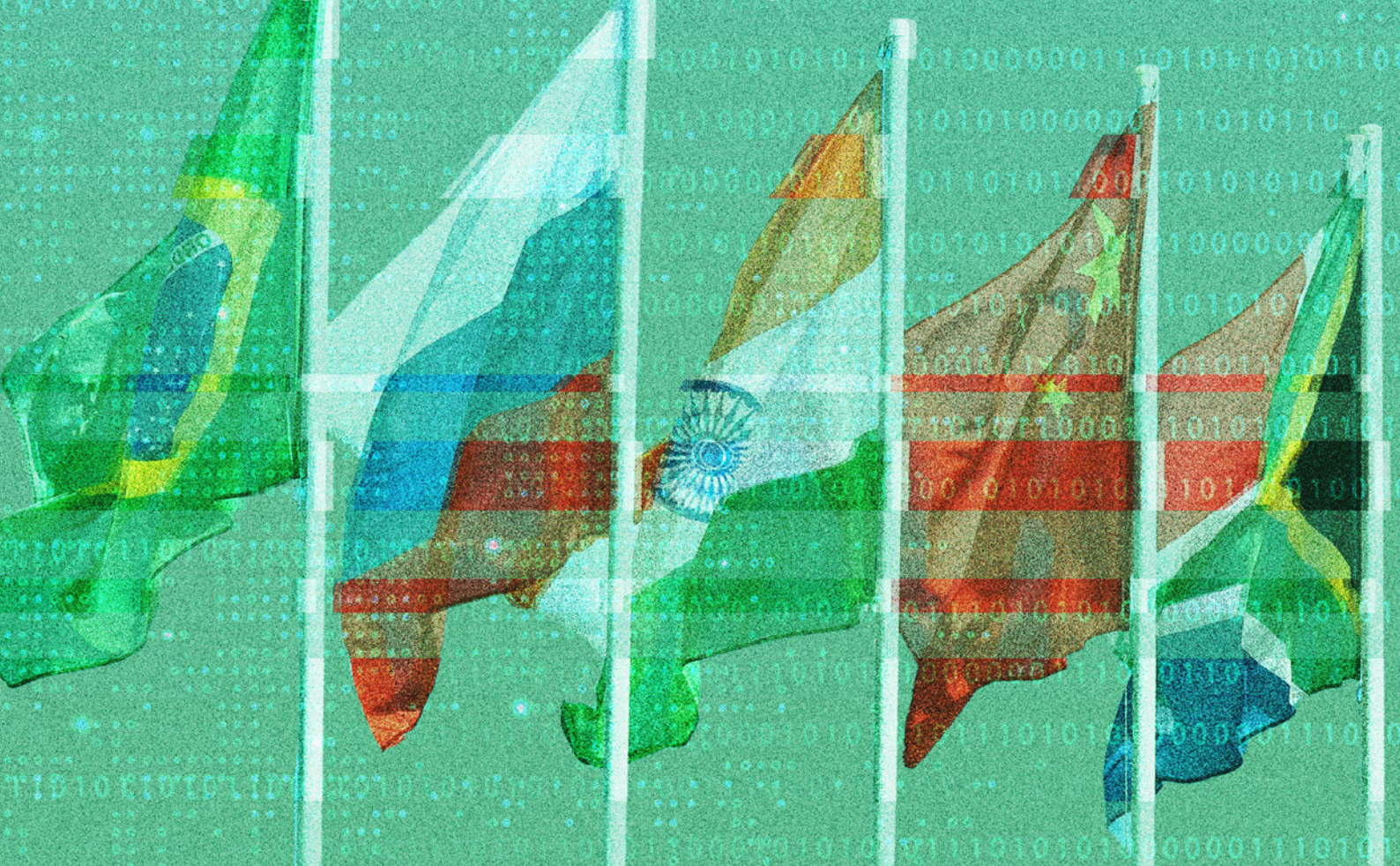
INSTITUTO IGARAPÉ
a think and do tank

VIGILANTISMO NO BRICS E A PANDEMIA DO COVID-19



Sumário

VIGILANTISMO NO BRICS E A PANDEMIA DO COVID-19

Introdução

O desenvolvimento exponencial da **tecnologia no século XXI** trouxe não só a possibilidade de uma transformação digital de serviços e acesso ao conhecimento, mas ampliou as preocupações com relação ao uso indiscriminado das mesmas para monitorar grupos, espaços públicos e outros ambientes. Países em desenvolvimento como o Brasil, Rússia, Índia, China e África do Sul (BRICS) são casos emblemáticos da expansão de práticas de vigilância.

O **Brasil**, primeiramente, contou com **grandes eventos** (Copa do Mundo e Olimpíadas) em 2014 e 2016, demandando maiores medidas de **segurança pública**. A **Rússia**, por sua vez, teve a Guerra Fria como fator histórico determinante para a prática da vigilância; já a **China**, ganhou notoriedade através de seu sistema de pontuação das atitudes dos cidadãos (**pontuação social**)[1] e o amplo uso de sistemas de **videomonitoramento** em diferentes cidades.[2] Na **Índia**, destaca-se o sistema biométrico de identificação via **reconhecimento facial**[3]; e, na **África do Sul**, tecnologias baseadas em dados geográficos (**geoespaciais**) são utilizadas há, pelo menos, três décadas.[4]

A **pandemia do COVID-19** deu novas proporções ao vigilantismo nos países BRICS, dos quais, com exceção da China, chegaram a encontrar-se, em julho de 2020**,** entre os **cinco países com o maior número de casos do mundo**[5], atrás apenas dos Estados Unidos. É nesse contexto que observamos que tecnologias que antes eram utilizadas para segurança pública e monitoramento

1 https://exame.com/mundo/black-mirror-com-sistemas-de-pontos-china-premia-ou-pune-cidadaos/

2 The New York Times (2018) apud Wu, Y.; Sun, I.; Hu, R. (2021).

3 Hickok, E.; ***et all*** (2021).

4 Silva, A.; Cá, T.; Rosenberg, F. (2020).

5 Worldmeters (2020) apud Hoirisch, C. (2020). p. 213.

de espaços fechados, ganharam novas funcionalidades ao integrarem medição de temperatura e outros mecanismos de rastreamento e coleta de dados.[6] Esse foi o caso de alguns aeroportos internacionais do Brasil que implementaram essas tecnologias para monitorar infectados e estratégias de prevenção, contenção e controle do contágio.

