



Anderson Röhe Fontão Batista

O sistema chinês de vigilância pública e reconhecimento facial: solução ou ameaça para o mundo?

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre (Opção profissional) pelo Programa de Pós-Graduação em Análise e Gestão de Políticas Internacionais da PUC-Rio.

Orientadora: Prof.^a Maria Elena Rodriguez Ortiz

Co-Orientadora: Prof.^a Manuela Trindade Viana

Rio de Janeiro
Julho de 2019

Anderson Röhe Fontão Batista

O sistema chinês de vigilância pública e reconhecimento facial: solução ou ameaça para o mundo?

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre pelo Programa de Pós-Graduação em Análise e Gestão de Políticas Internacionais da PUC-Rio. Aprovada pela Comissão Examinadora abaixo.

Prof.^a Maria Elena Rodriguez Ortiz

Orientadora

Instituto de Relações Internacionais – PUC-Rio

Prof.^a Manuela Trindade Viana

Co-Orientadora

Instituto de Relações Internacionais – PUC-Rio

Prof. Paulo Sérgio Wrobel

Instituto de Relações Internacionais – PUC-Rio

Prof. Mauricio Santoro Rocha

Departamento de Relações Internacionais da Universidade do Estado do Rio de Janeiro (UERJ)

Rio de Janeiro, 13 de Julho de 2019

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do autor e da orientadora.

Anderson Röhe Fontão Batista

O autor concluiu sua Graduação em Direito na Universidade Federal Fluminense – UFF em 1996 e sua Especialização em Relações Internacionais na Faculdade Damásio / Clio Internacional em 2016.

Ficha Catalográfica

Batista, Anderson Röhe Fontão

O sistema chinês de vigilância pública e reconhecimento facial : solução ou ameaça para o mundo? / Anderson Röhe Fontão Batista ; orientadora: Maria Elena Rodriguez Ortiz ; co-orientadora: Manuela Trindade Viana. – 2019.

59 f. : il. color. ; 30 cm

Dissertação (mestrado)–Pontifícia Universidade Católica do Rio de Janeiro, Instituto de Relações Internacionais, 2019.

Inclui bibliografia

1. Relações Internacionais – Teses. 2. China. 3. Chinês. 4. Vigilância. 5. Reconhecimento facial. 6. Cidades inteligentes. I. Ortiz, Maria Elena Rodriguez. II. Viana, Manuela Trindade. III. Pontifícia Universidade Católica do Rio de Janeiro. Instituto de Relações Internacionais. IV. Título.

CDD: 327

Agradecimentos

Primeiramente, agradeço aos apaixonados por cidades que tanto me influenciaram a escrever a cerca de nossa transição entre o velho e o novo, entre o físico, o biológico e o digital, entre tantos contrastes e paradoxos urbanos. Foram muitos domingos, pela manhã, percorrendo as ruas desertas para observar, fotografar e registrar essa transformação.

Sobretudo, meus sinceros agradecimentos aos professores Maria Elena Rodriguez, Manuela Trindade Viana, Paulo Sérgio Wrobel e Maurício Santoro Rocha por gentilmente fazerem parte da Banca de Dissertação do Mestrado Profissional em Análise e Gestão de Políticas Internacionais (MAPI).

O interesse pelo gigante asiático não vem de agora. Desde minha pós-graduação na Faculdade Damásio/ Clio Internacional tenho me dedicado às relações sino-brasileiras ao abordar continuidades e rupturas da PEB - Política Externa Brasileira e os pontos de convergência de seus esforços de inserção autônoma no mundo.

A dissertação, em particular, é fruto de um ano como pesquisador assistente acerca dos investimentos chineses no Brasil e América Latina junto ao Laboratório de Financiamento e Cooperação Internacional para o Desenvolvimento (LACID), de iniciativa do *BRICS Policy Center* e vinculado ao Instituto de Relações Internacionais da PUC-Rio. Em 2018, o BPC foi considerado o primeiro *think tank* em ciência e tecnologia do Brasil e o quinto do mundo em pesquisa transdisciplinar pelo *Global Go To Think Tank Index Report*. Que minha trajetória sirva de inspiração para aqueles que, um dia, como eu, sonharam em fazer parte da antiga casa de Affonso Arinos.

Resumo

Batista, Anderson Röhe Fontão; Ortiz, Maria Elena Rodriguez; Viana, Manuela Trindade. **O sistema chinês de vigilância pública e reconhecimento facial: solução ou ameaça para o mundo?** Rio de Janeiro, 2019. 59p. Dissertação de Mestrado - Instituto de Relações Internacionais, Pontifícia Universidade Católica do Rio de Janeiro.

Em termos de novas tecnologias de policiamento e prevenção da violência urbana, a China é uma referência global. São novas tecnologias digitais advindas da Quarta Revolução Industrial, como IA & Big Data, que resolveriam desde desigualdades sociais a déficits em infraestrutura urbana. A China, por meio de projetos de cidades inteligentes, planeja liderar a revolução digital para se tornar exemplo de sociedade avançada e inteligente. Pretende com isso não só implementar esse projeto domesticamente, mas também exportá-lo como modelo de desenvolvimento baseado em inovação e tecnologia. No entanto, há resistências a esse modelo, visto pelos EUA e boa parte de seus aliados como estratégia da China para ascender globalmente, mas de forma predatória e autoritária, ao estabelecer novos padrões de dependência externa via comércio, investimento e tecnologia. A China, como nova potência digital, também representaria uma ameaça ao tentar replicar sistemas de controle social e vigilância em massa por meio de seus sistemas de vigilância pública e reconhecimento facial. Uma vez que a China vem firmando parcerias estratégicas pelo mundo, é preciso que empresas e governos tenham uma posição clara diante de uma eventual reconfiguração global e estejam preparados para o desafio de se adaptar à revolução digital, levando em conta os impactos que o modelo chinês poderá causar, não só em termos de oportunidades, mas também de custo-benefício e riscos socioeconômicos, em virtude de especificidades locais, crises históricas e problemas estruturais.

Palavras-chave

China; vigilância; reconhecimento facial; cidades inteligentes; policiamento preventivo; segurança cidadã

Abstract

Batista, Anderson Röhe Fontão; Ortiz, Maria Elena Rodriguez. (Advisor). Viana, Manuela Trindade. (Co-Advisor). **The Chinese system of public surveillance and facial recognition: solution or threat to the world?** Rio de Janeiro, 2019. 59p. Dissertação de Mestrado - Instituto de Relações Internacionais, Pontifícia Universidade Católica do Rio de Janeiro.

In terms of new technologies for policing and prevention of urban violence, China is a global benchmark. These are new digital technologies from the Fourth Industrial Revolution, such as AI & Big Data, which would solve from social inequalities to deficits in urban infrastructure. China, through smart cities projects, plans to lead the digital revolution to become an example of prosperous and intelligent society. It intends not only to implement this project domestically, but also to export it as a development model based on innovation and technology. However, there are resistance to this model, seen by the US and many of its allies as China's strategy to move globally, but in a predatory and authoritarian way, by establishing new patterns of external dependence through trade, investment and technology. China, as a new digital power, would also be a threat in attempting to replicate social control and mass surveillance systems through its public surveillance and facial recognition systems. Once China has been closing strategic partnerships around the world, firms and governments need to have a clear position in the face of a possible global reconfiguration and be prepared for the challenge of adapting themselves to the digital revolution, taking into account the impacts that the Chinese model can cause not only in terms of opportunities, but also cost-benefit and socioeconomic risks, due to local specificities, historical crises and structural problems.

Keywords

China; surveillance; facial recognition; smart cities; preventive policing; citizen security.

Sumário

Introdução	10
1. O Projeto Global das Smart Cities: entre inovação, controle e vigilância.....	14
1.1. Smart Cities como ambiente de inovação e desenvolvimento tecnológico	15
1.2. Smart Cities como sistemas de controle e vigilância	17
2. Novos Sistemas de Controle e Vigilância Pública da Era Digital.....	19
2.1. Reconhecimento Facial e Hipervigilância	19
2.2. Mapeamento Digital e Profiling	22
3. Sistemas de Vigilância e Reconhecimento Facial na China.....	26
3.1 Hipervigilância do Ponto de Visto Interno	27
3.2. Hipervigilância do Ponto de Visto Externo	31
4. Estudo de Caso, Posicionamento e Proposições	36
5. Conclusão	44
6. Referências bibliográficas	47

Lista de Figuras

Figura 1. O reconhecimento facial opera da seguinte forma: câmeras inteligentes são instaladas em pontos estratégicos e com grande fluxo de pessoas. 1) A imagem do rosto é captada e, depois, 2) processada por um algoritmo treinado para identificar determinados pontos faciais (como as distâncias do nariz aos olhos; da boca ao queixo); marcas e cicatrizes; contorno da face; formato da extremidade do rosto) e as correlações entre eles (via aferição). 3) Essas informações são usadas para criar um arquivo em interface azul que descreve o rosto e 4) funciona como uma "identidade facial" que é guardada em banco de dados para futuras consultas. Uma vez cadastrada a "ID digital", uma central de monitoramento vai ser acionada e receber um alerta quando a pessoa desaparecida ou procurada por motivos de segurança pública estiver circulando pelo perímetro onde foram instaladas as câmeras de vigilância (Gomes In: UOL, 2019).....20

“Aqueles que renunciam à liberdade em troca de promessas de
segurança, acabarão sem uma nem outra”
George Orwell.

Introdução

Em 2019 causou muita repercussão a notícia de que a República Popular da China - RPC pretendia não só disseminar nacionalmente (Yau, 2019), mas também exportar seu modelo de vigilância, sobretudo para grandes cidades da América Latina (Ellis, 2019; Mozur, Kessel e Chan 2019). Repercussão ainda maior porque a China é considerada a sociedade mais vigiada do mundo (Zmoginski, 2019). Ainda que as iniciativas, muitas delas no Brasil, tenham sido projetos-piloto e *pro bono* (Ellis, 2019; Mozur, Kessel e Chan, 2019), há indícios de que se pretende não só continuar como ampliar essa parceria (Rebello In: UOL; Távora, Araújo e Sousa; Wenqian, 2019).

Diante desse cenário, muitos se perguntam se **existe o risco desse sistema se normalizar e de o mundo se tornar uma nova China**. Há quem diga que não, pois muitos desses países são democracias que possuem sistemas constitucionais de freios e contrapesos, assim como instituições sólidas, engajamento político e ativismo da sociedade civil que fiscalizariam eventual violação da intimidade e privacidade dos cidadãos (Estadão, 2019). Mas isso é suficiente para que o modelo chinês não se torne uma ameaça global?

Por tais razões, essa dissertação vê **a ascensão digital chinesa como fenômeno a ser estudado por policy makers para se entender o porquê de haver sistemas de vigilância naquele país**. A análise virá sobretudo pela trajetória chinesa: como um país majoritariamente rural se tornou a segunda economia global e como especificidades desse processo de transformação urbana moldaram o que é hoje a China, uma emergente tecnológica que apresenta o “sonho chinês” para o mundo.

Hoje, a crise de violência e insegurança não só ganha complexidade local, como também alcança visibilidade externa, uma vez que grandes cidades são vitrine e cartão postal para o mundo. Logo, em se tratando de estabilidade e segurança para o turismo e o investimento estrangeiro, há a imagem negativa da violência urbana projetada para o exterior (Comunitas, 2016). As grandes cidades passaram, então, a servir de laboratório de testes e experimentos para soluções mais criativas e inteligentes, sobretudo por meio de projetos de *smart cities*, a fim de retomar confiança e credibilidade em seu potencial.

Violência e *boom* urbano e demográfico são, então, as **variáveis**, escolhidas para analisar a transformação das cidades não apenas como polos de atração e oportunidade, como também local para experimentos e novas tecnologias digitais visando a melhoria da

máquina administrativa, da prestação de serviços e do ambiente de negócios (PWCCN 2018, 2019).

Em se tratando de novas tecnologias de policiamento e prevenção ao crime e à violência urbana, a China é uma referência global, sobretudo por seus apurados sistemas de reconhecimento facial. E ao tentar replicá-los, grandes cidades estão seguindo uma tendência mundial de automatização e aumento no uso de tecnologias digitais de vigilância por forças policiais. No entanto, essas novas formas de controle e vigilância deveriam ser usadas como meio auxiliar, e não como regra da abordagem policial e da tomada de decisões, já que tendem não só a acirrar preconceitos, racismos, desigualdades estruturais, como também reproduzi-los, servindo de instrumento de repressão de territórios e grupos mais vulneráveis, como jovens pobres e negros, moradores de favelas e periferias, minorias étnicas e raciais, e criminalização de ativistas e defensores de direitos humanos. Logo, ao invés de servir de solução, agravariam ainda mais a violência urbana (Pellegrini In: Carta Capital, 2015).

Toma-se como **exemplo** o caso da América Latina, região que concentra algumas das 50 cidades mais violentas do mundo (CCSPJP, 2017; Serrano-Berthet In: IDB, 2018). Dessas, mais da metade está no Brasil, em razão de homicídios, sobretudo da juventude pobre e negra (Pellegrini In: Carta Capital, 2015; Comunitas; Igarapé, 2016; Muggah, 2017). No entanto, não há uma situação de violência que justifique replicar políticas de repressão ao crime e supressão de liberdades e direitos (Alvarado, 2016). Existe, sim, urgência de reforma da política de segurança a fim de salvar vidas (em ambos os lados da violência) e reduzir altos índices de criminalidade.

O Problema apontado: há uma tendência de a solução dos problemas de insegurança e violência urbana ser centrada na ação da polícia. Logo, são apontados dois erros principais de abordagem do problema: a) o da repressão policial, sem atentar para a prevenção da violência; e b) mais recentemente, o da automação do policiamento.

Argumento: as políticas de segurança pública fracassam (tanto na fase de formulação quanto de implementação) pois está equivocada a abordagem do problema, insistindo-se no enfrentamento da violência urbana pela repressão da polícia, quando o ideal seria a conjugação de policiamento repressivo e preventivo. Agora, ao buscar inteligência e inovação tecnológica, aposta-se naquilo que a polícia é mais carente: em prevenção. Mas, para real enfrentamento da crise de insegurança e descontrole da violência urbana não basta importar técnicas de reconhecimento facial para auxiliar as forças de segurança pública na captura de foragidos da justiça e no combate ao crime organizado e tráfico de

armas e drogas. Primeiro, porque as realidades de China e América Latina, embora assemelhadas, possuem especificidades locais; logo, sem preparação e planejamento, se incorreria em riscos desnecessários (Muggah In: Instituto Igarapé, 2019). Segundo, porque os custos, sobretudo socioeconômicos, não compensariam os potenciais benefícios (Winter In: Americas Quarterly, 2019). As tecnologias digitais são ainda de eficácia e precisão bastante limitadas para serem comercializadas e operacionalizadas sem a devida supervisão e regulamentação. Isso porque a tecnologia por si só não opera milagres, devendo vir acompanhada de preparação, planejamento estratégico, capacitação profissional e treinamento. Não se trata, porém, de banir a entrada de novas tecnologias só porque originárias da China. É possível replicá-las, mas impondo limites, supervisão, código ético de conduta, responsabilização e prestação periódica de contas (não só em caso de dano).

Essa dissertação encoraja a solução para a crise advinda de uma política de segurança mais humana, transparente, ética e, portanto, menos centrada no controle, vigilância em massa e automação do policiamento preventivo.

Proposta: O que efetivamente deveria ser feito é a conjugação da ação da polícia à melhoria do bem-estar humano, tanto da população local (mediante policiamento preventivo; desenvolvimento e inclusão social; trabalho de base continuado e de aproximação comunitária), quanto do policial, por meio de um serviço de treinamento, capacitação profissional e acompanhamento psicossocial para mitigar a sobrecarga da atividade da polícia.

Defende-se, portanto, o aprofundamento da ideia de segurança mediante uma visão mais sistêmica, transdisciplinar e ampla do que o tradicional modelo militarizado, já que pensada sob a perspectiva de direitos (a partir de uma perspectiva menos conflitiva e mais cooperativa; portanto, mais humana e a longo prazo, de ênfase local e de amplo acesso da população ao direito à Cidade).

