Vigilância e privacidade nos tempos do corona: o caso chinês

Surveillance and privacy in corona times: the Chinese case

Vigilancia y privacidad en tiempos del corona: el caso chino

Giulia Neiva Armentano[1]
Maria Beatriz Peixoto Mello[2]
Marina Kronemberger dos Santos[3]

Resumo

Atualmente, acessar a Internet significa deter poder de informação, facilitação, visibilidade e agência no meio social. Contudo, muitos dos serviços oferecidos nesta vêm com um alto preço implícito, "mascarado" de gratuidade justamente porque somos o novo produto dessa era capitalista. O fato de gerarmos dados online sobre nós gera lucros imensos às empresas de tecnologia, o que mesmo trazendo avanços, leva ao questionamento: o que está sendo sacrificado para que essa inovação aconteça? Este artigo busca evidenciar, a partir de um estudo de caso sobre os avanços tecnológicos da China na luta contra o COVID-19, como a privacidade humana é cada vez mais afetada por um aparato de controle e vigilância constante do capital oferecido sob o pretexto de segurança.

Palavras-chave: Vigilância. Internet. Privacidade. Segurança. COVID-19. China.

Abstract

Today, accessing the Internet means accessing the power of information, facilitation, visibility and agency in the social environment. However, many of the services offered on the web come with a high implicit, "masked" price of gratuity precisely because we are the new product of this capitalism era. We generate data about ourselves online and it produces huge profits for technology companies, which although brings advances, raises the question: what is being sacrificed for this innovation to happen? This article aims to analyse, through a case study about China's technological advancements in the fight against COVID-19, how human privacy is increasingly affected by an apparatus of constant

1. Giulia Neiva Armentano é graduada em Relações Internacionais no Instituto de Relações Internacionais da Pontifícia Universidade Católica do Rio de Janeiro (IRI/PUC-Rio). Email: giulianeiva98@gmail.com
2. Maria Beatriz Peixoto Mello é graduanda em Relações Internacionais no Instituto de Relações Internacionais da Pontifícia Universidade Católica do Rio de Janeiro (IRI/PUC-Rio). Email: mariabiamello@gmail.com.
3. Marina Kronemberger dos Santos é graduada em Relações Internacionais no Instituto de Relações Internacionais da Pontifícia Universidade Católica do Rio de Janeiro (IRI/PUC-Rio). Email: marinakronemberger@hotmail.com

control and surveillance of the capital that is offered under the impression of security.

Keywords: Surveillance. Internet. Privacy. Security. COVID-19. China.

Resumen

Actualmente, acceder a Internet significa tener el poder de información, facilitación, visibilidad y agencia en el entorno social. Sin embargo, muchos de los servicios que se ofrecen en web tienen un alto precio implícito, "enmascarado" de gratuidad precisamente porque somos el nuevo producto de esta era capitalista. El hecho de que generemos datos en línea sobre nosotros genera inmensas ganancias a las empresas de tecnología, lo que aunque traiga avances, lleva a la pregunta: ¿qué se está sacrificando para que suceda esta innovación? Este artículo busca exponer, a partir de un estudio de caso sobre los avances tecnológicos de China en la lucha contra el COVID-19, cómo la privacidad humana se ve cada vez más afectada por un aparato de control y vigilancia constante del capital ofrecido bajo el pretexto de la seguridad.

Palabras clave: Vigilancia. Internet. Privacidad. Seguridad. COVID-19. China.

Introdução

Vivemos em um mundo onde aqueles sem uma conta de e-mail são invisibilizados, mas principalmente onde as redes sociais e a Internet em geral tornam a ansiedade soberana. Nessa "civilização da informação", os dados são um produto para comércio (ZUBOFF, 2018). Se você possui uma conta de e-mail, rede social, aplicativo de transporte, entretenimento, relacionamento ou mesmo bancário, muito provavelmente suas informações pessoais estão sendo comercializadas sem o seu consentimento nesse instante. Em troca, você recebe os "melhores" resultados nos sites de pesquisa, bem como o bombardeio diário de mais de 5 mil propagandas no seu *feed*. A este processo, de acordo com Shoshana Zuboff (2018), é dado o nome de "capitalismo de vigilância".

Essas condições de vigilância dos dados digitais e individuais se fazem cada vez mais presentes no nosso cotidiano e nas vidas dos indivíduos – nos nossos corpos, gestos, desejos e hábitos (YU, 2020). Todavia, apesar dessas formas de vigilância estarem imbuídas no nosso dia a dia,

> (...) tudo parece tão fluido, escorregadio e difícil de agarrar. Na verdade, parece corresponder à própria qualidade dos relacionamentos que caracterizam uma cultura orientada para o consumidor – em mutação divina e fluindo em canais e condutos em constante mudança. Isso tem sido chamado de 'vigilância líquida' (BAUMAN et al., 2014, p. 141, tradução nossa)[4].

4. "(...) it all seems so fluid, slippery, and hard to grasp. Indeed, it seems to match the very quality of relationships characterizing a consumer-oriented culture — fissiparous mutating, and flowing in ever-changing channels and conduits. This has been called 'liquid surveillance'".

Logo, é uma "vigilância líquida", cautelosa, que se faz presente de maneira silenciosa nas nossas vidas, de forma que seja minimamente percebida e naturalizada nas nossas relações individuais e sociais.

Se esse capitalismo de vigilância modificou a maneira como nos entendemos e nos relacionamos enquanto sociedade, essas tecnologias de controle da população por meio dos dados geram tensão entre a privacidade individual e a segurança, o que têm implicações tanto para as práticas e ferramentas de segurança nacional quanto para o domínio da segurança internacional (BAUMAN et al., 2014). Ademais, outro movimento de tensão presente nesta conjuntura de vigilância em massa é a rearticulação dos limites e fronteiras entre Estados e entre as esferas pública e privada, de modo que se desestabiliza essas noções historicamente estabelecidas (ABRAHAMSEN & WILLIAMS, 2009; BAUMAN et al., 2014).

E o debate sobre o aprofundamento de técnicas de vigilância na sociedade atual acaba se ampliando quando surge o coronavírus (COVID-19) em 2019 e a pandemia é declarada em 2020. Nesta conjuntura de um "estado de exceção sanitário" (AGAMBEN, 2020) para controle de um vírus altamente contagioso, o combate à pandemia inclui cientistas da computação e especialistas de dados (*big data*) na formulação de estratégias (WINTOUR, 2020). Assim, "(...) a vigilância digital é uma forma particularmente eficaz de controle social durante uma pandemia global porque atinge as pessoas no nível de seus corpos, gestos, desejos e hábitos" (YU, 2020, p. 3, tradução nossa)[5].