Nesse relatório, então, exploramos como os **BRICS** utilizaram tecnologia durante a pandemia do COVID-19.[7] Focamos nesse período não somente pela sua excepcionalidade, mas por representar um momento de alta implementação de tecnologias pelo setor público devido a fatores que vão desde a necessidade de manter serviços ao cidadãos, até preocupações com o controle e monitoramento de casos.

Apesar desses países representarem um importante agrupamento que possui estrutura multilateral de cooperação, a exemplo do estabelecimento do **Centro de Pesquisa e Desenvolvimento de Vacinas do BRICS - CPDV-BRICS**[8], nos referimos aos BRICS majoritariamente em sua capacidade enquanto potências econômicas. Visamos, dessa forma, contribuir para o melhor entendimento sobre práticas de implementação de tecnologias, enfatizando as complexidades das experiências de diferentes países no Sul Global. Sendo os BRICS **potências em ascensão** e entusiastas na produção e implementação de tecnologias no setor público, o mapeamento de diferentes padrões de uso de tecnologias de vigilância torna-se um importante exercício para uma visão mais complexa e diversa sobre projetos, experiências e políticas que caracterizam a vigilância em países em desenvolvimento.

A **China**, por exemplo, é uma das maiores **desenvolvedoras** do mundo em tecnologia (inteligência artificial, infraestrutura de telecomunicações e entre outras). O país vem disputando o protagonismo na transformação digital a partir de seu poderio econômico ao oferecer infraestrutura e planos de financiamento atraentes a outros países do Sul Global. O **Brasil, a Índia e a África do Sul**, por sua vez, são entusiastas na **implementação** de tecnologias e no desenvolvimento de planos de digitalização de diversos setores; e a **Rússia**, finalmente, é um país de destaque na **cibersegurança** e monitoramento de redes. Apresentamos nesse relatório, portanto, a descrição e análise do uso de **tecnologias de vigilância** em cada um dos países-membros referidos (em ordem, Brasil, Rússia, Índia, China e África do Sul), com foco no contexto da pandemia do COVID-19.

Países em desenvolvimento como o Brasil, Rússia, Índia, China e África do Sul (BRICS) são casos emblemáticos da expansão de práticas de vigilância.

6 Instituto Igarapé (2022).

7 O documento baseia-se em uma revisão de literatura em bases de dados (***desk research***, pesquisa secundária) tanto globais, quanto focadas em determinado país ou região.

8 https://cee.fiocruz.br/?q=Os-novos-justiceiros-lancamento-do-Centro-Brics-de-P%26D-de-Vacinas-e-a-guerra-Russia-X-EUA-Otan


Brasil

Brasil

Desde os megaeventos de 2014 e 2016 (Copa do Mundo e Olimpíadas), vem se consolidando uma cultura de **videomonitoramento** em massa no Brasil, no âmbito da segurança pública. Inclusive, na pesquisa realizada pelo Programa de Segurança Digital do Instituto Igarapé sobre tecnologias de vigilância na América Latina[9], que apresentou mais de 300 casos entre 2006 e 2021, o videomonitoramento foi a funcionalidade mais encontrada nos casos brasileiros.[10] Foi no contexto da crise sanitária, contudo, que a estrutura de vigilância pré existente ganhou novas perspectivas tanto internamente, quanto nas relações internacionais do país.

Diversos sistemas de câmeras com reconhecimento facial foram **adaptadas** para a **detecção do uso ou não de máscaras faciais**, medida que se tornou obrigatória em todo o país, bem como para a **medição de temperatura corpora**l, dado que a febre se mostrou um dos sintomas mais comuns da doença da COVID-19. Essas medidas foram empregadas frequentemente nos **aeroportos** internacionais do Brasil, a exemplo do Aeroporto Internacional Salgado Filho, em Porto Alegre (Rio Grande do Sul), com equipamentos da Zhejiang Dahua Technology (ZDT), empresa chinesa[11] - demonstrando o potencial de **múltipla funcionalidade** presente em tecnologias de vigilância.

Além disso, diversos **aplicativos** foram desenvolvidos no Brasil, como o "Monitora Covid-19"[12], que teve início na região Nordeste e foi ampliado para todo o país. Esse *app* foi desenvolvido a partir de uma **parceria público-privada** (nesse caso, as empresas Core e Novetech, o Departamento de Ciência, Tecnologia e Inovação - SECTI e o Departamento de Saúde do Estado da Bahia - SESAB), coletando dados de **geolocalização** e do **estado de saúde dos indivíduos**. Outros aplicativos, como o "Tô de Olho", aplicado na cidade de Parnamirim (Rio Grande do Norte), também realizava o monitoramento de **contato com infectados** *(contact tracing).*[13]

Diversos sistemas de câmeras com reconhecimento facial foram adaptadas para a detecção do uso ou não de máscaras faciais, medida que se tornou obrigatória em todo o país, bem como para a medição de temperatura corporal, dado que a febre se mostrou um dos sintomas mais comuns da doença da COVID-19.

9 Práticas de vigilância no Brasil não foram mais detalhadas aqui por constarem na pesquisa referida.

10 Instituto Igarapé (2022).

11 Data Privacy (2021).

12 Estamos Vigilando (2020).

13 https://ufrn.br/imprensa/noticias/37790/aplicativo-to-de-olho-facilitara-testagens-de-covid-19-em-parnamirim

Externamente, no âmbito do **BRICS**, o Brasil contou com o recebimento de insumos para a produção própria e a importação de **vacinas** dos outros países-membros, como a China e a Índia, para o combate a pandemia do COVID-19. No entanto, o governo brasileiro realizou ataques verbais ao governo chinês, dado o início da pandemia identificado até então na cidade de Wuhan; assim, apesar da China ser o maior parceiro comercial do país desde 2009, houve atraso na compra de suas vacinas pelo Brasil – reflexo do estremecimento das relações diplomáticas e comerciais entre os países.

Sucessivos episódios de atribuições do COVID-19 à China por parte do governo brasileiro contribuíram, então, para uma maior **politização** da pandemia no Brasil, dificultando a aceitação por parte da população de medidas como a vacinação e a quarentena. Todavia, apesar das dificuldades enfrentadas pelo país em estabelecer um **controle predominantemente sanitário**, a pandemia do COVID-19 não só contribuiu para a digitalização acelerada de serviços em parte da população, mas também para uma adoção ainda maior de tecnologias de vigilância no âmbito da saúde, muitas delas desenvolvidas por empresas chinesas.