Meio: a princípio, supervisão e monitoramento das tecnologias digitais de vigilância e reconhecimento facial; a longo prazo, regulamentação e planejamento estratégico, para que possam ser replicadas mediante mitigação de riscos e potencialização de benefícios.

O **Objetivo** primeiro é focar menos na tradicional política de confronto armado militarizado para, em seguida, se adotar uma nova política de segurança cidadã, mais humana, com uma visão menos repressiva e reativa para que se retome o conceito de ação

integrada e coordenada entre policiamento preventivo, desenvolvimento e inclusão social e de uso de dados e informação de forma mais inteligente, eficaz e eficiente.

As **análises** dessa dissertação virão a partir de uma visão macro sistêmica e multi/transdisciplinar, auxiliada por **metodologias** comparativas, segundo **critérios** quantitativos, qualitativos, temporais, de eficiência e eficácia.

O **Capítulo 1** aborda as questões da rápida urbanização global e do projeto das *smart cities*, assim como todo o esforço de transformar as cidades em espaços cada vez mais inteligentes e, portanto, mais seguros e integrados. Fala em seguida sobre paradoxos e contrastes das *smart cities* ou cidades digitais, vistas como ambiente de inovação e desenvolvimento tecnológico, mas também de violência, controle e vigilância. Já o **Capítulo 2** apresenta as novas formas de controle e vigilância da era digital por meio da hipervigilância de sistemas de reconhecimento facial, mapeamento e profiling.

O **Capítulo 3** contextualiza o sistema de vigilância e reconhecimento facial na China dos pontos de vista interno e externo, inter-relacionando-o com problemas típicos da China, como rápida urbanização, superpopulação e, por conseguinte, necessidade estatal de maior controle e monitoramento do comportamento social. Aborda, então, contrastes, paradoxos e a pressão chinesa em fazer sua transição tecnológica a fim de se tornar exemplo de sociedade inteligente, próspera e avançada para o mundo.

O **Capítulo 4** traz estudo de caso e o posicionamento dessa dissertação que, ao final, **conclui**, fazendo proposições para uma governança digital mais ética e transparente, assim como de uso de dados e informação de forma mais inteligente, eficaz e eficiente.

1. O Projeto Global das Smart Cities: entre inovação, controle e vigilância

Até 2050, espera-se que dois terços da população mundial vivam em cidades (Quartz). E dentre as razões para explicar esse fenômeno, está a que entende as cidades como polo de atração, ou seja, as pessoas passaram a se concentrar em aglomerados urbanos a partir do instante em que estes se tornaram sinônimo de oportunidade, riqueza, trabalho e melhor condição de vida. Isso faz com que as cidades se tornem ambientes mais próximos da realidade e onde o futuro acontece primeiro (Lifegate, 2017). É a vocação das cidades para que se tornem hubs ideais para experimentos, inovação e desenvolvimento tecnológico.

Robert Muggah (In: Igarapé, 2018), especialista em cidades, segurança e novas tecnologias, destaca ainda o aspecto transnacional das cidades. Hoje elas são lugares onde as pessoas não só vivem e buscam se sentir seguras, mas também prosperam, expressam criatividade e se interconectam com o mundo. Por isso, o esforço global de transformar cidades em espaços cada vez mais integrados, seguros e, assim, mais representativos do atual modo de vida dos cidadãos.

O mundo está mais urbano em razão principalmente de transformações tecnológicas e socioeconômicas ocorridas nas últimas décadas. Se no começo de século XIX apenas 10% das pessoas vivia nas cidades, um século depois saltou para um quarto da população mundial (PWCCN, 2019). Só na China, hoje são mais de 800 milhões de pessoas vivendo em megacidades que concentram quase toda a riqueza do país. E a perspectiva é que essa tendência continue (em 2006, 12 aglomerados urbanos representavam 71,34% do PIB total da China; já em 2015, essa proporção passou para 82,03%)(PWCCN, 2018).

Mas boa parte das cidades modernas cresceu de modo muito rápido, desorganizado e sem planejamento (Tabak e Moulin, 2014). Por isso a necessidade de se pensar em novos métodos e sistemas de gestão, controle e ordenamento dos territórios urbanos (Vieira, 2018).

Quando se fala em um modo melhor e mais inteligente de se viver em grandes cidades, hoje se pensa não só no fornecimento de serviços públicos de qualidade, mas também na sua integração física e em rede, a fim de combinar e interconectar uma série de sistemas e infraestruturas que viabilizem não só o desenvolvimento ambiental, mas também sócio econômico. Logo, há quem entenda que o uso de tecnologias de tratamento

de dados seria o primeiro passo para estabelecer a inteligência das cidades (Doneda e Machado, 2019).

Cidades inteligentes seriam, então, aquelas que, por meio da absorção de inovação tecnológica, sobretudo ligada à Tecnologias da Informação e Comunicação (TICs), à Internet das Coisas (IoT) e ao Big Data, conseguem otimizar o atendimento às suas demandas públicas (e que irão variar de acordo com as especificidades de cada cidade) (Doneda e Machado, 2019).

Assim, dentre os indicadores que irão aferir a inteligência das cidades estão não apenas serviços de saúde, iluminação, conectividade e segurança, mas também um controle centralizado, integrado e inteligente da informação dos sistemas e infraestruturas públicas (Doneda e Machado, 2019).

As cidades modernas são, então, como um ecossistema: um ambiente vivo e a céu aberto que cresce e se multiplica (Igarapé, 2018) por meio de complexas interações entre diferentes sistemas, leis, regulamentos e políticas que se retroalimentam e se reforçam mutuamente, transformando-se em plataforma comum e integrada para troca de informações e compartilhamento de dados entre máquinas e indivíduos, a fim de torná-las em espaços céleres, inteligentes e orientados para o bem-estar (PWCCN, 2018).

1.1. Smart Cities como ambiente de inovação e desenvolvimento tecnológico

O boom urbano e demográfico são os fatores que atualmente mais pressionam o planeta, em virtude dos impactos que provocam ao meio ambiente, mas sobretudo à população. No entanto, diante do dilema de melhorar a vida nas grandes cidades, mas também buscar mais recursos e meios de promover o seu crescimento, exigem-se estratégias bem mais complexas para que o desenvolvimento urbano seja sustentado.

É em razão disso que está em curso o projeto global das *smart cities* (Vicente In: Media Lab, 2018). O raciocínio por detrás desses projetos é que cidades inteligentes trariam melhoria nas condições de vida locais, ajudando assim a resolver tanto problemas de gestão urbana quanto de desigualdade social em todo o país, na melhor lógica do 'think global, act local'.

Estima-se que em todo o mundo foram lançados oficialmente mais de mil projetos-piloto de *smart cities*, e mais metade está na China (Phelan In: Healthxl, 2019).

Há sérias razões para que isso aconteça mais China do que em outra parte do planeta. A urbanização chinesa vem acontecendo de modo acelerado e em larga escala, em razão de seus 1,4 bilhão de habitantes (Phelan In; Healthxl, 2019). Realidade que a Índia, p.ex., ainda não enfrenta, pois, apesar de também ser um país superpopuloso, ainda permanece majoritariamente rural, o que minimiza em parte os impactos da pressão demográfica (Barros, 2016).

Ao acompanhar de perto a urbanização chinesa, verifica-se que taxa de residência urbana permanente cresce de maneira rápida e espantosa, subindo de 17,9% em 1978, para 53,7 % da população total em 2013 (China Daily, 2014). Estima-se, assim, que a taxa de urbanização (ou a proporção da população que vive em áreas urbanas) cresça de 58,52% em 2017 para quase 70% em 2030 (Aijaz In: ORJ, 2018).

A situação piora, uma vez que a China não possui apenas grandes cidades, mas também megacidades com mais de dez milhões de pessoas, tais como Pequim, Xangai, Guangzhou e Shenzhen, formando grandes aglomerados humanos (Myers In: WEF, 2016). Logo, não surpreende a atual demanda chinesa por cidades inteligentes (Phelan In: Healthxl, 2019).

Na China, o projeto de *smart cities* não só cresce (em 2018, eram mais de quinhentos) (Phelan In: Healthxl, 2019) como se justifica, já que os impactos da expansão urbana são gigantescos, principalmente para os 25% da população que vive em favelas (WE Forum, 2014), o que acarreta a sobrecarga nos serviços públicos de transporte, saúde e segurança em razão dos engarrafamentos, da poluição do ar e do aumento dos índices de criminalidade.

O governo reconhece as oportunidades e os desafios do momento e trabalha conjuntamente com o setor privado para promover e administrar o crescimento urbano chinês de maneira equitativa e ordenada. Para garantir o crescimento sustentável das cidades, o país colocou em prática uma série de políticas e planejamentos estratégicos em que ciência e tecnologia ganham destaque, sobretudo por meio do Plano Nacional de Nova Urbanização (2014-2020)(Gov, 2014) e o do 13º Plano Quinquenal de Desenvolvimento Econômico e Social (2016-2020)(Gov, 2016), revelando não só o compromisso chinês em acelerar o ritmo dessa transformação, mas também o que se pode esperar da China como política pública para as cidades (Aijaz In: ORJ 2018).

Assim, não só por ser o país mais populoso, mas por ter a maior população urbana do mundo (PWCCN, 2018), a China é o país que resolveu tomar a dianteira desse processo de transformação tanto urbana quanto tecnológica (Aijaz In: ORJ, 2018; Shi-Kupfer; Ohlberg In. MERICS, 2019). A China reconhece, então, o projeto de smart cities como solução para a maioria de seus problemas.

1.2. Smart Cities como sistemas de controle e vigilância

As cidades modernas apresentam-se como ambientes de contrastes e paradoxos, configurando-se em espaços de riqueza, oportunidades e inovação, mas também de pobreza, precarização, cerceamento e controle (Tabak e Moulin, 2014). A modernização digital das cidades é vista, portanto, como via de mão dupla, servindo tanto como força motor para o processo de transformação e solução de seus problemas estruturais, quanto força de estagnação, ao acirrar e reproduzir a noção de cidade como espaços de violência, exclusão social e forte pressão para os serviços públicos (Morozov In: Outras Palavras, 2019).

Por isso, acompanhar o processo de urbanização tem sido uma ferramenta útil não só para mensurar o crescimento global e seus impactos para a população local, como também avaliar o quão sustentáveis são hoje as grandes cidades.

Assim, nada melhor do que inovação e tecnologia para transformar as cidades em espaços de maior e melhor convivência. Essas novidades vêm, sobretudo, da era digital advinda da Quarta Revolução Industrial. (We Forum, 2016)¹.

Mas a ideia de interconectividade advinda da digitalização ou automação pressupõe também a de interdependência e vulnerabilidade. Para atender os mesmos propósitos de gestão urbana, esse ambiente depende cada vez mais da coleta e processamento da maior quantidade de dados possível, reunindo todas as informações disponíveis em uma base de dados integrada, ainda que sem o conhecimento e consentimento prévio da população, o que faz com que esses dispositivos sejam

¹ A Primeira Revolução Industrial usou água e vapor para mecanizar a produção. A Segunda utilizou energia elétrica para criar produção em massa. A Terceira se aproveitou da eletrônica e tecnologia da informação para automatizar a produção. Já a Quarta propicia uma revolução digital que vem ocorrendo desde meados do século passado; caracteriza-se por uma fusão de tecnologias que combina as esferas física, digital e biológica, intensificando o processo de transformação global em rapidez (via Big Data) e em escala (via Inteligência Artificial). We Forum, 2016.

potencialmente invasivos, já que é grande a probabilidade de abuso do direito, violação da privacidade e supressão das liberdades individuais (Braun In: Veja, 2018).

Assim, além de ser um projeto e modelo de governança, **as cidades inteligentes são, em sua própria fundação, um sistema de vigilância** (Wood e Mackinnon, 2019).

Tomando a segurança como exemplo de integração das cidades (Doneda e Machado, 2019), percebe-se o projeto original das smart cities também como laboratório de testes, de controle e vigilância (Wood e Mackinnon, 2019) e de urbanização militarizada (Graham, 2016), principalmente nos contextos dos grandes eventos internacionais, como os Jogos Olímpicos, em que se aceleram os processos de investimento em tecnologia e de desenvolvimento de centros integrados de comando e monitoramento (Bruno, 2018). Como consequência, essas cidades acabam se tornando em territórios desumanizados, tamanho o aparato de controle e automação advindo da multiplicidade de serviços informatizados, sensores físicos e sistemas digitais a fim de garantir maior conectividade e sensação de segurança. Dispositivos digitais que, paradoxalmente, foram criados não para influenciar ou interferir no modo de vida dos cidadãos, e sim lhes proporcionar prosperidade e bem-estar social (Vicente In: Media Lab, 2018).

E há interesses políticos - não só públicos, mas também privados - que objetivam usar as cidades para tal intento. Daí a emergência da chamada “autocracia digital” até mesmo por governos considerados liberais (Hou: In Surveillance & Society, 2017)(Anistia, 2019). É o que Shoshana Zuboff (2015) chama de “capitalismo de vigilância” e Pepe Escobar (In: Outras Palavras, 2016), descreve como “ditadura do algoritmo” já que as decisões cruciais não são tomadas por pessoas, mas por máquinas e algoritmos.

Nos capítulos a seguir, problematiza-se, sobretudo, *o como, para que, para quem, e a cargo de quem* são direcionadas as novas políticas de controle e vigilância urbana.

2. Novos Sistemas de Controle e Vigilância Pública da Era Digital

“A trajetória tecnológica é bastante clara: mais e mais dados serão produzidos sobre indivíduos: a manutenção desses dados, porém, ficará sob o controle de outros” (Zuboff apud Bruno, 2018).

Em tese, a busca por inovação tecnológica pressupõe o desejo de mudança do *status quo* e da realidade vigente. Mas ao invés de transformação social, as tecnologias digitais podem estar a serviço de novas formas de controle e vigilância (Bruno, 2018), assegurando que nada de novo e transformador aconteça na sociedade (Morozov In: Outras Palavras, 2019).

Isso ocorre porque a digitalização não apenas dinamiza a vida cotidiana, mas também opera de forma inteligente, produzindo informação. A informação é extraída a partir de inúmeros serviços de automação e compartilhamento hoje existentes, seja por meio de mecanismos de busca on-line; pagamento eletrônico; fluxo incessante de fotos, textos e mensagens eletrônicas e de uma infinidade de outras interações em chats, aplicativos de smartphones e redes sociais. Toda essa produção digital deixa rastros, o que faz com que os comportamentos individuais e coletivos sejam cada vez mais previsíveis e fáceis de controlar (e pior, de manobrar) (Bruno, 2018). Não por acaso, dados pessoais são os maiores ativos da atualidade (Belli, 2017).

É por conta da generalização da automação de todos os aspectos da vida contemporânea que a tendência de uso crescente de softwares e serviços inteligentes/digitais é tão controversa e alvo de críticas, não só em termos de eficiência, mas também de segurança de dados sensíveis e sigilosos (Belli, 2017). Aparentemente, às empresas de tecnologia importaria mais quantidade do que qualidade na extração e acumulação de dados pessoais. Todavia, enquanto não ficar claro *onde, até quando e para quais* fins serão destinados (Muggah In: Igarapé, 2019), é natural que ainda surjam desconfianças e resistências à nova era digital, ao menos durante a fase necessária para ajustes e transição tecnológica.

2.1. Reconhecimento Facial e Hipervigilância

Com o advento das tecnologias digitais, sobretudo do reconhecimento facial, vigilância e controle são alavancados a outro patamar, o da hipervigilância (Zmoginski,

2019). Não só porque máquinas digitais podem coletar e acumular dados, mas também porque produzem informação, ajudando a fazer prognósticos (por meio de Machine Learning ou máquinas de aprendizado) e a traçar perfis pelo método conhecido como Profiling (Hutchins, 2017).