Com a pandemia, diversos Estados no mundo todo implementaram ou ampliaram programas de vigilância que, para a *Human Rights Watch* (BROWN & TOH, 2021), permitem uma intromissão sem precedentes na privacidade das pessoas. Nesse sentido, o presente trabalho se propõe a discutir o papel da vigilância de dados no atual contexto da pandemia do COVID-19 e como isso afeta a segurança em nível global. O estudo é realizado a partir de uma pesquisa exploratória, por meio de um estudo de caso sobre a China: um caso expressivo por conta da articulação entre o setor privado e o domínio estatal na formulação de práticas, técnicas e tecnologias de vigilância.

5. "(...) digital surveillance is a particularly effective form of social control during a global pandemic because it takes hold of people at the level of their bodies, gestures, desires and habits".

Desse modo, em primeiro lugar abordamos as técnicas de vigilância utilizadas por grandes corporações do campo digital e pelo Estado sobre uma nova conjuntura de dificuldade de uma clara distinção entre os domínios público e privado, além dos efeitos diretos sobre a privacidade individual. Em um segundo momento, adentramos no caso específico da mobilização de dados pelo Estado chinês por meio do sistema de crédito social, que estava previsto de ser implementado em 2020. Discutimos como o uso de aplicativos para coleta de dados pessoais no atual contexto pode ser ampliado para um espectro de vigilância muito mais amplo, levando em consideração as possíveis consequências sobre a privacidade e segurança. Por fim, concluímos este artigo com uma exposição sobre a questão da privacidade de dados no contexto do coronavírus, bem como um questionamento acerca dos desafios que tais inovações impõem em um futuro próximo.

O digital que cada vez mais toma conta das nossas vidas: a articulação entre o público e o privado no controle da privacidade

De acordo com Shoshana Zuboff (2018), o capitalismo de vigilância se refere a um ciclo na lógica de acumulação mediada por computador: em primeiro lugar, mediante a ação do usuário, o dado é produzido e posteriormente, coletado e analisado, para então, retornar ao usuário como propaganda. Logo, à medida que cada vez mais objetos e tarefas cotidianas como educação, trabalho e lazer estão conectadas à Internet, maior é a padronização dos indivíduos – ou melhor, dos usuários – e, consequentemente, há a perda das subjetividades (ZUBOFF, 2018, p. 27-34), em um processo caracterizado pela violação sistêmica da privacidade individual.

A autora descreve como, num curto período de operação, a Google foi a principal responsável por definir as bases desse modelo econômico, se consolidando como pioneira do capitalismo de vigilância. Isto se deve principalmente à pressão dos investidores por maiores lucros e à oposição dos líderes quanto a cobrança pelo serviço de busca, fazendo com que a empresa se voltasse para um modelo de propaganda – e "[se] torn[asse] a maior e mais bem-sucedida empresa de *big data* por ter o site mais visitado e, portanto, possuir a maior quantidade de *data exhaust*" (ZUBOFF, 2018, p. 24-5; 32).

Em outras palavras, a geração de publicidades "com precisão e sucesso cada vez maiores" viabilizada pelo uso dos "dados de usuários

como matéria-prima para análise e produção de algoritmos", levou a um aumento expressivo das receitas da Google. E, assim, "aumentava a motivação para uma coleta de dados cada vez mais abrangente. A nova ciência de análise de *big data* explodiu, impulsionada em grande parte pelo sucesso retumbante da Google" (ZUBOFF, 2018, p. 32).

Conforme a tecnologia avança em um ritmo desenfreado, há o surgimento de uma nova arquitetura de poder, um novo tipo de autoritarismo que elimina a agência do sujeito, pois participar desse processo não é mais uma ação, uma escolha, é um resultado, um efeito do capitalismo de vigilância (ZUBOFF, 2018). De acordo com Zuboff,

> Como resultado da penetrante mediação por computador, quase todos os aspectos do mundo são traduzidos em uma nova dimensão simbólica à medida que eventos, objetos, processos e pessoas se tornam visíveis, cognoscíveis e compartilháveis de uma nova maneira. O mundo renasce como dados e o texto eletrônico é universal em escala e escopo (ZUBOFF, 2018, p. 23-24).

Ademais, quando se trata da esfera do mercado, nesse sentido, o texto eletrônico é previamente organizado pela lógica de acumulação, que produz suas próprias relações sociais e, consequentemente, suas concepções e usos de autoridade e poder (ZUBOFF, 2018, p. 22). Assim sendo, a autora defende que estamos vivendo um novo momento civilizatório marcado por uma imensa assimetria de poder e pelo fim das subjetividades. Isto é, na "civilização da informação", o texto eletrônico é a linguagem do poder e o *Big Data* é a mercadoria que garante poder aqueles que a detém (ZUBOFF, 2018). Como Zuboff e Rotenberg defendem, em última instância, trata-se da perda do Estado democrático, pois, sob constante vigilância, vive-se em uma prisão (SHAW, 2017; ZUBOFF, 2018).

Tal processo de observação contínua conta com um controle externo, remoto e subliminar disperso a partir das redes sociais graças aos avanços tecnológicos atuais. Esse monitoramento aparentemente imperceptível poderia ser rapidamente identificado pela população caso ela se questionasse acerca dos reais objetivos por trás de medidas à primeira vista demasiadamente vantajosas aos usuários. Contudo, essa indagação não é comum. Pelo contrário, o que se vê cada vez mais é uma alienação aos propósitos das grandes empresas privadas de tecnologia devido a uma acomodação generalizada aos benefícios oferecidos por elas. Como afirmado por Jean Guisnel no prefácio do livro "Tous fliqués! La vie privée sous surveillance" de Reg Whitaker, ...

> o indivíduo, em seu prazer por evoluir num universo tecnológico, não se preocupa em saber, e menos ainda em compreender, que as máquinas gerenciam seu dia a dia. Que cada um de seus atos e gestos é gravado, filtrado, analisado e, eventualmente, vigiado. Que, longe de libertá-lo de seus obstáculos físicos, a informática da comunicação constitui a ferramenta de vigilância e de controle mais incrível que o ser humano jamais pode criar (GUISNEL, 2001, p. XI).

Todavia, essa conjuntura de mecanismos de vigilância da vida individual por meio de entidades e corporações privadas não significa o fim da estrutura do Estado nacional. Na verdade, é uma rearticulação dos limites e divisões entre os domínios público e privado. As distinções entre o público e o privado estão cada vez mais confusas:

> Por um lado, vemos uma interação complexa entre agências públicas e privadas, não menos agências corporativas e de mercado de capitais, ao invés de uma cidadania liberal; por outro lado, vemos evidências de redes complexas de agências de inteligência e segurança que parecem ter alcançado considerável autonomia tanto do Estado quanto da sociedade civil (...), tanto da soberania do Estado quanto da soberania popular (BAUMAN et al., 2014, p. 136, tradução nossa)[6].