Entretanto, sendo um país em desenvolvimento, como o restante do BRICS, o Brasil ainda **carece de uma mentalidade sólida sobre tecnologia, como o entendimento comum em conceitos de cibersegurança e robustez na legislação de dados**.

Programa de Segurança Digital do Instituto Igarapé sobre tecnologias de vigilância na América Latina, que apresentou mais de 300 casos entre 2006 e 2021, o videomonitoramento foi a funcionalidade mais encontrada nos casos brasileiros. Foi no contexto da crise sanitária

O Marco Civil da Internet, por exemplo, foi instituído há menos de uma década, em 2014, e a aprovação da Lei Geral de Proteção de Dados Pessoais (LGPD) se deu apenas em 2018.[14] Com isso, na pandemia, passou a haver um maior debate sobre possíveis **violações aos direitos humanos** através de **discriminações raciais e/ou de gênero,** consequentes das tecnologias de **reconhecimento facial**; e sobre maior **invasão e uso indevido de dados,** facilitado pelo trabalho e estudo remoto.

Assim, observa-se que o Brasil possui experiência na implementação de tecnologias de vigilância para segurança pública, mas, com a pandemia do COVID-19, essa experiência teve que ser repensada e exigiu a ampliação das expertises para o setor de saúde. Esse panorama, em um país com alta densidade populacional e descostume de isolamento devido ao clima tropical e distanciamento geográfico de grandes guerras, permitiu, alinhado à cobertura vacinal, um maior controle da crise sanitária.

14 Instituto Igarapé (2021).


Rússia

Rússia

Snowden asked President Putin, "Does Russia intercept, store or analyze in any way the communications of millions of individuals?" Putin denied Russian mass surveillance, saying "Thank God, our special services are strictly controlled by the state and society, and their activity is regulated by law"[15]

O poder da vigilância da Rússia teve início no século XVIII, quando os russos precisavam, de algum modo, monitorar grupos de ingleses que os auxiliavam em grandes obras.[16] Já havia o entendimento da impossibilidade de se vigiar a todos; mas a ideia era a de que essa prática conscientizasse a outros, prevenindo comportamentos considerados indevidos. Historicamente, porém, a Rússia se tornou amplamente conhecida pela sua capacidade de vigiar tanto internamente quanto externamente, através das demandas de espionagem e contraespionagem ao longo da Guerra Fria e o funcionamento da principal agência russa de serviços secretos nesse período, a KGB.

Apesar da prática da vigilância ter custos políticos, econômicos e sociais, ela ocorre na Rússia com ampla **aceitação** por parte da população. O aplicativo de mensagens *Telegram*, criado por um russo, negou o acesso dos seus dados ao governo do país[17], mas, em um panorama macro, a sociedade russa é convencida da importância da vigilância para o combate a crimes, por exemplo.

(...) quem vive, ou permanece na Rússia por algum tempo, apercebe-se de que o governo é flexível no que respeita a notícias ou conteúdos sobre vários aspectos da vigilância existente no país. (...) a simples passagem de uma informação, mesmo que falsa, sobre as novas tecnologias estarem a ajudar o governo a implementar ferramentas de vigilância (...) é suficiente para que a consciência daqueles que poderiam cometer algum tipo de comportamento não aceite, os condicione a não agir[18]

15 Tradução livre: "Snowden perguntou ao Presidente Putin "A Rússia intercepta, armazena, analisa de alguma forma a comunicação dos seus milhares de indivíduos? Putin negou a vigilância em massa, dizendo 'Obrigado, Deus, nossos serviços especiais são estritamente controlados pelo estado e sociedade, e suas atividades são reguladas pela lei". Lewis, J. A. (2014).

16 Ramos, H. (2014). p. 143.

17 https://www.tecmundo.com.br/telegram/118300-governo-russo-telegram-criptografia.htm.

18 Ramos, H. (2014). p. 144.

Com o advento das tecnologias digitais, a vigilância na Rússia passou a caracterizar-se, especificamente, por amplas e integradas bases de dados. Em termos de práticas, observa-se, a nível nacional, o Sistema para Atividades Operativas de Investigação (***System for Operative Investigative Activities* - SORM**), servindo ao Serviço Secreto Russo (FSB) desde 1994, com a coleta, análise e armazenamento de ligações, e-mails, históricos na internet, pagamentos, entre outras redes de dados. O sistema já foi atualizado e aprimorado em diversos momentos (SORM-1 - 1995, SORM-2 - 1998 e SORM-3 - 2014), acompanhando a evolução da tecnologia.

Além disso, em julho de 2012, uma nova lei assinada por Putin ampliou a autonomia e capacidade técnica do serviço secreto em lidar com dados da internet, como armazenar bases com os nomes de visitantes de determinados endereços eletrônicos e bloquear um conteúdo específico ao invés de toda uma página (essa última medida se assemelha ao sistema utilizado na China). Outra lei assinada por Putin autoriza o Estado a acessar a geolocalização de todos os veículos do país.[19]

No entanto, no início da pandemia, por estar entre os dez países mais populosos do mundo, a Rússia surpreendeu a comunidade internacional por apresentar um baixo número de casos.[20] Isso pode ser explicado por diversos fatores, como (1) o tamanho do país, possibilitando mais facilmente o isolamento de determinadas áreas, (2) a quantidade limitada de testes de qualidade, (3) diagnósticos incorretos, (4) subnotificações - ausência de registros de mortes causadas pelo vírus de forma indireta, e (5) a possível manipulação de estatísticas - em Moscou, há relatos de emissão de certificados falsos de vacinação, descartando doses de vacinas.[21] Essa suspeita torna-se mais séria com a conjuntura de, em 2020, o Presidente russo, Vladimir Putin, ter solicitado emendas que o permitissem concorrer a mais duas reeleições. Ou seja, permanecer na presidência por mais 12 anos, já estando há quase 24 (a serem completados em 2024), o que soma 36 anos no poder. E, em 2021, essa medida foi aprovada.

na Rússia, a primeira prática de vigilância associada à tentativa de combate a pandemia surgiu em Moscou, com a implementação de tecnologias de reconhecimento facial, a fim de monitorar pessoas que retornavam do exterior.