Hoje em dia existem métodos que também fazem esse tipo de mapeamento identitário, mas em menor escala e abrangência. Isso porque a tecnologia do reconhecimento facial é capaz não só de identificar pessoas suspeitas em aeroportos e placas de automóveis roubados, mas também localizar pessoas desaparecidas e reconhecer rostos no meio da multidão. Seu intuito é, de fato, transformar a cidade em um laboratório vivo e a céu aberto servido de milhões de pessoas e de seus dados pessoais (Intervozes In: Media Lab UFRJ, 2019).

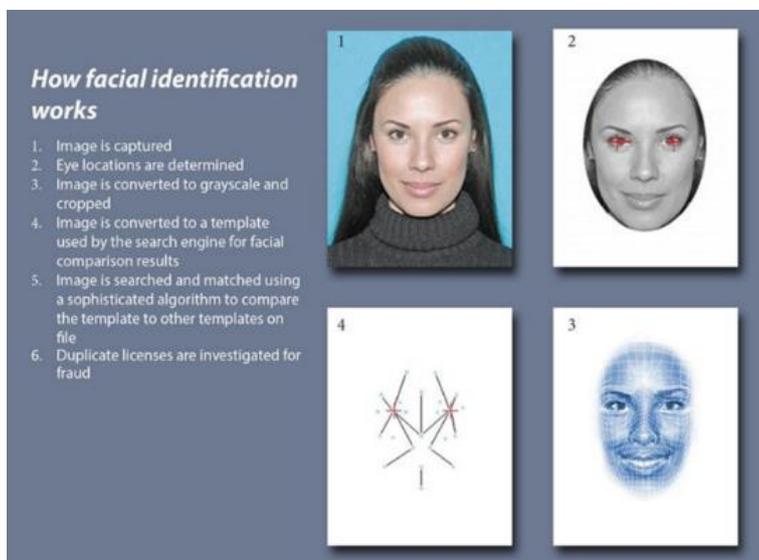


Figura 1. O reconhecimento facial opera da seguinte forma: câmeras inteligentes são instaladas em pontos estratégicos e com grande fluxo de pessoas. 1) A imagem do rosto é captada e, depois, 2) processada por um algoritmo treinado para identificar determinados pontos faciais (como as distâncias do nariz aos olhos; da boca ao queixo); marcas e cicatrizes; contorno da face; formato da extremidade do rosto) e as correlações entre eles (via aferição). 3) Essas informações são usadas para criar um arquivo em interface azul que descreve o rosto e 4) funciona como uma "identidade facial" que é guardada em banco de dados para futuras consultas. Uma vez cadastrada a "ID digital", uma central de monitoramento vai ser acionada e receber um alerta quando a pessoa desaparecida ou procurada por motivos de segurança pública estiver circulando pelo perímetro onde foram instaladas as câmeras de vigilância (Gomes In: UOL, 2019).

Fonte: Iowa Department of Transportation, <https://www.eff.org/pages/face-recognition>.

Sistemas de reconhecimento facial são considerados mais perigosos pois agem diferente de outras formas de vigilância e controle, já que vão além da mera identificação. Ao traduzir dados sobre outros dados (metadados) esses sistemas tornam-se mais propensos ao risco (de discriminação e estigmatização de grupos vulneráveis), a erros de diagnóstico (falsos positivos) e ao abuso de direito (monetização de dados pessoais/sensíveis por empresas e grandes corporações privadas) (Intervozes In: Media Lab UFRJ, 2019).

Mas para que a vigilância e o reconhecimento facial ganhem tamanho alcance e extensão (e, operem como um ecossistema de vigilância), é necessária a combinação de outros recursos tecnológicos como Inteligência Artificial, Big Data, computação em nuvem e Machine Learning, pois sem a associação entre eles não é possível fazer uma identificação precisa (CCTCI, 2019). Isso ocorre porque esse ambiente de hipervigilância depende do processamento da maior quantidade de dados possível, reunindo e cruzando todas as informações disponíveis em um centro de controle e comando integrados.

O reconhecimento facial opera, então, partir da seguinte premissa: quanto mais ampla a base de dados, maior a precisão. Assim, a coleta de dados pessoais de forma isolada não preocuparia tanto. O problema está no tratamento dos dados, ou seja, no seu processamento. É nessa fase secundária que se verifica onde (se ambiente aberto ou controlado), em que contexto (público ou privado), como e até quando os dados serão armazenados; de que forma e para qual utilidade serão empregados; por quem e sob responsabilidade de qual autoridade.

O que preocupa, destarte, é o alcance que será dado àquela informação original, se será compartilhada ou terceirizada (passada para terceiros), com ou sem fins econômicos; para quantos servidores e quais bancos de dados. Assim, o risco maior não está na simples captura de dados (por cookies e aplicativos de geolocalização), mas na combinação e cruzamento dessas informações (Gomes In: UOL, 2019). Há perigo também no armazenamento (em nuvem) uma vez que os dados podem ser hackeados, assim como na eventual manipulação daquela informação por um sem número de processadores ou operadores (entes secundários) que poderiam se locupletar da mercantilização de dados.

Todo esse raciocínio também funciona dentro da lógica reversa, ou seja, de que quanto mais descentralizado o processo de reconhecimento, menores são as chances de se punir e buscar os responsáveis pelo erro de diagnóstico, pela invasão de privacidade e pelo eventual vazamento de informação.

Esses sistemas de reconhecimento tornam-se também mais perigosos dada a facilidade com que a informação ou os dados são disponibilizados/acessados: a) é comum que uma foto de rosto já tenha sido disponibilizada pelo usuário nas redes sociais, sem que seja preciso seu consentimento prévio para coleta de dados; b) bancos de dados contendo nome e face dos cidadãos, como carteira de motorista, também já existem, o que facilita tanto a coleta quanto o armazenamento e cruzamento de dados; c) rostos também são mais difíceis de esconder e podem ser observadas à distância, ao contrário da impressão digital; d) rostos são mais fáceis de rastrear, visto que a vigilância via reconhecimento facial pode ser configurada usando câmeras que já existem nas ruas, reduzindo seus custos operacionais. Logo, em termos comparativos, torna-se uma tecnologia ao mesmo tempo bem mais barata, mas com alto potencial ofensivo (Chinoy In: NYT, 2019).

2.2. Mapeamento Digital e Profiling

A controvérsia acerca da digitalização fica ainda maior em razão do poder preditivo que esse aparato tecnológico possa vir a ter, sobretudo se usado no policiamento urbano (Doneda; Machado 2019), uma vez que este opera – ou deveria fazê-lo - dentro da presunção legal de inocência (Távora, Araújo e Sousa, 2019).

Assim, excluídos os custos materiais do reconhecimento facial, como fica a questão dos impactos e custos sociais? E como é medido o alcance do mapeamento digital e mensurada a abrangência de seu dano (Tam In: SCMP, 2019)?

Para medir o alcance e extensão do dano, antes é preciso falar das 3 camadas da identidade digital. Isso porque os cuidados do cidadão comum só protegem a primeira delas (Szymielewicz, 2019)

Para Katarzyna Szymielewicz (2019), co-fundadora da Panoptykon Foundation, a primeira camada é aquela que você controla. Consiste em dados que você alimenta em mídias sociais e aplicativos móveis, ou seja, aquilo que você espontaneamente revela em suas informações de perfil, suas postagens públicas e mensagens privadas, curtidas de publicações, consultas de pesquisa, fotos enviadas, testes e enquetes realizados, participação em eventos, sites visitados e outros tipos de interações conscientes.

A segunda camada é feita de observações comportamentais. Ela não faz parte das escolhas que se faz de forma consciente, mas de metadados que contextualizam essas

escolhas. Logo, contém informações que provavelmente não se desejaria compartilhar com todos, como localização em tempo real e detalhes de relacionamentos íntimos e contatos profissionais. Ela também rastreia os padrões de quando se está on-line e off-line, conteúdo clicado, tempo gasto lendo, valor e padrão de compras, e até dinâmica e velocidade de digitação e movimentos dos dedos na tela. Assim, são vários recursos psicológicos que algumas empresas acreditam revelar as emoções de uma pessoa.

A terceira camada é composta de interpretações da primeira e da segunda. Os dados pessoais são analisados por vários algoritmos e comparados com os dados de outros usuários para correlações estatísticas significativas. Esta camada é capaz de inferir conclusões não apenas sobre o que fazemos, mas sobre quem somos baseados em nosso comportamento e metadados. Assim, é muito mais difícil controlar a terceira camada, pois embora se possa controlar as entradas (postar fotos no Instagram, p. ex.), não se sabe o algoritmo que está emitindo a saída (essa pessoa precisar tirar férias e viajar) (Szymielewicz, 2019).

A tarefa dos algoritmos de mapeamento de perfil é, então, adivinhar coisas que não seriam reveladas de forma espontânea, como fraquezas, perfil psicométrico, nível de QI, situação familiar, vícios, doenças, relacionamentos, pequenas obsessões (por jogos ou pornografia), e ainda compromissos profissionais (como viagens a trabalho, preparação de projetos e pesquisas). Assim, a coleta de dados extraída da rede social ou do histórico de cartão de crédito é mais confiável do que aquilo que a pessoa expressa ou revela (Christl e Spiekermann, 2016), pois o perfil online nem sempre é construído sobre fatos e interações pessoais. Muitas das decisões que afetam sua vida, agora são ditadas pela interpretação do perfil de dados (Regattieri In: Media Lab UFRJ).

Com a era digital, os processos decisórios também se tornam automatizados, uma vez que as decisões não são mais tomadas apenas por pessoas, mas por algoritmos extraídos da combinação de IA e Big Data. Quando as informações são acessadas/disponibilizadas, os algoritmos (ou a sequência de 1s e 0s que representam um indivíduo) transformam dados em perfis (profiling), o que lhes permite fazer previsões, julgamentos e interpretações comportamentais. Assim, os dados mais valiosos sobre nós são inferidos além do nosso controle, e pior, sem nosso consentimento (Szymielewicz, 2019).

Essa tendência à algoritmização ainda descamba para situações mais complexas já que os algoritmos não são objetos neutros nem autônomos, mas modelados e assim carregados de (pré) conceitos e juízos de valor (Regattieri In: Media Lab UFRJ). Assim, o

mesmo mapeamento de perfis que é usado para o profiling criminal, ou seja, para ajudar a categorizar grupos recorrentemente propensos ao crime, pode também levar à seletividade racial. E uma vez traçados os perfis propensos ao crime, os lugares onde são praticados também se transformam em regiões propensas ao crime (manchas criminais ou hot spots). Na prática, é olhar seletivo da polícia para determinados grupos e territórios vulneráveis (Hutchins, 2017).

É por conta disso que Dave Maass, especialista em liberdade na internet, é contra a tendência mundial no aumento de uso de tecnologias de vigilância por forças policiais (Vicente, 2019). Sistemas de vigilância costumam errar muito (Vicente, 2019), a exemplo da Rekognition da empresa Amazon, que falhou em testes com congressistas norte-americanos, confundindo-os com procurados pela polícia (Estadão, 2018). Assim, o fato de você ser inocente não significa que você não possa ser identificado como culpado ou suspeito.

Logo, em se tratando de controle e vigilância é necessário que se desconstrua a lógica do “não tenho nada a perder” ou de que “sou um bom cidadão logo não serei punido” (IRIS, 2019). Isso porque seu alcance é muito maior do que se imagina. Sem haver qualquer tipo de comunicação ou aviso prévio, esta é feita quando, onde e por quem menos se espera (Intervozes In: Media Lab UFRJ; Revista Forum, 2019).

Mas apesar do reconhecimento facial falhar muito (Vicente, 2019), empresas de tecnologia chinesa têm conseguido se aproximar da perfeição: a MegVii, p. ex., pode dizer com 99,98% de precisão quem é determinada pessoa, desde que seus dados biométricos estejam no banco acessado por ela (Zmozinski, 2019).

Está-se, portanto, diante de um dilema ético-legal-político, pois quanto mais precisas forem as tecnologias de mapeamento e reconhecimento facial, maior será a legitimidade para sua implementação, já que a maior acuidade tende a diminuir eventuais controvérsias e questionamentos sobre os perigos da automação, da biometria e mapeamento digital para restrições de liberdade e direitos civis, bem como para a ampliação e a reprodução de discriminações estruturais (Intervozes In: Media Lab UFRJ, 2019).

No próximo capítulo, o objetivo é ressaltar o papel das reformas, da modernização e dos sucessivos sistemas de controle e centralização estatal para entender o que hoje é a China (Leigh e Martin In: Bloomberg, 2019), uma sociedade que apesar de

aberta ao comércio internacional, ainda continua a seguir um modelo dirigista e políticas neo-mercantilistas (Thayer e Friend In: The Diplomat, 2018).

3. Sistemas de Vigilância e Reconhecimento Facial na China

Desde a vigência da política de reforma e abertura, em 1978, a economia da China vem crescendo fortemente (BBC, 2018). Com a abertura econômica, a sociedade chinesa caminhou em direção a um modo de vida urbano, mas também globalizado, o que incidiu no aumento do poder aquisitivo e no nível de consumo dos dias atuais (Cariello In: CEBC, 2019).

A abertura significou também a incorporação de certos valores e modos de vida ocidentais, o que fez com que esse “gigantesco organismo social” reproduzisse padrões dessa cultura e economia globalizadas. O chamado “sonho chinês” (o equivalente ao “*way of life*” estadunidense) reafirma, portanto, o compromisso da China de harmonizar presente e passado, mas construindo uma modernidade própria (Cariello In: CEBC, 2019).

Apesar dos altos e baixos desses quarenta anos de reformas, a China tem conseguido superar suas dificuldades estruturais. Uma das conquistas foi ter conseguido tirar 740 milhões de pessoas da pobreza (BBC, 2018). E o sentimento de satisfação popular com a política econômica do governo é o que tem gerado legitimidade para o Partido Comunista Chinês (PCC). Mas embora os números continuem invejáveis, sobretudo para os padrões globais, esses não dão conforto suficiente para o PCC governar (Martins, 2019).

O ano de 2019 é um momento importante para a China. O PCC quer usar o 70º aniversário da fundação da República Popular como um olhar para trás acerca das grandes realizações da China sob a liderança do partido. O ano também é marcado por pressões internas para que o governo Xi Jinping cumpra com prazos anunciados pelo PCC como metas para as próximas décadas. Seu cumprimento significaria a realização bem-sucedida de uma sociedade “moderadamente próspera” na China (MERICS, 2019).

Outra importante meta a ser atingida é o da política industrial “Made in China 2025”, por meio da revolução digital e do desenvolvimento doméstico de setores high-tech como robótica, biotecnologia, inteligência artificial, novas energias, automação, veículos elétricos e equipamentos ferroviários e aeroespaciais de ponta (Kennedy In: CSIS, 2015). Seu objetivo é alcançar a autossuficiência e reduzir a dependência tecnológica externa, mas também imprimir uma marca de que o país deixou de ser um mero copador para se tornar referência em inovação (Atkinson e Foote In: ITIF, 2019).

Logo, em se tratando de modernização e rejuvenescimento nacional pensa-se em um processo com características chinesas (Thayer e Friend In: *The Diplomat*, 2018), ou seja, baseado em um modelo que vê na urbanização a solução para os problemas específicos da China (Looney e Rithmire In: HBS, 2016); e, por isso, historicamente baseado em políticas de controle populacional e de natalidade (política do filho único e sistemas de controle migratório, como o Hukou) (Looney e Rithmire In: HBS, 2016) e, mais recentemente, com a era digital, de maior monitoramento do comportamento dos cidadãos.

Assim, além dos problemas tradicionais da China com superpopulação e pressão demográfica, juntaram-se novas questões de uma China rica e próspera (tais como, rápida urbanização, envelhecimento populacional e ascensão socioeconômica de uma elite jovem e urbana) que, uma vez associadas, causam uma enorme pressão para o país. Por isso, as razões do governo para se criar, na China, instituições que historicamente limitem os acessos à terra, ao trabalho e ao capital (Looney e Rithmire In: HBS, 2016).