Para Rita Abrahamsen e Michael C. Williams (2009), a racionalidade das corporações privadas – lógicas de defesa da globalização e do neoliberalismo – é internalizada para dentro dos domínios públicos e estatais, em que o Estado pode até assumir ativamente uma posição de defesa dos processos de globalização e neoliberalização, que implicam no desmonte da esfera pública.

Essa interação pode ocorrer em diversos campos, como o domínio da segurança. A diluição das fronteiras entre Estado e setor privado no campo da segurança, para Abrahamsen e Williams, gera assemblages globais da segurança ("global security assemblages"), cenários onde "agentes globais e locais, públicos e privados de segurança e suas normatividades interagem, produzindo novas instituições, práticas e formas de governança da segurança" (Abrahamsen & Williams, 2009, p. 3, tradução nossa). Portanto, não é um processo de simples transferência de funções públicas para atores privados, mas é um desenvolvimento das relações entre segurança e Estados soberanos com entidades privadas, em que há uma mis-

6. "On the one hand, we see a complex interaction between public and private agencies, not least agencies of corporate and market capital rather than of liberal citizenship; and on the other, we see evidence of complex networks of intelligence and security agencies that seem to have achieved considerable autonomy from both state and civil society (...), from both state sovereignty and popular sovereignty".

tura entre as estruturas de poder político e de autoridade com as operações do capital global.

E nesse contexto de diluição das fronteiras entre público e privado, a vigilância ocupa um importante espaço:

> A interseção complexa entre o público e o privado é mais aparente no ciberespaço do que em qualquer outro lugar. Há aqui tanto intimidade quanto presença pública. Entretanto, é o íntimo que prevalece, independente do fato do sujeito das práticas ciber comunicativas ser completamente consciente do ciberespaço que, enquanto tal, é aberto ao mundo, vulnerável ao olhar do outro, do hacker, do marketeiro, ou até mesmo do Estado. O 'ser digital'' (...) é o ser conectado e em rede, presente neste terreno distinto de interação social, um espaço desenhado e habilitado por códigos em rede que não reconhecem fronteira a não ser a técnica (BAUMAN et al., 2014, p. 138, tradução nossa, grifo nosso)[7].

Dessa forma, as práticas de vigilância de dados contam com uma forte interação e cooperação entre os setores público e privado, "as diferentes dimensões de segurança, orquestradas por agências governamentais, mas habilitadas pela cooperação com corporações digitais" (BAUMAN et al., p. 143, tradução nossa).

Os Mecanismos de Vigilância do Estado Chinês

Segundo a *Human Rights Watch* (2021), o governo chinês já cometeu diversos abusos de direitos humanos sob o pretexto de garantia de maior segurança pública e sanitária frente a pandemia do COVID-19. Contudo, tais ações não estão restritas ao cenário atual. Pelo contrário, a China já vinha desenvolvendo sistemas de vigilância que controlam diariamente a vida de seus cidadãos há anos.

Em 2018, um mecanismo que começou a ser implementado pela startup Watrix para atuar em conjunto com o já presente sistema de reconhecimento facial foi um software de identificação do indivíduo pelo seu andar, não importando se o rosto está visível à câmera ou se a pessoa está de costas (El País, 2018). Outro exemplo seria a atuação conjunta

7. "The complex intersection of the public and the private is nowhere more sharply apparent than in cyberspace. There is here both intimacy and a public presence. However, it is the intimate that prevails, irrespective of the fact that the subject of cyber-communicative practices is fully aware that cyberspace, as such, is open to the world, vulnerable to the gaze of the stranger, variously the hacker, the marketeer, or even the state. 'Digital being' (...) is connected and networked being, present in this distinctive terrain of social interaction, a space drawn and enabled by networked codes that recognize no boundary as such except the technical".

da OpenPower Foundation – liderada por executivos da Google e IBM – com a empresa chinesa Semptian e a americana Xilinx no desenvolvimento de microprocessadores para aumentar a eficácia do processamento de alto volume de dados, permitindo um monitoramento online e sigiloso de mais de 200 milhões de habitantes (GALLAGHER, 2019).

Todavia, o mecanismo de vigilância que se mostrou mais expressivo e no qual focamos no presente artigo, é o Sistema de Crédito Social chinês, o qual leva esse controle constante para outro nível ao atingir todos os aspectos da vida social. Segundo Mareike Ohlberg, pesquisadora do Mercator Institute for China, em entrevista para a revista Wired (KOBIE, 2019, p. 2, tradução nossa), esses usos e abusos de dados para mapeamento do comportamento humano "não são um 'fenômeno chinês'. Mas caso [o sistema chinês] se concretize como o planejado, ainda assim seria algo muito único. É ao mesmo tempo único, mas parte de uma tendência global".

Após um período de testes desde 2014 em algumas regiões da China, o sistema de crédito seria finalizado em 2020 e a partir de então implementado em todo o país. Todavia, com a pandemia da COVID-19, o sistema não foi oficialmente implementado, mas o país emitiu em dezembro de 2020 as diretrizes para o desenvolvimento do seu sistema de crédito social (REUTERS, 2020).

Com o intuito de verificar a credibilidade tanto de cidadãos como de empresas, o sistema consiste em uma extensa e variada coleta de dados desses atores, principalmente do seu comportamento online, já contando com a participação de mais de 40 governos locais e iniciativas semelhantes de forma independente por parte de grandes empresas chinesas, como a Alibaba e a Tencent (ZYLBERMAN, 2020). O trabalho em conjunto com companhias privadas se dá pelo objetivo de desenvolver tecnologias e algoritmos necessários para a operação desse sistema de processamento de dados em larga escala, que forja o sistema de crédito social (TIMOFEEVA, 2020).

O governo chinês apresenta que o principal propósito da introdução desse sistema de crédito é promover o "valor da honestidade" na sociedade chinesa. Portanto, os créditos sociais são um meio de "mensuração e aprimoramento da 'confiança' na sociedade e na economia, de modo que irá ajudar a desenvolver a cultura da 'sinceridade'" (TIMOFEEVA, 2020, p. 14, tradução nossa). Tal sistema implica em uma classificação dos indivíduos e empresas em relação ao seu comportamento no meio social. A avaliação dos cidadãos é calculada por 5 categorias: (1) condições materiais, como renda, histórico de crédito, pagamento

das contas; (2) segurança, isto é, seus dados pessoais e confirmação das suas informações; (3) conexões sociais, dados relacionados a sua educação e rede de amizades; (4) obediência às leis – diligência, *feedback* positivo sobre o governo; e (5) comportamento de consumo, suas compras, preferências de bens e serviços etc. (TIMOFEEVA, 2020).