19 Ramos, H. (2014). p. 146.

20 Hoirisch, C. (2020). p. 214.

21 https://www.washingtonpost.com/world/europe/moscow-fake-vaccine-coronavirus/2021/06/26/0881e1e4-cf98-11eb-a224-bd59bd22197c_story.html

Mas, na Rússia, a primeira prática de vigilância associada à tentativa de combate a pandemia surgiu em Moscou, com a implementação de tecnologias de **reconhecimento facial**, a fim de monitorar pessoas que retornavam do exterior. Implementada no âmbito do **programa "Cidade Segura"**, essa iniciativa é de caráter local e existe desde 2018, mas foi adaptada ao contexto da crise sanitária e sofreu críticas pela aparente concentração em regiões mais pobres[22], o que traz à tona, novamente, a problemática da possível **discriminação** no uso de tecnologias de vigilância.

Como mencionado, a Rússia contribuiu externamente para o combate da pandemia através da **produção e exportação de vacinas**, principalmente, priorizando o **BRICS**, a quem propôs o compartilhamento de doses. Entretanto, podendo essa iniciativa ter sido entendida como uma tentativa da Rússia de se **destacar no sistema internacional**, o país pode ter subestimado a capacidade de outros produzirem vacinas com insumos ou de forma autônoma[23], o que gerou complicações no processo de comercialização em termos de cotação no mercado e tempo de entrega.

Por último, apesar da existência do SORM, de sistemas locais de videomonitoramento e da produção e exportação de vacinas durante a pandemia do COVID-19, **decisões políticas** (sobre a cultura de vigilância) e a **baixa publicação de estudos** sobre, principalmente em um período de crise sanitária global, associam o governo russo à **falta de transparência**. Somado a isso, a invasão da Rússia na Ucrânia traz incertezas sobre a contínua tentativa de integração do grupo do BRICS, pois, apesar do Brasil ter condenado o ato, Índia, China e África do Sul não o fizeram e permanecem com constantes desafios socioeconômicos internos.

22 Raghunath, P. (2021).

23 Hoirisch, C. (2020). p. 320.


India

Índia

A prática da vigilância na Índia possui histórica base normativa: a Lei Indiana do Telégrafo (Indian Telegraph Act), data de 1885, e a Lei da Tecnologia da Informação (Information Technology Act), promulgada em 2000. Mesmo com a necessidade de vigilância sanitária devido a diversas doenças e, mais recentemente, a pandemia do COVID-19, essas seguem sendo as legislações mais importantes do país sobre vigilância, tendo em vista que a maior parte dessa prática se dá via telecomunicações[24] - no caso da pandemia, via aplicativo. Mas, devido a presença significativa de muçulmanos (14%)[25] e determinadas castas e tribos na Índia, o país registra casos de discriminação no que diz respeito a tecnologia de reconhecimento facial, uma das suas práticas de vigilância mais comuns.[26]

No entanto, em 2018, a partir do lançamento da **plataforma "DigiYatra"** pelo Ministério da Aviação Civil, teve início o uso da tecnologia de reconhecimento facial para processamento automático de embarque de passageiros em aeroportos como os de Bangalore, Hyderabad e Delhi. A coleta de dados é feita voluntariamente, até uma hora antes do voo, com os passageiros consentindo sobre o fornecimento do conteúdo na plataforma e as imagens sendo armazenadas pelo tempo máximo da viagem.

A Autoridade de Identificação Única da Índia[27] (*Unique Identification Authority of India* - UIDAI) passou a incluir, assim, o reconhecimento facial no sistema nacional indiano de identidade, chamado "*Aadhaar*". E, com o êxito da implementação desse tipo de tecnologia nos aeroportos, está sendo estudada a possibilidade de **expandir essa prática de vigilância para as estações de trens** do país.[28]

Contudo, há **outros casos concretos** da contribuição da tecnologia de reconhecimento facial para a segurança pública da Índia:[29]

- Identificação correta de 3 mil crianças desaparecidas (2018);
- Identificação de participantes em manifestações políticas (2019);
- Uso do "Sistema Punjab de Inteligência Artificial" (***Punjab Artificial Intelligence System* - PAIS**) pela Polícia do estado de Punjab, a partir do qual, quando suspeitos são confrontados, suas fotos podem ser analisadas em uma base de dados com nomes enviados pelas prisões da região;
- Uso do **aplicativo "*Pehchaan*"**, que, com a tecnologia de reconhecimento facial avançada da Microsoft, fornece o grau de confiabilidade de imagens de rosto pertencentes a uma mesma pessoa;
- De forma similar, a polícia da cidade de Chennai utiliza, desde 2017, a **tecnologia *Face Tagr***, combinando bases de dados criminais do país e imagens em tempo real dos circuitos de televisão;
- Uso da tecnologia da empresa NEC para o monitoramento de indivíduos de interesse, na cidade de Surat.

---

24 Siddiqui, N. Singh, B. (2021) p. 33.

25 https://www1.folha.uol.com.br/mundo/2019/12/medida-contra-muculmanos-ajuda-a-transformar-india-em-nacao-para-hindus.shtml

26 Juntas, as populações referidas somaram, em 2015, 55% das prisões (Hickock, 2021, p. 8).

27 Tradução livre.

28 Hickok, E. *et al*. (2021).

29 Hickok, E. *et al*. (2021). p. 11-13.

Em relação a pandemia do COVID-19, a maior medida de vigilância por parte do governo, desenvolvida em onze idiomas indianos, foi a criação do **aplicativo "*Aarogya Setu*",** para monitoramento de contato entre indivíduos e disseminação de informações, tendo sido obrigatório para o trânsito em locais públicos, como edifícios, trens e metrôs, e para pessoas em constante circulação, como comerciantes, jornalistas de campo e entregadores. O app ganhou destaque pela tentativa de uma maior proteção de dados, evitando vazamentos como os ocorridos nos estados de Karnataka e nas cidades de Delhi e Nagpur, mas sua política de uso não foi considerada clara pela população.

Para o controle vacinal, foi desenvolvido o sistema Rede de Inteligência da Vacina de COVID (***COVID Vaccine Intelligence Network - CoWIN***), permitindo a geração do certificado digital de vacinação com um código QR. Entretanto, ao permitir o uso generalizado do sistema, o governo abriu brechas para um compartilhamento indevido de dados (o certificado contém nome, idade, gênero, detalhes da identidade e registro de saúde), sem requerer uma medida de autenticação de quem está apresentando o certificado.[30]

Além disso, como consequência da pandemia, o trabalho remoto se consolidou como uma realidade e, na Índia, tecnologias de áudio e imagem passaram a ser utilizadas por empresas como Tech Mahindra, XNSPY, Madurai Corporation e EmpMonitor, para **monitorar empregados durante o horário comercial**. Inclusive, a Corporação Municipal de Panchkula exigiu de seus funcionários o uso do dispositivo "Monitoramento de Eficiência Humana" - ***Human Efficiency Tracker***[31].