Esse parece ser o caso da implantação do Sistema de Crédito Social – SCS, já que, de todos os métodos de monitoramento na China, é a medida que mais impressiona, em virtude não só de sua sofisticação, mas também de seu alcance, uma vez que a vigilância deixa de ser um projeto piloto em certas localidades e passa a ser implementado em todo o país (Kainz, Wat, Wang e Kao In: SCMP, 2019).

3.1 Hipervigilância do Ponto de Visto Interno

Embora considerado mais um programa de fidelidade do que um sistema de classificação de crédito, o Sesame Credit Scores foi o primeiro sistema de monitoramento a incorporar dados on-line e off-line para gerar pontuações dos cidadãos com base em categorias específicas (Huang In: Quartz, 2015).

Em algumas regiões do país, o governo também se utiliza da Plataforma de Articulação de Operações Integradas (IJOP, sigla em inglês), atuando em paralelo com o SCS. A IJOP reúne um grande volume de informações necessárias para o pleno funcionamento do programa de monitoramento do comportamento social. Para a ala crítica ao governo, faria parte de um mega sistema chinês de vigilância e controle por meio de filmagens de câmeras de segurança, reconhecimento facial, registro de históricos bancários e outros mecanismos de observação em massa, desde controle de conteúdo e de acessos à internet ao controle de antecedentes criminais. O objetivo é criar um grande

banco de dados contendo o perfil de todos os cidadãos que vivem na China, inclusive estrangeiros residentes (IMIL, 2018).

Na prática, contudo, existiriam tanto barreiras físicas e tecnológicas à pretensão de o SCS ser, já em 2020, um sistema totalmente integrado e operacional (Creemers In: New America, 2018), quanto críticas, sobretudo se seu uso for enviesado para fins políticos de repressão, censura e constante vigilância de opositores ao regime (Vicente, 2019). Governo este que é considerado um dos mais restritivos do mundo (Braun, 2018). Assim, por meio do SCS, a vigilância na China chega ao ápice, já que não se trata apenas de chats, aplicativos e games, e sim de um complexo sistema estatal de controle em massa.

Em 2019, são lembrados os 30 anos do massacre na Praça da Paz Celestial (Tiananmen), em Pequim. Fontes não oficiais estimam que, em apenas dez horas, as tropas do governo tenham matado mais de mil pessoas; dentre elas, manifestantes pró democracia e liberdade de imprensa. A morte do reformista liberal Hu Yaobang é o que teria provocado uma onda sem precedentes de manifestações. Primeiro, em razão do ritmo lento das reformas democráticas e que, depois, se estendeu a questões como inflação e aumento dos custos de vida. Episódio que depois virou tabu e foi proibido de ser comentado na China Continental (Vartanian In: CBC, 2014; Globo News, 2019).

Todos os anos, o 4 de junho é marcado por uma vigília que reúne milhares de pessoas em Hong Kong, único lugar em que se pode lembrar o massacre (Vartanian In: CBC, 2014; Globo News, 2019). Na verdade, a questão que está no centro das manifestações é a histórica tensão do modelo “dois sistemas, um país” (Cheung e Hughes In: BBC, 2019).

Mas, desde Tiananmen, pouco restou daquele ativismo político na RPC. Hoje, as manifestações são mais relacionadas às políticas públicas e questões éticas, religiosas e trabalhistas (Santoro In: Boletim Lua Nova, 2019).

Para ativistas de direitos humanos, como Yang Jianli e Rose Tang, uma das sobreviventes ao massacre, o momento atual é pior, pois mais sombrio. O PCC tem se valido de táticas diversionistas que vão desde campanhas de reeducação e revisionismo histórico (tratando manifestantes pacíficos de Tiananmen como contra-revolucionários) a um controle mais rigoroso pelo governo já que, agora, este usa tecnologia de forma massiva e em larga escala, sobretudo por meio de reconhecimento facial (Vartanian In: CBC 2014; Globo News, 2019) para perseguir minorias (ex. caso dos Uighurs na

província de Xingiang, submetidos ao um massivo regime de vigilância e cárcere em campos de detenção)(Santoro In: Boletim Lua Nova, 2019; Mozur In: NYT, 2019).

Porém, ao contrário do que se possa imaginar, o controle realizado pelo PCC não é visto como uma ameaça; é até preferível que seus dados fiquem sob controle do Estado do que confiá-los a uma empresa privada (Zmoginski, 2019). Assim, compreender o paternalismo estatal como um sistema arbitrário ou mesmo de espionagem remete a uma paranoia do Ocidente e, sobretudo, à resiliência de uma ideologia anticomunista e visão anacrônica de guerra fria. Afinal, os valores asiáticos não são os mesmos do Ocidente (Sen, 1997).

Para entender essa complexa relação, mormente pela ótica ocidental, é preciso olhar para a China em constante movimento. É o que afirma Janaína Câmara da Silveira, jornalista que morou em Pequim de 2007 a 2013. **Em entrevista concedida para essa dissertação**, ela afirma que os chineses mudam costumes, cidades, consumo e tecnologia de formas muito rápidas, como se o país estivesse sempre evoluindo (BBC, 2018). Em 1989, pouca gente estava na classe média e menos ainda na universidade. A China nem estava na OMC. Já os tempos atuais são outros: os jovens têm mais possibilidades de emprego, carreira, estudos e viagens. O povo chinês estaria então mais interessado em manter sua estabilidade social. Já as chamadas “ferramentas de controle” são vistas como balizadoras de um comportamento coletivo harmônico. No atual governo, os controles aumentaram no fluxo de discussão e informação e, nesse ponto, há fricções com a população. Mas não que ela perceba movimentos organizados antissistema.

O intenso e prolongado crescimento econômico também contribui para que não ocorram mais tensões como aquelas que levaram às manifestações de 1989. Protestos são vistos como risco para a prosperidade alcançada (Santoro In: Boletim Lua Nova, 2019).

Ademais, o governo chinês tem sido hábil em convencer a população de que o PCC, o povo e a nação são um todo indivisível (Vartanian In: CBC, 2014). Isso faz com que o cidadão médio confie no governo e não o veja como ameaça ou inimigo. Essa simbiose faz com que sistemas de reconhecimento facial sejam extremamente populares (Kostka In: Merics, 2017), a ponto de 83% dos chineses entendê-los como recurso positivo para aumentar a sensação de segurança (Zmozinski, 2019). Esse dado não os faz indiferentes ou alienados, mas apontam o controle estatal como uma realidade aceita pelos chineses (Gan In: SCMP, 2019).

A combinação de rápida urbanização com sistemas de controle na China, por sua vez, mostra-se perversa e explosiva na perspectiva a longo prazo, já que incerto seu impacto absoluto (Braun, 2018; O’Flaherty In: Forbes, 2019). Um desses efeitos colaterais foi criar uma grande lacuna no modo de vida próspero entre aqueles que vivem nas cidades e os que ainda habitam o campo, provocando um sério conflito geracional. Enquanto os chineses nascidos depois de 1980 vêem a China como uma potência global, rica e de gostos sofisticados, sede de algumas das maiores e mais inovadoras *startups* de tecnologia do mundo, seus pais têm uma vida bem mais modesta, pois nasceram em tempos difíceis, desde guerra, à décadas de longo caos social e fome generalizada (Ma In: Jingdaily, 2019).

Tais mudanças no consumo e no comportamento tem despertado a atenção do governo para a necessidade de uma maior vigilância social. Por isso, Pequim planeja que seu novo Sistema de Crédito Social (SCS) esteja completamente operacional até 2020, funcionando como uma espécie de *ranking* de confiança do governo nas empresas e nos cidadãos, a fim de estimular o cumprimento das leis e tradições, seja premiando os bons, seja punindo maus comportamentos, segundo critérios que vão desde multas de trânsito e fumar em local proibido até acúmulo de dívidas, recusa de ingresso no serviço militar obrigatório e postagem de notícias falsas na internet (Braun, 2018).

Assim, as novas tecnologias digitais terão função chave no recolhimento de dados e informações para o SCS (IMIL, 2018). Por outro lado, um sistema massivo de recompensas e punições preocupa, pois a China é líder mundial em penas de morte (Anistia, 2018), sobretudo para crimes como fraude fiscal, corrupção e tráfico de drogas.

Não por acaso a China é considerada a sociedade mais vigiada no mundo (Zmoginski, 2019). Mas, independentemente de serem medidas ortodoxas, se autoritárias ou não, sobretudo pela ótica do Ocidente (e longe de justificar a repressão na China e afirmar que os fins justificam os meios), são questões complexas a serem enfrentadas por poucos países além da China. Afinal, a Teoria das Relações Internacionais costuma ter certa dificuldade para entender questões que fogem da coerência e do senso comum, como as relacionadas a outras culturas e à influência de potências (não-ocidentais) na ordem internacional (Reus-Smit In: Foreign Policy, 2019).

3.2. Hipervigilância do Ponto de Visto Externo

Os chineses são conhecidos não só por sua cultura e tradição milenares, mas também por sua resiliência e estrategismo (Vaz In: Folha UOL, 2018). Assim, na visão dessa dissertação, apesar de já ser a segunda maior economia do mundo, à China não interessaria confrontar a hegemonia estadunidense e, por conseguinte, desmontar o sistema internacional que lhe conferiu sucesso (Friend In: The Diplomat 2018), e sim manter sua inserção autônoma, *status* de país em desenvolvimento e tratamento diferenciado na OMC, sobretudo para que sua penetração entre os países de menor desenvolvimento se dê de forma mais fluída e, assim, com menor resistência e alarmismo (Friend In: The Diplomat, 2018).

Mas apesar de sua habitual visão de não interferência e confrontação, a ascensão global da China ainda é vista com resistência e desconfiança por considerá-la não só uma violadora sistemática de direitos humanos, mas também uma ameaça aos valores preconizados pelo Ocidente (Friend In: The Diplomat, 2018).

Outro problema a ser enfrentado é a ideia chinesa de experimentação por detrás de conceitos como “desenvolve primeiro, regulamenta depois” (MERICS, 2019) ou até que encontre algum tipo de resistência (Bruno, 2018). Assim, há dúvidas se a China está realmente disposta a criar um ambiente de mercado mais ético, transparente e estável para uma concorrência mais justa, previsível e sustentável. A falta de padrões e maior proteção, sobretudo de regulamentação do setor de tecnologia, tem sido arriscada: em fevereiro, uma empresa chinesa que opera sistemas de reconhecimento facial vazou informações de 2,5 milhões de pessoas, incluindo números de identidade; dados de localização, sexo, etnia e endereço; data de aniversário e foto do passaporte. Em novembro de 2018, um cientista chinês já havia chocado o mundo ao anunciar os primeiros bebês geneticamente modificados (MERICS, 2019).

Ademais, especialistas, ativistas e defensores de direitos humanos acreditam que se sistemas de monitoramento do comportamento social saírem conforme planejado na China, o Sistema de Crédito Social (SCS) pode se tornar um dos projetos mais complexos e em larga escala já desenvolvidos por um governo (IMIL, 2018).

O receio se justifica. Ainda que promovido para coibir fraudes e corrupção, estimulando o cumprimento de leis e regulamentos por empresas e pela população, o SCS chinês pode ter seu uso enviesado, ou seja, deixaria de ser sistema público de pontuação social para também se tornar um aparelho de controle social, vigilância em massa e

policiamento constantes, seja diretamente pelo governo ou em parceria com corporações privadas. Mas os “olhos” do Estado que tudo sabe e vê poderiam acabar surtindo efeito contrário, já que alguns fariam de tudo para escapar de *blacklists* e, assim, burlar seu sistema de privilégios, recompensas e punições (Foucault, 1999).

Ao terem seus comportamentos vigiados e perfis comparados, as pessoas não seriam elas mesmas e mudariam seus hábitos, modos de agir e padrões de consumo em busca não apenas de pontuação e acesso a melhores serviços (Braun, 2018), mas também de aprovação e aceitação no meio social: ao melhor estilo *Big Brother* de George Orwell (Gan In: SCMP, 2019), *Nosedive* de Black Mirror (Kostka In: Merics, 2017), *What Happened to Monday* da Netflix. Logo, preocupa a vigilância como política de governo, uma vez que deixa de ser ficção e distopia para virar realidade (Anistia, 2018).

Além do medo, a visão externa, de um modo geral, é de resistência ao modelo chinês de vigilância (Johnson In: Foreign Policy, 2019), principalmente dos EUA e boa parte de seus aliados (Canadá, Reino Unido, Austrália e Nova Zelândia). Não por acaso estes formam os Five Eyes (Reuters In: UOL, 2019), grupo que propõe uma regulamentação mais rígida das tecnologias emergentes, sobretudo da Inteligência Artificial & Big Data (MERICS, 2019). Os pedidos por mais regulamentação no setor, particularmente no que se refere à inclusão de padrões éticos e proteção aprimorada de dados pessoais, advém do fato de que, atualmente, as empresas privadas são responsáveis só quando ocorrem falhas técnicas ou violações de dados sensíveis, não havendo um código permanente de conduta (Microsoft, 2018).

Esse problema se agrava quanto é notória a proximidade do governo (leia-se Partido Comunista Chinês – PCC) com as empresas chinesas (Munro In: The Guardian, 2018), não havendo uma diferenciação nítida entre o público e o privado. Eis, então, o cerne da questão da vigilância: quando esse sistema se normaliza e deixa de servir apenas para questões de segurança.

Hoje, o dilema da ética e transparência é enfrentado principalmente pela Huawei, gigante chinesa de telecomunicações e rede móvel de quinta geração (5G), alvo de recente boicote pela Google (Muñoz In: El País Brasil, 2019). Mesmo tendo conseguido diminuir a criminalidade em megacidades como Shenzhen (Gomes In: UOL, 2019), a Huawei é acusada de espionagem, roubo de tecnologia e invasão de privacidade (Reuters In: CNBC, 2019), mormente em razão de seu apurado sistema de reconhecimento facial em câmeras de vigilância. A diferença das câmeras da Huawei para outros dispositivos de vigilância é o alto grau de precisão no reconhecimento de objetos e pessoas e os alertas

que o sistema dá ao controlador, aperfeiçoados por sistemas de inteligência artificial (IA). As imagens capturadas pelas câmeras ficam armazenadas em um banco de dados na nuvem, de fácil acesso pelo controlador, seja este uma autoridade pública ou corporação privada (Huawei, 2018).

O caminho da proibição do reconhecimento facial pela polícia já foi tomado por cidades dos EUA como São Francisco, ícone global em inovação e tecnologia, justamente por considerar que os riscos superavam os potenciais benefícios (Estadão, 2019).

Por outro lado, críticos argumentam que há muita hipocrisia em relação ao banimento ou mesmo às restrições impostas à entrada da Huawei no exterior, uma vez que o reconhecimento facial já é feito em aeroportos e outros ambientes controlados, assim como em pontos estratégicos de grande fluxo de pessoas. No Brasil, por exemplo, o reconhecimento facial é uma realidade desde 2011, instalado em capitais e grandes centros urbanos como São Paulo, Rio de Janeiro, Salvador e Campinas (Igarapé, 2019). Sem falar em sistemas de biometria instalados para coibir fraudes em bilhetes de transporte urbano.

Por ironia, empresas chinesas não foram as únicas a se envolver em escândalos de vigilância, invasão de privacidade e falta de limites éticos entre o público e o privado, vide os casos dos EUA e Grã Bretanha (Mozur, Kessel e Chan, 2019) com a Google (Street View) no início dos anos 2000 (Bruno, 2018), a NSA (O Globo, 2017) e o Facebook e a Cambridge Analytica (IRIS, 2018). Ironia maior é saber que na cidade de Nova York, sobretudo após os ataques de 11 de setembro, a polícia vem usando softwares chineses de reconhecimento facial (Chen In: SCMP, 2019). Destarte, ao contrário das clivagens entre Estados, percebe-se que as transações subnacionais, sobretudo parcerias entre cidades globais, continuam a fluir.