Logo, aqueles que não respeitam as regras de convivência comunitária além de entrarem para uma "lista negra" sofrem punições como limitações quanto ao acesso a empregos públicos, boas instituições de ensino, compra de passagens em meios de transporte, entre outros. Por outro lado, aqueles que respeitam o ordenamento social entram em uma "lista vermelha", sendo exemplos de como um bom cidadão deve se portar e recompensado por isso com uma série de benefícios. Segundo informações da RFI France (2020), um relatório do Centro Nacional de Informações sobre Crédito Público datado de março de 2019 divulgou que "nada menos que 23 milhões de chineses com 'classificação ruim' foram proibidos de viajar pelos tribunais: 17,5 milhões de passagens aéreas canceladas e 5,5 milhões de assentos de trem recusados" (ZYLBERMAN, 2020).

De modo geral, as estratégias chinesas voltadas para tecnologias de vigilância se baseiam no equilíbrio entre a modernização econômica e o controle político. Isto é, segundo Nir Kshetri (2019), o principal objetivo do governo é manter o monopólio do poder do Partido Comunista da China (PCC) e, consequentemente, o regime político do país. Para isso, as novas técnicas de vigilância são empregadas de forma a garantir o seu domínio político, prevenindo que a oposição o conteste. Assim, o sistema de crédito social "é visto como uma tentativa do PCC de aproveitar os avanços da computação e das telecomunicações e usar tecnologias sofisticadas, como inteligência artificial, para aumentar seu domínio sobre o público", punindo comportamentos entendidos como contrários aos interesses do PCC (KSHETRI, 2020, p. 15-16).

Dessa forma, além das preocupações já existentes do Ocidente, que julgam esse novo sistema como "orwelliano" e temem pelas suas empresas presentes no mercado chinês, um outro elemento também se destaca nessa situação: a inexistência de uma lei nacional que regule o crédito social. Por mais que algumas províncias e localidades como Xangai, Zhejiang, Hebei, Hubei e Shaanxi tenham desenvolvido seus próprios regulamentos locais limitando a coleta desenfreada de dados pessoais, isso ainda não é uma realidade integral no país, o que abre espaço para uma reflexão acerca de como a temática da segurança global seria impactada (ZYLBERMAN, 2020).

Ou seja, visto que este é um instrumento governamental orientado pelos interesses dos líderes do partido, a capacidade de manipulação do comportamento da população é surpreendente. Isso toma proporções ainda maiores quando consideramos que "a privacidade não é vista como uma questão importante na China" e a pontuação de cada pessoa é pública. Qualquer um pode entrar no site da "Credit China" e verificar a classificação de outras pessoas. Ademais, é preciso levar em conta que a "pontuação de uma pessoa também é uma função das opiniões políticas e comportamentos dos seus amigos e conhecidos. Isso significa que indivíduos que se opuseram publicamente à ideologia do PCC ou não pagaram dívidas provavelmente terão conexões mais limitadas" (KSHETRI, 2020, p. 17-8).

Nesse contexto, a pandemia do novo coronavírus possibilita uma oportunidade única para a implementação e o desenvolvimento de tecnologias de vigilância ao redor do mundo, em especial o sistema de vigilância chinês. Conforme o novo coronavírus ultrapassou as fronteiras da China, as preocupações com a saúde pública mundial ganharam novas proporções, especialmente após a Organização Mundial de Saúde, no dia 11 de março de 2020, definir a COVID-19 como pandemia (BBC Brasil, 2020) e as declarações de líderes estatais descrevendo a situação como "uma guerra contra um inimigo invisível" (WINTOUR, 2020).

Vigilância e o novo coronavírus: contexto chinês, preocupações globais

Segundo Wintour (2020, n.p), "ideologias concorrentes, blocos de poder, líderes e sistemas de coesão social estão sendo testados na corte da opinião mundial". Isto é, nos encontramos em um contexto em que as tensões entre as grandes potências se intensificam e as políticas adotadas pelos países são desafiadas conforme a vida da população é colocada em risco e a política internacional sofre mudanças permanentes. De acordo com o *think tank Crisis Group*, é possível identificar, até o momento, duas narrativas concorrentes ganhando força: na primeira, entende-se que os países devem se unir na luta contra o COVID-19, prezando pela cooperação; enquanto a outra defende que os países devem lidar separadamente com a questão de forma a melhor se protegerem contra a doença (WINTOUR, 2020).

E embora não exista um consenso quanto a qual dessas narrativas vai prevalecer no sistema internacional, nem como será a

distribuição de poder no cenário global do pós-coronavírus, é possível perceber cada vez mais a presença da *big data* quando falamos de privacidade, segurança e controle sanitário durante a pandemia. Pode-se dizer que a epidemia não é combatida somente por virologistas, epidemiologistas e líderes de Estado, mas também por cientistas da computação e especialistas de *big data* (WINTOUR, 2020). E o combate à pandemia na China é um grande exemplo. Wintour traz uma previsão de que...

> [a] China agora será capaz de vender seu Estado policial digital como um modelo de sucesso contra a pandemia. A China mostrará a superioridade de seu sistema com ainda mais orgulho. (...) [O]s eleitores ocidentais, atraídos pela segurança e pela comunidade, podem estar dispostos a sacrificar essas liberdades. Há pouca liberdade em ser forçado a passar a primavera fechado em seu próprio apartamento (WINTOUR, 2020, n.p.).

O controle, o monitoramento das pessoas e as restrições sobre como podem interagir, no espaço físico ou na internet, não é algo inteiramente novo na China. Principalmente à medida que o sistema de crédito social vem se consolidando nos últimos anos e os aplicativos de monitoramento do coronavírus se multiplicaram neste contexto pandêmico. Um exemplo disso são aplicações voltadas para a área da saúde que são capazes de rastrear se o indivíduo teve contato com alguém infectado, nas quais – por meio do uso de QR Codes – os usuários podem compartilhar seus dados pessoais e até históricos de viagens. As diferentes cores nos aplicativos indicam diferentes níveis de risco: o código vermelho significa que a pessoa está (ou provavelmente está) com coronavírus, enquanto o código amarelo indica que a pessoa teve contato com um indivíduo infectado e o código verde indica que o usuário está sem sintomas de COVID (ANKEL, 2020). Logo, o código verde garante movimento irrestrito e permite que a pessoa viaje e ande pela cidade, enquanto o usuário com código amarelo ou vermelho não pode se locomover, precisa ficar em sete dias de quarentena (código amarelo) ou devem fazer quatorze dias de quarentena (código vermelho) (CHABBA, 2020).