A vigilância sanitária, porém, é presente na Índia antes mesmo da pandemia, pelo Programa de Vigilância de Doenças (***Disease Surveillance Program* - IDSP**), sendo o país constante palco de milhares de casos de dengue e malária. O programa funciona de forma preventiva e tratativa, com medidas necessárias para mitigar o impacto de contágios no segundo país mais populoso do mundo (Siddiqui; Bhupinde, 2021, p. 31). Nesse sentido, na política de Visão da Índia para 2035 - ***India's Vision 2035***[32], a vigilância na saúde pública é tida como prioritária para a política e bem-estar do país.

Portanto, pode-se afirmar que a vigilância em massa na índia é marcada pela tecnologia de **reconhecimento facial** e, devido a um histórico de diversas doenças, **possui o foco em saúde pública**.

Uso do "Sistema Punjab de Inteligência Artificial" (Punjab Artificial Intelligence System - PAIS) pela Polícia do estado de Punjab, a partir do qual, quando suspeitos são confrontados, suas fotos podem ser analisadas em uma base de dados com nomes enviados pelas prisões da região;

30 Hickok, E.; ***et all*** (2021).

31 https://play.google.com/store/apps/details?id=com.hets.hets&hl=en_US&gl=US

32 Siddiqui, N. Singh, B. (2021). p. 40.


China

China

Diferente dos outros países do BRICS, a China se destaca pela sua crescente posição de **potência econômica e mercadológica**, atuando como **fornecedora mundial de tecnologias de telecomunicação.** Essas exportações contam com a logística da ***Belt and Road Initiative***, uma Nova Rota da Seda com infraestrutura de investimento vigente na Ásia, África e Europa, configurando a posição externa da China no mercado de tecnologias (de vigilância) sob o contexto de uma **disputa geopolítica**.

Tabela - Ameaça à privacidade pela vigilância eletrônica nos EUA, Turquia e China

USA	Mean	Std. Dev.	TURKEY	Mean	Std. Dev.	CHINA	Mean	Std. Dev.
Responsible usage develops civil rights and liberties	**3.73**	**0.72**	**Responsible usage develops civil rights and liberties**	**4.23**	**0.95**	**Responsible usage develops civil rights and liberties**	**4.24**	**0.71**
Usage of IT for campus security in my university is necessary for preventing crime	3.63	0.83	Lawful usage of surveillance is not a threat to security of citizens	3.91	0.87	Governments should control Internet to prevent possible threats to security of citizens	4.07	0.90
Governmental control of Internet poses a threat to freedom of information	3.60	1.07	Governments should control Internet to prevent possible threats to security of citizens	3.67	1.06	Usage of IT for campus security in my university is necessary for preventing crime	3.57	0.98
Governmental control of Internet poses a threat to freedom of thought	3.37	1.02	Usage of IT for campus security in my university is necessary for preventing crime	3.55	1.10	Governmental control of Internet poses a threat to freedom of information	3.44	0.86
Lawful usage of surveillance is not a threat to security of citizens	3.27	0.89	Government abuse of IT is low in my country	3.30	1.08	Lawful usage of surveillance is not a threat to security of citizens	3.28	0.87
Government abuse of IT is low in my country	3.26	0.86	Governmental control of Internet poses a threat to freedom of thought	3.05	1.19	Governmental control of Internet poses a threat to freedom of thought	3.24	0.82
Usage of IT for campus security in my university is sufficient for preventing crime	2.96	0.99	Governmental control of Internet poses a threat to freedom of information	2.97	1.17	Government abuse of IT is low in my country	3.14	0.93
Governments should control Internet to prevent possible threats to security of citizens	2.90	1.07	Usage of IT for campus security in my university is sufficient for preventing crime	2.78	1.08	Usage of IT for campus security in my university is sufficient for preventing crime	3.02	0.98

**Mean range is between "1" and "5".*

Fonte: Aydin et al., 2013, p. 73.

Internamente, a vigilância no país mais populoso do mundo é fortemente caracterizada por **câmeras de videomonitoramento que são aceitas pela maioria da população chinesa**, conforme pesquisa realizada[33], **apesar da falta de transparência sobre seu uso e tratamento de dados**. A pandemia do COVID-19, porém, demandou o aumento da prática de vigilância, intensificando a necessidade de uma maior legislação sobre o tema, principalmente pelo papel central da China no desenvolvimento e inovação de tecnologias desse tipo.

A vigilância associada à saúde e combate à pandemia foi respaldada em uma infraestrutura de segurança pública existente. Em 2018, o Ministério da Segurança Pública, maior autoridade no policiamento chinês, anunciou a instalação de 200 milhões de câmeras em espaços públicos pelo país[34], com a expectativa inicial de atingir 600 milhões (de câmeras) até 2020.[35] Na tabela abaixo, porém, é apresentada, em uma escala de 1 a 5, uma comparação quantitativa da ameaça à privacidade pela vigilância eletrônica nos Estados Unidos, Turquia e China, tendo essa última apresentando resultados mais altos que os outros países, em todos os aspectos.

Apesar dos valores apresentados, a sociedade chinesa demonstra, em sua maioria, **apoiar o videomonitoramento** público, enxergando contribuição para o combate ao crime e para a percepção de segurança. Em tecnologias de reconhecimento facial, especificamente, há relatos de maus tratos de indivíduos detectados[36]; mesmo assim, esse tipo de tecnologia é defendido por 83% da população, destacando-se também o benefício da agilidade em filas de aeroportos[37]. Como na Rússia, a cultura de vigilantismo chinesa não é recente - na Revolução Cultural (1949), os cidadãos eram organizados em unidades de trabalho, facilitando a vigilância governamental[38], com o país acreditando na influência desta no comportamento dos indivíduos.

Internamente, a vigilância no país mais populoso do mundo é fortemente caracterizada por câmeras de videomonitoramento que são aceitas pela maioria da população chinesa

33 Wu, Y.; Sun, I.; Hu, R. (2021).

34 The New York Times (2018) apud Wu, Y.; Sun, I.; Hu, R. (2021).

35 Bischoff, P. (2022).

36 https://www.uol.com.br/tilt/noticias/redacao/2021/03/23/china-ja-usa-reconhecimento-facial-em-quase-100-dos-seus-espacos-publicos.htm.