Ainda assim, a ascensão tecnológica da China corre o risco de não acontecer de maneira pacífica. A própria tensão entre China e EUA faz parte de um debate mais amplo do que a habitual rivalidade em termos de comércio e tarifas (Rossi In: Folha UOL, 2019). Na verdade, está em curso não uma guerra convencional, mas a disputa pela liderança tecnológica e a divisão do mundo em esferas digitais de influência (Lee, 2017), já que os embates mais importantes não serão decididos nos territórios de China ou EUA, mas em mercados de terceiros (Silveira In: CEBRI, 2019), um dilema a ser enfrentado sobretudo na Europa em razão da expansão da tecnologia 5G (Brattberg, 2019).

A China sai frente dessa disputa pois é o país que tem mais investido na exportação desse modelo de desenvolvimento urbano baseado em inovação e tecnologia digital, principalmente para a América Latina (Vicente In: Media Lab, 2018), em razão do vácuo deixado pelos EUA em suas tradicionais zonas de influência (CEPAL, 2018). Enquanto a Doutrina Trump aposta no protecionismo e isolacionismo dos EUA, a China de Xi Jinping investe em integração digital não só da Eurásia, mas também estendendo seu alcance transoceânico à América Latina por meio da Belt and Road Initiative - BRI (Outras Palavras In: Observatório dos BRICS, 2018). Ao todo, a China tem 171 acordos de cooperação com 123 países (Wenqian, 2019).

Os chineses visam preencher o quanto logo essa lacuna, explorando novos espaços de cooperação em países como Brasil, Equador, México, Panamá, Venezuela e Argentina (Toyama in: Asia Nikkei, 2018; Ellis, 2019), sobretudo exportando e ajudando a internacionalizar o sistema chinês de vigilância (Mozur, Kessel, Chan 2019) para a região que concentra algumas das cidades mais violentas do mundo (CCSPJP, 2017; Serrano-Berthet In: IDB, 2018) e onde o número de homicídios em 2015 era quatro vezes maior que a média global (Alvarado, 2016; Serrano-Berthet In: IDB, 2018). Ainda que entre 2017 e 2018 tenha se verificado uma queda significativa de homicídios no Brasil, os índices ainda preocupam (Igarapé, 2019).

Além de salvar vidas e recompor famílias devastadas pela criminalidade (Pellegrini In: Carta Capital, 2015) há também um forte argumento econômico para facilitar a entrada de novos mecanismos de controle da violência urbana (Comunitas, 2016). Acredita-se que o subcontinente esteja gastando mais no combate à violência do que esteja recebendo de investimento estrangeiro direto (Winter In: Americas Quarterly 2019). Tudo isso faz com que a América Latina seja o maior projeto de influência da China no exterior (Vila-Nova In: Folha UOL, 2019).

O Governo Xi Jinping tem se esforçado para minimizar os efeitos negativos da BRI e da ascensão global da China como um todo (Outras Palavras In: Observatório dos BRICS, 2018) tentando contornar as críticas de que a política expansionista chinesa é agressiva e predatória, de que usa tecnologias sujas e destrutivas, pouco verdes, transparentes, pouco afeitas aos valores democráticos ocidentais (MERICS, 2019).

A rivalidade entre EUA e China aumenta ainda mais quando a ascensão global chinesa e o crescente processo de (re) orientalização do mundo vem acompanhado do declínio relativo do Ocidente e crescente crise das instituições democráticas e econômicas mundiais (Martins, 2019).

Essa mudança geopolítica romperá, então, com dois paradigmas, significando tanto mudança na ordem internacional quanto nos próprios rumos da globalização: de uma globalização neoliberal do Consenso de Washington para uma globalização interdependente liderada pela China e o Consenso de Beijing. Na prática, são apresentados ao mundo dois modelos econômico e político distintos: o Ocidente propondo economia de mercado e democracia representativa e o Oriente marcado pela presença estatal no mercado e pelo autoritarismo na política (Outras Palavras In: Observatório dos BRICS, 2018).

Fenômeno que a HRW (2019) e Anistia (2019) vem chamando de emergência de uma “autocracia digital” caracterizada pela supressão de liberdades individuais e violação sistemática de direitos humanos, o que inclui o atual governo da China.

Não é à toa que o aumento da demanda por sistemas de vigilância coincide com uma guinada global para o autoritarismo (Hou In: Surveillance & Society, 2017).

Toda essa discussão é pertinente, pois se insere nos debates acerca de um possível processo de reconfiguração global (ou reglobalização) e de quais seriam os impactos para o Brasil (se o Brasil deveria ou não se adaptar a essa nova realidade, a fim de não correr riscos ou perder oportunidades em razão de uma decisão tardia)(CEBRI, 2018). Nas palavras do professor Maurício Santoro, “o Brasil precisa se decidir sobre a China ou ficará para trás” (Santoro In: Época, 2019). É o que veremos a seguir.

4. Estudo de Caso, Posicionamento e Proposições

No Brasil, bem no início do atual governo, bancada do partido foi à China para importar técnicas de reconhecimento facial, tendo em mente apresentar projeto de lei para torná-la obrigatória em locais públicos, auxiliando as forças de segurança pública no combate ao crime. A ideia é adotar no Brasil a mesma tecnologia de vigilância utilizada na China (Rebello In: UOL, 2019). Dentre os casos recentes de reconhecimento facial no país, está o de Marcos Vinícius de Jesus Neri, um homem negro e foragido da polícia que foi preso depois de ser flagrado por uma câmera chinesa da Huawei no Carnaval de Salvador. Fantasiado de melindrosa e com uma metralhadora de brinquedo na mão, Marcos Vinícius havia sido condenado por homicídio com arma de fogo (Távora, Araújo e Sousa, 2019). A iniciativa da Secretaria de Segurança Pública da Bahia teria sido o primeiro caso de prisão decorrente de reconhecimento facial no Brasil (Huawei, 2018).

Considerando os aspectos envolvidos, eis o posicionamento e as proposições:

a) Crime e violência urbana estão entre os maiores desafios da América Latina, em razão dos altos índices de homicídios, sobretudo no Brasil, em razão da morte de jovens pobres e negros (Pellegrini In: Carta Capital, 2015). A solução requer agir em muitas frentes, mas melhorar o funcionamento das instituições de segurança está no topo das prioridades (Alvarado In: o Globo, 2016). Isso requer um novo modelo de segurança pública baseada mais em evidências do que em crenças e experiências pessoais, aproximando o conhecimento científico à prática nas ruas (Comunitas, 2016). E as evidências demonstram que o aprimoramento das polícias contribui para a redução dos índices de violência, ao menos no curto prazo (Alvarado In: O Globo, 2016).

b) O reconhecimento facial, como forma de auxílio e aprimoramento das forças policiais, mostra que a tecnologia, quando bem empregada e de forma inteligente (via cruzamento de dados e troca de informações para checar e verificar a identidade de um indivíduo) aumenta a eficácia e a eficiência do policiamento.

c) Dentro dessa **nova concepção de segurança que se prioriza não a repressão, mas a prevenção da violência**, municípios passam a ter um papel fundamental. Fala-se, então, em **Segurança Cidadã e no crescente protagonismo e poder político das cidades**, por meio da construção de uma agenda proativa, horizontal e compartilhada, fruto da concertação, articulação e amplo debate entre instituições públicas, secretarias municipais, academia, empresários e representantes da sociedade civil. Esse foi o caso da cidade de Medellín que, sem deixar de lado a repressão, passou a ser mais focada em

prevenção e aproximação comunitária, por meio de investimentos em educação, urbanismo e infraestrutura de bairros pobres da Colômbia (Comunitas, 2016).

d) Com prevenção e trabalho de base, o problema da violência e do crime deixa de ser responsabilidade exclusiva do governo e passa a ser enfrentado através de políticas públicas planejadas, integradas e multidisciplinares. Também deixa de ser centrado na ação da polícia, saindo de uma visão tradicional reativa (de atuação somente após a ocorrência do crime) para uma atitude de prevenção da violência. Evita-se a sobrecarga da atividade policial e possíveis danos psicológicos e econômicos decorrentes do crime, como a morte precoce de jovens e negros (Comunitas, 2016), perfil de indivíduos com mais probabilidade de morte violenta no Brasil (IPEA, 2019).

e) Sistemas de vigilância, por outro lado, quando deixam de ser de interesse exclusivamente público, passam a ser modelados de maneira seletiva e territorializada, servindo como mecanismo de criminalização de grupos vulneráveis (Anistia; HRW 2019).

f) Ao mapear comportamentos criminais e categorizar indivíduos, corre-se o risco de se estigmatizar determinados grupos (seletividade étnica, racial e de gênero) e territórios onde se praticam as infrações (manchas criminais ou hot spots). Ressalta-se o perigo que isso representa para liberdades e direitos civis, sobretudo em governos autoritários que possam empregar tal recurso para efeito de repressão, perseguição e vigilância em massa.

g) Sistemas de reconhecimento facial costumam ser imprecisos e falhos com negros, latinos e indígenas em razão da sub-representação das minorias nos campos da STEM (ciência, tecnologia, engenharia e matemática). Logo, também podem servir como método de controle social e político (Pellegrini In: Carta Capital, 2015), seja acirrando e reproduzindo práticas ilegítimas, preconceituosas e discriminatórias, seja identificando certos grupos ao invés de outros (McCullom, 2017).

h) É por conta da imprecisão (caso dos falsos positivos) que há tanta controvérsia quanto ao uso do reconhecimento facial em determinados setores, sobretudo pelo perigo que seu poder preditivo representa para a área da segurança pública. No Brasil, a prisão de suspeitos sem que tenha havido flagrante torna-se um imbróglio jurídico constitucional.

i) Sistemas de reconhecimento facial através de vídeo monitoramento e mecanismos de georreferenciamento e biometria aumentam significativamente a distância entre controlados e controladores, visto que a vigilância é alavancada a outro patamar, a da hipervigilância. Na tentativa de localizar e reconhecer foragidos da justiça no meio da multidão, sistemas de vigilância expõem milhares de outras pessoas. Isso viola os princípios da intimidade, do contraditório e da presunção de inocência, já que parte do pressuposto de que todos ali presentes são culpados ou suspeitos em potencial (Távora, Araújo e Sousa, 2019).

j) Quanto mais extensa a base de dados e avançada a tecnologia, maior o poder de precisão (mas também maior seu poder de alcance). O método do reconhecimento facial é comparativo por aferição, ou seja, a imagem é captada, comparada e, em seguida, processada; portanto, os detalhes captados irão variar conforme o grau de complexidade da tecnologia utilizada, assim como da extensão e abrangência do banco de dados. Logo, sem uma abordagem técnica de clara aferição (via IA), a partir de uma boa base de dados estatísticos (Big Data), tal recurso tecnológico passa a ter eficácia limitada.

l) Outro fator a ser considerado, além da coleta e captura de dados, é o da produção de informação sobre as pessoas, seja a partir da invasão da intimidade e privacidade, seja da terceirização e mercantilização de informações sigilosas, dados sensíveis para seguradoras, planos de saúde e outras empresas com fins privados. Este seria o caso da empresa chinesa Huawei, por meio de parcerias estabelecidas com as principais operadoras de telecomunicações no país. A Huawei nega que detenha o controle dessas informações; estas seriam armazenadas por um tempo e, depois, eliminadas. Mas, na prática, as parcerias são estratégicas devido à vasta clientela de operadoras de telefonia móvel e banda larga que compra acesso à fibra ótica para a instalação de câmeras de vigilância (Huawei, 2018).

m) A questão da terceirização também funciona dentro da lógica reversa, ou seja, de que quanto mais descentralizado o processo de produção de informação, menores são as chances de se punir e buscar os responsáveis pelo erro, pela invasão de privacidade e pelo eventual vazamento de dados sensíveis e de informação sigilosa.

n) A diferença das câmeras chinesas está, então, no alto grau de precisão no reconhecimento de pessoas e objetos (Huawei 2018), fato que a torna potencialmente mais invasiva e perigosa, sobretudo em relação a seus concorrentes.

Tecnologias de reconhecimento facial são, portanto, intrusivas, aumentando consideravelmente as assimetrias de poder gerada por relações de vigilância. O grande dilema da atualidade é como construir um ambiente em que IA, Big Data e automação digital se conciliem e sejam motivo de inclusão e não de exclusão social. São paradoxos causados pelo desejo de hiperconectividade, segurança e automatização (algoritmização) de amplo aspecto da vida cotidiana. Os cidadãos, por sua vez, ficam cada vez mais dependentes tecnologicamente e, assim, mais vulneráveis e expostos ao abuso de poder, violações de liberdades e direitos civis.

O caminho da proibição do reconhecimento facial foi tomado por cidades como São Francisco, justamente por considerar que os riscos superavam os potenciais benefícios. Mas ao optar pela negação da tecnologia, as cidades correm o risco de ficar paradas no tempo ou à margem da evolução que se espera a partir da revolução digital.

Quando empregado apenas para efeito de mapeamento estatístico e categorização de perfis criminais, o reconhecimento facial busca reduzir custos gerenciais e operacionais do policiamento. Já quando operado ou controlado por empresas ou governos sem maior compromisso com a sociedade, o interesse pode ser outro, de caráter simplista e imediatista, concentrado mais em trazer sensação de ordem e segurança para a população do que propriamente resolver problemas estruturais de insegurança e violência urbana. Sistemas de vigilância seriam, então, mais eficazes para resolver problemas de governança e do ambiente de negócios do que transformar a realidade das grandes cidades. A própria China é acusada de usar a revolução digital para esse fim. Ao monetizar a rede 5G, a China apoiaria efetivamente o projeto das smart cities como também contribuiria para a base de sustentação das chamadas “sociedades inteligentes”, legitimando-se como potência global (PWCCN, 2019).

Quando se trata de inteligência e inovação tecnológica, as cidades estão seguindo uma tendência mundial de aumento no uso de tecnologias digitais de vigilância por forças policiais, apostando-se naquilo que a polícia é mais carente: em prevenção. Mas ao apostar somente em automação e tecnologia, deixa-se a descoberto o outro lado da segurança, que é o aparelhamento humano, não só em termos de proteção da população vulnerável, mas também do policial carente de melhor treinamento, formação profissional e capacitação técnica. Sem falar na reestruturação da política de drogas e armas e dos sistemas judicial, carcerário e prisional (Winter In: Americas Quarterly, 2019). Afinal, a tecnologia por si só não é capaz de transformar uma realidade estabelecida por anos de violência e violações sistemáticas de liberdades e direitos humanos. Um sistema de

polícia corrupto, por exemplo, não será resolvido somente pela tecnologia (Vicente, 2019).

Ao priorizar o aparelhamento da segurança pela via automatizada, contribui-se também para outros desdobramentos no longo prazo; problemas que extrapolam a agenda de securitização, trazendo impactos não apenas socioeconômicos, mas também riscos de dependência tecnológica, perda de soberania, em uma espécie de reedição do colonialismo (Munro In: The Guardian 2018) ².

Por essas razões, as tecnologias digitais são ainda de eficácia e precisão bastante limitadas para serem comercializadas e operacionalizadas sem a devida supervisão e regulamentação. Acredita-se, entretanto, que a tecnologia digital, quando bem empregada e de forma inteligente (Winter In: Americas Quarterly, 2019), pode ser a resposta para solucionar muitos dos problemas e desigualdades sociais do século XXI. Inovações tecnológicas são, portanto, bem-vindas e não deveriam representar perigo, mas sim o uso que é feito delas. Por isso mesmo, reconhece-se que a tecnologia não é neutra nem apolítica, podendo ser canalizada para a tomada de decisões em determinados momentos históricos, seja visibilizando ou invisibilizando grupos e agendas em detrimento de outro(a)s.

Logo, percebe-se uma forte **interconexão entre cidades modernas, vigilância digital e neoliberalismo** (Bruno, 2018). Assuntos que não só se inter-relacionam; mas também confundem os limites entre o público e o privado, assim como o cível e o militar.

A rápida expansão das cidades gerou a necessidade de adaptação para a realidade do século XXI, mediante novos padrões de gerenciamento, controle e vigilância dos espaços urbanos. Por isso o surgimento de um novo urbanismo digital que fica no limiar das necessidades do mercado e da militarização (Barreira, 2017).