Assim, basta que o indivíduo possua o WeChat (aplicação de mensagens instantâneas) ou o Alipay (plataforma de pagamento online do grupo Alibaba) para que o software já instalado nestes seja capaz de traçar sua movimentação, o qual uma vez munido das informações de saúde do indivíduo, emite as cores verde, amarelo ou vermelho, que determinam se este pode sair de casa e para onde

pode ir (ANKEL, 2020; CHABBA, 2020). Nessa que é uma tentativa de prevenir uma segunda onda de alto contágio no país e já conta com a participação de duzentas cidades chinesas, apesar de ainda incerto como o sistema classifica as pessoas, a maior preocupação repousa sobre até que extensão essa tecnologia de controle de dados pode ser utilizada à despeito da privacidade individual.

Ademais, ao longo de 2020 a crise decorrente da pandemia levou a mudanças no Sistema de Crédito Social de forma a orientar o comportamento de empresas, punindo aquelas que descumprissem as normas sanitárias e incentivando a contenção do COVID-19. Assim, quando a situação no país já estava mais controlada, o crédito social foi usado para estimular o retorno ao trabalho, "premiando" em alguns locais os negócios que melhor implementassem as medidas de prevenção com "pontos especiais" e reduzindo taxas para empresas com boa pontuação de crédito advinda do pagamento dos trabalhadores em dia (REILLY; LYU; ROBERTSON, 2021).

Um dos principais legados da pandemia sobre o Sistema de Crédito Social talvez seja justamente a tecnologia de monitoramento por QR Codes, que permite aos consumidores checarem "as credenciais de empresas e funcionários em certos setores identificados como sem altos padrões da indústria, incluindo aluguel e serviços de habitação" (Reilly; Lyu; Robertson, 2021, n.p. tradução nossa).

Cidades chinesas, de acordo com reportagem da revista Wired (2020), usam experimentos de sistemas de crédito social, de forma mais independente, para controlar a circulação de pessoas (e, consequentemente, do vírus). Em Hangzhou, o seu sistema de crédito social envolve uma lista negra em que as autoridades publicam nomes de cidadãos (e parte dos seus números de identidade) que falsificaram o seu histórico de viagem. Essa informação fica pública por um ano no website "Credit Hangzhou", segundo a reportagem. Outras cidades também expandiram suas regulamentações de crédito social para incluir a perda de créditos para quem criar rumores que atrapalham os esforços para controlar o vírus, quem fabrica máscaras falsas ou de baixa qualidade e outros suprimentos médicos. Em Rongcheng, província de Shandong, doações em dinheiro ou materiais para apoiar trabalhos essenciais durante a pandemia aumentam as pontuações dos cidadãos.

Dessa forma, uma das principais preocupações futuras em relação ao contexto da pandemia atual, segundo a Human Rights Watch (2020, n.p), é o perigo que "programas de rastreamento móvel, que pretendem ser medidas temporárias até que a pandemia

esteja sob controle e uma vacina esteja disponível, podem se tornar características permanentes de um regime de vigilância expandido", levando a um comprometimento da privacidade e dos direitos humanos, elemento ainda mais agravante em locais que já fazem uso de uma vigilância intrusiva, como é o caso da China.

Em última instância, as medidas de restrição à circulação e de monitoramento impostas ao redor do mundo podem impactar até sobre o entendimento do que é ser humano. Para Giorgio Agamben (2020, n.p), "o vírus levou ao apagamento dos 'nossos semelhantes'" uma vez que qualquer um pode ser um possível portador do vírus, mudando nossa percepção de nossos pares para inimigos em potencial. "Uma vez que 'o inimigo não está em algum lugar externo, está dentro de nós', nossa humanidade comum intrinsecamente constitui uma ameaça à segurança" (SHANI, 2020, n.p, tradução nossa). Logo, é possível observar uma inversão da lógica de segurança: as ameaças não são mais exclusivas ao exterior, mas também podem vir de dentro dos próprios indivíduos, o que acaba por legitimar uma espécie de "estado de exceção" (AGAMBEN, 2004) motivado por questões sanitárias e caracterizado pelo controle dos corpos, pelo monitoramento do movimento. Ou seja, "[um] 'Security State', um Estado em que por razões de segurança (neste caso de "saúde pública"), pode-se impor qualquer limite às liberdades individuais" (AGAMBEN, 2020, n.p.).

Desse modo, o caso chinês é especialmente expressivo desse fenômeno, percebido pela articulação entre o setor privado e o domínio estatal na formulação de práticas, técnicas e tecnologias de vigilância – adotadas no campo da segurança. A vigilância digital e de dados na China é uma das mais desenvolvidas que presenciamos nos dias de hoje: o "Great Firewall", de regulação da internet, o sistema de crédito social e os sistemas de vigilância sanitária em tempos de COVID-19 são os seus principais exemplos.

Isso é o que Abrahamsen e Williams (2009) consideram como a "privatização da segurança", a introdução de racionalidades e entidades privadas na governança da segurança, e a constituição de "assemblagens globais de segurança" – esse imbricamento entre os domínios público e privado, uma diluição de suas barreiras, em que suas normatividades interagem e produzem novas instituições, práticas e formas de governança da segurança. No entanto, como os autores bem apresentam em seu artigo, esse maior vínculo operacional entre os domínios público e privado, inclusive no campo da segurança, também é fortemente perceptível em Estados

democráticos. Nesse sentido, a preocupação com as possíveis consequências do fortalecimento das tecnologias de vigilância para questões de segurança e privacidade é uma inquietação global. A vigilância de dados, assim como a declaração de "estados de emergência" se fazem presentes tanto em regimes totalitários quanto democráticos devido a nova era do "capitalismo da vigilância" (ZUBOFF, 2018; SHANI, 2020).

A segurança é o termo mobilizado para promover e justificar a vigilância de dados – seja a segurança nacional, internacional, sanitária. Segurança se refere às condições em que o valor da liberdade deve alcançar seus limites, uma negociação em que liberdade e privacidade podem ser suspensas em prol da segurança (BAUMAN et al., 2014). Em leituras autoritárias, totalitárias e fascistas, o Estado triunfa sobre a soberania popular, tendo decisão arbitrária sobre a questão. Já na tradição democrática, a segurança possui uma condição limitada, devido ao pretexto de que a democracia deve acomodar as demandas sociais. Porém,

> [d]ada a gama de ameaças plausíveis que as sociedades contemporâneas enfrentam e, especialmente, a capacidade de uma ampla gama de agências de segurança para destacar algumas ameaças em vez de outras e empurrar a necessidade de segurança como o princípio básico que rege nossas vidas, o que costumava ser entendido como opções autoritárias são realizadas de modo a parecerem desejáveis, até mesmo naturais (BAUMAN et al., 2014, p. 137, tradução nossa)[8].