37 https://www.uol.com.br/tilt/noticias/redacao/2019/01/19/a-sociedade-mais-vigiada-do-mundo-como-a-china-usa-o-reconhecimento-facial.htm.

38 Aho, Brett.; Duffield, R. (2020). p. 193.

Além disso, a China tem dedicado atenção à criação de políticas de processamento de dados, tendo criado, em 2021, novos direitos quanto à privacidade e proteção de informações pessoais, com Beijing, especificamente, também adotando uma nova Lei de Segurança de Dados - *Data Security Law*/DSL.[39] No entanto, iniciativas como essa não têm freado a vigilância no país; ao contrário, como evidencia o novo projeto de videomonitoramento desde 2018, a prática do vigilantismo tem se intensificado e legislações recentes devem auxiliá-la.

Por fim, para além de medidas internas no combate a pandemia do COVID-19, como o uso de **drones para a entrega de medicamentos**[40], e o desenvolvimento de **aplicativos de monitoramento de contato**[41], a China teve um papel internacional central na "**diplomacia de vacinas**", forte entre o BRICS, inicialmente, bem como o desenvolvimento e exportação de tecnologias de vigilância.

Internamente, assim, a China apresenta um dilema entre a implementação de vigilância em massa com êxito e a falta de publicização de seus processos; enquanto, no exterior, a tecnologia chinesa tem sido cada vez mais utilizada. Nesse contexto, apesar das acusações de desrespeito aos direitos humanos quanto à privacidade de dados, é na China que está **o futuro da tecnologia**[42], como microdispositivos, computação quântica e as redes para *Internet das Coisas/Internet of Things - IoT.*[43]

---

39 Ainda em 2020, a China expôs o interesse em lançar uma Iniciativa Global de Segurança de Dados, mas não foi adiante até então - Belli, L. (2021). p. 8.

40 Botes, M. (2021) p. 481.

41 Esse aplicativo foi bem recebido pela população chinesa e expunha a lei de cibersegurança do país, mas ainda levantou polêmicas sobre o uso de dados - Botes, M. (2021), p. 192.

42 Botes, M. (2021). p. 286.

43 Considerado o melhor sistema de informação geoespacial implementado durante a pandemia, a China também desenvolveu, juntamente ao Centro para Sistemas de Ciência e Engenharia da Universidade de Johns Hopkins (*Johns Hopkins University's Centre for Systems Science and Engineering*) e a Organização Mundial da Saúde - OMS (*World Health Organization* - WHO), o "*HealthMap"*, mapa com apresentação, em tempo real, de síndromes respiratórias - Botes, M. (2021), p. 481.


África
do Sul

África do Sul

Devido às condições socioeconômicas da África, o continente tem como desafio, há décadas, o enfrentamento de diversas **questões de saúde**. Com isso, o já existente **Centro Africano para Controle e Prevenção de Doenças (CDC)**, na pandemia do COVID-19, adaptou-se e focou na formação e **capacitação** de pessoal, mas também tratou de outros importantes assuntos, como a necessidade da prática de **vigilância.**[44] Assim, em parceria com a Organização Mundial da Saúde (OMS), foram desenvolvidas no CDC as seguintes medidas: 1) ampliação do **diagnóstico laboratorial**, incluindo subtipagem e sequenciamento genômico; 2) melhoria de **controle nos pontos de entrada,** bem como o uso de uma **plataforma uniformizada da Covid-Tech**; 3) fortalecimento das **medidas de prevenção e controle de infecções**; e 4) implementação das **medidas de saúde pública e sociais.**[45]

Na África do Sul, em específico, foram lançados durante a pandemia a **plataforma "*COVID Connect*"**, construída pela Fundação Praekelt para execução de questionário de sintomas e os resultados de testes[46], e o **sistema "*Covid Alert South*"**, para monitoramento de contato (de mais de 15 minutos e, havendo uma posterior testagem positiva, envio de SMS para as pessoas que haviam convivido nas últimas duas semanas)[47]. Como país em desenvolvimento, porém, o acesso de celulares com acesso a **internet não é uma realidade de toda a população**[48].

No que tange a saúde pública na África, uma outra prática existente (essa mais antiga), é a **vigilância geoespacial**, na qual, ainda sobre a COVID-19, a **ferramenta "*The Rural Innovation Assessment*"**, desenvolvida pelo Human Sciences Research Council, foi utilizada para apoiar as decisões do governo e estimular a inovação em determinadas regiões.[49] Além disso, o *hub* de Objetivos de Desenvolvimento Sustentável da Universidade de Pretória, por exemplo, criou o "**Mapa de Comunidades Vulneráveis"**, usando dados públicos como demografia, estado de saúde, mobilidade e níveis de pobreza.[50] A Lei da Agência de Espaço da África do Sul, porém, não proíbe nem regulamenta a comercialização desse tipo de dado em geolocalização; dessa forma, ocorrem debates sobre esses **marcos legais** no país.[51]

---

44 Silva, A.; Cá, T.; Rosenberg, F. (2020). p. 355.

45 Silva, A.; Cá, T.; Rosenberg, F. (2020). p. 358.

46 https://mybroadband.co.za/news/software/361219-major-concerns-over-south-africas-covid-19-contact-tracing.html

47 Antes do aplicativo "*Covid Alert*", foi utilizado um mecanismo de monitoramento de contato, no qual o aviso às pessoas com quem se havia convivido se dava pelo compartilhamento, via sms, de um código. Contudo, como foi detectado que o uso do bluetooth para geolocalização infringiu a privacidade de dados, o aplicativo "*Covid Alert*", também administrado pelo governo, foi questionado pela população (Botes, 2021, p. 492).

48 https://researchictafrica.net/2021/10/31/south-africas-covid-19-information-app-most-popular-with-urban-dwellers-women-and-youth/

49 Botes, M. (2021). p. 479.

50 Botes, M. (2021), p. 478.

51 Botes, M. (2021), p. 502.

Assim como na maior parte do mundo, esse tipo de tecnologia tem sido desenvolvido por empresas privadas chinesas, principalmente, que visam a modernizar cada vez mais "cidades inteligentes" ("smart cities") pela África.

A tecnologia de vigilância sanitária na África do Sul é reflexo, então, dos desafios socioeconômicos da África, como a existência de diversas doenças e a falta de acesso a tecnologia por parte da população, voltando-se a uma postura preventiva acerca do surgimento e disseminação de novas questões de saúde, como foi a pandemia do COVID-19, e fazendo uso, tradicionalmente, de tecnologias geoespaciais.

