet-security-protection-and-management-regulations-1997.html>. Acesso em: 12 dez. 2020.

STATE COUNCIL. **Human Rights in China.** Information Office of the State Council Of the People's Republic of China, , nov. 1991. Disponível em: <http://www.chinahumanrights.org/html/2014/WP_0724/36.html>. Acesso em: 14 dez. 2020

STATE COUNCIL. **Planning Outline for the Establishment of a Social Credit System (2014-2020)**, 2014. Tradução de Rogier Creemers. Disponível em: https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/. Acesso em: 5 dez. 2019.

STATE COUNCIL. **The Internet in China**, 8 jun. 2010. Disponível em: <https://china.usc.edu/prc-state-council-internet-china-june-8-2010>. Acesso em: 13 dez. 2020

STRITTMATTER, K. **We have been harmonized life in China's surveillance state**. [s.l.] Custom House, 2020.

STUENKEL, O. **Post-western world: how emerging powers are remaking global order**. Malden, MA: Polity, 2016.

SZCZUDLIK, J. **China-Led Multilateralism: The Case of the 17+1 Format**, 2020. In: An emerging china-centric order China's Vision for a New World Order in Practice. Seattle, Washington: The National Bureau of Asian Research, 25 ago. 2020. Disponível em: <https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/>. Acesso em: 8 dez. 2020.

THE GUARDIAN. **XKeyscore: NSA tool collects "nearly everything a user does on the internet"**, 2013a. Disponível em: <http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>. Acesso em: 8 nov. 2020.

THE GUARDIAN. **XKeyscore presentation from 2008 – read in full**, 2013b. Disponível em: <http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation>. Acesso em: 8 nov. 2020b.

TRIBUS, M.; MCIRVINE, E. C. Energy and Information. **Scientific American**, v. 225, n. No. 3 (September 1971), p. 179–190, 1971.

ÜNVER, H. A. **Politics of Digital Surveillance, National Security and Privacy**. Centre for Economics and Foreign Policy Studies, 2018. Disponível em: <https://www.jstor.org/stable/resrep17009>. Acesso em: 30 out. 2020.

WASHINGTON POST. **Transcript of Mark Zuckerberg's Senate hearing**, 2018. Disponível em: <https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/>. Acesso em: 10 dez. 2020.

WEE, S.-L. China Uses DNA to Track Its People, With the Help of American Expertise. **The New York Times**, 21 fev. 2019.

WEISER, M. The Computer for the 21st Century. **Scientific American**, September 1991.

WELCH, M. **Scapegoats of september 11th: Hate crimes and state crimes in the war on terror**. New Brunswick, N.J: Rutgers University Press, 2006.

WORDEN, A. **China at the UN Human Rights Council: Conjuring a "Community of Shared Future for Humankind"?**, 2020. In: An emerging china-centric order China's Vision for a New World Order in Practice. Seattle, Washington: The National Bureau of Asian Research, 25 ago. 2020. Disponível em: <https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/>. Acesso em: 8 dez. 2020.

WORLD HEALTH ORGANIZATION. **Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19)**, 2020. Disponível em: <https://www.who.int/publications-detail-redirect/report-of-the-who-china-joint-mission-on-coronavirus-disease-2019-(covid-19)>. Acesso em: 4 dez. 2020.

XINHUA. **China's health authorities urge universal health code recognition**, 2020a. Disponível em: <http://xinhuanet.com/english/2020-12/10/c_139579767.htm>. Acesso em: 11 dez. 2020.

XINHUA. **Xi Focus: Chronicle of Xi's leadership in China's war against coronavirus**, 2020b. Disponível em: <http://www.xinhuanet.com/english/2020-09/07/c_139349538.htm>. Acesso em: 4 dez. 2020.

XINHUA. **Full Text: Remarks by Chinese President Xi Jinping at 15th G20 Leaders' Summit**, 2020c. Disponível em: <http://xinhuanet.com/english/2020-11/21/c_139533609.htm>. Acesso em: 11 dez. 2020.

ZORN, W.; HAUBEN, J.; PLUBELL, A. **How the Lost E-mail Message 'Across the Great Wall…' Brought People Together**. Karlsruhe: Karlsruhe Institute of Technology, 2014. Disponível em: <https://www.informatik.kit.edu/downloads/HQarticle-08Feb2014-final-version-engl.pdf>

ZUBOFF, S. **The age of surveillance capitalism: the fight for a human future at the new frontier of power**. New York: PublicAffairs, 2019.