Dessa forma, há o perigo cada vez maior de técnicas autoritárias de vigilância de dados e violação da privacidade serem incorporadas em regimes democráticos.

Segundo Nicholas Wright, o risco é alto: "Se as democracias não conseguirem transformar o futuro da vigilância global a seu favor, os concorrentes autoritários digitais estarão prontos para oferecer seu próprio modelo ao mundo" (WRIGHT, 2020, n.p). Enquanto isso, cada vez mais por meio de aplicações que controlam a saúde, ranqueamentos disciplinares, previsão de ações e comportamentos futuros mediante análise algorítmica, entre outros, parecemos nos aproximar de uma realidade desprovida de pensamento crítico e agência cidadã.

8. "Given both the range of plausible threats confronting contemporary societies, and especially the capacity of a broad range of security agencies to highlight some threats rather than others and to push the need for security as the primary principle governing our lives, what used to be understood as authoritarian options are made to seem desirable, even natural".

De modo semelhante, Friedewald et al. (2017) apontam que, ao olhar para a manipulação do conceito no contexto de segurança, a perspectiva predominante é amplamente reduzida a debates sobre como encontrar o equilíbrio entre privacidade e segurança, o que assume e consequentemente promove a ideia de que a vigilância orientada por dados (*data-driven surveillance*) é a única solução para qualquer ameaça. Todavia, o uso generalizado de mecanismos de vigilância em nome da segurança muitas vezes coloca em segundo plano questões ligadas à legislação e regulamentação.

Como resultado, é alimentada a noção de que incidentes de segurança têm uma maior relevância do que os de privacidade. Enquanto questões ligadas a terrorismo, por exemplo, recebem atenção imediata da mídia e do *policy-making*, somente violações de grande escala de privacidade chegam às manchetes e dificilmente recebem alguma resposta do setor público ou têm alguma ação concreta. Segundo Friedewald et al. (2017, p. 6-7, tradução nossa),

> Fortes diferenças na visibilidade e no imediatismo das consequências das violações de privacidade, por um lado, e dos incidentes de segurança, por outro, são fatores adicionais que contribuem para esse fenômeno. Os últimos geralmente estão impactando diretamente as pessoas em questão; as violações de privacidade, por outro lado, podem acontecer de maneira imperceptível. As consequências de tais violações só podem se tornar visíveis com longos atrasos. Devido a esses atrasos, pode ser difícil associar formas específicas de discriminação a violações de privacidade e pode ser ainda mais difícil fornecer prova de relações causais[9].

O que os autores buscam, portanto, é justamente desafiar a suposição de que mais segurança requer menos privacidade e mais vigilância implica necessariamente mais segurança. Eles defendem a ideia de que a privacidade não só é um direito fundamental, mas também desempenha um papel central no exercício de outros direitos e liberdades fundamentais, para equilibrar poderes entre Estado e cidadãos, para o desenvolvimento democrático, social e econômico, ou autonomia individual. Trata-se, em última instância, de um componente essencial da segurança online devido ao seu

9. "Strong differences in visibility and immediateness of the consequences of privacy violations, on the one hand, and of security incidents, on the other, are additional factors contributing to this phenomenon. The latter are usually directly impacting the concerned persons; privacy violations, on the other hand, can happen in an unnoticeable manner. The consequences of such violations may only become visible with long delays. Owing to these delays, it might be difficult to associate specific forms of discrimination to infringements of privacy and even more difficult to provide proof for causal relationships".

papel primordial sobre a "proteção de cidadãos contra (o abuso de) poderes estatais" (FRIEDEWALD et al. 2017, p. 6-7).

De todo modo, em regimes totalitários e democráticos, a vigilância está sendo aceita pelos seus subordinados. Para Bauman et al. (2014), existem três fatores que nos auxiliam a compreender porque a vigilância ainda aparenta ser aceita acriticamente por vários cidadãos: familiaridade, medo e diversão. A familiaridade é considerada como um fator crítico para a aceitação da vigilância, pois a vigilância atualmente é tão invasiva e tem tantas dimensões que simplesmente se tornou parte da vida cotidiana. Desse modo, as pessoas não percebem mais e, então, não pensam sobre as capacidades de vigilância. A vigilância é entendida como dada, é normal e comum.

O medo é um sentimento facilmente mobilizado por diferentes atores, com fortes consequências. Os governos, as companhias de segurança e a mídia têm um papel ativo na mobilização do medo. O medo funciona para as empresas que vendem novos equipamentos de vigilância e segurança; para governos que consideram sua tarefa permitir às forças de mercado rédea solta e manter a segurança; e para a mídia, que depende da polarização do "bem contra o mau", os "mocinhos *versus* os bandidos" (BAUMAN et al., 2014).

Além disso, segundo David Campbell (1992), essa necessidade de vigilância constante em relação a um "inimigo", ao que ele chama de evangelização do medo, não é algo do passado. A diferença é que agora esse "inimigo" não somente é invisível (como um vírus, tanto no seu sentido digital quanto no seu sentido sanitário), mas também é comum a todos os Estados, além de não poder ser combatido de forma unilateral, aparentemente. Na visão do autor, "o Estado fundamenta sua legitimidade na promessa de segurança aos seus cidadãos" (CAMPBELL, 1992, p. 56), contudo, o desafio que se apresenta atualmente é se essa transparência e capacidade de agência dos cidadãos – nos quais a democracia se baseia – conseguirão ser mantidas pelo aparato estatal em uma sociedade onde as fronteiras entre o meio digital e o ambiente físico tornam-se cada vez mais permeáveis e a tomada de decisão cada vez menos reside na esfera individual.

Por fim, a diversão também é um importante motivo para que a vigilância seja amplamente aceita nas sociedades atuais, inclusive as democráticas.

> Na chamada Web 2.0, as informações não são fornecidas apenas por grandes organizações – todos participam. (...) Esta 'vigilância social' (...) é decididamente divertida para os participantes. (...) As redes so-

> ciais continuam a ser extremamente populares e, embora possa ser um meio potente de formação de opiniões políticas e de protesto, [o meio] também fornece a matéria-prima de dados para as empresas e, como Snowden nos mostrou, para a polícia e para agências de inteligência (BAUMAN et al., 2014, p. 142, tradução nossa, grifo nosso)[10].