Em relação a tecnologia de **reconhecimento facial**, por fim, a África conta com seu uso em países como o Zimbábue, Uganda e a própria África do Sul, para combater roubos, fraudes e outras ameaças, como o terrorismo, ainda presente no continente. Assim como na maior parte do mundo, esse tipo de tecnologia tem sido desenvolvido por empresas privadas chinesas, principalmente, que visam a modernizar cada vez mais "cidades inteligentes" ("***smart cities***") pela África.

Como na vigilância geoespacial, porém, apesar da existência de uma legislação correlata - **Lei POPI 2013** e a de **Cybercrimes**, de 2017[52], essas são apenas tentativas de se reduzir os diversos efeitos da aplicação de tecnologias emergentes nos estados africanos, a exemplo da coleta e uso de dados de forma abusiva.

Portanto, além de dados de geolocalização, a vigilância na África do Sul é altamente relacionada à tecnologia de reconhecimento facial. Mas, com a pandemia do COVID-19, cujo enfrentamento se deu em forte processo de colaboração com o restante do continente africano, houve o foco no desenvolvimento de aplicativos como o mecanismo de uso das referidas formas de vigilância. Em todas essas frentes, porém, está presente o debate sobre legislações e o desafio da desigualdade social.

52 https://issafrica.org/iss-today/future-of-facial-recognition-technology-in-africa

Considerações Finais

Assim, como a **digitalização** abriu espaço para novas formas de **vigilantismo**, a **pandemia do COVID-19** ampliou o escopo, os meios e os setores envolvidos na aplicação de tecnologias de vigilância, em especial no **setor da saúde**. No **BRICS**, grupo de países **populosos** e economicamente **emergentes**, Rússia e China foram mais rápidas no desenvolvimento de **testes** de detecção e desenvolvimento de **vacinas**, construindo, na crise vigente, uma **vigilância sanitária**[53] [54], mas a atuação conjunta nesse período evoluiu para a **"diplomacia da vacina"**, com cooperação em pesquisa e priorização para exportação de doses.

Entretanto, sobre vigilância estatal, apesar do maior estímulo à diminuição da circulação de pessoas **(*lockdowns*) no Brasil, Índia e África do Sul**, esses países não praticaram o mesmo vigilantismo que a Rússia e a China, seja por **questões regulatórias**, seja pela **falta de uso de tecnologias** por larga parcela de suas populações e de **incentivos econômicos** para se implementação, em diversas cidades e de forma experimental, tecnologias de vigilância.

No **Brasil**, primeiramente, foi identificado o uso de **variadas tecnologias**, bem como um processo de **politização** da pandemia, o que tornou a vigilância ainda mais polêmica. Na **Rússia**, em segundo lugar, observa-se uma **tentativa de destaque** no sistema internacional no enfrentamento da crise sanitária, além de, internamente, a **cultura de vigilância** também parecer se sobrepor à falta de transparência sobre essa prática, que se expandiu durante a pandemia. Terceiro, na **Índia**, foram identificados **diversos exemplos** de uso de tecnologias de vigilância tanto à nível nacional, quanto municipal. Apesar do entusiasmo com soluções tecnológicas, essas apresentam em grande medida um uso problemático do **reconhecimento facial** e ampla coleta de dados em ações **preventivas no âmbito da saúde**.

Na **China**, por sua vez, semelhante à Rússia, apesar da falta de transparência no vigilantismo, existe uma percepção pública de que seus benefícios são maiores do que os riscos quando se trata de videomonitoramento; além disso, o país é **referência internacional** nesse tipo de tecnologia. Por último, na **África do Sul**, as medidas de vigilância seguem sendo práticas implementadas, a exemplo do foco em tecnologias **geoespaciais**, e, como a Índia, o país possui como desafio recorrente o enfrentamento de diversas **doenças**.

Não há, portanto, uma **convergência entre os países do BRICS** como um todo no que diz respeito à implementação de tecnologias de vigilância (e, mais recentemente, voltadas ao setor de saúde), com exceção do uso de **videomonitoramento**, conforme identificado na pesquisa realizada para esse relatório. Contudo, há **convergências bilaterais**.

53 "O reforço dos sistemas de vigilância da saúde, a seu turno, implica a integração e a orientação por problemas das intervenções de vigilância **epidemiológica**, vigilância **sanitária**, vigilância **alimentar e nutricional**, vigilância **em saúde do trabalhador e da trabalhadora** e vigilância em **saúde ambiental**, além de **ações intersetoriais** em todas as esferas". A vigilância é, então, um conceito composto por diversas frentes - Souza, L. Giovanella, L. (2021). p. 139.

54 Oliveira, J. et al (2021). p. 251.

Para o futuro, o BRICS demonstra desejar construir uma **governança** que reflita a realidade de um mundo em transformação, levando em conta suas condições comuns e seus papéis como países do sistema internacional.[55] [56] O Novo Banco de Desenvolvimento (**Nem Development Bank - NDB**), banco do BRICS, criado em 2014, é uma medida em direção a esse interesse, e o **Centro de Pesquisa e Desenvolvimento de Vacinas do BRICS**, criado durante a pandemia do COVID-19, representa uma iniciativa de cooperação em **pesquisa,** o que pode ser continuado e aprofundado não apenas no setor de saúde.

Finalmente, entende-se que o BRICS deve atuar **conjuntamente no desenvolvimento e troca de experiências de tecnologias de vigilância**; afinal, o grupo de países já possui um **Memorando de Entendimento para Cooperação em Ciência, Tecnologia e Inovação**, bem como uma iniciativa de **Parceria Digital** - *BRICS Digital Partnership*.[57] Além disso, seus **países-membros** são **desenvolvedores ou entusiastas** da implementação desse tipo de tecnologia que, sendo **tendência** em todo o mundo, contribuirá para uma **maior inserção** do grupo nessa dinâmica.

Assim, como a digitalização abriu espaço para novas formas de vigilantismo, a pandemia do COVID-19 ampliou o escopo, os meios e os setores envolvidos na aplicação de tecnologias de vigilância, em especial no setor da saúde.

55 Stuenkel, O. (2020) apud Petrone, F. (2021). p. 2.

56 Veja a Declaração de Nova Delhi, da XIII Cúpula do BRICS, em setembro de 2021, sob o tema "BRICS @ 15: Cooperação Intra-BRICS para a Continuidade, a Consolidação e o Consenso", com iniciativas do bloco em diversos âmbitos. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/xiii-cupula-brics-declaracao-de-nova-delhi

57 Belli, L. (2021). p. 3.

Referências

Aho, Brett.; Duffield, R. (2020) Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China, Economy and Society, 49:2, 187-212, DOI: 10.1080/03085147.2019.1690275.