Para que as cidades se tornem espaços mais eficientes, competitivos e sustentáveis no futuro, é preciso que, a todo momento, empresas e governos procurem gerenciar riscos, reduzir gastos e baratear custos. Fato que, se por um lado, gera disputas

² O professor Paulo Esteves (In IE-UFRJ 2017), ao se referir à eventuais assimetrias provocadas pela internacionalização ou ascensão global da China, fala no estabelecimento de novos padrões de dependência externa via comércio, investimento e tecnologia, sobretudo para o Sul Global. A dependência viria em decorrência de desequilíbrios da relação no longo prazo. Esses países não teriam recursos, estrutura ou amadurecimento institucional para negociar de igual para igual e arcar com eventual endividamento com o país asiático; a China, portanto, teria de ser mais transparente e responsável antes de se lançar para o mundo (China's Going Out) e exportar seu modelo de desenvolvimento.

políticas pela monetização de dados pessoais, do outro, gera resistência e necessidade de controle das técnicas de informação e comunicação e, conseqüente, limitação do amplo acesso aos benefícios gerados pela tecnologia digital (SCMP, 2019).

Assim, pode-se afirmar que a origem da retórica de que a RPC representa uma ameaça à segurança não está exatamente no aumento do déficit comercial dos EUA (Outras Palavras In: Observatório dos BRICS, 2018), mas sim no ideal chinês de interdependência hegemônica e prosperidade compartilhada. Agora, quando a China disponibiliza tecnologias de vigilância para governos que antes não podiam pagar, ela ganha principalmente a fidelização de mercados preferenciais (Mozur, Kessel e Chan, 2019). O problema de fundo, portanto, não se resume às perdas competitivas, mas à questão do monopólio e transferência de tecnologia via financiamento e facilitação dos acessos ao desenvolvimento antes restrito a um reduzido grupo de países.

Assim, banir ou mesmo impor restrições à entrada de novas tecnologias só porque originárias de um país distante como a China, de civilização, cultura e valores distintos e desconhecidos por boa parte da sociedade, é negar o papel da ciência e tecnologia como processo de transformação. Banaliza-se ainda mais quando estão envolvidas rivalidades sistêmicas e interesses geopolíticos pela liderança tecnológica.

Trata-se de desafios a serem enfrentados por toda comunidade internacional, já que um ambiente de excessiva regulação não é ruim apenas para o ambiente de negócios, mas também cria barreiras para que empresas e potências emergentes entrem e contestem o poder estabelecido. Como estamos em um processo de transição e adaptação tecnológica (Muggah In: Instituto Igarapé, 2019), resta saber se o discurso chinês de desenvolvimento mútuo é verdadeiro ou trata-se de mera retórica.

Mas espera-se que, ao final dessa dissertação, tenha se conseguido firmar o argumento de que a ascensão global da China vem movida mais por uma necessidade de autopreservação do que de controle e dominação do mundo. Autopreservação entendida em várias conotações, desde sustentação do modo atual de vida chinês, de legitimidade do PCC ou da própria identidade nacional, a fim de que na China não se repita a fragmentação política que aconteceu com a ex-URSS. Por outro lado, ao adquirir expertise tecnológica e, assim, ganhar confiança no “sonho chinês”, a China põe de lado sua habitual postura confuciana e assume uma posição mais assertiva no mundo. Tal posicionamento se evidencia não só ao implementar domesticamente um modelo próprio de urbanização baseado em inovação e tecnologia, mas também ao tentar replicá-lo externamente, sobretudo em outros países em desenvolvimento e com dificuldades

semelhantes às suas (mas cujo quesito “necessidade” não se compara à da China). A realidade urbana da América Latina é um bom exemplo.

Porém, é bom lembrar que, se a China optou por esse modelo de desenvolvimento, o fez da maneira consciente e, sobretudo, por intermédio de planejamento estratégico, gerenciamento de riscos e redução de danos. Ou seja, ao sopesar prós (ganhar tempo, aproveitar a janela demográfica e mão de obra excedente) e contras (conflitos geracionais e discrepâncias socioeconômicas), a China assumiu o risco e resolveu que compensava apostar no salto tecnológico, mesmo que diante de implicações para o povo chinês.

E é diante dos impactos negativos para a população que pairam a maioria das críticas, do ceticismo e das desconfianças quanto à ascensão da China como nova potência digital. No entanto, os fundamentos para tamanha resistência procedem somente em parte.

Há muita hipocrisia por parte de outras potências. Há anos EUA e Grã-Bretanha também observam o comportamento de seus cidadãos (Muggah In: Instituto Igarapé, 2019). E, apesar de envolvidos em sucessivos escândalos de espionagem e invasão de privacidade, nem por isso deixaram de fazê-lo (o emprego de Body Cameras na abordagem policial é um bom exemplo de tecnologia de uso controverso, mas que hoje vem se normalizando). Contudo, aos olhos da comunidade internacional, o mesmo não poderia ser feito pela China, em razão de ser um regime autoritário pouco comprometido com transparência e responsabilidade (Mozur, Kessel e Chan, 2019).

Não é à toa que, agora, empresas como a Microsoft demandem códigos permanentes de conduta e maior regulamentação no setor das TICs. As principais preocupações com o reconhecimento facial são com relação a seu atual estágio de desenvolvimento, sua disseminação de maneira indiscriminada em todos os setores da sociedade e seu uso como programa de governo (Microsoft, 2018). Para resolver esses problemas seria necessário maior empenho nos processos de regulamentação legislativa e de aperfeiçoamento da tecnologia (Microsoft, 2018).

Por hora, é preciso transparência e maior informação por parte da China para que a replicação de novas formas de vigilância urbana não seja vista como uma ameaça externa, sobretudo no campo da segurança pública. Assim como sinalização de fornecedores privados de que haverá prestação de contas, auditoria, apuração e

responsabilização dos culpados não só em caso de invasão de privacidade e violação de dados, mas de forma permanente.

Já no âmbito local de seus parceiros, algumas medidas são bem simples e de baixo custo, como a promoção de debates e audiências públicas acerca das consequências da tecnologia (principalmente antes que sistemas de vigilância se normalizem e exacerbam os problemas já existentes com automação, vigilância em massa e violação de direitos humanos em razão do uso excessivo da força policial).

É preciso também mais divulgação e campanhas midiáticas sobre prós e contras da vigilância massiva e contínua, para que as análises não sejam precipitadas ou mesmo enviesadas. Com isso, gera-se maior engajamento popular e visibilidade, assegurando que a informação esteja disponível para todos. É uma maneira também de aproveitar o conhecimento da comunidade local para complementar as lacunas de dados administrativos e de estatísticas criminais (Muggah In: Instituto Igarapé, 2019).

Percebe-se que a resistência é maior na segurança do que em outros setores, por isso a importância de diagnósticos críticos para também se falar sobre oportunidades e benefícios da tecnologia no combate e prevenção da violência: auxiliando, por exemplo, na localização de crianças desaparecidas (Microsoft, 2018).

Há outras medidas cabíveis, como aceleração do processo de regulamentação; maior comprometimento com qualidade e precisão da tecnologia; testagens, certificações e trocas de experiências; supervisão humana; envolvimento claro e franco com fornecedores privados; fixação de métricas claras para monitoramento e avaliação de resultados e, principalmente, identificação adequada de onde e quando as novas tecnologias estão sendo testadas, não bastando o mero aviso que o cidadão está sendo vigiado, mas consentimento para fins específicos (Microsoft, 2018).

Por ironia, todo o debate acerca da privacidade nasceu da necessidade de aperfeiçoamento dessas novas tecnologias de vigilância e vídeo monitoramento e, por conseguinte, do aprofundamento das questões de aviso e consentimento; equidade e não discriminação racial, étnica e de gênero; transparência e prestação de contas; e de garantias e salvaguardas para as liberdades democráticas (Microsoft, 2018).

5. Conclusão

A América Latina é considerada um dos lugares mais violentos do mundo, havendo mais homicídios na região que a média global, sobretudo em razão da morte de jovens pobres e negros nas grandes cidades do Brasil. Mas não há uma situação de violência que justifique políticas de repressão ao crime e supressão de liberdades e direitos individuais. Existe, sim, urgência de reforma da política de segurança a fim de reduzir os índices de homicídios e dos altos custos da criminalidade para a região, assim como salvar vidas tanto de civis quanto de policiais.

Hoje, a crise de violência e insegurança ganha complexidade local já que grandes cidades são cartão postal para o mundo. Logo, em se tratando de estabilidade e segurança para o turismo e o investimento estrangeiro, fica a imagem negativa da violência urbana que é projetada para o exterior. Grandes cidades passaram, então, a servir de laboratório de testes e de novos experimentos tecnológicos, sobretudo por meio de projetos de *smart cities*, a fim de se tornarem mais inteligentes e seguras, retomando assim confiança e credibilidade em seu potencial de transformação.

Em se tratando de novas tecnologias de policiamento e prevenção da violência urbana, a China é uma referência global, sobretudo por seus apurados sistemas de reconhecimento facial. Ao tentar replicá-los, grandes cidades estão seguindo uma tendência de aumento no uso de tecnologias digitais de vigilância por forças policiais. No entanto, deveriam ser usadas como meio auxiliar, e não como regra na abordagem policial e na tomada de decisões. Sem preparação e planejamento, tendem não só a acirrar preconceitos, racismos, desigualdades estruturais, como também reproduzi-las, podendo servir tanto de mecanismo de vigilância de certos territórios e grupos mais vulneráveis, como moradores de favelas e periferias, quanto de censura, criminalização e encarceramento em massa de ativistas e defensores de direitos humanos. Por isso, antes de ganharem força de lei, sistemas de vigilância e reconhecimento facial deveriam ser avaliados e sopesados.

Na América Latina, as políticas de segurança falham porque costumam ser de responsabilidade exclusiva do governo e centradas somente na ação da polícia, sobrecarregando a atividade policial. Logo, está equivocada a abordagem do problema tanto na sua fase de formulação quanto de implementação, insistindo-se no enfrentamento da violência urbana pelo confronto armado militarizado, quando o ideal seria a conjugação de repressão e prevenção da violência.

Agora, quando se busca inteligência e inovação tecnológica, aposta-se naquilo que o policiamento é mais carente, ou seja, em prevenção, sobretudo para torná-lo uma atividade menos arriscada e de menor custo operacional. No entanto, para real enfrentamento da crise de insegurança e descontrole da violência urbana, não basta importar técnicas de reconhecimento facial para auxiliar as forças de segurança no combate ao tráfico de armas e drogas, crime organizado e captura de foragidos da justiça. Primeiro, porque se incorreriam em riscos desnecessários e, segundo, porque os custos socioeconômicos não compensariam os potenciais benefícios. As tecnologias digitais são ainda de eficácia e precisão bastante limitadas para serem comercializadas e operacionalizadas sem supervisão e regulamentação adequadas. A tecnologia *de per se* não é uma solução milagrosa e, por isso, deve vir associada ao planejamento estratégico e melhor aparelhamento humano.

Não se trata, porém, de banir a entrada das novas tecnologias só pelo fato de que são originárias da China, considerada uma das sociedades mais repressivas e vigiadas do mundo. Ainda que China e América Latina tenham realidades distintas, é possível replicar o modelo chinês, mas mediante algum tipo de limite, supervisão, regulamentação legislativa e responsabilização; assim como transparência, código ético de conduta e prestação periódica de contas (e não apenas quando ocorrem violações de direitos humanos e uso excessivo da força policial). *Encoraja-se, portanto, a solução para a crise de violência urbana por intermédio de uma política de segurança mais humana e menos centrada no controle, vigilância em massa e automação do policiamento preventivo.*

A proposta é de conjugação da ação da polícia à melhoria do bem-estar social, tanto da população (mediante desenvolvimento e inclusão social; trabalho de base continuado e de aproximação comunitária), quanto do policial (mediante treinamento, capacitação profissional e acompanhamento psicossocial). Defende-se, portanto, o aprofundamento da ideia de segurança mediante uma visão mais sistêmica e ampla do que o tradicional modelo repressivo, já que pensada sob a perspectiva de direitos (de forma menos conflitiva e mais cooperativa; logo, mais humana e a longo prazo, de ênfase local e de amplo acesso da população ao direito à Cidade).

O objetivo é focar menos na tradicional política de confronto armado e centrada na ação da polícia para, então, se adotar uma nova política segurança com visão menos repressiva e reativa, e que retome o conceito de segurança cidadã, de ação multidisciplinar, integrada e coordenada entre policiamento preventivo, desenvolvimento e inclusão social, e de uso de dados de forma mais inteligente, eficaz e eficiente.

A princípio, isso será feito por meio de auditorias, mecanismos de certificação e monitoramento das tecnologias digitais de vigilância e reconhecimento facial. E, a longo prazo, via planejamento estratégico e regulamentação pública, a fim de mitigar riscos, reduzir danos e potencializar benefícios. Assim, direitos individuais e liberdades democráticas serão preservados e haverá bem menos perigo de um sistema de vigilância em massa se normalizar.

6. Referências bibliográficas

AIJAZ, Rumi. **China's urban transformation strategy**. In: ORF. Publicado em 20 jun. 2018. Disponível em: <https://www.orfonline.org/expert-speak/41760-china-urban-transformation-strategy/>. Acesso em 19 jun. 2019.

ALVARADO, Natalie. **Por que as reformas da polícia fracassam?** In: O Globo. Publicado em 9 out. 2016. Disponível em: <https://oglobo.globo.com/opiniao/por-que-as-reformas-da-policia-fracassam-20258604>. Acesso em 20 mar. 2019.

ANISTIA INTERNACIONAL. **Brasil: discurso anti-direitos não pode se tornar política governamental**. Publicado em 28 out. 2018. Disponível em: <https://anistia.org.br/noticias/brasil-discurso-anti-direitos-nao-pode-se-tornar-politica-governamental/>. Acesso em 21 mar. 2019.

_____. **O Estado dos Direitos Humanos no Mundo. Informe 2017/2018**. Disponível em: <https://anistia.org.br/wp-content/uploads/2018/02/informe2017-18-online1.pdf>. Acesso em 20 jun. 2019.

ATKINSON, Robert D.; FOOTE, Caleb. **Is China Catching Up to the United States in Innovation?** In: ITIF. Publicado em 8 abr. 2019. Disponível em: <https://itif.org/publications/2019/04/08/china-catching-united-states-innovation>. Acesso em 20 jun. 2019.

BARREIRA, Marcos. **Depois do Modelo Olímpico: As Favelas Cariocas Entre o Mercado e a Militarização** In: Revista Continentes (UFRRJ), ano 6, n. 10, 2017.

BARROS, Mariana. **De maioria rural, Índia vive o desafio de criar cidades que não se tornem ilhas de prosperidade em um mar de miséria**. In: VEJA. Publicado em 5 dez. 2016. Disponível em: <https://veja.abril.com.br/blog/cidades-sem-fronteiras/de-maioria-rural-india-vive-o-desafio-de-criar-cidades-que-nao-se-tornem-ilhas-de-prosperidade-em-um-mar-de-miseria/>. Acesso em 21 jun. 2019.

BELLI, Luca. **Seus dados são o novo petróleo: mas serão verdadeiramente seus?** In: O Globo. Publicado em 1 jun. 2017. Disponível em: <https://oglobo.globo.com/opiniao/seus-dados-sao-novo-petroleo-mas-serao-verdadeiramente-seus-21419529>. Acesso em 20 jun. 2019.

BRATTBERG, Erik. **Should Europe Buy Chinese 5G Technology?** Publicado em 18 mar. 2019. Disponível em: <https://carnegieendowment.org/2019/03/18/should-europe-buy-chinese-5g-technology-pub-78610>? Acesso em 30 mar. 2019.

BRAUN, Julia. **Na China, atos dos cidadãos valerão pontos e limitarão seus projetos.** In: VEJA. Publicado em 15 nov. 2018. Disponível em: <https://veja.abril.com.br/mundo/na-china-atos-dos-cidadaos-valerao-pontos-e-limitarao-seus-projetos/>. Acesso em: 19 mar. 2019.