Desse modo, o entretenimento proveniente da participação e interação nas redes sociais faz com que mais pessoas estejam sujeitas às estruturas e tecnologias da vigilância presentes no meio digital, sabendo ou não desses "termos e condições" que permitem a violação da privacidade. Segundo Firmino (2017, p. 26), esse é um "(...) modo de vigilância e controle mais disperso e menos centralizado", que vai além "de uma questão do poder central do Estado ou de grandes corporações exercendo uma única força de controle". Com a dispersão de tecnologias como a Internet das Coisas e a "naturalização do uso de mídias sociais", as pessoas são transformadas em "um sistema móvel de vigilância", o que caracteriza a "mais recente forma de securitização de espaços e lugares" (FIRMINO, 2017, p. 26).

Portanto, é possível perceber que a vigilância de dados e informações (nas esferas social e digital) é um fenômeno com forte presença no nosso cotidiano, sejam regimes totalitários, sejam democráticos. Ademais, a pandemia do novo coronavírus representou – e continua representando – um momento de exploração e intensificação de tecnologias de vigilância em massa, sob a justificativa da segurança sanitária nacional e global.

Ao longo desta seção, argumentamos que essa conjuntura global da vigilância se dá por meio de uma articulação entre Estado e corporações privadas (especialmente as ligadas à segurança, dados e meios digitais). Esse controle e patrulhamento dos indivíduos pode se dar por modelos centralizados de gestão urbana e de segurança, mas também por aplicações móveis e redes sociais – que são maneiras mais dispersas de vigilância. De todo modo, a vigilância de dados e a violação da privacidade digital – em nome da segurança – está se tornando um forte debate no campo global, sem pretensões de ser resolvido facilmente.

10. "In the so-called Web 2.0, information is not just provided by large organizations — rather, everyone participates. (...) This 'social surveillance' (...) is decidedly enjoyable for participants. (...) Social media continue to be hugely popular, and while they can be a potent means of shaping political opinion and protest, they also provide the raw materials of data for both corporations and, as Snowden has shown us, police and intelligence agencies".

Considerações finais: os efeitos da pandemia sobre a vigilância global

Não podemos prever o que irá acontecer com a vigilância em massa no pós-pandemia, mas podemos perceber que os fenômenos de vigilância digital e de dados, privatização da segurança e assemblagem global da segurança – que já se faziam fortemente presentes nas últimas décadas – vêm se fortalecendo cada vez mais neste período. Isso ainda com a justificativa da necessidade da vigilância para a segurança sanitária do país e do globo. Desse modo, existe uma forte preocupação com a privacidade individual frente às medidas de vigilância digital pelos aplicativos de controle e rastreamento para prevenção ao coronavírus, por exemplo (BROWN & TOH, 2021; HUMAN RIGHTS WATCH, 2020).

Há também um viés teórico que argumenta que as tecnologias de rastreamento recém empregadas durante a pandemia configuram uma nova forma de vigilância estatal, como apresenta Evgeny Morozov (2020). Por sua vez, essa nova forma de vigilância estatal reflete as novas características do capitalismo no século XXI. Nesse sentido, o autor defende que, num cenário pós-pandemia, seria preciso adotar um caminho "pós-solucionista" capaz de dar à população soberania sobre as plataformas digitais. Isto é, de forma a evitarmos o controle eterno do nosso comportamento por parte das Big Tech e/ou do Estado, seria preciso que as pessoas tivessem o controle efetivo das tecnologias de vigilância (MOROZOV, 2020).

Em uma visão mais pessimista, o filósofo Giorgio Agamben (2020) discute que também existe uma hipótese de que estamos dando lugar a um novo despotismo de perversidade dos controles e cessação de toda atividade política: um "Security State", em que um Estado em que por razões de segurança (como de saúde pública), pode impor qualquer limite às liberdades individuais. É um contexto também de "desconstrução da própria política", em que a segurança mudou o foco "da política para o policiamento e do governo para o gerenciamento" – usando sistemas de vigilância eletrônicos, debilitando a própria possibilidade da política, simultaneamente com o crescimento de todas as formas de vigilância (BAUMAN et al., 2014, p. 141).

Nesse sentido, o papel da vigilância de dados no atual contexto da pandemia do COVID-19 se mostra como um elemento chave no que pode ser entendido como uma virada nos estudos de segurança em um futuro próximo. Sem dúvidas a pauta de discussão

desse novo cenário dará uma nova conotação à privacidade e a sua importância no ambiente internacional, além de como esta será manipulada pelos – até então – dois principais atores que a disputam (Estados e Big Techs).

No caso chinês, essa imbricação entre público e privado desponta como uma das primeiras formas de organização nesse novo contexto, contando com um sistema de crédito classificatório que coloca em xeque as liberdades individuais e os direitos humanos. Sendo assim, a grande preocupação que se apresenta atualmente é se essa intensificação da vigilância será algo temporário e restrito à aplicações móveis, ou se será expandida para outras esferas do cotidiano de tal maneira a impulsionar uma reestruturação da agenda de segurança internacional.

Referências

ABRAHAMSEN, Rita; WILLIAMS, Michael C. "Security Beyond the State: Global Security Assemblages in International Politics". **International Political Sociology**, v. 3, n. 1, 2009, p. 1-17.

A CHINA já pode identificar seus cidadãos só pela forma de andar: depois de instalar o sistema de 'rating' para avaliar se os habitantes são bons cidadãos, o gigante asiático volta a explorar novas tecnologias para detectar as caminhadas. **El País**, Madri, 10 nov. 2018. Disponível em: https://brasil.elpais.com/brasil/2018/11/10/politica/1541853964_264737.html. Acesso em: 29 abr. 2021.

AGAMBEN, Giorgio. **Estado de Exceção**. São Paulo: Boitempo, 2004.

AGAMBEN, Giorgio. "Pandemia, novas reflexões. Entrevista com Giorgio Agamben". [Entrevista concedida a] Quodlibet, 22 de abril de 2020. Tradução de Moisés Sbardelotto. **Revista IHU On-line**, 23 abr. 2020. Disponível em: http://www.ihu.unisinos.br/78-noticias/598295-pandemia-novas-reflexoes-entrevista-com-giorgio-agamben. Acesso em: 12 jul. 2020.

ANKEL, Sophia. "As China lifts its coronavirus lockdowns, authorities are using a color-coded health system to dictate where citizens can go. Here's how it works". **Business Insider**, Nova York, 07 abr. 2020. Disponível em: https://www.businessinsider.com/coronavirus-china-health-software-color-coded-how-it-works-2020-4. Acesso em: 23 jun. 2020.

BAUMAN, Zygmunt et al. "After Snowden: Rethinking the Impact of Surveillance". **International Political Sociology**, v. 8, n. 2, 2014. p. 121–144.

BBC. Coronavirus: OMS declara pandemia. **BBC Brasil**, 11 mar. 2020. Disponível em: https://www.bbc.com/portuguese/geral-51842518. Acesso em: 05 jul. 2020.