Belli, L. (2021) "Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation", *The African Journal of Information and Communication (AJIC)*. South Africa, (28). doi: 10.23962/10539/32208.

Bischoff, P. (2022). *Surveillance camera statistics*: which cities have the most CCTV cameras? Comparitech.

Botes, M. (2021) The use of geospatial surveillance data for public-health emergency and disaster management in South Africa: a review with legal recommendations. 2021. Journal of South African Law,(3):474-503.

Data Privacy (2021). *Dados Virais* - Uma Investigação sobre Tecnologias baseadas em Dados Pessoais, Usadas no Combate à COVID-19 no Brasil.

Estamos Vigilando (2020). *Solicitudes Brasil*.

Hickok, E.; *et all* (2021). *Facial Recognition Technology in India*.

Hoirisch, C. (2020). *Brics na Covid-19*: multilateralismo, capacidade tecnológica e colaboração em PD&I. In: Buss, P.; Fonseca, L. (org.). *Diplomacia da saúde e Covid-19*: reflexões a meio caminho. Rio de Janeiro: Observatório Covid-19 Fiocruz; Editora Fiocruz, 2020. p. 213-230. (Série Informação para Ação na Covid-19).

_____. *Quo vadis, Brics?* Colaboração biofarmacêutica, diplomacia vacinal dos BRICs e (des)motivações para o cumprimento dos compromissos acordados sobre vacinas Covid-19. (2020). In: Buss, P.; Burger, P. (org.). *Diplomacia da saúde*: respostas globais à pandemia. Rio de Janeiro: Edicioneis ALASAG, p. 317-328. (Centro de Relações Internacionais em Saúde da Fiocruz).

Instituto Igarapé. (2021). *Portal Brasileiro de Cibersegurança*.
Disponível em: https://ciberseguranca.igarape.org.br/

_____. (2022). *Implementação de Tecnologias de Vigilância no Brasil e na América Latina*. Programa de Segurança Digital.

Lewis, J. A. (2014). ***Reference Note on Russian Communications Surveillance***. Center for Strategic & International Studies.

Oliveira, J.; et all. (2021). ***The role of intergovernmental relations in response to a wicked problem***: an analysis of the COVID-19 crisis in the BRICS countries. Brazilian Journal of Public Administration, Rio de Janeiro 55 (1): 243-260.

Petrone, F. (2021). ***The future of global governance after the pandemic crisis***: what challenges will the BRICS face? International Policy.

Raghunath, P. (2021). ***COVID-19 and Non-personal data in the Indian Context:*** On the Normative Ideal of Public Interest. In: COVID-19 from the Margins: Pandemic invisibilities, Policies and Resistance in the Datafied Society. Milan, S.; Treré, E.; Masiero, S. (edit). Theory on Demand #40. Amsterdam, Institute of Network Cultures, pp. 200 - 202.

Ramos, H. (2014). ***O Novo Panóptico Russo:*** A Vigilância na Rússia do Século XVIII à Era Digital. Observatorio (OBS*) Journal, vol.8 - nº3, 131-147.

Siddiqui, N.; Singh, B. (2021). Surveillance of Public Health in India: Prospects and Challenges.

Silva, A.; Cá, T.; Rosenberg, F. (2020). ***A Resposta à Pandemia no Continente Africano e na CPLP.*** In: Buss, P.; Burger, P. (org.). ***Diplomacia da saúde***: respostas globais à pandemia. Rio de Janeiro: Edicioneis ALASAG, p. 355-366. (Centro de Relações Internacionais em Saúde da Fiocruz).

Souza, L.; Giovanella, L. (2020) ***Os Serviços de Saúde sob o Impacto da Covid-19.*** In: Buss, P.; Burger, P. (org.). ***Diplomacia da saúde***: respostas globais à pandemia. Rio de Janeiro: Edicioneis ALASAG, p. 135-150. (Centro de Relações Internacionais em Saúde da Fiocruz).

Stuenkel, O. ***The BRICS and the future of global order***, 2nd ed. Lanham: Lexignton Books.

The New York Times. (2018). Inside China's' Dystopian Dreams: A.I., Shame and Lots of Cameras.

Wu, Y.; Sun, I.; Hu, R. (2021). ***Cooperation with Police in China***: Surveillance Cameras, Neighborhood Efficacy and Policing. Social Science Quartely, Volume 102, Number 1.

Zhang, H.; Guo, C.; Deng, Y.; Fan, G. (2019). ***Can Video Surveillance Systems Promote the Perception of Safety?*** Evidence from Surveys on Residents in Beijing, China. Sustaiability 11 (6): 1595.

Autoras

Carolina Ambinder
Pesquisadora

Daisy Bispo Teles
Pesquisadora

Revisoras

Melina Risso
Diretora de Pesquisa

Louise Marie Hurel
Pesquisadora

Equipe de Comunicação

Eliane Azevedo
Gerente de Comunicação

Ana Carolina Duccini
Coordenadora de Comunicação

Raphael Durão
Coordenador Criativo

Gabriela Aguiar
Designer

INSTITUTO IGARAPÉ
a think and do tank

O Instituto Igarapé é um think and do tank independente, que desenvolve pesquisas, soluções e parcerias com o objetivo de impactar tanto políticas como práticas públicas e corporativas na superação dos principais desafios globais. Nossa missão é contribuir para a segurança pública, digital e climática no Brasil e no mundo. O Igarapé é uma instituição sem fins lucrativos e apartidária, com sede no Rio de Janeiro e atuação do nível local ao global.

O programa de Segurança Digital do Instituto Igarapé se dedica ao desenvolvimento de pesquisas interdisciplinares, facilitação de diálogos intersetoriais e promoção de espaços de confiança e conscientização para o avanço de políticas digitais. Trabalhamos com temas como segurança digital, crimes na Internet, inteligência artificial, Internet das coisas, proteção de dados e cidades inteligentes. Construímos plataformas, pensamos criticamente sobre o impacto dessas tecnologias na sociedade e trabalhamos para abordar os desafios à proteção de direitos digitais mediante o avanço da implementação de tecnologias em nosso dia a dia.

Instituto Igarapé

Rio de Janeiro - RJ - Brasil
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org
instagram.com/igarape_org/

igarape.org.br

igarape.org.br

INSTITUTO IGARAPÉ
a think and do tank