30 de setembro de 2021

# BOLETIM (ANTI)SEGURANÇA 18

## Inteligência artificial, policiamento preditivo e fronteiras biométricas: vinte anos do atentado às torres gêmeas e os legados planetários do Ato Patriota

UNIFESP
Universidade Federal de São Paulo

LASINTEC
Laboratório de Análise em Segurança Internacional e Tecnologias de Monitoramento


# BOLETIM (ANTI)SEGURANÇA N. 18

**Este Boletim é um projeto de pesquisa e extensão do Departamento de Relações Internacionais da EPPEN-UNIFESP Osasco**

**Coordenação:** Acácio Augusto, professor do Departamento de Relações Internacionais da EPPEN-UNIFESP)

**Vice-coordenação:** Fabíola Fanti, professora visitante do Departamento de Relações Internacionais da EPPEN-UNIFESP

**Pesquisa e Redação:** Acácio Augusto, Ana Beatriz Luz, Augusto Gottberg, Bruna Ghirardello, Fabíola Fanti, Helena Wilke, Ivo Ferreira, João Paulo Gusmão, Júlia Tibiriçá, Lucas Alencar de Araújo, Mariana Janot, Matheus Marestoni, Milena Cunha, Pedro Lázaro, Thaiane Mendonça e Yasmin Teixeira

**Edição e Formatação:** João Paulo Gusmão e Júlia Tibiriçá

**Capa:** Thaiane Mendonça



EPPEN UNIFESP Osasco
Rua Oleska Winogradow, n° 100 – Sala 313 – Jd. das Flores -Osasco – SP
CEP: 06110-295
Telefone: (11) 2284-6900

# Inteligência artificial, policiamento preditivo e fronteiras biométricas:
## vinte anos do atentado às torres gêmeas e os legados planetários do Ato Patriota

*Security is the new prosperity.*
*Surveillance is the new democracy.*
**Naomi Klein**

É extensiva a literatura que vem sendo produzida, desde 2001, sobre os imbricamentos entre práticas e dispositivos de segurança e de monitoramento que sucederam a reação norte-americana ao atentado às torres gêmeas, representados em grande medida pela narrativa em torno da chamada Guerra ao Terror. No contexto de consolidação de uma reformada arquitetura de gestão da paranóia que viria, posteriormente, a caracterizar a Estratégia de Segurança Nacional de George W. Bush, uma ampla gama de parcerias público-privadas foi mobilizada na reestruturação e facilitação de programas estatais de vigilância mediada por tecnologias computo-informacionais, cujo apoio político e comprometimento financeiro de setores estratégicos, em âmbito nacional e internacional, muito se associa à (re)produção reiterada de inimigos imprecisos e, por vezes, imaginários.

O Ato Patriota (do inglês, *Patriot Act*, instituído pela lei "*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*", de 26 de outubro de 2001) entra em vigor menos de cinquenta dias depois dos episódios do 11 de Setembro, e representa, desde então, um importante pilar para a ampliação do acesso, coleta e armazenamento de dados por uma variedade de agências do Estado. Foi, por exemplo, por meio do Ato Patriota que se consolidou a possibilidade de quebra de sigilos bancários, fiscais, de registros acadêmicos e médicos, de dados de provedores de internet e telefonia para investigação sob justificativa de potencial envolvimento com atividade terrorista.

Todo o espectro de telecomunicações e de registros eletrônicos da população estadunidense, à época, foi então disponibilizado para fins de inteligência policial com substantivo apoio da sociedade civil, uma vez instaurado o clima de ameaça. Ao longo dos anos seguintes, evidências têm demonstrado que as práticas daquilo que se

torna conhecido como *intelligence-led policing* (policiamento conduzido por inteligência, em tradução livre) ou *smart policing* são marcadas por tendências escancaradamente racistas e tem tido impactos particularmente significativos para populações imigrantes em território estadunidense. Seguramente, encontramos nesses usos das tecnologias de policiamento eletrônico/inteligente uma via para se pensar uma governamentalização do Racismo de Estado do século XX que mantém seus resquícios nos Estados governamentalizados pelas tecnologias de governo disciplinares e biopolíticas da modernidade liberal.

Na medida em que as décadas seguintes assistiram ao contínuo fomento de uma cultura da suspeição permanente, em parte articulada com a prolongada ocupação do Iraque, emergiram questões em torno da necessidade de limites à imposição de uma racionalidade securitária sobre as prerrogativas de privacidade alegadamente garantidas pelas democracias liberais. Mais do que potencializar a difusão e ampliação de práticas de monitoramento já existentes, o crescimento do complexo securitário-industrial de vigilância que angariou legitimidade pública a partir do 11 de Setembro implicou também em um processo de espraiamento de uma certa concepção estratégica de Segurança Nacional ao redor do planeta. Isso se expressa na forma de um regime institucionalizado de *smart borders* (fronteiras inteligentes, em tradução livre), na triagem em aeroportos e espaços de trânsito em geral, e na intensa fiscalização de transações financeiras. Assim, desde 2001, a racionalidade governamental da segurança nacional estadunidense implica na articulação[1] , em nível planetário, de polícias federais e serviços de inteligência através de sistemas informacionais integrados e na conversão de toda a população do planeta em indivíduos passíveis de suspeita e investigação. Uma lógica que opera pelo entendimento de que nada se assemelha mais ao terrorista do que o cidadão comum.