BRUNO, Fernanda (Org). **Tecnopolíticas da Vigilância: perspectivas da margem.** 1ª ed. São Paulo: Editora Boitempo, 2018.

BBC. **Reformas econômicas: 9 gráficos que mostram a transformação da China em 40 anos.** Disponível em: <https://www.bbc.com/portuguese/internacional-46599555>. Publicado em 19 dez. 2018. Acesso em 20 jun. 2019.

CARIELLO, Tulio. **O que esperar do governo chinês em 2019?** In: CEBC. Carta Brasil China. Edição 22, Abril, 2019. Disponível em: <http://cebc.org.br/download/3894/>. Acesso em 29 abr. 2019.

CCTCI - Comissão de Ciência e Tecnologia, Comunicação e Informática. **Audiência Pública: A Questão das Tecnologias de Reconhecimento Facial para Aplicação em Segurança Pública no Brasil.** In: Câmara dos Deputados. Publicado em 3 abr. 2019. Disponível em: <https://edemocracia.camara.leg.br/audiencias/sala/840>. Acesso em 5 abr. 2019.

CCSPJP - Consejo Ciudadano para la Seguridad Pública y la Justicia Penal. 2018. **Ranking de ciudades 2017.** Disponível em: <https://www.seguridadjusticiaypaz.org.mx/ranking-de-ciudades-2017;> <https://www.scribd.com/document/373324071/Las-50-Ciudades-Mas-Violentas-del-Mundo-2017#download>. Acesso em 20 jun. 2019.

CEBRI - Centro Brasileiro de Relações Internacionais. **O Choque de Globalizações: Impactos sobre o Brasil.** Breaking News #16. Publicado em nov. 2017. Disponível em: <http://cebri.org/portal/publicacoes/cebri-artigos/o-choque-de-globalizacoes-impactos-sobre-o-brasil>. Acesso em 28 jan. 2019.

CEPAL - Comisión Económica para América Latina y el Caribe. **Explorando nuevos espacios de cooperación entre América Latina y el Caribe y China.** Publicado em jan. 2018. Disponível em: https://repositorio.cepal.org/bitstream/handle/11362/43213/1/S1701250_es.pdf. Acesso em 20 jun. 2019.

CHEN, Stephen. **The Chinese technology helping New York police keep a closer eye on the United States' biggest city.** In: SCMP. Publicado em 11 jan. 2019. Disponível em: <https://www.scmp.com/news/china/science/article/2181749/chinese-technology-helping-new-york-police-keep-closer-eye-united>. Acesso em 21 abr. 2019.

CHEUNG, Helier; HUGHES, Roland. **Why are there protests in Hong Kong? All the context you need.** In: BBC. Publicado em 13 jun. 2019. Disponível em: <https://www.bbc.com/news/world-asia-china-48607723>. Acesso em 16 jun. 2019.

CHINA DAILY. **China's Urbanization Plan 2014-2020.** Publicado em 18 mar 2014. Disponível em: http://www.chinadaily.com.cn/business/2014-03/18/content_17355936.htm. Acesso em 3 maio 2019.

CHINOY, Sahil. **We Built an ‘Unbelievable’(but Legal) Facial Recognition Machine.** In: NYT. Publicado em 16 abr. 2019. Disponível em: <https://www.nytimes.com/interactive/2019/04/16/opinion/facial-recognition-new-york-city.html>. Acesso em 6 maio 2019.

CHRISTL, Wolfie; SPIEKERMANN, Sarah. **Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy (2016).** In: Cracked Labs. Disponível em: <https://crackedlabs.org/en/networksofcontrol>. Acesso em 4 maio 2019.

COMUNITAS. **Segurança pública: concepção tradicional x nova concepção (2016).** Disponível em: <http://www.comunitas.org/portal/seguranca-publica-concepcao-tradicional-x-nova-concepcao/>. Acesso em 22 jun. 2019.

CREEMERS, Rogier. **China’s ‘Social Credit System’ Isn’t What It Sometimes Seems—So Far.** In: New America. Publicado em 14 maio 2018. Disponível em <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-social-credit-system-isnt-what-it-sometimes-seems-so-far/>. Acesso em 20 jun. 2019.

DE SOUSA, Marcelo Lopes. **Militarização da Questão Urbana.** In: Passa Palavra. Publicado em 3 dez. 2010. Disponível em: <http://passapalavra.info/2010/12/32598/>. Acesso em 22 jun. 2019.

DONEDA, Danilo; MACHADO, Diego. **Cidades inteligentes, dados pessoais e direitos dos cidadãos no Brasil.** In: CyberBRICS. Publicado em 22 maio 2019. Disponível em: <https://cyberbrics.info/cidades-inteligentes-dados-pessoais-e-direitos-dos-cidadaos-no-brasil/>. Acesso em 30 maio 2019.

ESCOBAR, Pepe. **A silenciosa ditadura do algoritmo.** In: Outras Palavras. Publicado em 18 out. 2016. Disponível em: <https://outraspalavras.net/sem-categoria/a-silenciosa-ditadura-do-algoritmo/>. Acesso em 5 mar. 2019.

ELLIS, Evan. **Chinese Surveillance Complex Advancing in Latin America.** In: Newsmax. Publicado em 12 abr. 2019. Disponível em: <https://www.newsmax.com/evanellis/china-surveillance-latin-america-cameras/2019/04/12/id/911484/>. Acesso em 15 abril 2019.

ESTADÃO. **São Francisco proíbe uso de reconhecimento facial pela polícia.** Publicado em 15 maio 2019. Disponível em: <https://internacional.estadao.com.br/noticias/geral,sao-francisco-proibe-uso-de-reconhecimento-facial-pela-policia,70002830018>. Acesso em 17 maio 2019.

_____. **Serviço de reconhecimento facial da Amazon falha em testes com congressistas americanos.** Publicado em 26 jul. 2018. Disponível em: <https://link.estadao.com.br/noticias/empresas,servico-de-reconhecimento-facial-da-amazon-falha-em-testes-com-congressistas-americanos,70002416996.amp>. Acesso em 15 jun. 2019.

ESTEVES, Paulo. **O Desenvolvimento da China com Paulo Esteves.** In: Seminário: "Economia Política do Desenvolvimento da China". Canal do Instituto de Economia da Universidade Federal do Rio de Janeiro. Publicado em 29 jun. 2017. Disponível em: <https://youtu.be/MNCGIdTCw00>. Acesso em 4 dez. 2018.

FOUCAULT, Michel. **Vigiar e Punir: nascimento da prisão.** Tradução de Raquel Ramallete. 20ª edição. Editora Vozes, Petrópolis, 1999.

GOMES, Helton Simões. **Reconhecimento facial usado na China é testado no Brasil; saiba como opera.** Publicado em 18 jan. 2019. Disponível em: <https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/01/18/reconhecimento-facial-usado-na-china-e-testado-no-brasil-saiba-como-opera.htm>. Acesso em 1 abr. 2019.

GOVERNO CENTRAL DA CHINA. **13º Plano Quinquenal de Desenvolvimento Econômico e Social (2016-2020).** Publicado em dez. 2016. Disponível em: <http://en.ndrc.gov.cn/policyrelease/201612/P020161207645766966662.pdf>. Acesso em 20 mar. 2019.

_____. **Plano Nacional de Nova Urbanização (2014-2020).** In: Xinhua. Publicado em 16 mar. 2014. Disponível em: http://www.gov.cn/zhengce/2014-03/16/content_2640075.htm. Acesso em 20 mar. 2019.

GAN, Nectar. **The complex reality of China's social credit system: hi-tech dystopian plot or low-key incentive scheme?** In: SCMP. Publicado em 7 fev. 2019. Disponível em: <https://www.scmp.com/news/china/politics/article/2185303/hi-tech-dystopia-or-low-key-incentive-scheme-complex-reality>. Acesso em 20 mar. 2019.

GRAHAM, Stephen. **Cidades Sitiadas: O Novo Urbanismo Militar.** Coleção Estado de Sítio. Coord. Paulo Arantes. Tradução de Alyne Azuma. 1ª ed. São Paulo: Boitempo, 2016.

HIDALGO, Anne; MOORE, Clover; KOIKE, Yuriko; DE LILLE, Patricia. **Cities are where the future happens first.** An open letter by the mayors of Paris, Tokyo, Sydney and Cape Town. In: Lifegate. Publicado em 11 fev. 2017. Disponível em: <https://www.lifegate.com/people/news/c40-mayors-cities-future>. Acesso em 19 jun. 2019.

HOU, Rui. **Neoliberal governance or digitalized autocracy? The rising market for online opinion surveillance in China.** In: Surveillance & Society 15(3/4): 418-424, 2017. Disponível em: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6610/6418>. Acesso em 20 jun. 2019.

HUANG, Zheping. **All Chinese citizens now have a score based on how well we live, and mine sucks.** In: Quartz. Publicado em 9 out. 2015. Disponível em: <https://qz.com/519737/all-chinese-citizens-now-have-a-score-based-on-how-well-we-live-and-mine-sucks/>. Acesso em 20 mar. 2019.

HUAWEI. **China Huawei faz parceria com Oi para câmeras de reconhecimento facial.** Publicado em 16 out. 2018. Disponível em: <https://e.huawei.com/br/news/br/2018/201810162158>. Acesso em 3 abr. 2019.

_____. **Oi firma parceria estratégica com Huawei e avança na reestruturação operacional para transformação da rede e crescimento do negócio.** Publicado em 25 jul. 2018. Disponível em: <https://www.huawei.com/br/press-events/news/br/2018/julho/oi%20e%20huawei>. Acesso em 3 abr. 2019.

HRW – Human Rights Watch. **World Report 2019.** Disponível em: <https://www.hrw.org/pt/world-report/2019>. Acesso em 20 jun. 2019.

HUTCHINS, Renée M. **Racial Profiling: The Law, the Policy, and the Practice (2017)** Publicado em https://digitalcommons.law.umaryland.edu/fac_pubs/1594/. Acesso em: 20 jun. 2019.

IMIL – Instituto Millenium. **Na China, Atos dos Cidadãos Valerão Pontos e Limitarão Seus Projetos.** Publicado em 16 nov. 2018. Disponível em: <https://www.institutomillenium.org.br/blog/na-china-atos-dos-cidadaos-valerao-pontos-e-limitarao-seus-projetos/>. Acesso em 20 jun. 2019.

INSTITUTO IGARAPÉ. [Nota Técnica] **O que explica a grande queda no índice de homicídios no Brasil?** Publicado em 14 maio 2019. Disponível em: <https://igarape.org.br/nota-tecnica-o-que-explica-a-grande-queda-no-indice-de-homicidios-no-brasil/>. Acesso em 18 jun. 2019.

_____. **Observatório de Homicídios.** Disponível em: <https://igarape.org.br/apps/observatorio-de-homicidios/>. Acesso em 18 jun. 2019.

_____. **Reconhecimento Facial no Brasil.** Disponível em: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>. Acesso em 15 jun. 2019.

INTERVOZES. **Reconhecimento facial no Carnaval: riscos tecnológicos nada divertidos.** In: Media Lab UFRJ. Publicado em 14 mar. 2019. Disponível em: <http://medialabufrj.net/blog/2019/03/reconhecimento-facial-no-carnaval-riscos-tecnologicos-nada-divertidos/>. Acesso em 20 mar. 2019.

IPEA- Instituto de Pesquisa Econômica Aplicada. **Atlas da Violência: Brasil registra mais de 65 mil homicídios em 2017.** Publicado em 5 jun. 2019. Disponível em: http://www.ipea.gov.br/portal/images/stories/PDFs/relatorio_institucional/190605_atlas_da_violencia_2019.pdf. Acesso em 1 jul. 2019.

IRIS - Instituto de Referência em Internet e Sociedade. **Privacy on Facebook: what can we learn from Cambridge Analytica.** Publicado em 19 mar. 2018. Disponível em: <http://irisbh.com.br/en/privacy-on-facebook-cambridge-analytica/>. Acesso em 20 jun. 2019.

_____. **Vigilância é uma solução ou uma ameaça à segurança pública?** Publicado em 22 abr. 2019. Disponível em: <http://irisbh.com.br/vigilancia-e-uma-solucao-ou-uma-ameaca-a-seguranca-publica/>. Acesso em 20 jun. 2019.

JOHNSON, Keith; GROLL, Elias. **The Improbable Rise of Huawei.** In: Foreign Policy. Publicado em 3 abr. 2019. Disponível em: <https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/>. Acesso em 20 jun. 2019.

KAINZ, Joe; WAT, Karif; ZHANG, Dayu; WANG, Tom; KAO, Shanshan. **China's 'social credit system' explained.** In: SCMP. Publicado em 25 mar. 2019. Disponível em: <https://www.scmp.com/video/china/3003200/company-aims-monetise-chinas-social-credit-system>. Acesso em 20 jun. 2019.

KENNEDY, Scott. **Made in China 2025.** In: CSIS. Publicado em 15 jun. 2015. Disponível em: <https://www.csis.org/analysis/made-china-2025>. Acesso em 10 mar. 2019.

KOSTKA, Genia. **China's social credit systems are highly popular – for now.** In: MERICS. Publicado em 17 set. 2018. Disponível em: <https://www.merics.org/en/blog/chinas-social-credit-systems-are-highly-popular-now>. Acesso em 20 mar. 2019.

LEE, John. **The rise of China's tech sector: The digital great game.** Publicado em 5 maio 2017. Disponível em: <https://www.lowyinstitute.org/the-interpreter/rise-china-s-tech-sector-digital-great-game>. Acesso em 21 maio 2019.

LEIGH, Karen; MARTIN, Peter. **How the Tiananmen Square Protests Shaped Modern China.** In: Bloomberg. Publicado em 29 maio 2019. Disponível em: <https://www.bloomberg.com/news/articles/2019-05-29/how-the-tiananmen-square-protests-shaped-modern-china-quicktake>. Acesso em 5 jun. 2019.

LOONEY, Kristen; RITHMIRE, Megh. **Urbanization with Chinese Characteristics? China's Gamble for Modernization.** In: HBS – Harvard Business School. Disponível em: http://www.hbs.edu/faculty/Publication%20Files/UrbanizationChina_RithmireLooney_notes_055bd268-913f-4c1c-8bb0-8c14c8855b83.pdf. Acesso em 20 jun. 2019.

MA, Arnold. **For Your Eyes Only — 5 Chinese New Year Ads You Shouldn't Miss.** In: Jingdaily. Publicado em 19 fev. 2019. Disponível em: <https://jingdaily.com/chinese-new-year-ads/>. Acesso em: 20 mar. 2019.

MARTINS, Umberto. **O duelo entre EUA e China no centro da geopolítica mundial.** Publicado em 14 mar. 2019. Disponível em: <https://i21.org.br/todo-mundo/o-duelo-entre-eua-e-china-no-centro-da-geopolitica-mundial/>. Acesso em 20 mar. 2019.

MCCULLOM, Rod. **Facial Recognition Technology Is Both Biased and Understudied.** Publicado em 17 maio 2017. Disponível em: <https://undark.org/article/facial-recognition-technology-biased-understudied/>. Acesso em 19 jun. 2019.

MERICS – Mercator Institute for China Studies. **China Update 5/2019. February 22 - March 15, 2019.** Disponível em: <https://www.merics.org/en/newsletter/china-update-52019#china-and-the-world>. Acesso em 20 maio 2019.

_____. **China Update 8/2019. April 5 – May 9, 2019.** Disponível em: https://www.merics.org/sites/default/files/2019-05/MERICS_China_Update_8_2019_EN_final_1.pdf. Acesso em 12 maio 2019.

MICROSOFT. **Reconhecimento facial: é hora de agir.** Publicado em 6 de dez. 2018. Disponível em <https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/>. Acesso em 1 jul. 2019.

MOROZOV, Evgeny. **A Tecnologia da Adaptação — e como vencê-la.** In: Outras Palavras. Publicado em 17 maio 2019. Disponível em: <https://outraspalavras.net/internetemdisputa/nao-estamos-condenados-a-tecnologia-da-adaptacao/>. Acesso em 10 jun. 2019.