BROWN, Deborah & TOH, Amos. "Technology is Enabling Surveillance, Inequality During the Pandemic". In: **Human Rights Watch Website,** 4 mar. 2021. Di-

sponível em: https://www.hrw.org/news/2021/03/04/technology-enabling-surveillance-inequality-during-pandemic. Acesso em: 3 mai. 2021.

CAMPBELL, David. **Writing Security**: United States Foreign Policy and the Politics of Identity. Minneapolis: University Of Minnesota Press, 1992.

CHABBA, Seerat. "Coronavirus tracking apps: How are countries monitoring infections?". **Deutsche Welle (DW)**, Bonn, 27 abr. 2020. Disponível em: https://www.dw.com/en/coronavirus-tracking-apps-how-are-countries-monitoring-infections/a-53254234. Acesso em: 23 jun. 2020.

FIRMINO, Rodrigo José. Securitização, vigilância e territorialização em espaços públicos na cidade neoliberal. **Risco: Revista de Pesquisa em Arquitetura e Urbanismo**, v. 15, n. 1, p. 23-35, 2017.

FRIEDEWALD, Michael et al. **Surveillance, Privacy and Security**: Citizens' Perspectives. New York: Routledge, 2017.

GALLAGHER, Ryan. Como gigantes da tecnologia dos EUA estão ajudando a construir a vigilância em massa da China: ONG liderada por executivos da Google e da IBM está trabalhando com a Semptian, empresa que monitora a atividade na internet de 200 milhões de chineses. **The Intercept Brasil**. 16 jul. 2019. Disponível em: https://theintercept.com/2019/07/16/vigilancia-em-massa-da-china/. Acesso em: 29 abr. 2021.

GUISNEL, Jean. Préface. In: WHITAKER, Reg. **Tous fliqués! La vie privée sous surveillance**. Paris: Editora Denoël, 2001.p.XI-XIV. (Prefácio). Citado na página XI.

HUMAN RIGHTS WATCH. "China: Seekers of Covid-19 Redress Harassed". In: **Human Rights Watch Website,** 2021. Disponível em: https://www.hrw.org/node/377547. Acesso em: 29 abr. 2021.

HUMAN RIGHTS WATCH. "Covid-19 Apps Pose Serious Human Rights Risks". In: **Human Rights Watch Website**, 13 mai. 2020. Disponível em: https://www.hrw.org/news/2020/05/13/covid-19-apps-pose-serious-human-rights-risks. Acesso em: 10 jul. 2020.

KOBIE, Nicole. The complicated truth about China's social credit system: china's social credit system isn't a world first but when it's complete it will be unique. The system isn't just as simple as everyone being given a score though. **Wired**. 07 jun. 2019. Disponível em: https://www.wired.co.uk/article/china-social-credit-system-explained. Acesso em: 29 abr. 2021.

KSHETRI, Nir. "China's Social Credit System: Data, Algorithms and Implications". **IT PROFESSIONAL**, v. 22, n. 2, 2020, p. 14-18.

MOROZOV, Evgeny. "The tech 'solutions' for coronavirus take the surveillance state to the next level". **The Guardian**, Londres, 15 abr. 2020. Disponível em: https://www.theguardian.com/commentisfree/2020/apr/15/tech-coronavirus--surveilance-state-digital-disrupt. Acesso em: 14 jul 2020.

REILLY, Jessica; LYU, Muyao; ROBERTSON, Megan. China's Social Credit System: Speculation vs. Reality. How far along is China's much-hyped social credit system

– and where is it heading next? **The Diplomat**, mar 30 2021. Disponível em: https://thediplomat.com/2021/03/chinas-social-credit-system-speculation-vs-reality/. Acesso em: 30 abr 2021.

REUTERS. China issues rules on social credit system amid public concerns. **Reuters**, 24 dez. 2020. Disponível em: https://www.reuters.com/world/china/china-issues-rules-social-credit-system-amid-public-concerns-2020-12-24/. Acesso em 5 mai. 2021.

SHANI, Giorgio. Securitizing 'Bare Life'? Human Security and Coronavirus. **E-International Relations**, 03 abr 2020. Disponível em: https://www.e-ir.info/2020/04/03/securitizing-bare-life-human-security-and-coronavirus/. Acesso em: 27 abr 2021.

SHAW, Jonathan. "The Watchers: Assaults on privacy in America". **Harvard Magazine**, jan-fev. 2017. Disponível em: https://harvardmagazine.com/2017/01/the-watchers. Acesso em: 10 jul. 2019.

TIMOFEEVA, E.A. "The Transition to a Digital Society in the People's Republic of China (Development and Implementation of the Social Credit Score System)". In: ASHMARINA et al. (Eds.). **Digital Transformation of the Economy:** Challenges, Trends and New Opportunities. Nova York: Springer Nature, 2020. p. 103-110.

WINTOUR, Patrick. "Coronavirus: who will be winners and losers in new world order?". **The Guardian**, Londres, 11 abr 2020. Disponível em: https://www.theguardian.com/world/2020/apr/11/coronavirus-who-will-be-winners-and-losers-in-new-world-order. Acesso em: 20 jun 2020.

WIRED. China is using coronavirus to boost its dystopian social credit system. **Wired**, 3 mar. 2020. Disponível em: https://www.wired.co.uk/article/china-social-credit-coronavirus. Acesso em: 2 mai. 2021.

WRIGHT, Nicholas. "Coronavirus and the Future of Surveillance: Democracies Must Offer an Alternative to Authoritarian Solutions". **Foreign Affairs**, Nova York, 06 abr 2020. Disponível em: https://www.foreignaffairs.com/articles/2020-04-06/coronavirus-and-future-surveillance. Acesso em: 14 jul. 2020.

YU, Ai. "Digital surveillance in post-coronavirus China: A feminist view on the price we pay". **Gender, Work, and Organization**, 2020. p. 1-4. Disponível em: https://europepmc.org/article/pmc/pmc7280578. Acesso em: 13 jul. 2020.

ZUBOFF, Shoshana. "Big Other: Capitalismo de Vigilância e Perspectivas para uma Civilização de Informação". In.: CARDOSO, Bruno et al. **Tecnopolíticas da vigilância:** Perspectivas da margem. São Paulo: Boitempo, 2018. p. 17 - 68.

ZYLBERMAN, Joris. "China chega à fase final de sistema de avaliação de cidadãos e preocupa Ocidente". **RFI France**, Paris, 02 jan. 2020. Disponível em: http://www.rfi.fr/br/mundo/20200102-em-2020-china-termina-de-testar-seu-sistema-de-cr%C3%A9ditos-sociais-e-assusta-ocidente. Acesso em: 15 jun. 2020.

Recebido em: 23 de dezembro de 2020
Aprovado em: 17 de maio de 2021