A disseminação internacional de políticas de automação de fronteiras e de policiamento preditivo, portanto, - ambas impulsionadas por investimentos crescentes em tecnologias de inteligência artificial - fornece elementos pertinentes para a reflexão sobre a internacionalização das exceções institucionalizadas pelo Ato Patriota de 2001 e pela Estratégia de Segurança Nacional de 2002.

A automação de fronteiras corresponde a um projeto transnacionalizado por excelência e constitui um impecável modelo de vigilância eletrônica global, fazendo com

[1] GATES, Kelly. *The globalization of homeland security*. Nova Iorque: Routledge, 2012.

que indivíduos em trânsito que **pretendem** chegar a um determinado destino sejam submetidos a procedimentos de triagem e monitoramento muito antes de se aproximarem das fronteiras territoriais propriamente ditas, quiçá antes mesmo de darem início à viagem. Embora interpretações dos eventos do 11 de Setembro tenham argumentado, por vezes, que a Guerra ao Terror impactou negativamente nos fluxos globais de bens e pessoas frequentemente associados ao que se convencionou chamar de globalização, o que muito rapidamente se observa é a configuração de fronteiras des-territorializadas e compartilhadas em programas de cooperação erguidos em torno de sistemas de monitoramento. Nesse sentido, observa-se a intensificação de fluxos transfronteiriços de vigilância, tal como o do complexo industrial que se beneficia diretamente deste processo. Sistemas integrados de companhias aéreas são, talvez, o exemplo mais emblemático deste movimento.

Sistemas automáticos de controle de fronteiras (do inglês, *automated border control systems*) agregam sistemas distintos de reconhecimento biométrico, reconhecimento facial e passaportes eletrônicos, incluindo recentemente espelhos digitais para a captura de imagens sequenciais para fins de biometria[2]. A sequência de testagens de identidade culmina, é claro, na intervenção de um agente de segurança, caso qualquer conduta ou característica qualificada como desviante seja identificada[3]. Em 2018, por exemplo, o programa piloto do *iBorderCtrl* (*Intelligent Portable Control System*)[4], inicialmente instalado nas fronteiras da Hungria, Grécia e Letônia, lançou mão de tecnologia de inteligência artificial para um sistema de detecção de mentiras aplicado por um guarda virtual a partir de um questionário a ser respondido por todos que pretenderem cruzar as fronteiras[5]. Somados a tecnologias de reconhecimento facial configuradas para identificar emoções – principalmente sensíveis a categoria "medo"[6]–, as soluções tecnológicas para o controle de fronteiras europeu tem recorrido também à robótica em programas sob testagem na Grécia, Bulgária e Sérvia, cuja intenção é construir uma rede articulada de veículos não tripulados aéreos, aquáticos e terrestres, configurados para atuar como **enxames**. Para além das preocupações com

---

[2] Thales Group, *New ABC eGates: Smaller footprint, modular design and faster passenger processing*.; Accenture, *Rethinking travel with intelligent operations*.

[3] DEL RIO, José Sanchez et al. *Automated Border Control e-gates and facial recognition systems*. Computer & Security, 62, 2016.

[4] ver: https://www.iborderctrl.eu/The-project

[5] Amnesty International. *Automated technologies and the future of Fortress Europe*. 28/03/2019

[6] CHOUDHURY, S. Amazon says its facial recognition can now identify fear. CNBC News, 14/08/2019

monitoramento de dados biométricos, o programa *ROBORDER* representa adicionais riscos na medida em que pode implicar também a automação de veículos armados. Iniciativas semelhantes já foram registradas nos Emirados Árabes Unidos, Israel, Marrocos, Indonésia, Índia, Usbequistão, Kuwait, Hong Kong, Panamá, Austrália, Argentina, entre outros. No Brasil, São Paulo[7] e Rio de Janeiro[8] já contam há alguns anos com mecanismos análogos.

A elaboração de perfis algorítmicos, a obrigatoriedade de documentos de identidade digitais e as tecnologias de análise comportamental correspondem a práticas que prometem a previsão do futuro, a fim de antecipar a ação sobre atividades terroristas e criminosas **porvir**. O conjunto de princípios, portanto, que orienta a adoção de sistemas automatizados de controle de fronteiras – preocupados com fluxos migratórios crescentes –, norteia também o investimento e a difundida adesão às práticas de policiamento preditivo sob a névoa dos escombros das torres gêmeas.