MOULIN, Carolina e TABAK, Jana. **Humanitarismo e a Favela Global: violência urbana e ação humanitária no Rio de Janeiro.** Contexto Internacional [online]. 2014, vol.36, n.1, pp.43-74. Disponível em: <http://dx.doi.org/10.1590/S0102-85292014000100002>. Acesso em 20 jun. 2019.

MOZUR, Paul. **One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority.** In: NYT. Publicado em 14 abr. 2019. Disponível em: <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html>. Acesso em 20 jun. 2019.

_____. KESSEL, Jonah M.; CHAN, Melissa. **Made in China, Exported to the World: The Surveillance State.** In: The New York Times. Publicado em 24 abr. 2019. Disponível em: <https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html>. Acesso em 30 abr. 2019.

MYERS, Joe. **You knew China's cities were growing. But the real numbers are stunning.** In: World Economic Forum - WEF. Publicado em 20 jun. 2016. Disponível em: <https://www.weforum.org/agenda/2016/06/china-cities-growing-numbers-are-stunning>. Acesso em 25 abr. 2019.

MUGGAH, Robert. **Cidade precisa de poder para enfrentar as questões globais, diz especialista.** In: Folha UOL. Disponível em: <http://www1.folha.uol.com.br/cotidiano/2017/11/1934311-cidade-precisa-de-poder-para-enfrentar-as-questoes-globais-diz-especialista.shtml>. Acesso em 3 dez. 2018.

_____. **Robert Muggah: “A city is a place to connect”.** In: Instituto Igarapé. Publicado em 28 jun. 2018. Disponível em: <https://igarape.org.br/robert-muggah-a-city-is-a-place-to-connect/> Acesso em 3 dez. 2018.

_____. **The Rise of Citizen Security in Latin America and The Caribbean (2017).** In: Alternative Pathways to Sustainable Development: Lessons from Latin America, International Development Policy Series N°.9. pp. 291-322.

_____. **“Se as regras do uso da tecnologia não forem claras, podem gerar problemas à polícia”, afirma Robert Muggah.** In: Instituto Igarapé. Publicado em 28 maio 2019. Disponível em: <https://igarape.org.br/se-as-regras-do-uso-da-tecnologia-nao-forem-claras-podem-gerar-problemas-a-policia-afirma-robert-muggah/> Acesso em 15 jun. 2019.

MUÑOZ, Ramón. **Google rompe com a Huawei, cujos celulares ficarão sem ‘apps’ e atualizações.** In: El País Brasil. Publicado em 20 maio 2019. Disponível em:

https://brasil.elpais.com/brasil/2019/05/19/economia/1558294622_546268.html.

Acesso em 22 maio 2019.

MUNRO, Kelsey. **China’s social credit system ‘could interfere in other nations’ sovereignty’.** In: The Guardian. Publicado em 27 jun. 2018. Disponível em: <https://www.theguardian.com/world/2018/jun/28/chinas-social-credit-system-could-interfere-in-other-nations-sovereignty>. Acesso em 21 jun. 2019.

O’FLAHERTY, Kate. **China Facial Recognition Database Leak Sparks Fears Over Mass Data Collection.** In: Forbes. Publicado em 18 fev. 2019. Disponível em: <https://www.forbes.com/sites/kateoflahertyuk/2019/02/18/china-facial-recognition-database-leak-sparks-fears-over-mass-data-collection/#6a08e786fb40>. Acesso em 20 mar. 2019.

O GLOBO. **Snowden: Vazamento prova que EUA pagaram para espionar softwares.** Publicado em 7 mar. 2017. Disponível em: <https://oglobo.globo.com/mundo/snowden-vazamento-prova-que-eua-pagaram-para-espionar-softwares-21026190>. Acesso em 15 jun. 2019.

OUTRAS PALAVRAS. **O século 21 será chinês?** In: Observatório dos BRICS. Publicado em 21 jun. 2018. Disponível em: <https://observatoriodosbricsunila.wordpress.com/2018/06/28/o-seculo-21-sera-chines/>. Acesso em 20 mar. 2019.

PHELAN, Hanna. **Can China's Smart Cities Improve Public Health?** Publicado em 17 maio 2019. Disponível em: <https://www.healthxl.com/blog/can-chinas-smart-cities-improve-public-health/> Acesso em 30 maio 2019.

PELLEGRINI, Marcelo. **Segurança Pública brasileira é improdutiva, violenta e reproduz desigualdades.** In: Carta Capital. Publicado em 12 mar. 2015. Disponível em: <https://www.cartacapital.com.br/sociedade/seguranca-publica-brasileira-e-improdutiva-violenta-e-reproduz-desigualdades-3055.html>. Acesso em 20 jun. 2019.

PWCCN- PWC CHINA. **Chinese Cities of Opportunity 2018.** Disponível em: <https://www.pwccn.com/en/research-and-insights/chinese-cities-of-opportunities-2018-report.html>. Acesso em 04 abr. 2019.

_____. **Chinese Cities of Opportunity 2019.** Disponível em: <https://www.pwccn.com/en/research-and-insights/chinese-cities-of-opportunities-2019-report.pdf>. Acesso em 04 abr. 2019.

QUARTZ. **The 2050 Project**. Disponível em: <https://qz.com/se/the-2050-project/>. Acesso em: 04 abr. 2019.

REBELLO, Aiuri. **Bancada do PSL vai à China importar sistema que reconhece rosto de cidadãos**. Publicado em 16 jan. 2019. Disponível em: <https://noticias.uol.com.br/politica/ultimas-noticias/2019/01/16/bancada-do-psl-vai-a-china-para-importar-tecnicas-de-reconhecimento-facial.htm>. Acesso em 30 mar. 2019.

REGATTIERI, Lorena. **Algoritmização da Vida: Revirando os Fundamentos da Automação**. In: Media Lab UFRJ. Disponível em: <http://medialabufrj.net/projetos/algoritmizacao-da-vida-revirando-os-fundamentos-da-automacao/>. Acesso em: 20 jun. 2019.

REUTERS. **Assegurando o futuro do 5G: Quais são os problemas?** In: UOL. Publicado em 24 abr. 2019. Disponível em: <https://noticias.uol.com.br/tecnologia/noticias/reuters/2019/04/24/assegurando-o-futuro-do-5g-quais-sao-os-problemas.htm>. Acesso em 21 mar. 2019.

_____. **US intelligence reportedly says Huawei funded by Chinese state security**. In: CNBC. Publicado em 20 abr. 2019. Disponível em: <https://www.cnbc.com/2019/04/20/us-intelligence-reportedly-says-huawei-funded-by-chinese-state-security.html>. Acesso em 25 abr. 2019.

REUS-SMIT, Christian. **International Relations Theory Doesn't Understand Culture**. In: Foreign Policy. Publicado em 21 mar. 2019. Disponível em: <https://foreignpolicy.com/2019/03/21/international-relations-theory-doesnt-understand-culture/>. Acesso em 30 mar. 2019.

REVISTA FORUM. **Crítico do “Estado Hacker”, ativista alemão de direitos digitais participa de eventos em SP e Rio**. Publicado em 2 maio 2019. Disponível em: <https://www.revistaforum.com.br/critico-do-estado-hacker-ativista-alemao-de-direitos-digitais-participa-de-eventos-em-sp-e-rio/>. Acesso em 5 maio 2019.

ROSSI, Clóvis. **China, 3º na cama de Brasil e EUA**. In: Folha UOL. Publicado em 21 mar. 2019. Disponível em: <https://www1.folha.uol.com.br/colunas/clovisrossi/2019/03/china-3o-na-cama-de-brasil-e-eua.shtml>. Acesso em 30 mar. 2019.

SANTORO, Mauricio. **Brasil precisa se decidir sobre a China ou ficará para trás [artigo]**. In: Época. Publicado em 16 abr. 2019. Disponível em: <https://epoca.globo.com/brasil-precisa-se-decidir-sobre-china-ou-ficara-para-tras-artigo-23603820>. Acesso em 24 abr. 2019.

_____. **Os 30 anos do Massacre da Praça da Paz Celestial e o Novo Ativismo Político na China.** In: Boletim Lua Nova. Publicado em 4 jun. 2019. Disponível em: <https://boletimluanova.org/2019/06/04/os-30-anos-do-massacre-da-praca-da-paz-celestial-e-o-novo-ativismo-politico-na-china/>. Acesso em: 7 jun. 2019.

SCHWAB, Klaus. **The Fourth Industrial Revolution: what it means, how to respond.** In: We Forum. Publicado em 14 jan. 2016. Disponível em: <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>. Acesso em 27 maio 2019.

SEM FRONTEIRAS. **Os 30 anos do massacre na Praça da Paz Celestial.** In: Globo News. Publicado em 30 maio 2019. Disponível em: <https://globosatplay.globo.com/globonews/v/7656741/>. Acesso em: 1 jun. 2019.

SEN, Amartya. **Human Rights and Asian Values** (1997). Carnegie Council on Ethics and International Affairs. New York, US.

SERRANO- BERTHET, Rodrigo. **Smart Spending on Citizen Security.** Chapter 7. In: Better spending for better lives: how Latin America and the Caribbean can do more with less (2018). IDB – Inter-American Development Bank. Disponível em: <https://flagships.iadb.org/en/DIA2018/chapter-7-smart-spending-citizen-security-beyond-crime-and-punishment>. Acesso em 20 jun. 2019.

SHI-KUPFER, Kristin; OHLBERG, Mareike. **China's Digital Rise: Challenges for Europe.** In: MERICS n.7 April 2019. Disponível em: https://www.merics.org/sites/default/files/2019-04/MPOC_No.7_ChinasDigitalRise_web_final.pdf. Acesso em 20 jun. 2019.

SILVEIRA, Janaína Camara da. **Breaking News #30 "Life after the trade war".** March 2019. In: CEBRI - Centro Brasileiro de Relações Internacionais. Disponível em: <http://cebri.org/portal/publicacoes/cebri-artigos/cebri-breaking-news-30-life-after-the-trade-war>. Acesso em 13 maio 2019.

SZYMIELEWICZ, Katarzyna. **Your digital identity has three layers, and you can only protect one of them.** Publicado em 25 jan. 2019. Disponível em: <https://qz.com/1525661/your-digital-identity-has-three-layers-and-you-can-only-protect-one-of-them/>. Acesso em 20 jun. 2019.

TAM, Luisa. **The road to hell is paved with good intentions. What price will society pay for China's social credit system?** In: SCMP. Publicado em 25 fev. 2019. Disponível em: <https://www.scmp.com/news/hong-kong/society/article/2187571/road-hell-paved-good-intentions-what-price-will-society-pay>. Acesso em 20 jun. 2019.

TÁVORA, Fernanda; ARAÚJO, Gabrielle; SOUSA, Jordan. **Scanner facial abre alas e ninguém mais se perde no Carnaval (e fora dele)**. In: Tab Uol. Publicado em 11 mar. 2019. Disponível em: <https://tab.uol.com.br/noticias/redacao/2019/03/11/carnaval-abre-alas-para-o-escaner-facial-reconhece-milhoes-e-prende-seis.htm>. Acesso em 20 mar. 2019.

THAYER, Bradley A.; FRIEND, John M. **The World According to China**. In: The Diplomat. Publicado em 3 out. 2018. Disponível em: <https://thediplomat.com/2018/10/the-world-according-to-china/>. Acesso em 20 mar. 2019.

THE AI NOW INSTITUTE. **AI Now Report 2018**. Publicado em dez. 2018. Disponível em: https://ainowinstitute.org/AI_Now_2018_Report.pdf. Acesso em 1 jul. 2019.

TOYAMA, Naoyuki. **China woos an Argentina neglected by American indifference**. In: Asia Nikkei. Publicado em 30 jul. 2018. Disponível em: <https://asia.nikkei.com/Politics/International-relations/China-woos-an-Argentina-neglected-by-American-indifference>. Acesso em 20 mar. 2019.

VARTANIAN, Talin. **How China has rewritten the history of Tiananmen Square**. In: CBC. Publicado em 31 maio 2014. Disponível em: <https://www.cbc.ca/news/world/how-china-has-rewritten-the-history-of-tiananmen-square-1.2657042>. Acesso em 20 jun. 2019.

VAZ, Tatiana. **Marcas 'made in China' conquistam confiança do consumidor brasileiro**. In: Folha UOL. Publicado em 14 set. 2018. Disponível em: <https://www1.folha.uol.com.br/seminariosfolha/2018/09/marcas-made-in-china-conquistam-confianca-do-consumidor-brasileiro.shtml>. Acesso em 20 mar. 2019.

VICENTE, João Paulo. **Reconhecimento facial erra muito, e você deveria se preocupar com isso**. Publicado em 27 maio 2019. Disponível em: <https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/05/27/tecnicas-de-vigilancia-como-identificacao-facial-ainda-sao-falhas.htm>. Acesso em 20 jun. 2019.

VICENTE, Victor. **Dobras 21. Origens da Cidade Inteligente e os Revolucionários Chilenos**. In: Media Lab UFRJ. Publicado em out. 2018. <http://medialabufrj.net/blog/2018/10/dobras-21-origens-da-cidade-inteligente-e-os-revolucionarios-chilenos/>. Acesso em 20 jun. 2019.

VIEIRA, Letícia Maria. **A contenção da política: usos de videomonitoramento para controle social nos espaços públicos de São Paulo**. In: Catálogo USP. Disponível em: <http://www.teses.usp.br/teses/disponiveis/8/8136/tde-26022019-104511/pt-br.php>. Acesso em 19 jun. 2019.

VILA-NOVA, Carolina. **China mira América Latina em seu maior projeto de influência exterior.** In: Folha UOL. Publicado em 24 mar. 2019. Disponível em: <https://www1.folha.uol.com.br/mundo/2019/03/china-mira-america-latina-em-seu-maior-projeto-de-influencia-exterior.shtml>. Acesso em 2 jun. 2019.

WE FORUM. **Population living in slums (% of urban population), 2014** Disponível em: <https://data.worldbank.org/indicator/EN.POP.SLUM.UR.ZS>. Acesso em: 10 jun. 2019.

_____. **The Fourth Industrial Revolution: what it means, how to respond, 2016.** Disponível em: <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>. Acesso em: 10 jun. 2019.

WENQIAN, Zhu. **China has signed 171 B&R cooperation documents.** Publicado em 07 mar. 2019. Disponível em: <https://eng.yidaiyilu.gov.cn/qwyw/rdxw/81686.htm>. Acesso em 23 jun. 2019.

WINTER, Brian. **CHEGA! A epidemia de assassinatos da América Latina precisa de soluções democráticas urgentes.** In: Americas Quarterly. Publicado em 24 jul. 2018. Disponível em: <https://www.americasquarterly.org/content/homicidereduction-leader-english>. Acesso em 19 jun. 2019.

WOOD, David M.; MACKINNON, Debra. **Partial Platforms and Oligoptic Surveillance in the Smart City.** In: Surveillance & Society 17 (1/2) : 176-182, 2019. Disponível em: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13116/8492>. Acesso em: 19 jun. 2019.

YAU, Thomas. **Company aims to monetise China's social credit system.** In: South China Morning Post. Publicado em 25 mar. 2019. Disponível em: <https://www.scmp.com/video/china/3003200/company-aims-monetise-chinas-social-credit-system>. Acesso em 30 mar. 2019.

ZMOGINSKI, Felipe. **A sociedade mais vigiada do mundo: como a China usa o reconhecimento facial.** In: UOL. Publicado em 19 jan. 2019. Disponível em: <https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/01/19/a-sociedade-mais-vigiada-do-mundo-como-a-china-usa-o-reconhecimento-facial.htm>. Acesso em: 19 jun. 2019.

ZUBOFF, Shoshana. **Big other: surveillance capitalism and the prospects of an information civilization.** In: Journal of Information Technology (2015) 30, 75–89. Disponível em: <https://cryptome.org/2015/07/big-other.pdf>. Acesso em 20 jun. 2019.