Popularizada pelo longa metragem *Minority Report* (não por acaso lançado em 2002), a noção de policiamento preditivo diz respeito à coleta e armazenagem de *big data* para responder a crimes do futuro. Constata-se até o momento que tecnologias de reconhecimento facial, câmeras com dispositivos biométricos, análise de mídias sociais correspondem às principais fontes de dados para inteligência policial ao redor do mundo. O *PredPol*, programa cujo piloto nos Estados Unidos data de 2009, já é difundido na maior parte do país. O caso Chinês se tornou alvo de considerável atenção de organizações de proteção à privacidade, conforme relatório da Human Rights Watch[9], segundo o qual a *Integrated Joint Operations Platform* (IJOP) coletaria dados de câmeras de circuito interno, dispositivos de reconhecimento biométrico e de dispositivos de interceptação e escuta eletrônica infiltrados em redes de internet sem fio. Utilizado pela polícia na região de Xinjiang, o IJOP submeteu a população muçulmana entre 12 e 65 anos inclusive a procedimentos obrigatórios de coleta de DNA para a alimentação de bancos de dados para padrões e perfis de risco.

Países como Argélia, Argentina, Austrália, Bolívia, Chile, Canadá, Colômbia, Equador, Egito, França, Alemanha, Índia,

[7] São Paulo Viracopos implements ABC eGates: increase in passenger needs automated solutions. Passenger Self Service, 14/01/2016

[8] RIOgaleão - Tom Jobim to introduce ABC e-gates this month. Passenger Self Service, 25/06/2016

[9] Human Rights Watch. Interview: China's Big Brother App: unprecedented view into Mass Surveillance of Xinjiang's Muslims. 01/05/2019

Indonésia, Irã, Israel, Japão, Quênia, Líbano, México, Nova Zelândia, Panamá, Filipinas, Laos, Uganda, Rússia, África do Sul, Turquia, Reino Unido e Uruguai estão entre os conhecidos adeptos a políticas de *smart policing*. Seguidos pela França, Alemanha, Israel e Japão, China e Estados Unidos aparecem como principais fornecedores de tecnologia de inteligência artificial para os referidos fins, representados principalmente pela Hikvision, Huawei, Dahua, IBM, Palantir e Cisco. Apenas a chinesa Huawei é responsável pela exportação para mais de 50 países, dentre os quais mais de 30 fazem parte da nova rota da seda[10].

Em anos recentes, o Brasil tem ganhado espaço como um mercado interessante para a iniciativa privada chinesa, tal como exemplificado pela inauguração de um laboratório da Huawei no Estado de São Paulo[11], ainda em 2018, e pela disponibilização dos serviços de automação de inteligência artificial da Microsoft (*Azure*), um ano antes[12]. Em 2019, uma delegação de deputados federais e senadores do PSL fizeram viagem à China para o desenvolvimento de um projeto de lei para obrigar a implantação de reconhecimento facial em espaços públicos, a despeito das tensões testemunhadas desde o início do mandato de Jair Bolsonaro entre sua administração e o mercado chinês. Ao lado das americanas Bosch e IBM, a Dahua chinesa – liderança na produção de equipamentos para câmeras de monitoramento de circuito interno – também tem se difundido por projetos de cidades inteligentes pelo país, tendo sido a principal fornecedora para "soluções de segurança"[13] implementadas em Boa Vista (RO), com a combinação de dados multimodais e mais de 100 câmeras de monitoramento em tempo real espalhadas pela cidade.

Na última semana do mês de setembro deste ano, foi lançado um edital pelo Instituto Igarapé, *think and do tank* especializada em segurança pública, climática e digital e suas consequências para a democracia, para a seleção de municípios brasileiros com o objetivo de realizar uma implementação experimental da tecnologia "CrimeRadar". Esta utiliza ferramentas conhecidas como *machine learning* que atuam por meio de três eixos: i) algoritmo *back-end* de predição, voltado para calcular qual local e horário um tipo de evento terá chances de ocorrer; ii) *dashboard*, que permite aos usuários

[10] FELDSTEIN, S. The Global Expansion of AI Surveillance. 17/09/2019

[11]. Hawei opens a new IoT lab in Brazil. BNAMERICAS, 06/12/2018

[12] Azure Automation available in Brazil South Region. Microsoft, 20/07/2017

[13] Security Informed, Dahua Security Solution for Public Safety in Boa Vista.

compreenderem os fatores de concentração de determinadas ocorrências e qualifiquem o uso de recursos; iii) estratégia de impacto social, mitigando operações discriminatórias.

Assim, como efeito das ações de contraterror, explicita-se como o desenvolvimento dessas tecnologias de monitoramento por ONGs de direitos humanos, bem como a implementação delas por governos de Estado e outras institucionalidades, sofistifica o aparato policial voltado historicamente para a preservação da propriedade privada e estatal, reforçando a perpetuação da segregação espacial e a operacionalização seletiva do aparato penal, dirigido, sobretudo, contra negros e pobres. Por conseguinte, a função de "estratégia de impacto social" evidencia que o racismo inerente à política de segurança é algo esperado e tolerável, desde que em níveis considerados razoáveis para a racionalidade neoliberal. O que mais uma vez nos remete às derivas do contraterrorismo implementado desde o 11 de setembro, isto é, um conjunto de práticas e dispositivos de segurança e monitoramento que demarcaram a planetarização do racismo biopolítico.